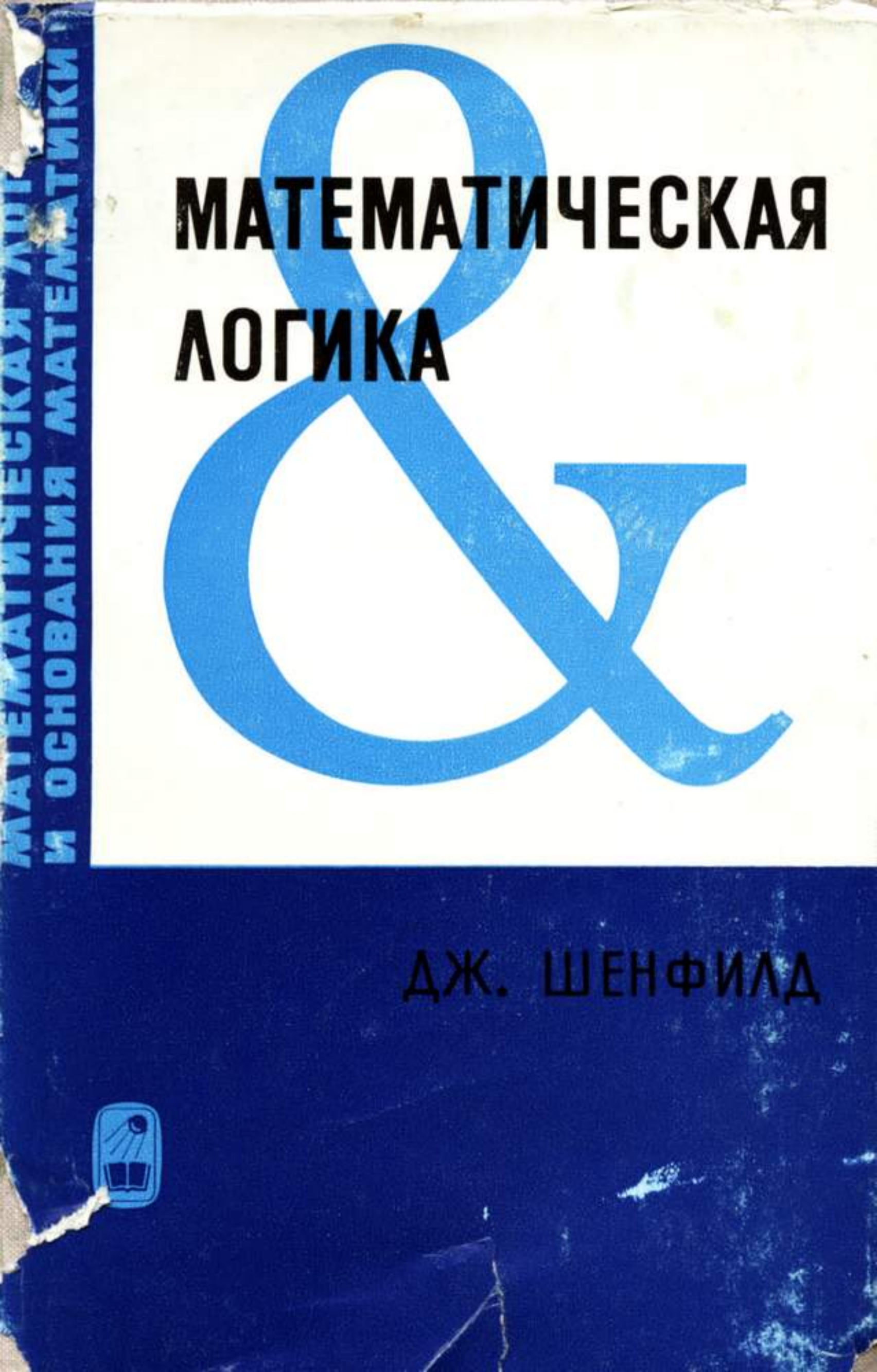




МАТЕМАТИЧЕСКАЯ ЛОГИКА



ДЖ. ШЕНФИЛД



МАТЕМАТИЧЕСКАЯ ЛОГИКА И ОСНОВАНИЯ МАТЕМАТИКИ

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1975

МАТЕМАТИЧЕСКАЯ ЛОГИКА

Дж. ШЕНФИЛД

Перевод с английского
И. А. ЛАВРОВА и И. А. МАЛЬЦЕВА

Под редакцией
Ю. Л. ЕРШОВА

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1975

JOSEPH R. SHOENFIELD

MATHEMATICAL
LOGIC

ADDISON-WESLEY
PUBLISHING COMPANY
1967

ОГЛАВЛЕНИЕ

Предисловие редактора	7
Предисловие	9
Глава 1. Природа математической логики	11
1.1. Аксиоматические системы (11). 1.2. Формальные системы (13). 1.3. Синтаксические переменные (19).	
Глава 2. Теории первого порядка	23
2.1. Функции и предикаты (23). 2.2. Функции истинности (25). 2.3. Переменные и кванторы (28). 2.4. Языки первого порядка (31). 2.5. Структуры (37). 2.6. Логические аксиомы и правила (40). Задачи (44).	
Глава 3. Теоремы в теориях первого порядка	47
3.1. Теорема тавтологии (47). 3.2. Результаты о кванторах (54). 3.3. Теорема дедукции (56). 3.4. Теоремы эквивалентности и равенства (58). 3.5. Пренексная форма (62). Задачи (65).	
Глава 4. Проблема характеризации	67
4.1. Теорема редукции (67). 4.2. Теорема полноты (70). 4.3. Теорема непротиворечивости (79). 4.4. Теорема Эрбрана (84). 4.5. Добавление функциональных символов (90). 4.6. Расширения с помощью определений (93). 4.7. Интерпретации (98). Задачи (103).	
Глава 5. Теория моделей	108
5.1. Теорема компактности (108). 5.2. Изоморфизмы и подструктуры (111). 5.3. Мощность моделей (122). 5.4. Совместная непротиворечивость (124). 5.5. Полные теории (128). 5.6. Категоричность (138). Задачи (144).	
Глава 6. Неполнота и неразрешимость	162
6.1. Вычислимость (162). 6.2. Рекурсивные функции (165). 6.3. Явные определения (168). 6.4. Номера последовательностей (174). 6.5. Тезис Чёрча (180). 6.6. Номера выражений (185). 6.7. Представимость (190). 6.8. Теорема Чёрча и теорема о неполноте (196). 6.9. Неразрешимость (201). Задачи (206).	

© Перевод на русский язык,
Главная редакция
физико-математической литературы
издательства «Наука», 1975 г.

Глава 7. Теория рекурсии	215
7.1. Частичные функции (215). 7.2. Функционалы и отношения (220). 7.3. Свойства рекурсивных функционалов (226). 7.4. Индексы (234). 7.5. Арифметическая иерархия (239). 7.6. Относительная рекурсивность (244). 7.7. Степени (252). 7.8. Аналитическая иерархия (258). 7.9. Гиперарифметические отношения (262). 7.10. Теорема характеризации (267). 7.11. Теоремы о базисе (276). Задачи (283).	
Глава 8. Натуральные числа	300
8.1. Арифметика Пеано (300). 8.2. Теорема о доказательствах непротиворечивости (307). 8.3. Доказательство непротиворечивости (315). 8.4. Применения доказательства непротиворечивости (327). 8.5. Арифметика второго порядка (334). Задачи (343).	
Глава 9. Теория множеств	348
9.1. Аксиомы для множеств (348). 9.2. Систематическое построение теории множеств (352). 9.3. Ординалы (359). 9.4. Кардиналы (369). 9.5. Интерпретации теории множеств (379). 9.6. Конструктивные множества (393). 9.7. Аксиома конструктивности (401). 9.8. Вынуждение (408). 9.9. Доказательства независимости (422). 9.10. Большие кардиналы (436). Задачи (452).	
Приложение I. Проблема тождества слов	459
Приложение II. Неразветвленное вынуждение	482
Предметный указатель	520

ПРЕДИСЛОВИЕ РЕДАКТОРА

В настоящее время интерес к математической логике и теории алгоритмов непрерывно растет. Все большее число высших учебных заведений включает в обязательную программу обучения курсы математической логики, теории алгоритмов или их фрагменты. Специалисты в области ЭВМ начинают осознать, что эти разделы математики являются фундаментом для построения действительно необходимой сейчас хорошей теории математического обеспечения и теории вычислений. Многие специалисты далеких от математики разделов науки начинают сознательно знакомиться с достижениями математической логики. За последние годы вышли переводы многих хороших книг по математической логике и теории алгоритмов, однако ни эти переводы, ни довольно бедный ассортимент отечественных книг не могут полностью удовлетворить запросы читателей. Предлагаемая вниманию читателей книга сочетает в себе (относительную) простоту изложения с почти энциклопедической полнотой содержания. Ее выход в русском переводе будет полезен широкому кругу советских читателей.

Книга Дж. Шенфилда «Математическая логика» вышла в США в 1967 г. и в настоящее время, после прошедших семи лет, становится ясным, что она завоевала постоянные симпатии специалистов и стала, в определенном смысле, «канонической» книгой. Это проявляется, например, в том, что ссылки на нее в журнальных статьях делаются чаще, чем на какие-нибудь другие систематические изложения основ математической логики. Чем это можно объяснить? Прежде всего краткостью, полнотой и тщательностью отбора материала. Полнота изложения книги весьма впечатляющая. При сравнительно небольшом объеме она содержит практически все теоремы, заслужившие всеобщее признание специалистов, в области математической логики, теории моделей и теории алгоритмов. Так, например, книга

содержит: теорию счетно категоричных теорий, решение проблемы Поста о степенях неразрешимости, основные результаты о независимости в аксиоматической теории множеств и многое, многое другое. Впервые в такой книге изложено гёделевское доказательство непротиворечивости арифметики, использующее функционалы высших типов. Краткость книги достигнута многими авторскими находками в способе подачи материала. Многие важные результаты излагаются в упражнениях, которые составляют необходимую органическую часть книги. К сожалению, стремление к краткости иногда приводит и к некоторым потерям. Написанная довольно понятно в целом, книга в некоторых местах становится трудно понимаемой.

Ряд важных теорем книги снабжен указаниями на их авторство. В основном эти указания точны, но имеются и досадные упущения. Так не отмечено, что теорема полноты и теорема компактности в полном объеме (для любой сигнатуры) принадлежат выдающемуся советскому математику академику А. И. Мальцеву.

Книга имеет 9 глав и 2 приложения. Главы 1—5, 9 и приложение II переведены И. А. Лавровым, главы 6—8 и приложение I — И. А. Мальцевым.

Автор любезно предоставил в распоряжение редактора и переводчиков список замеченных опечаток и неточностей и высказал пожелание в присоединении в качестве второго приложения статьи автора «Неразветвленное вынуждение». Редактор благодарен Дж. Шенфилду за полезное сотрудничество. Пожелание автора о включении статьи «Неразветвленное вынуждение», содержащей замечательное упрощение изложения результатов о независимости в аксиоматической теории множеств, выполнено. При переводе были исправлены замеченные опечатки и неточности (указанные и не указанные автором) без всяких особых указаний на это. В переводе имеется совсем немного примечаний, сделанных редактором и переводчиками. При этом сознательно подавлялось возникающее иногда желание делать замечания, основной целью которых являлась бы демонстрация того, что редактор (переводчик) понимают то, о чем идет речь в книге. Как показывает опыт, чтение книг, снабженных многочисленными такими примечаниями, оказывается довольно мучительным делом.

Ю. Л. Еришов

ПРЕДИСЛОВИЕ

Редко бывает, чтобы автор учебника по математике не жаловался на недостаток места для изложения своего предмета. Сегодня невозможно описать во вводных курсах анализа, алгебры или топологии даже все центральные направления исследований. Это в какой-то мере возможно в математической логике, но и здесь приходится отбрасывать многие интересные разделы. Поэтому я пытался собрать главные результаты только в кажущихся мне центральными направлениях математической логики: теории доказательств, теории моделей, теории рекурсии, аксиоматической теории чисел и теории множеств. При этом я не хочу создавать предубеждения против многозначных логик, типов рекурсивной эквивалентности и других специальных вопросов; читатель должен изучать их где-нибудь в другом месте. Особенно важной из опущенных тем является интуиционизм; наличие соответствующих учебников и некомпетентность автора в этом вопросе являются главными моими оправданиями.

Но и главные направления не могут быть описаны полностью; однако я пытался предложить несколько нетривиальных теорем и доказательств в каждом из этих направлений. Число результатов значительно увеличено благодаря задачам. Это не шаблонные упражнения, а важные результаты, доказательства которых часто требуют значительного обобщения методов, изложенных в тексте книги. Я надеюсь, что сделанные указания будут достаточными для того, чтобы хороший студент решил эти задачи, но он не должен быть обескуражен, если многие из этих задач покажутся ему очень трудными.

Математическая логика всегда была тесно связана с философией математики. Я обычно избегаю философских рассуждений, за исключением тех мест, где они тесно связаны с математическим материалом. Иногда, излагая некоторую

точку зрения, я не буду при этом извиняться за то, что я не отмечаю противоположной точке зрения, также широко распространенной.

Эта книга значительно расширена по сравнению с конспектом курса математической логики, прочитанного несколько раз, начиная с 1958 г., в университете имени Дьюка. Часть материала взята из курса по теории рекурсии, прочитанного в Стенфордском университете в 1964—1965 гг. Включенный материал несколько больше, чем я обычно читаю в одногодном курсе.

Так как я предназначаю эту книгу в качестве учебника для аспирантов первого года обучения, то от читателя требуется достаточная математическая зрелость. С другой стороны, необходим лишь ограниченный запас математических знаний. Достаточно знания простейших свойств натуральных чисел и множеств, а также некоторого знакомства с современной алгеброй. Но некоторые задачи требуют знакомства с более сложными темами.

Только небольшая часть результатов книги принадлежит автору. Я не стремился указывать автора каждого результата; имена, данные важнейшим теоремам, просто дают читателю представление о людях, создававших эту науку. Я также опускаю все библиографические ссылки. Но одну книгу, имеющую для меня особое значение, я хотел бы отметить: это книга Клини «Введение в метаматематику».

Наряду с имеющимися опубликованными источниками я использовал беседы и переписку со многими логиками. Я хотел бы, в частности, поблагодарить Джона Аддисона, Соломона Фейермана, Азриэля Леви, Анджее Мостовского, Ричарда Платека, Хартли Роджерса, Дэна Скотта, Клиффорда Спектора, В. В. Тейта и Роберта Воота. Этот список не исчерпывающий, но я надеюсь, что многие другие примут мою общую благодарность за их содействие.

Особенно я обязан Георгу Крайзелю. Именно в дискуссиях и переписке с ним за многие годы я пришел к выводу, что математическая логика является не собранием разрозненных результатов, а действенным методом изучения некоторых наиболее интересных проблем, стоящих перед математиками. Я считаю, что успех этой книги будет зависеть от того, насколько она передаст эту идею читателю.

Дарем, Северная Каролина
Май 1967

Д. Р. Ш.

ПРИРОДА МАТЕМАТИЧЕСКОЙ ЛОГИКИ

1.1. Аксиоматические системы

Логика изучает умозаключения, а математическая логика изучает те типы умозаключений, которыми пользуются математики. Поэтому, чтобы найти правильный подход к математической логике, мы должны исследовать методы, которыми пользуются в математике.

Отличительной чертой математики, в противоположность другим наукам, является использование доказательств, а не наблюдений. Физик может выводиться физические законы из других физических законов, но как окончательное подтверждение физического закона он обычно рассматривает согласованность с экспериментом. Математик может при случае использовать наблюдение: например, он может измерить углы многих треугольников и прийти к выводу, что сумма этих углов всегда равна 180° . Однако он признает этот факт как математический закон только тогда, когда это будет доказано.

Несмотря на это, ясно, что невозможно доказать все математические законы. Самые первые законы, которые принимаются, не могут быть доказаны, так как нет более ранних законов, из которых они могут быть выведены. Поэтому мы должны выбрать некоторые начальные законы, называемые *аксиомами*, которые принимаются без доказательства; остальные законы, называемые *теоремами*, доказываются, исходя из аксиом.

На каком основании мы принимаем аксиомы? Здесь мы могли бы пытаться применить наблюдение, но это не очень практично и не в духе математики. Поэтому мы пытаемся выбрать в качестве аксиом такие законы, которые, как мы полагаем, очевидны по самой природе рассматриваемых понятий.

Так мы сводим большое число законов к небольшому числу аксиом. Похожее сведение происходит и с математи-

ческими понятиями. Мы обнаруживаем, что можно определить некоторые понятия в терминах других понятий. Но опять-таки самые первые понятия, которые мы используем, не могут быть определены, так как нет более ранних понятий, в терминах которых их можно было бы определить. Поэтому мы выбираем некоторые понятия, называемые *основными понятиями*, которые остаются неопределенными; остальные понятия, называемые *производными понятиями*, определяются в терминах основных. К основным понятиям, так же как и к аксиомам, предъявляется требование: они должны быть столь просты и ясны, что мы можем понимать их без точного определения.

В любом утверждении можно заменить производные понятия основными понятиями, в терминах которых они определены. В частности, это можно сделать для аксиом. Поэтому можно предполагать, что все понятия, которые встречаются в аксиомах, являются основными.

Теперь можно следующим образом описать то, что делает математик. Он предлагает нам некоторые основные понятия и некоторые аксиомы об этих понятиях. Затем он объясняет нам эти понятия, пока мы не поймем их достаточно хорошо, чтобы увидеть, что аксиомы являются истинными. Далее он переходит к определению производных понятий и доказывает теоремы об основных и производных понятиях. Здание, которое он строит, состоящее из основных понятий, производных понятий, аксиом и теорем, называется *аксиоматической системой*. Это может быть аксиоматической системой для всей математики или для некоторой части математики такой, как планиметрия или теория действительных чисел.

До сих пор мы предполагали, что описываем какие-то заранее подразумеваемые понятия. Но даже в этом случае можно придумать и другие понятия, которые делают наши аксиомы истинными. В этом случае все доказанные теоремы будут также истинными для этих новых понятий. Это приводит математиков к построению аксиоматических систем, аксиомы которых являются истинными для многих понятий. Типичным примером является множество аксиом для групп. Мы называем такие аксиоматические системы *современными*, в противоположность *классическим* аксиоматическим системам, о которых говорилось раньше. В действительности, конечно, разница не в самой аксиоматической системе, а в замысле ее построения.

Руководствуясь этими замечаниями, мы начинаем изучение математической логики с изучения аксиоматических систем. В итоге это приведет нас к разнообразным проблемам, ряд которых будет лишь косвенно связан с аксиоматическими системами.

1.2. Формальные системы

Аксиома (или теорема) может рассматриваться с двух точек зрения. Мы можем воспринимать ее как некоторое предложение, т. е. объект, находящийся на бумаге, когда мы записали эту аксиому, или интересоваться смыслом этого предложения, т. е. фактом, который выражен этой аксиомой. Казалось бы, последнее кажется более важным. Очевидная цель предложения — выражать смысл этого предложения ясно и точно. Это очень полезная цель, но, по-видимому, мало чего дающая для оснований математики.

При этом существуют два важных довода в пользу изучения аксиом и теорем именно как предложений. Во-первых, если мы удачно выберем язык для выражения аксиом, то структура предложения будет до некоторой степени отражать смысл аксиомы. Поэтому можно изучать понятия, входящие в аксиоматическую систему, изучая структуру предложений, выражающих аксиомы. Это особенно ценно для современных аксиоматических систем, так как для них наше интуитивное понимание основных понятий может быть очень слабым.

Второй довод состоит в том, что понятия математики обычно очень абстрактны и поэтому трудны для понимания. Между тем предложение является конкретным объектом; таким образом, изучая аксиомы как предложения, мы подходим к абстрактному через конкретное.

Бесспорно одно: мало пользы в изучении конкретных объектов (в отличие от абстрактных), если мы не подходим к ним конкретно или конструктивно. Например, когда мы хотим доказать, что некоторый конкретный объект с каким-то свойством существует, мы должны фактически построить такой объект, а не просто показать, что несуществование такого объекта привело бы к противоречию.

О доказательствах, которые оперируют с конкретными объектами конструктивно, говорят, что они *финитны*.

Другое описание этого термина, предложенное Крайзелем, состоит в следующем: доказательство финитно, если мы можем сделать его *обозримым*. Конечно, ни одно из этих описаний не является очень точным, но мы можем применять их во многих случаях для решения того, будет данное доказательство финитным или нет.

Поскольку фундаментальное различие между конкретными и абстрактными объектами принято во внимание, появляются разнообразные вопросы, на которые можно ответить, лишь изучая финитные доказательства. Например, Гильберт, первым начавший такое изучение, считал, что только финитная математика может быть безоговорочно оправдана нашей интуицией. Абстрактная же математика вводится для получения более легких или элегантных доказательств финитных результатов. Поэтому Гильберт предложил программу с целью показать, что всю общепризнаваемую абстрактную математику (или ее существенную часть) можно рассматривать подобным образом. Вопрос о том, как далеко можно продвинуть эту программу, представляет очевидный интерес даже для тех, кто не разделяет точку зрения Гильберта на абстрактную математику.

Изучение аксиом и теорем как предложений называется *синтаксическим* изучением аксиоматических систем; изучение смысла этих предложений называется *семантическим* изучением аксиоматических систем. По причинам, изложенным выше, мы будем часто различать синтаксический и семантический аспекты наших исследований. Когда это возможно и достаточно удобно, наши синтаксические исследования будут финитными. Мы всегда будем рассматривать аксиомы и теоремы как предложения и, следовательно, как синтаксические объекты; когда мы хотим изучать их семантически, мы говорим о смысле аксиом или теорем.

Введем понятие *формальной системы*, которое будет сопровождать нас в нашем синтаксическом изучении. Грубо говоря, формальная система представляет собой синтаксический аспект аксиоматической системы. Дадим точное определение.

Первой частью формальной системы является ее *язык*. Как указывалось раньше, язык должен быть выбран так, чтобы структура предложений по возможности отражала

их смысл. По этой причине, как, впрочем, и по другим, для наших формальных систем обычно будут использоваться искусственные языки.

Чтобы определить язык, нужно прежде всего определить его *символы*. В случае русского языка *) символами будут буквы, цифры и знаки препинания. Большинство наших искусственных языков будет иметь бесконечно много символов.

Любая конечная последовательность символов языка называется *выражением* этого языка. Понятно, что символ может несколько раз появляться в выражении; каждое такое появление называется *вхождением* этого символа в данное выражение. Число вхождений символов в выражение называется *длиной* этого выражения. (Таким образом, русское выражение *ботинок* имеет длину 7.) Мы допускаем в качестве выражения пустую последовательность; это единственное выражение длины 0.

Одно выражение может встречаться внутри другого выражения. Каждое такое появление называется *вхождением* первого выражения во второе. Например, русское выражение *он* имеет 2 вхождения в русское выражение *понтон*. Однако вхождениями не считаются те случаи, когда символы первого выражения встречаются во втором выражении в другом порядке или разделяются другими символами. Таким образом, *он* не имеет вхождений в выражения *нос* или *война*.

Большинство выражений в алфавите русского языка не имеет смысла. Среди осмысленных выражений имеются (повествовательные) предложения, которые приблизительно могут быть описаны как выражения, которые утверждают некоторый факт. Мы будем требовать, чтобы в каждом языке некоторые выражения языка выделялись как *формулы* этого языка; под ними будем подразумевать такие выражения, которые утверждают некоторый факт.

Язык считается полностью определенным, когда определены его символы и формулы. Это делает язык чисто синтаксическим объектом. Конечно, большинство наших языков будут иметь определенную семантику (возможно, не единственную), но эта семантика не считается частью

*) В оригинале, естественно, всегда речь идет об английском языке. — Прим. перев.

языка. Язык формальной системы F будем обозначать через $L(F)$.

Следующей частью формальной системы являются ее *аксиомы*. Наше единственное требование состоит в том, чтобы каждая аксиома была формулой языка формальной системы.

Нам нужна также третья часть формальной системы, которая позволит нам получать теоремы из аксиом. Это достигается с помощью *правил вывода*, которые часто будут называться просто *правилами*. Каждое правило вывода утверждает, что при некоторых условиях одна формула, называемая *заключением* правила, может быть *выведена* из некоторых других формул, называемых *посылками* правила.

Как же определить *теоремы* формальной системы F ? Очевидно, они должны удовлетворять следующим двум законам:

- (i) аксиомы системы F являются теоремами системы F ;
- (ii) если все посылки некоторого правила системы F являются теоремами системы F , то заключение этого правила является теоремой системы F .

Более того, желательно, чтобы формула была теоремой системы только тогда, когда это следует из этих двух законов. Поэтому мы можем определить теорему системы F как формулу, которая является теоремой на основании законов (i) и (ii).

Можно дать более явное описание теорем системы F . Пусть S_0 — множество аксиом; это формулы, о которых можно заключить, что они являются теоремами на основании закона (i). Пусть S_1 — множество формул, которые являются заключениями правил, посылки которых находятся в множестве S_0 ; это формулы, о которых можно заключить, что они являются теоремами на основании закона (ii). Пусть S_2 — множество формул, которые являются заключениями правил, посылки которых находятся в множествах S_0 и S_1 ; это также теоремы на основании закона (ii). Таким же путем строятся множества $S_3, S_4, \dots$. Пусть S_ω — множество формул, которые являются заключениями правил, посылки которых находятся по крайней мере в одном из множеств $S_0, S_1, \dots$; это опять-таки теоремы согласно закону (ii). Продолжаем этот процесс до тех пор, пока по закону (ii) нельзя будет получить новых теорем; вот теперь мы имеем все теоремы.

Определение только что описанного типа называется *обобщенным индуктивным определением*. Обобщенное индуктивное определение семейства объектов C состоит из некоторого множества законов, каждый из которых говорит о том, что при подходящих предположениях некоторый объект x лежит в C . Некоторые из этих предположений могут говорить о том, что какие-то объекты, определенным образом связанные с x , лежат в C . Когда дается такое определение, всегда подразумевается, что объект лежит в C , только если это следует из данных законов. Можно дать более явное описание C , аналогичное сделанному выше.

В качестве другого примера предположим, что мы определили 0 и *последователь* и хотим определить *натуральные числа*. (Натуральные числа — это неотрицательные целые числа 0, 1, 2, ... Последователем натурального числа является следующее большее натуральное число.) Можно дать такое обобщенное индуктивное определение:

- (i) 0 есть натуральное число;
- (ii) если y есть натуральное число, то последователь y есть натуральное число.

Чтобы доказать, что каждая теорема системы F имеет некоторое свойство P , достаточно доказать, что формулы, имеющие свойство P , удовлетворяют законам, указанным в определении *теоремы*. Другими словами, достаточно доказать, что:

- (i') каждая аксиома системы F имеет свойство P ;
- (ii') если все посылки некоторого правила системы F имеют свойство P , то заключение этого правила имеет свойство P .

Из (i') и (ii') следует, что каждый элемент множеств $S_0, S_1, \dots, S_\omega, \dots$, построенных выше, имеет свойство P ; поэтому каждая теорема имеет свойство P . Данное таким способом доказательство называется доказательством *индукцией по теоремам*; предположение в (ii'), что все посылки правила имеют свойство P , называется *индуктивным предположением*.

Более общо, предположим, что семейство C определено с помощью обобщенного индуктивного определения. Тогда, чтобы доказать, что каждый объект семейства C имеет свойство P , достаточно доказать, что объекты, имеющие свойство P , удовлетворяют законам данного определения.

Такое доказательство называется доказательством *индукцией по объектам семейства S* . Упомянутые в этих законах предположения, что некоторые объекты принадлежат семейству S , превращаются в таком доказательстве в предположение о том, что некоторые объекты имеют свойство P ; эти предположения называются *индуктивными предположениями*. Читатель легко заметит, что если S есть семейство натуральных чисел, полученное с помощью обобщенного индуктивного определения, данного выше, то *доказательство индукцией* и *индуктивное предположение* имеют их обычный смысл.

Правило формальной системы F называется *конечным*, если оно имеет только конечное число посылок. Почти все правила, которые мы будем рассматривать, будут конечными.

Пусть F — формальная система, все правила которой конечны. Под *доказательством* в системе F мы понимаем конечную последовательность формул, каждая из которых есть либо аксиома, либо заключение правила, посылки которого предшествуют этой формуле в доказательстве. Если A есть последняя формула доказательства P , то мы говорим, что P есть *доказательство формулы A* .

Покажем, что формула A системы F является теоремой тогда и только тогда, когда существует доказательство формулы A . Прежде всего, как следует из законов (i) и (ii), каждая формула доказательства является теоремой; следовательно, если формула A имеет доказательство, то она является теоремой. Обратное докажем индукцией по теоремам. Если A — аксиома, то сама формула A является доказательством формулы A ; следовательно, A имеет доказательство. Теперь предположим, что A может быть выведена из формул $B_1, \dots, B_n$ по некоторому правилу системы F . По индуктивному предположению каждая из формул B_i имеет доказательство. Если мы поместим эти доказательства одно за другим и добавим формулу A в конце этой последовательности, то получим доказательство формулы A .

Будем писать $\vdash_F \dots$ в качестве сокращения для *... есть теорема системы F* . Если не возникает путаницы, нижний индекс F опускаем.

Основные понятия аксиоматической системы будут соответствовать некоторым символам или выражениям формаль-

ной системы, связанной с данной аксиоматической системой. Производные понятия, так как они определяются в терминах основных понятий, в общем случае будут соответствовать более сложным выражениям. Если важному производному понятию соответствует весьма сложное выражение, может оказаться желательным ввести новый символ как сокращение этого выражения. Мы можем также пожелать ввести сокращения, чтобы сделать некоторые выражения более короткими или более удобными для чтения.

По этим причинам мы позволяем себе вводить в любой язык новые символы, называемые *определяемыми символами*. Каждый такой символ может комбинироваться определенным способом с символами данного языка и ранее определяемыми символами, чтобы образовать выражения, называемые *определяемыми формулами*. Каждая определяемая формула является сокращением некоторой формулы языка. (В этой терминологии сокращение не обязано быть более коротким, чем выражение, которое оно сокращает.) Для каждого определяемого символа мы должны дать *определение* этого символа; это должно быть правилом, говорящим, как строить определяемые формулы с новым символом и как для каждой такой определяемой формулы найти формулу данного языка, которую она сокращает.

Подчеркиваем, что определяемые символы *не* являются символами языка, а определяемые формулы *не* являются формулами языка. Более того, когда мы говорим что-либо о некоторой определяемой формуле, мы в действительности говорим о формуле языка, которая была сокращена (при условии, что имеется какое-нибудь отличие). Так, длина определяемой формулы не есть число вхождений символов в определяемую формулу, а есть число вхождений символов в формулу, которую данная определяемая формула сокращает.

1.3. Синтаксические переменные

Рассматривая формальные системы, мы будем изучать выражения точно так же, как в анализе изучаются действительные числа. В обоих случаях исследования проводятся на русском языке, с добавлением некоторых специальных символов, приспособленных к исследованию. Рассмотрим некоторые специальные символы, используемые в анализе,

и введем аналогичные специальные символы для исследования формальных систем.

Прежде всего в анализе используются имена для некоторых действительных чисел, например, 3 , $-\frac{1}{2}$, π . Нам также нужны имена для выражений. Мы находимся в благоприятной ситуации, так как мы можем дать имя каждому выражению при соглашении, что каждое выражение должно использоваться как имя для самого себя. Это соглашение неудобно для тех, кто пишет учебники по анализу: имя должно быть выражением, а действительное число не является выражением.

Однако при этом соглашении возникает одна опасность. Выражение может (в языке, который мы до сих пор рассматривали) быть именем какого-либо объекта, теперь оно стало также и именем для самого себя. Так, *Бостон* является именем некоторого города, но в связи с нашим соглашением это выражение есть также имя некоторого слова в русском алфавите. Мы избавлены от этого неудобства, потому что мы будем изучать лишь искусственные языки и при их изучении будем пользоваться русским языком. Так, если выражение входит в контекст искусственного языка, оно есть имя некоторого объекта; когда же выражение входит в контекст русского языка, оно есть имя самого этого выражения *).

Другим важным типом символов, используемых в анализе, являются *переменные*. В противоположность имени, которое имеет только одно значение, переменная имеет много значений. В анализе переменная может означать любое действительное число; или, как мы будем говорить, *область изменения* переменной есть совокупность действительных чисел. Однако переменная сохраняет постоянное значение на протяжении некоторого контекста. Формула, содержащая переменные, также имеет много значений — одно значение для каждого распределения действительных чисел как значений переменных, входящих в формулу. Например, $x = x$ может означать $2 = 2$ и $\pi = \pi$; $x = y$ имеет эти же значения, а также $2 = 5$. Когда в анализе

*) Во избежание какой-либо путаницы в некоторых книгах наше соглашение заменено другим: выражение ставится в кавычки, если оно используется в качестве имени самого этого выражения.

утверждается какая-то формула, содержащая переменные, то подразумевается, что все значения этой формулы являются истинными.

Подобным же образом мы будем использовать *синтаксические переменные*, только вместо действительных чисел их область изменения будет состоять из выражений изучаемого языка. Поэтому синтаксическая переменная может означать любое выражение языка, но значение этой переменной остается фиксированным на протяжении некоторого контекста. Формула, содержащая синтаксические переменные, имеет много значений — одно значение для каждого распределения выражений как значений каждой синтаксической переменной, входящей в формулу. Если такая формула утверждается, то подразумевается, что все значения этой формулы являются истинными.

Чтобы дать пример использования синтаксических переменных и выражений как имен для самих себя, предположим, что x есть символ формальной системы F . Предположим также, что мы получаем некоторую новую формулу системы F всякий раз, когда добавляем символ x справа к некоторой формуле системы F . Условившись использовать символ u в качестве синтаксической переменной, можно выразить это следующим образом: если u есть формула, то выражение, полученное добавлением x справа к u , есть формула.

В анализе некоторые переменные имеют область изменения, состоящую только из части всех действительных чисел. Например, обычно область изменения i и j состоит только из натуральных чисел. Мы часто будем использовать синтаксические переменные, область изменения которых состоит лишь из некоторых выражений рассматриваемого языка. Если A используется в качестве синтаксической переменной, область изменения которой состоит из формул, то утверждение в конце предыдущего абзаца может быть сокращено до следующего: выражение, полученное из A добавлением справа символа x , есть формула.

В анализе xy обозначает результат умножения x на y . Если u и v — синтаксические переменные, то мы будем использовать запись uv для выражения, полученного сцеплением u и v , т. е. написанием u и затем написанием v сразу после u . Такое же соглашение используется для других синтаксических переменных. Оно же может использо-

ваться и в комбинации синтаксических переменных с именами выражений. Например, утверждение в конце предыдущего абзаца может быть сделано более коротким: Ax есть формула.

Для синтаксических переменных будут использоваться полужирные буквы. В частности, **u** и **v** будут означать синтаксические переменные, область изменения которых состоит из всех выражений; **A** , **B** , **C** и **D** будут означать синтаксические переменные, область изменения которых состоит из формул. Другие синтаксические переменные будут введены позднее. При использовании полужирных букв для синтаксических переменных будем иметь в виду, что можно образовывать новые синтаксические переменные добавлением штрихов и индексов и эти новые синтаксические переменные будут иметь ту же область изменения, что и старые переменные. Таким образом, **A'** и **A_1** являются синтаксическими переменными, область изменения которых состоит из формул.

В заключение добавим еще пару слов. Во-первых, если две различные синтаксические переменные встречаются в одном контексте, они не обязательно означают разные выражения (аналогично в анализе x и y не обязательно означают различные действительные числа). Во-вторых, синтаксические переменные *не* являются символами рассматриваемого языка; они являются символами, добавленными к русскому алфавиту, чтобы помочь исследованию этого языка.

ТЕОРИИ ПЕРВОГО ПОРЯДКА

2.1. Функции и предикаты

Как уже отмечалось, мы хотим изучать формальные системы, в которых структура языка связана с подразумеваемым смыслом языка. Теперь мы выберем класс формальных систем, обладающих этим свойством, который достаточно широк, чтобы включать в себя формализации обычных аксиоматических систем математики.

Наша первая задача — описать языки, которые будут использоваться в этих формальных системах. Перед тем, как это сделать точно, мы неформально исследуем понятия, которые встречаются в математических аксиоматических системах, и введем для них некоторые обозначения. Некоторые из этих понятий являются общими для всех аксиоматических систем. Мы называем их *логическими понятиями*; они будут рассматриваться в следующих двух параграфах. В этом параграфе мы рассматриваем природу остальных понятий, которые называются *нелогическими понятиями*.

Начнем с примера. Предположим, что мы хотим построить язык для изучения натуральных чисел. Типичной формулой в таком языке была бы формула $2 + 1 < 4$. Что означает каждый символ в этой формуле?

Ясно, что 2, 1 и 4 представляют конкретные натуральные числа. Можно думать, что символ $+$ представляет объект, который связывает с каждой парой (a, b) натуральных чисел третье натуральное число, а именно, сумму a и b . Можно считать, что символ $<$ представляет некоторый объект, который отличает пары натуральных чисел (a, b) , у которых a меньше b , от тех пар (a, b) , для которых a не меньше b . Поэтому мы будем использовать этот символ для представления семейства всех пар (a, b) таких, что a меньше b .

Можно объяснить это короче, вводя терминологию теории множеств *). *Множество* или *класс* есть семейство некоторых объектов. Пусть A и B — множества; *отображением из A в B* называется сопоставление каждому объекту из A некоторого объекта из B . Если F обозначает отображение и F сопоставляет элемент b из B элементу a из A , то мы говорим, что b является *значением F для аргумента a* , и пишем $F(a)$ вместо b . n -кой в A называется последовательность из n (не обязательно различных) объектов из A . n -ку, состоящую из объектов $a_1, a_2, \dots, a_n$ в указанном порядке, мы обозначаем через $(a_1, a_2, \dots, a_n)$. Отображение из множества n -ок в A в B называется *n -арной функцией из A в B* . Подмножество множества n -ок в A называется *n -арным предикатом на A* . Если P обозначает такой предикат, то $P(a_1, \dots, a_n)$ будет обозначать, что n -ка $(a_1, \dots, a_n)$ принадлежит P . Вместо 1-арный мы говорим *унарный*, а вместо 2-арный — *бинарный*. Заметим, что унарная функция из A в B есть отображение из A в B , а унарный предикат на A есть подмножество множества A .

Условимся также, что существует ровно одна 0-ка в A и обозначим ее через $()$. 0-арная функция из A в B полностью определена своим значением для аргумента $()$. Мы будем отождествлять эту функцию с этим значением. Это означает, что 0-арная функция из A в B есть просто некоторый элемент из B .

Возвратимся к нашему примеру; пусть N — множество натуральных чисел. Тогда $+$ представляет бинарную функцию из N в N , а $<$ — бинарный предикат на N . Мы также можем считать, что 1, 2 и 4 представляют 0-местные функции из N в N .

В математической аксиоматической системе мы будем иметь некоторое множество объектов, играющее такую же роль, как и множество натуральных чисел в вышеприведенном примере. Это множество называется *универсумом* аксиоматической системы, а его элементы — *индивидами* системы. Функции из универсума в универсум называются

*) Этот параграф не нужно рассматривать как введение в элементарную теорию множеств; мы предполагаем, что читатель с ней уже знаком. Наша цель здесь — лишь ввести ее терминологию и понятия. Аксиоматическое изложение теории множеств будет дано в главе 9; до этого будут использоваться лишь элементарные результаты.

индивидуальными функциями; предикаты на универсуме называются *индивидуальными предикатами*. Среди символов, которые нужны для формализации аксиоматической системы, находятся имена для некоторых индивидов, индивидуальных функций и индивидуальных предикатов. (С точки зрения нашего истолкования 0-арных функций первое есть частный случай второго.)

Можно было бы подумать, что для некоторых аксиоматических систем необходимо иметь несколько универсумов. Например, в планиметрии мы должны иметь множество точек и множество прямых. Однако можно взять за универсум множество всех точек и прямых, а затем ввести символы для множества точек и множества прямых (рассматривая каждый как унарный индивидуальный предикат).

Мы ограничиваемся аксиоматическими системами, в которых универсум не пуст, т. е. содержит по крайней мере один индивид. Это является техническим соглашением; оно, очевидно, не исключает ни одного интересного случая.

Для любого множества A мы можем построить бинарный предикат, который состоит из всех пар, у которых первый и второй элементы являются одним и тем же элементом из A . Этот предикат называется *предикатом равенства на A* . Мы будем использовать символ $=$ для обозначения предиката равенства на универсуме.

Рассмотрение, которое было проведено, предполагало, что мы формализуем какую-то классическую аксиоматическую систему. Для современной аксиоматической системы результаты будут те же, за исключением того, что мы имеем в виду несколько различных универсумов. Так, если мы формализуем теорию полей, то возможными универсумами являются различные поля. Нам следовало бы затем ввести символы для функций сложения и умножения в поле и т. д.

2.2. Функции истинности

Символы, которые рассматривались в предыдущем параграфе, позволяют нам строить некоторые простые формулы. Введем еще некоторые символы, которые помогут нам строить более сложные формулы из этих простых формул. Например, мы введем символ $\&$ и будем понимать его

как союз *и*. Тогда мы можем построить формулу $2 < 4 \& 6 = 3$ из формул $2 < 4$ и $6 = 3$.

Примечательной особенностью формулы $A \& B$ является то, что для того, чтобы узнать, будет ли $A \& B$ истинной или ложной, нужно лишь знать, будет ли A истинной или ложной и будет ли B истинной или ложной; нам не нужно знать, что означают A и B . Мы можем выразить это проще, введя следующую терминологию. Выберем два объекта, **И** и **Л**, которые назовем *истинностными значениями*. Не имеет значения, чем являются эти объекты, важно лишь то, что они отличаются друг от друга. Затем мы приписываем истинностное значение каждой формуле следующим образом: мы приписываем **И** каждой истинной формуле и **Л** каждой ложной формуле. Тогда мы видим, что истинностное значение $A \& B$ определяется истинностными значениями A и B .

Функцией истинности называется функция из множества истинностных значений в множество истинностных значений. Вышеприведенное замечание можно переформулировать так: существует бинарная функция истинности $H_{\&}$ такая, что если a и b — истинностные значения A и B соответственно, то $H_{\&}(a, b)$ есть истинностное значение $A \& B$. Эта функция истинности задается с помощью равенств:

$$\begin{aligned} H_{\&}(\text{И}, \text{И}) &= \text{И}, \\ H_{\&}(\text{И}, \text{Л}) &= H_{\&}(\text{Л}, \text{И}) = H_{\&}(\text{Л}, \text{Л}) = \text{Л}. \end{aligned}$$

Затем мы вводим символ $\vee$, понимая его как союз *или*. Будет ли истинностное значение $A \vee B$ определяться по истинностным значениям A и B ? Конечно, $A \vee B$ ложна, когда A и B обе ложны, и истинна, когда в точности одна из A и B истинна. Если A и B обе истинны, то в повседневной речи мы можем считать, а можем и не считать A или B истинным; но в математике это выражение всегда считается истинным. Именно такой математический смысл союза *или* мы придаем символу $\vee$. Так, если a и b — истинностные значения A и B соответственно, то истинностное значение $A \vee B$ есть $H_{\vee}(a, b)$, где $H_{\vee}$ — бинарная функция истинности, определенная следующим образом:

$$\begin{aligned} H_{\vee}(\text{И}, \text{И}) &= H_{\vee}(\text{И}, \text{Л}) = H_{\vee}(\text{Л}, \text{И}) = \text{И}, \\ H_{\vee}(\text{Л}, \text{Л}) &= \text{Л}. \end{aligned}$$

Теперь введем символ $\rightarrow$, понимая его как союз *если ... , то*; таким образом, $A \rightarrow B$ означает *если A , то B* . В математике мы считаем утверждение *если A , то B* неверным только в случае, когда A истинна, а B ложна. Если A ложна, то *если A , то B* является верным, хотя и не интересным утверждением. Символу $\rightarrow$ мы придаем именно такой математический смысл союза *если ... , то*. Тогда символу $\rightarrow$ соотносится, аналогично выше рассмотренному, функция истинности $H_{\rightarrow}$, определенная так:

$$\begin{aligned} H_{\rightarrow}(\text{И}, \text{И}) &= H_{\rightarrow}(\text{Л}, \text{И}) = H_{\rightarrow}(\text{Л}, \text{Л}) = \text{И}, \\ H_{\rightarrow}(\text{И}, \text{Л}) &= \text{Л}. \end{aligned}$$

Теперь введем символ $\leftrightarrow$, понимая его как *тогда и только тогда*. Ясно, что $A \leftrightarrow B$ истинна, если A и B обе истинны или обе ложны, а в остальных случаях $A \leftrightarrow B$ ложна. Следовательно, символу $\leftrightarrow$ соотносится функция истинности $H_{\leftrightarrow}$, определенная так:

$$\begin{aligned} H_{\leftrightarrow}(\text{И}, \text{И}) &= H_{\leftrightarrow}(\text{Л}, \text{Л}) = \text{И}, \\ H_{\leftrightarrow}(\text{И}, \text{Л}) &= H_{\leftrightarrow}(\text{Л}, \text{И}) = \text{Л}. \end{aligned}$$

Далее мы введем символ $\neg$, понимая его как частицу *не*; таким образом, $\neg A$ означает *не A* . Если A имеет истинностное значение a , то $\neg A$ имеет истинностное значение $H_{\neg}(a)$, где $H_{\neg}$ — унарная функция истинности, определенная так:

$$H_{\neg}(\text{И}) = \text{Л}, \quad H_{\neg}(\text{Л}) = \text{И}.$$

Простые рассуждения показывают, что некоторые из этих символов могут быть определены в терминах других. Например, $A \rightarrow B$ означает, что или A ложна или B истинна; следовательно, $A \rightarrow B$ означает то же самое, что и $\neg A \vee B$. Более формально это можно сделать так. Если a и b — истинностные значения A и B соответственно, то истинностное значение $A \rightarrow B$ есть $H_{\rightarrow}(a, b)$, а истинностное значение $\neg A \vee B$ есть $H_{\vee}(H_{\neg}(a), b)$. Но для любых a и b

$$H_{\rightarrow}(a, b) = H_{\vee}(H_{\neg}(a), b),$$

в чем мы можем убедиться, перебирая все возможности. Таким же образом мы видим, что $A \& B$ означает то же самое, что и $\neg(A \rightarrow \neg B)$, и что $A \leftrightarrow B$ означает то же самое, что и

$$(A \rightarrow B) \& (B \rightarrow A).$$

Следовательно, все наши символы определяются в терминах $\neg$ и $\forall$. (Можно показать, что каждый символ, имеющий некоторую функцию истинности, сопоставленную с ним, как в рассмотренных выше случаях, можно определить в терминах $\neg$ и $\forall$; см. задачу 1.)

2.3. Переменные и кванторы

Применяя введенные выше понятия, мы можем выразить довольно сложные факты о конкретных натуральных числах. Однако мы не сможем выразить даже такой простой *общий* закон, как: *каждое натуральное число равно самому себе*.

Для этой цели введем *индивидуальные переменные*. Они подобны переменным из анализа, рассмотренным ранее, но их область изменения представляет собой индивиды, а не действительные числа. Таким образом, индивидуальную переменную можно понимать как любой индивид, но ее значение остается фиксированным на протяжении всего контекста. Формула, содержащая индивидуальные переменные, имеет много значений — одно значение для каждого распределения индивидов как значений каждой индивидуальной переменной в формуле. Если мы утверждаем такую формулу, то мы утверждаем, что все ее значения истинны.

Так как в наших языках будут встречаться лишь индивидуальные переменные, мы будем называть их просто *переменными*. В качестве переменных мы будем употреблять символы x , y , z и w , добавляя к ним штрихи для образования новых переменных, если они понадобятся. Так, если универсум есть множество натуральных чисел, то мы можем утверждать, что каждое натуральное число равно самому себе, утверждая справедливость формулы $x = x$.

Хотя теперь мы можем *утверждать*, что каждый индивид имеет некоторое свойство, у нас нет формулы, *означающей*, что каждый индивид имеет это свойство. Чтобы показать неудобство этого, предположим, что мы высказали утверждение $x = 0$. Мы бы тогда утверждали ошибочно, что каждое натуральное число равно 0. Можно надеяться сделать это утверждение справедливым, поставив перед ним символ $\neg$. Но утверждать $\neg(x = 0)$ — это значит утверждать, что каждое натуральное число не равно 0; а это также неверно.

Чтобы преодолеть эту трудность, введем символ $\forall$, который будет означать *для всех индивидов*. Таким образом, $\forall x(x = 0)$ означает *для всех натуральных чисел x имеем $x = 0$* , т. е. *каждое натуральное число равно 0*. Теперь, чтобы получить правильное утверждение, что не каждое натуральное число равно 0, мы утверждаем $\neg \forall x(x = 0)$.

Большинство наших предыдущих замечаний о переменных ложны, если они применяются к переменной x в $\forall x(x = 0)$. Эта формула имеет только одно значение, в то время как $x = 0$ имеет много значений. Мы получаем конкретное значение для $x = 0$, подставляя 2 вместо x ; однако если мы подставляем 2 вместо x в $\forall x(x = 0)$, то получаем бессмысленное выражение $\forall 2(2 = 0)$. С другой стороны, если мы подставим y вместо x в $\forall x(x = 0)$, то получим формулу $\forall y(y = 0)$, которая имеет тот же смысл, что и $\forall x(x = 0)$ (а именно, что каждое натуральное число равно 0). В противоположность этому $x = 0$ и $y = 0$ не обязательно имеют одинаковые значения; это зависит от выбора значений для x и y .

Чтобы разделить эти два случая, мы называем вхождение переменной x в $x = 0$ *свободным* вхождением, а вхождения переменной x в $\forall x(x = 0)$ — *связанными* вхождениями. Если мы воспользуемся описанными выше особенностями, для того чтобы отличать свободные и связанные вхождения переменных, то мы увидим, что связанные вхождения переменных имеются и в анализе. Рассмотрим

переменную x в $\int_0^1 \sin x \, dx$. Это выражение имеет единствен-

ное значение, и оно равно некоторому действительному числу. Если мы подставим 2 вместо x , то получим бес-

смысленное выражение $\int_0^1 \sin 2 \, d2$. Если мы подставим y

вместо x , то получим $\int_0^1 \sin y \, dy$, которое имеет тот же смысл, что и $\int_0^1 \sin x \, dx$ (хотя в этом иногда трудно убе-

дить студентов первого курса). Другим примером связанного вхождения переменной является вхождение пере-

менной n в $\sum_{n=1}^k x_n$.

Теперь введем символ $\exists$, означающий для некоторого индивида. Таким образом, $\exists x (x=0)$ означает для некоторого натурального числа x имеем $x=0$, т. е. некоторое натуральное число равно 0. Мы можем также читать $\exists x$ как *существует индивид x такой, что*; например, $\exists x (x=0)$ означает, что *существует натуральное число x такое, что $x=0$* . Если применять вышеприведенный критерий, то мы видим, что вхождение x в $\exists x (x=0)$ является связанным.

Вхождение выражения $\forall x$ или $\exists x$ влияет только на те свободные вхождения переменной x в формуле, которая написана за ним. Таким образом, в формуле

$$\forall x (x=5) \vee \exists x (x < 2) \vee x=7$$

первые два вхождения x не связаны со следующими двумя вхождениями, а последнее вхождение не связано с первыми четырьмя. Аналогично, в формуле

$$\forall x (x=5 \rightarrow \exists x (x < 7))$$

первые два вхождения x не связаны с последними двумя. Мы можем всегда избежать таких формул, переименовав переменную. Так мы могли бы заменить первую формулу на

$$\forall y (y=5) \vee \exists z (z < 2) \vee x=7,$$

а вторую на

$$\forall x (x=5 \rightarrow \exists y (y < 7)).$$

Однако не всегда удобно совершенно исключать такие формулы. Если $\forall x$ или $\exists x$ поставлено перед формулой, у которой нет свободных вхождений x , то смысл этой формулы не меняется.

Необязательно брать в качестве неопределяемых символов оба символа $\forall$ и $\exists$; мы можем определить $\forall$ в терминах $\exists$. Вначале заметим, что $\exists x \neg (x=0)$ означает, что *некоторое натуральное число не равно 0*. Следовательно, $\neg \exists x \neg (x=0)$ означает *нет натурального числа, не равного 0*, т. е. *каждое натуральное число равно 0*. Это означает то же, что и формула $\forall x (x=0)$. Такие же рассуждения показывают, что $\forall x A$ всегда означает то же, что и $\neg \exists x \neg A$; следовательно, можно определить $\forall x A$ как $\neg \exists x \neg A$. (Аналогично мы можем определить $\exists x A$ как $\neg \forall x \neg A$.)

2.4. Языки первого порядка

Теперь мы имеем все необходимое, чтобы перейти к точному определению того типа языка, который мы хотим рассматривать.

Язык первого порядка имеет следующие символы:

(а) переменные

$$x, y, z, w, x', y', z', w', x'', \dots;$$

(б) n -арные функциональные символы и n -арные предикатные символы для каждого n ;

(в) символы $\neg$, $\vee$ и $\exists$.

Для каждого n число n -арных функциональных символов может быть равно 0 или не равно 0, конечно или бесконечно. То же самое и для предикатных символов, за исключением того, что среди бинарных предикатных символов должен быть символ равенства $=$.

Любой 0-арный функциональный символ называется константой. Функциональный символ или предикатный символ, отличный от $=$, называется *нелогическим символом*; остальные символы называются *логическими*.

Для ссылок иногда будет удобно иметь фиксированный порядок переменных. Тот порядок, в котором они перечислены выше, мы называем *алфавитным порядком*.

Заметим, что мы не включили скобки и запятые, которые мы использовали в предыдущих параграфах для указания группировки символов. Оказывается группировка символов однозначно определяется и без них, если сделать одно изменение в наших обозначениях: писать $\vee AB$ вместо $A \vee B$. Конечно, мы можем затем ввести обозначение $A \vee B$ по определению.

Мы применяем x, y, z и w как синтаксические переменные, областью изменения которых являются переменные; f и g как синтаксические переменные, областью изменения которых являются функциональные символы; p и q как синтаксические переменные, областью изменения которых являются предикатные символы; e как синтаксическую переменную, областью изменения которой являются константы.

Предположим, что мы имеем семейство символов, описанных выше. Определим *термы* с помощью обобщенного индуктивного определения.

(i) Переменная есть терм.

(ii) Если $u_1, \dots, u_n$ — термы и f — n -арный символ, то $fu_1 \dots u_n$ — терм.

В частности, по правилу (ii) константа есть терм. Ясно, что термы — это как раз те выражения, значениями которых являются индивиды. Мы будем применять a, b, c и d как синтаксические переменные, областью изменения которых являются термы.

Атомная формула — это выражение вида $ra_1 \dots a_n$, где r — n -арный символ. Определим *формулы* с помощью следующего обобщенного индуктивного определения:

- (i) всякая атомная формула есть формула;
- (ii) если u — формула, то $\neg u$ — формула;
- (iii) если u и v — формулы, то $\vee uv$ — формула;
- (iv) если u — формула, то $\exists x u$ — формула.

Для этих двух обобщенных индуктивных определений мы имеем соответствующие формы доказательств по индукции. Однако обычно проще использовать индукцию по длине термина или формулы. Иногда мы будем применять индукцию по высоте формулы, где *высота* определяется как число вхождений символов $\neg$, $\vee$ и $\exists$ в формулу.

Язык первого порядка определяется как язык с символами и формулами, описанными выше. Таким образом, язык первого порядка полностью определяется своими нелогическими символами. Этими символами могут быть любые символы, которые еще не выбраны для других целей. Однако мы договоримся, что если некоторый символ используется как n -арный функциональный символ в одном из языков первого порядка, то он может быть использован в другом языке первого порядка только как n -арный функциональный символ; аналогично для предикатных символов. Отсюда следует, что если два языка первого порядка имеют одинаковые нелогические символы, то они совпадают.

Указателем называется выражение, которое является либо термом, либо формулой. Как видно из определений термина и формулы, каждый указатель имеет вид $uv_1 \dots v_n$, где u — символ, $v_1, \dots, v_n$ — указатели, а n — натуральное число, определяемое по u . Например, если u — переменная, то $n=0$; если u — k -арный функциональный символ, то $n=k$; если u есть $\exists$, то $n=2$. Назовем n *индексом* u .

Скажем, что два выражения *сравнимы*, если одно из них может быть получено из другого добавлением к нему справа некоторого выражения (возможно, пустого). Если uv и $u'v'$ сравнимы, то u и u' сравнимы; если uv и uv' сравнимы, то v и v' сравнимы.

Лемма 1. Если $u_1, \dots, u_n, u'_1, \dots, u'_n$ — указатели, а $u_1 \dots u_n$ и $u'_1 \dots u'_n$ сравнимы, то u_i есть u'_i для $i=1, \dots, n$.

Доказательство. Проведем индукцию по длине $u_1 \dots u_n$. Запишем u_1 как $vv_1 \dots v_k$, где v — символ индекса k , а $v_1, \dots, v_k$ — указатели. Так как u'_1 начинается с v , то оно имеет вид $vv'_1 \dots v'_k$, где $v'_1, \dots, v'_k$ — указатели. Значит, u_1 сравнимо с u'_1 , а $v_1 \dots v_k$ сравнимо с $v'_1 \dots v'_k$. По индуктивному предположению v_i есть v'_i для $i=1, \dots, k$; следовательно, u_1 есть u'_1 . Отсюда следует, что $u_2 \dots u_n$ сравнимо с $u'_2 \dots u'_n$ и по индуктивному предположению u_i есть u'_i для $i=2, \dots, n$.

Следующая теорема является точной формулировкой нашего утверждения о том, что в языке первого порядка запятые и скобки не обязательны для восстановления группировки символов.

Теорема построения. Каждый указатель можно записать единственным способом в виде $uv_1 \dots v_n$, где u — некоторый символ индекса n , а $v_1, \dots, v_n$ — указатели.

Доказательство. Нужно доказать только единственность. В этом случае u должен быть первым символом указателя; следовательно, u и n определяются однозначно. Остается показать, что если $uv_1 \dots v_n$ совпадает с $uv'_1 \dots v'_n$ и $v_1, \dots, v_n, v'_1, \dots, v'_n$ — указатели, то v_i есть v'_i для $i=1, \dots, n$. Это следует из леммы 1.

Лемма 2. Каждое вхождение любого символа в указатель u начинает вхождение некоторого указателя в u .

Доказательство. Проведем индукцию по длине u . Запишем u как $vv_1 \dots v_k$, где v — символ индекса k , а $v_1, \dots, v_k$ — указатели. Если рассматриваемое вхождение символа есть начальное v , то оно начинает u . В противном случае это вхождение есть вхождение в некоторое v_i и по индуктивному предположению начинает вхождение некоторого указателя в v_i . Следовательно, оно начинает вхождение некоторого указателя и в u .

Теорема о вхождении. Пусть u — символ индекса n , а $v_1, \dots, v_n$ — указатели. Тогда любое вхождение

указателя v в $uv_1, \dots, v_n$ есть либо всё $uv_1, \dots, v_n$, либо часть одного из v_i .

Доказательство. Предположим, что начальный символ вхождения v есть начальное u в $uv_1 \dots v_n$. Тогда v есть $uv'_1 \dots v'_n$, где $v'_1, \dots, v'_n$ — указатели. Так как v сравнимо с $uv_1 \dots v_n$, то $v'_1 \dots v'_n$ сравнимо с $v_1 \dots v_n$. По лемме 1 v_i есть v'_i для $i=1, \dots, n$; так что v есть всё $uv_1 \dots v_n$.

Теперь предположим, что начальный символ вхождения v находится внутри v_i . По лемме 2 этот символ начинает вхождение некоторого указателя v' в v_i . Ясно, что v и v' сравнимы, тогда по лемме 1 v есть v' . Следовательно, v есть часть v_i .

Дадим теперь точные определения свободных и связанных вхождений. Вхождение x в A связано в A , если x входит в часть A вида $\exists xB$ *); в противном случае это вхождение свободно в A . Скажем, что x свободно (связано) в A , если некоторое вхождение x в A свободно (связано). (Заметим, что x может быть как свободным, так и связанным в A .) Как следует из теоремы о вхождении, если u отлично от x , то свободные вхождения x в $\neg A$, $\bigvee AB$ и $\exists yA$ — это в точности свободные вхождения x в A и в B . Конечно, x не имеет свободных вхождений в $\exists xA$.

Будем обозначать через $b_x[a]$ выражение, полученное из b заменой каждого вхождения x на a ; будем обозначать через $A_x[a]$ выражение, полученное из A заменой каждого свободного вхождения x на a . Используя индукцию по длине b и A , легко доказываем, что $b_x[a]$ есть терм, а $A_x[a]$ есть формула.

Вообще говоря, $A_x[a]$ утверждает про индивид, обозначенный через a , то же самое, что A утверждает про индивид, обозначенный через x , но это верно не во всех случаях. Так, предположим, что A есть $\exists y (x=2y)$, x есть x , а a есть $y+1$. Тогда A утверждает, что x — четное число; но $A_x[a]$, которое есть $\exists y (y+1=2y)$, не утверждает, что $y+1$ — четное число. Эта трудность возникла, конечно, потому, что y в подставляемом терме $y+1$ стало связанным. Мы хотим исключить такие возможности.

*) Напомним, что B — синтаксическая переменная для формул, так что $\exists xB$ — подформула формулы A . — Прим. ред.

Будем говорить, что a допустим для подстановки вместо x в A , если для каждой переменной y , входящей в a , в A нет части вида $\exists yB$, содержащей вхождение x , которое свободно в A . Теперь условимся, что если встречается выражение $A_x[a]$, то A , x и a таковы, что a допустим для подстановки вместо x в A . Заметим, что это условие наверняка выполняется, когда a не содержит переменных, или когда A не содержит переменных, или когда A не содержит связанных вхождений переменных.

Теперь обобщим это понятие на случай нескольких переменных. Пусть $b_{x_1, \dots, x_n}[a_1, \dots, a_n]$ обозначает терм, полученный из b заменой всех вхождений $x_1, \dots, x_n$ на $a_1, \dots, a_n$ соответственно; пусть $A_{x_1, \dots, x_n}[a_1, \dots, a_n]$ обозначает формулу, полученную из A заменой всех свободных вхождений $x_1, \dots, x_n$ на $a_1, \dots, a_n$ соответственно. Эти понятия используются при ограничении, что $x_1, \dots, x_n$ — различные переменные. Если встречается $A_{x_1, \dots, x_n}[a_1, \dots, a_n]$, то A , $x_1, \dots, x_n$, $a_1, \dots, a_n$ таковы, что a_i допустим для подстановки вместо x_i в A для $i=1, \dots, n$. Мы будем опускать нижние индексы $x_1, \dots, x_n$, если они будут несущественны или ясны из контекста.

Введем теперь некоторые определяемые символы. Во всех теориях $(A \vee B)$ есть сокращение для $\bigvee AB$; $(A \rightarrow B)$ — сокращение для $(\neg A \vee B)$; $(A \& B)$ — сокращение для $\neg(A \rightarrow \neg B)$; $(A \leftrightarrow B)$ — сокращение для $((A \rightarrow B) \& (B \rightarrow A))$; $\forall xA$ — сокращение для $\neg \exists x \neg A$. Если u — бинарный предикатный или функциональный символ, то (aub) есть сокращение для uab ; если u — бинарный предикатный символ, то $(a \neg b)$ есть сокращение для $\neg(aub)$. В каждом случае определяемые формулы — это те выражения, которые получаются из формул, когда определяемые символы заменяются согласно только что указанным правилам.

Можно показать, что скобки, введенные в определениях, приведенных выше, достаточны для определения группировки символов. Однако, так как мы не намерены изучать определяемые символы, такой общий результат нам не нужен. Нам нужно только, чтобы каждая определяемая формула, которую мы пишем, была сокращением единственной формулы языка. По этой причине мы

будем опускать скобки, когда они не являются необходимыми для определения группировки символов; например, мы пишем $x = y \rightarrow y = x$ вместо

$$((x = y) \rightarrow (y = x)).$$

С другой стороны, мы можем для удобства чтения употреблять и лишние скобки и запятые. Так мы часто будем писать $u(a_1, \dots, a_n)$ вместо $ua_1 \dots a_n$, если u есть функциональный или предикатный символ. Следующее соглашение поможет нам опускать еще больше скобок: если имеется выбор, то мы предпочитаем записывать формулу в виде $A \rightarrow B$ или $A \leftrightarrow B$, чем в виде $A \vee B$ или $A \& B$. Следовательно, $A \rightarrow B \vee C$ должна читаться как

$$A \rightarrow (B \vee C),$$

а $A \& B \leftrightarrow C$ должна читаться как $(A \& B) \leftrightarrow C$.

Мы также вводим соглашение *правого сочетания* опущенных скобок. Это означает, что $A \vee B \vee C$ должно читаться как $A \vee (B \vee C)$; $A \vee B \vee C \vee D$ должно читаться как $A \vee (B \vee (C \vee D))$ и т. д. То же соглашение используется для последовательности формул, связанных символом $\&$, или последовательности формул, связанных символом $\rightarrow$. Заметим также, что $A_1 \vee \dots \vee A_n$ означает, что по крайней мере одна из $A_1, \dots, A_n$ истинна; $A_1 \& \dots \& A_n$ означает, что все $A_1, \dots, A_n$ истинны; и $A_1 \rightarrow \dots \rightarrow A_n \rightarrow B$ означает, что если все $A_1, \dots, A_n$ истинны, то B истинна. Во всех случаях мы допускаем и $n=1$. Если мы пишем $A_1 \rightarrow \dots \rightarrow A_n \rightarrow B$, то мы даже допускаем, что n может быть равно 0; в этом случае это просто формула B .

Мы называем $\neg A$ отрицанием A ; $A \vee B$ — дизъюнкцией A и B ; $A \& B$ — конъюнкцией A и B ; $A \rightarrow B$ — импликацией B из A ; $A \leftrightarrow B$ — эквивалентностью A и B ; $\exists x A$ — подтверждением A с помощью x ; $\forall x A$ — обобщением A с помощью x . Мы также называем $A_1 \vee \dots \vee A_n$ дизъюнкцией $A_1, \dots, A_n$, а $A_1 \& \dots \& A_n$ — конъюнкцией $A_1, \dots, A_n$. Однако если мы просто говорим, что формула есть дизъюнкция или конъюнкция, то мы подразумеваем, что это дизъюнкция или конъюнкция двух формул. Выражения $\exists x$ и $\forall x$ называются *кванторами по x* ; первый есть *квантор существования*, а второй — *квантор всеобщности*.

2.5. Структуры

Теперь приступим к строгому описанию семантики языков первого порядка. Как уже указывалось, семантика языка первого порядка состоит из универсума и содержательного смысла каждого нелогического символа. Записывая это детально, мы приходим к следующему определению.

Пусть L — язык первого порядка. Структура $\mathcal{A}$ для L состоит из следующего:

(i) непустого множества $|\mathcal{A}|$, называемого *универсумом $\mathcal{A}$* ; элементы из $|\mathcal{A}|$ называются *индивидами* структуры $\mathcal{A}$;

(ii) n -арной функции $f_{\mathcal{A}}$ из $|\mathcal{A}|$ в $|\mathcal{A}|$ для каждого n -арного функционального символа f из L (в частности, $e_{\mathcal{A}}$ является индивидом из $\mathcal{A}$ для каждой константы e из L);

(iii) n -арного предиката $p_{\mathcal{A}}$ на $|\mathcal{A}|$ для каждого n -арного предикатного символа p из L , отличного от $=$.

Мы хотели бы, чтобы формула A была истинной в $\mathcal{A}$, если все ее значения истинны в $\mathcal{A}$. Поэтому было бы удобно, если бы для каждого значения A мы имели формулу, которая выражает именно это значение. Так как значения A получаются с помощью задания значений индивидов для каждой свободной переменной формулы A , то ясно, что нам нужны имена для индивидов. Это приводит нас к следующим определениям.

Пусть $\mathcal{A}$ — структура для L . Для каждого индивида a из $\mathcal{A}$ мы выбираем новую константу, называемую *именем индивида a* . При этом подразумевается, что разные имена выбираются для разных индивидов. Язык первого порядка, полученный из L добавлением всех имен индивидов из $\mathcal{A}$, обозначим через $L(\mathcal{A})$. Мы используем i и j в качестве синтаксических переменных, областью изменения которых являются имена.

Выражение называется *свободным от переменных*, если оно не содержит переменных. Определим теперь индивид $\mathcal{A}(a)$ из $\mathcal{A}$ для каждого терма a из $L(\mathcal{A})$, свободного от переменных. Определение дается индукцией по длине a . Если a — имя, то $\mathcal{A}(a)$ — индивид, для которого a является именем. Если a — не имя, то (так как он свободен от переменных) он имеет вид $fa_1, \dots, a_n$, где f —

функциональный символ из L . Тогда полагаем $\mathcal{A}(a)$ равным $f_A(\mathcal{A}(a_1), \dots, \mathcal{A}(a_n))$.

Замечание. В вышеприведенном определении мы неявно применяли теорему построения, когда считали, что a может быть записано в виде $fa_1 \dots a_n$ единственным образом. Мы будем часто так неявно использовать теорему построения в определениях индукцией по длине терма или формулы.

Формула A называется *замкнутой*, если в ней нет переменных, свободных в A . (Это означает, что A имеет только одно значение.) Мы определим теперь истинностное значение $\mathcal{A}(A)$ для каждой замкнутой формулы A языка $L(\mathcal{A})$. Определение дается индукцией по длине A . Если A есть $a=b$, то a и b должны быть свободными от переменных (так как A замкнута). Положим

$\mathcal{A}(A)=\mathbf{I}$ тогда и только тогда, когда $\mathcal{A}(a)=\mathcal{A}(b)$

(т. е. тогда и только тогда, когда $\mathcal{A}(a)$ и $\mathcal{A}(b)$ одинаковы). Если A есть $pa_1 \dots a_n$, где p отлично от $=$, то положим

$\mathcal{A}(A)=\mathbf{I}$ тогда и только тогда, когда $p_A(\mathcal{A}(a_1), \dots, \mathcal{A}(a_n))$

(т. е. тогда и только тогда, когда n -ка $(\mathcal{A}(a_1), \dots, \mathcal{A}(a_n))$ принадлежит предикату p_A). Если A есть $\neg B$, то $\mathcal{A}(A)$ есть $H_{\neg}(\mathcal{A}(B))$. Если A есть $B \vee C$, то $\mathcal{A}(A)$ есть $H_{\vee}(\mathcal{A}(B), \mathcal{A}(C))$. Если A есть $\exists xB$, то $\mathcal{A}(A)=\mathbf{I}$ тогда и только тогда, когда $\mathcal{A}(B_x[i])=\mathbf{I}$ для некоторого i из $L(\mathcal{A})$.

Ясно, что $\mathcal{A}(A \rightarrow B)=H_{\rightarrow}(\mathcal{A}(A), \mathcal{A}(B))$ и аналогичное справедливо для $\&$ и $\leftrightarrow$. Имеем

$\mathcal{A}(A_1 \vee \dots \vee A_n)=\mathbf{I}$ тогда и только тогда, когда $\mathcal{A}(A_i)=\mathbf{I}$ по крайней мере для одного i ,

и

$\mathcal{A}(A_1 \& \dots \& A_n)=\mathbf{I}$ тогда и только тогда, когда $\mathcal{A}(A_i)=\mathbf{I}$ для всех i .

Также

$\mathcal{A}(\forall xA)=\mathbf{I}$ тогда и только тогда, когда $\mathcal{A}(A_x[i])=\mathbf{I}$ для каждого i из $L(\mathcal{A})$.

Если A — формула языка L , то $\mathcal{A}$ -частным случаем формулы A назовем любую замкнутую формулу вида $A[i_1, \dots, i_n]$ языка $L(\mathcal{A})$. Формула A языка L называется *истинной* в $\mathcal{A}$, если $\mathcal{A}(A)=\mathbf{I}$ для каждого

$\mathcal{A}$ -частного случая A' формулы A . В частности, замкнутая формула A языка L истинна в $\mathcal{A}$ тогда и только тогда, когда $\mathcal{A}(A)=\mathbf{I}$.

Докажем лемму, показывающую, что $b_x[a]$ и $A_x[a]$ имеют должные значения.

Лемма. Пусть $\mathcal{A}$ — структура для L , a — терм языка $L(\mathcal{A})$, свободный от переменных, i — имя для $\mathcal{A}(a)$. Если b — терм языка $L(\mathcal{A})$, в котором нет переменных, за исключением x , то $\mathcal{A}(b_x[a])=\mathcal{A}(b_x[i])$. Если A — формула языка $L(\mathcal{A})$, в которой нет свободных переменных, за исключением x , то $\mathcal{A}(A_x[a])=\mathcal{A}(A_x[i])$.

Доказательство. Первое утверждение докажем индукцией по длине b . Если b — имя, то $b_x[a]$ и $b_x[i]$ оба представляют собой b ; таким образом, утверждение очевидно. Если b — переменная, то она должна быть x ; тогда $b_x[a]$ есть a и $b_x[i]$ есть i . Но $\mathcal{A}(a)=\mathcal{A}(i)$ по выбору i . Если b есть $fb_1 \dots b_n$, где f — функциональный символ из L , то, используя индуктивные предположения, получаем

$$\begin{aligned} \mathcal{A}(b[a]) &= \mathcal{A}(fb_1[a] \dots b_n[a]) \\ &= f_A(\mathcal{A}(b_1[a]), \dots, \mathcal{A}(b_n[a])) \\ &= f_A(\mathcal{A}(b_1[i]), \dots, \mathcal{A}(b_n[i])) \\ &= \mathcal{A}(fb_1[i] \dots b_n[i]) \\ &= \mathcal{A}(b[i]). \end{aligned}$$

Докажем второе утверждение индукцией по длине A . Если A есть $b=c$, то, применяя первое утверждение, получаем

$$\begin{aligned} \mathcal{A}(A[a]) &= \mathbf{I} \leftrightarrow \mathcal{A}(b[a]) = \mathcal{A}(c[a]) \\ &\leftrightarrow \mathcal{A}(b[i]) = \mathcal{A}(c[i]) \\ &\leftrightarrow \mathcal{A}(A[i]) = \mathbf{I}. \end{aligned}$$

Если A есть $pb_1 \dots b_n$, где p отлично от $=$, то доказательство подобно предыдущему. Если A есть $\neg B$, то

$$\begin{aligned} \mathcal{A}(A[a]) &= H_{\neg}(\mathcal{A}(B[a])) \\ &= H_{\neg}(\mathcal{A}(B[i])) \\ &= \mathcal{A}(A[i]). \end{aligned}$$

Если A есть $B \vee C$, то доказательство аналогично. Пусть A есть $\exists yB$. Мы можем предполагать, что y отлично от x ,

так как в противном случае $A_x[a]$ и $A_x[i]$ равны A . Тогда

$$\begin{aligned} \mathcal{A}(A_x[a]) = \mathbf{И} &\leftrightarrow \mathcal{A}(\exists y B_x[a]) = \mathbf{И} \\ &\leftrightarrow \mathcal{A}(B_{x,y}[a, j]) = \mathbf{И} \text{ для некоторого } j \\ &\leftrightarrow \mathcal{A}(B_{x,y}[i, j]) = \mathbf{И} \text{ для некоторого } j \\ &\leftrightarrow \mathcal{A}(\exists y B_x[i]) = \mathbf{И} \\ &\leftrightarrow \mathcal{A}(A_x[i]) = \mathbf{И}. \end{aligned}$$

2.6. Логические аксиомы и правила

Если мы формулируем классическую аксиоматическую систему в языке первого порядка L , то мы имеем в виду конкретное значение языка L , т. е. конкретную структуру $\mathcal{A}$ для L . Мы хотим, чтобы все теоремы нашей формальной системы были истинны в $\mathcal{A}$. Чтобы гарантировать это, мы требуем, чтобы все аксиомы были истинны и все правила были таковы, что истинность заключения следует из истинности посылок, или, как мы будем говорить, заключение есть *следствие* посылок.

Некоторые формулы языка L истинны просто по смыслу логических символов; они истинны в каждой структуре для L . Например, $x=x$ имеет такое свойство. Про такие формулы говорят, что они являются *логически истинными*. Некоторые из наших аксиом, называемые *логическими аксиомами*, будут логически истинными. Другие аксиомы, называемые *нелогическими аксиомами*, будут истинными из-за конкретных свойств структуры $\mathcal{A}$.

Мы говорим, что A есть *логическое следствие* множества формул Γ , если она есть следствие Γ по смыслу значений логических символов, т. е. если A истинна в каждой структуре для L , в которой истинны все формулы из Γ . Можно ожидать, что правила также разделяются на два класса: *логические правила*, у которых заключение является логическим следствием посылок, и *нелогические правила*, у которых заключение является следствием посылок только благодаря специфическим свойствам структуры $\mathcal{A}$. Однако мы можем совсем обойтись без нелогических правил. Так, предположим, что мы хотим иметь возможность вывести B из $A_1, \dots, A_n$. Тогда B будет следствием $A_1, \dots, A_n$; следовательно, $A_1 \rightarrow \dots \rightarrow A_n \rightarrow B$ является истинной и ее можно при-

нять в качестве нелогической аксиомы. Но B является логическим следствием формул $A_1, \dots, A_n$ и $A_1 \rightarrow \dots \rightarrow A_n \rightarrow B$; таким образом, если мы имеем достаточно много логических правил, то мы можем вывести B из $A_1, \dots, A_n$ и аксиомы $A_1 \rightarrow \dots \rightarrow A_n \rightarrow B$.

Теперь опишем логические аксиомы и правила. Пусть L — язык первого порядка. *Пропозициональная аксиома* есть формула вида $\neg A \vee A$. *Аксиома подстановки* есть формула вида $A_x[a] \rightarrow \exists x A$. *Аксиома тождества* есть формула вида $x = x$. *Аксиома равенства* есть формула вида

$$x_1 = y_1 \rightarrow \dots \rightarrow x_n = y_n \rightarrow f x_1 \dots x_n = f y_1 \dots y_n$$

или вида

$$x_1 = y_1 \rightarrow \dots \rightarrow x_n = y_n \rightarrow p x_1 \dots x_n \rightarrow p y_1 \dots y_n.$$

Логическая аксиома есть формула, являющаяся пропозициональной аксиомой, аксиомой подстановки, аксиомой тождества или аксиомой равенства.

Покажем теперь, что логические аксиомы являются истинными. Пусть $\mathcal{A}$ — структура для L . $\mathcal{A}$ -частный случай пропозициональной аксиомы имеет вид $\neg A \vee A$; имеем

$$\mathcal{A}(\neg A \vee A) = H_V(H_{\neg}(\mathcal{A}(A)), \mathcal{A}(A)) = \mathbf{И}.$$

$\mathcal{A}$ -частный случай аксиомы подстановки имеет вид $A_x[a] \rightarrow \exists x A$. Пусть $\mathcal{A}(A_x[a] \rightarrow \exists x A) = \mathbf{Л}$. Тогда $\mathcal{A}(A_x[a]) = \mathbf{И}$ и $\mathcal{A}(\exists x A) = \mathbf{Л}$. Если i есть имя $\mathcal{A}(a)$, то из последнего равенства следует, что $\mathcal{A}(A_x[i]) = \mathbf{Л}$, хотя из первого равенства и леммы из § 2.5 следует, что $\mathcal{A}(A_x[i]) = \mathbf{И}$. Получаем противоречие. $\mathcal{A}$ -частный случай аксиомы тождества имеет вид $i = i$; следовательно, $\mathcal{A}(i) = \mathcal{A}(i)$, $\mathcal{A}(i = i) = \mathbf{И}$. Доказательство для аксиом равенства оставляем читателю.

Введем теперь пять правил вывода. (Заметим, что эти правила конечны.)

Правило расширения. $B \vee A$ следует из A .

Правило сокращения. A следует из $A \vee A$.

Правило ассоциативности. $(A \vee B) \vee C$ следует из $A \vee (B \vee C)$.

Правило сечения. $B \vee C$ следует из $A \vee B$ и $\neg A \vee C$.

Правило $\exists$ -введения. Если x не является свободной в B , то $\exists x A \rightarrow B$ следует из $A \rightarrow B$.

Мы хотим сейчас показать, что заключение каждого правила есть логическое следствие посылок этого правила. Проверим это только для последних двух правил, оставляя читателю доказательство для первых трех.

Предположим, что $A \vee B$ и $\neg A \vee C$ являются истинными в $\mathcal{A}$. Пусть $B' \vee C'$ является $\mathcal{A}$ -частным случаем формулы $B \vee C$. Очевидно, мы можем выбрать $\mathcal{A}$ -частный случай A' формулы A так, что $A' \vee B'$ есть $\mathcal{A}$ -частный случай формулы $A \vee B$, а $\neg A' \vee C'$ есть $\mathcal{A}$ -частный случай формулы $\neg A \vee C$. Тогда

$$\mathcal{A}(A' \vee B') = \mathcal{A}(\neg A' \vee C') = \mathbf{И}.$$

Следовательно, $\mathcal{A}(A') = \mathbf{И}$ или $\mathcal{A}(B') = \mathbf{И}$, а $\mathcal{A}(A') = \mathbf{Л}$ или $\mathcal{A}(C') = \mathbf{И}$. Отсюда следует, что или $\mathcal{A}(B') = \mathbf{И}$ или $\mathcal{A}(C') = \mathbf{И}$ (в соответствии с тем, будет ли $\mathcal{A}(A') = \mathbf{Л}$ или $\mathcal{A}(A') = \mathbf{И}$). Следовательно, $\mathcal{A}(B' \vee C') = \mathbf{И}$.

Предположим, что $A \rightarrow B$ истинна в $\mathcal{A}$, а переменная x не является свободной в B . $\mathcal{A}$ -частный случай формулы $\exists x A \rightarrow B$ имеет вид $\exists x A' \rightarrow B'$. Предположим, что $\mathcal{A}(\exists x A' \rightarrow B') = \mathbf{Л}$. Тогда $\mathcal{A}(\exists x A') = \mathbf{И}$ и $\mathcal{A}(B') = \mathbf{Л}$. Из первого следует, что $\mathcal{A}(A'_x[i]) = \mathbf{И}$ для некоторого i ; следовательно, $\mathcal{A}(A'_x[i] \rightarrow B') = \mathbf{Л}$. Это невозможно, так как $A'_x[i] \rightarrow B'$ является $\mathcal{A}$ -частным случаем формулы $A \rightarrow B$.

Теперь можно определить класс формальных систем, которые мы собираемся изучать. *Теорией первого порядка* или просто *теорией* называется формальная система T такая, что

(i) языком формальной системы T является язык первого порядка;

(ii) аксиомами формальной системы T являются логические аксиомы языка $L(T)$ и некоторые другие аксиомы, называемые *нелогическими аксиомами*;

(iii) правилами формальной системы T являются правило расширения, правило сокращения, правило ассоциативности, правило сечения и правило $\exists$ -введения.

Для того чтобы задать теорию, мы должны задать лишь ее нелогические символы и ее нелогические аксиомы; все остальное дано по определению теории. Заметим также, что логические аксиомы и правила определены, как только язык выбран; они не зависят от нелогических аксиом.

Приведем два примера теорий. Первая теория, которую мы обозначим через N , формализует классическую систему аксиом для натуральных чисел. Нелогическими символами для N будут константа 0, унарный функциональный символ S (который обозначает функцию следования), бинарные функциональные символы $+$ и $\cdot$, бинарный предикатный символ $<$. Нелогическими аксиомами N являются:

- | | |
|-----------------------------------|---|
| N1. $Sx \neq 0$. | N6. $x \cdot Sy = (x \cdot y) + x$. |
| N2. $Sx = Sy \rightarrow x = y$. | N7. $\neg(x < 0)$. |
| N3. $x + 0 = x$. | N8. $x < Sy \leftrightarrow x < y \vee x = y$. |
| N4. $x + Sy = S(x + y)$. | N9. $x < y \vee x = y \vee y < x$. |
| N5. $x \cdot 0 = 0$. | |

Наш второй пример теории формализует современную аксиоматическую систему для групп. Она называется *элементарной теорией групп* и обозначается через G . Единственным нелогическим символом теории G является бинарный функциональный символ $\cdot$. Нелогические аксиомы теории G следующие:

- G1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
 G2. $\exists x (\forall y (x \cdot y = y) \& \forall y \exists z (z \cdot y = x))$.

Под *моделью* теории T мы понимаем структуру для $L(T)$, в которой все нелогические аксиомы являются истинными. Формула является *истинной* в T , если она является истинной в каждой модели теории T или, что эквивалентно, если она является логическим следствием нелогических аксиом теории T .

Примеры.

1. Мы построим модель для N , взяв в качестве универсума множество натуральных чисел и обычные значения индивидов, функций и предикатов в качестве нелогических символов N . Эта модель называется *стандартной моделью* для N и обозначается через $\mathcal{N}$.

2. Структура для $L(G)$ может быть описана как непустое множество (универсум) вместе с бинарной операцией (функцией, соответствующей символу $\cdot$). Такая структура будет моделью теории G тогда и только тогда, когда она есть группа.

Теорема истинности. Если T — теория, то каждая теорема теории T является истинной в T .

Доказательство. Применяем индукцию по теоремам. Если A — нелогическая аксиома, то утверждение верно по определению модели. Если A — логическая аксиома, то утверждение мы уже доказали выше. Если A — заключение правила, то утверждение следует из индуктивных предположений и фактов, доказанных ранее.

Если, формулируя нелогические аксиомы, мы имеем в виду определенную структуру или несколько структур, мы обязательно выберем эти аксиомы так, чтобы они были истинными в этих структурах. Тогда эти структуры являются моделями для теории, и в силу теоремы истинности все теоремы рассматриваемой теории будут истинными в этих структурах. Таким образом, мы видим, что наши логические аксиомы и правила являются корректными.

Теперь возникает вопрос: можем ли мы получить больше выгоды, если добавим другие логические аксиомы или правила? Один из путей установить, что это не так, состоит в доказательстве обращения теоремы истинности: каждая формула, истинная в T , является теоремой теории T . Тогда, если новая логическая аксиома или правило дают новую теорему, то эта теорема не должна быть логическим следствием нелогических аксиом, и следовательно, новая аксиома или правило должны быть некорректными. Мы установим это обращение теоремы истинности позднее; сначала нам придется исследовать некоторые следствия логических аксиом и правил.

Задачи

1. n -арная функция истинности H называется *определимой в терминах функций истинности* $H_1, \dots, H_k$, если H имеет определение

$$H(a_1, \dots, a_n) = \dots,$$

где правая часть построена из $H_1, \dots, H_k, a_1, \dots, a_n$, а также запятых и скобок.

(а) Пусть $H_{d,n}$ — функция истинности, определенная так: $H_{d,n}(a_1, \dots, a_n) = \mathbf{I}$ тогда и только тогда, когда $a_i = \mathbf{I}$ по крайней мере для одного i ;

пусть функция истинности $H_{c,n}$ определена так: $H_{c,n}(a_1, \dots, a_n) = \mathbf{I}$ тогда и только тогда, когда $a_i = \mathbf{I}$ для всех i . Показать, что каждая функция истинности определима в терминах $H_{\neg}$ и некоторых из $H_{d,n}$ и $H_{c,n}$.

(б) Показать, что каждая функция истинности определима в терминах $H_{\neg}$ и $H_{\vee}$. [Использовать (а).]

(в) Показать, что каждая функция истинности определима в терминах $H_{\neg}$ и $H_{\wedge}$. [Использовать (б).]

(г) Показать, что каждая функция истинности определима в терминах $H_{\neg}$ и $H_{\&}$. [Использовать (б).]

(д) Показать, что $H_{\neg}$ не определима в терминах $H_{\vee}$, $H_{\rightarrow}$, $H_{\&}$ и $H_{\leftrightarrow}$.

2. (а) Пусть H_d — функция истинности, определенная так:

$$H_d(a, b) = \mathbf{I} \text{ тогда и только тогда, когда } a = b = \mathbf{I}.$$

Показать, что каждая функция истинности определима в терминах H_d . [Использовать 1 (б).]

(б) Пусть H_s — функция истинности, определенная так:

$$H_s(a, b) = \mathbf{I} \text{ тогда и только тогда, когда } a = b = \mathbf{I}.$$

Показать, что каждая функция истинности определима в терминах H_s . [Использовать 1 (б).]

(в) Функция истинности H называется *сингулярной*, если существуют функция истинности H' и некоторое i такие, что $H(a_1, \dots, a_n) = H'(a_i)$ для всех $a_1, \dots, a_n$. Показать, что если H сингулярна, то каждая функция истинности, определяемая в терминах H , является сингулярной.

(г) Показать, что если H — бинарная функция истинности такая, что каждая функция истинности определима в терминах H , то H есть H_d или H_s . [Показать, что $H(\mathbf{I}, \mathbf{I}) = \mathbf{I}$ и $H(\mathbf{J}, \mathbf{J}) = \mathbf{I}$, и использовать (в).]

3. Показать, что если uv и vv' — указатели, то либо v , либо v' является пустым выражением.

4. Показать, что результат замены a на x в терме есть терм, и что результат замены a на x в формуле есть формула.

5. Пусть T — теория, у которой нет нелогических символов и нелогических аксиом.

(а) Показать, что $\neg \neg(x=x) \vee \neg(x=x)$ является теоремой теории T , не доказуемой без пропозициональных аксиом. [Пусть f — отображение из множества формул в множество истинностных значений такое, что $f(A) = \mathbf{I}$, если A атомная; $f(\neg A) = \mathbf{J}$; $f(A \vee B) = f(A) \vee f(B)$; $f(\exists x A) = \mathbf{I}$. Показать, что если A доказуема без пропозициональных аксиом, то $f(A) = \mathbf{I}$.]

(б) Показать, что $x=x \rightarrow \exists x(x=x)$ является теоремой теории T , не доказуемой без аксиомы подстановки. [Поступать, как и в (а), положив $f(A) = \mathbf{I}$ для атомных A ; $f(\neg A) = H_{\neg}(f(A))$; $f(A \vee B) = H_{\vee}(f(A), f(B))$; $f(\exists x A) = \mathbf{J}$.]

(в) Показать, что $x=x$ есть теорема теории T , не доказуемая без аксиомы тождества. [Пусть $f(A) = \mathbf{J}$ для атомных A ; $f(\neg A) = H_{\neg}(f(A))$; $f(A \vee B) = H_{\vee}(f(A), f(B))$; $f(\exists x A) = f(A)$. Для проверки аксиомы подстановки доказать, что $f(A_x[a]) = f(A)$.]

(г) Показать, что $x=y \rightarrow x=z \rightarrow x=x \rightarrow y=z$ есть теорема теории T , не доказуемая без аксиомы равенства. [Образум L' из $L(T)$ добавлением констант e_1, e_2, e_3 . Для замкнутой формулы A языка L'

определим $f(A)$ так:

$$\begin{aligned} f(e_i = e_j) &= \mathbf{И} \leftrightarrow i \leq j; \\ f(\neg A) &= H_{\neg}(f(A)); \\ f(A \vee B) &= H_{\vee}(f(A), f(B)); \\ f(\exists x A) &= \mathbf{И} \leftrightarrow f(A_x[e_i]) = \mathbf{И} \text{ для некоторого } i. \end{aligned}$$

Показать, что если A доказывается в T без аксиом равенства, то $f(A) = \mathbf{И}$ для каждой формулы A' , полученной из A заменой каждой переменной на некоторое e_i во всех свободных вхождениях этих переменных.]

(д) Показать, что $x = x \vee (x \neq x \vee x = x)$ есть теорема теории T , не доказуемая без правила расширения. [Пусть $f(A) = \mathbf{И}$ для атомных A ;

$$\begin{aligned} f(\neg A) &= H_{\neg}(f(A)); \\ f(A \vee B) &= H_{\vee}(f(A), H_{\neg}(f(B))); \\ f(\exists x A) &= f(A). \end{aligned}$$

(е) Показать, что $\neg \neg(x = x)$ есть теорема теории T , не доказуемая без правила сокращения. [Пусть $f(A) = \mathbf{И}$ для атомных A ; $f(\neg A) = f(\exists x A) = \mathbf{Л}$; $f(A \vee B) = \mathbf{И}$. Чтобы доказать $\neg \neg(x = x)$ в T , получить $x = x \vee \neg \neg(x = x)$ как заключение правила сечения и затем использовать правило сечения для доказательства $\neg \neg(x = x) \vee \neg \neg \neg(x = x)$.]

(ж) Показать, что $\neg(x \neq x \vee x \neq x)$ есть теорема теории T , не доказуемая без правила ассоциативности. [Пусть f — отображение из множества формул в множество целых чисел такое, что

$$\begin{aligned} f(A) &= 0 \text{ для атомных } A; \\ f(\neg A) &= 1 - f(A); \\ f(A \vee B) &= f(A) \cdot f(B) \cdot (1 - f(A) - f(B)); \\ f(\exists x A) &= f(A). \end{aligned}$$

Показать, что если A выводима без правила ассоциативности, то $f(A) = 0$.]

(з) Показать, что $\neg \neg(x = x)$ есть теорема теории T , не доказуемая без правила сечения. [Пусть $f(A) = \mathbf{И}$ для атомных A ; $f(\neg A) = \mathbf{И}$, если $f(A) = \mathbf{Л}$ или A атомная, $f(\neg A) = \mathbf{Л}$ в противном случае; $f(A \vee B) = H_{\vee}(f(A), f(B))$; $f(\exists x A) = f(A)$.]

(и) Показать, что $\exists x(x \neq x) \rightarrow x \neq x$ есть теорема теории T , не доказуемая без правила $\exists$ -введения. [Пусть $f(A) = \mathbf{И}$ для атомных A ; $f(\neg A) = H_{\neg}(f(A))$; $f(A \vee B) = H_{\vee}(f(A), f(B))$; $f(\exists x B) = \mathbf{И}$.]

ТЕОРЕМЫ В ТЕОРИЯХ ПЕРВОГО ПОРЯДКА

3.1. Теорема тавтологии

На протяжении всей этой главы будем предполагать, что теория T фиксирована, и будем исследовать те теоремы, которые могут быть доказаны в T .

В следующей главе мы покажем, что если B есть логическое следствие $A_1, \dots, A_n$ и $A_1, \dots, A_n$ — теоремы, то B — теорема. В этом параграфе мы докажем некоторый частный случай этого результата. Грубо говоря, это такой случай, в котором то, что B есть следствие $A_1, \dots, A_n$, выясняется с использованием лишь правил для вычисления истинностных значений $\neg C$ и $C \vee D$ по истинностным значениям C и D .

Формула называется *элементарной*, если она атомная формула или подтверждение. *Истинностной оценкой* теории T называется некоторое отображение из множества всех элементарных формул теории T в множество истинностных значений.

Пусть V — истинностная оценка теории T . Будем определять истинностное значение $V(A)$ для каждой формулы A теории T индукцией по длине A . Если A — элементарная формула, то $V(A)$ уже определено. Если A есть $\neg B$, то $V(A) = H_{\neg}(V(B))$. Если A есть $B \vee C$, то $V(A) = H_{\vee}(V(B), V(C))$. Из этого определения и определений $\rightarrow$, $\&$ и $\leftrightarrow$ мы видим, что $V(B \rightarrow C) = H_{\rightarrow}(V(B), V(C))$ и аналогично для $\&$ и $\leftrightarrow$. Кроме того, имеем $V(A_1 \vee \dots \vee A_n) = \mathbf{И}$ тогда и только тогда, когда $V(A_i) = \mathbf{И}$ по крайней мере для одного i ,

и

$V(A_1 \& \dots \& A_n) = \mathbf{И}$ тогда и только тогда, когда $V(A_i) = \mathbf{И}$ для всех i .

Скажем, что B — *тавтологическое следствие* $A_1, \dots, A_n$, если $V(B) = \mathbf{И}$ для каждой истинностной оценки V такой, что $V(A_1) = \dots = V(A_n) = \mathbf{И}$. Формула A называется *тавтологией*, если она есть тавтологическое следствие пустой

последовательности формул, т. е. если $V(A) = И$ для каждой истинностной оценки V . Легко видеть, что B — тавтологическое следствие $A_1, \dots, A_n$ тогда и только тогда, когда $A_1 \rightarrow \dots \rightarrow A_n \rightarrow B$ — тавтология.

Покажем теперь, что для данных $A_1, \dots, A_n, B$ можно в конечное число шагов определить, будет B тавтологическим следствием $A_1, \dots, A_n$ или нет. В связи с последним утверждением предыдущего абзаца достаточно показать, что для данной формулы A мы можем определить, будет A тавтологией или нет. Используя индукцию по сумме длин A_i , покажем, как определить, будет ли $A_1 \vee \dots \vee A_n$ тавтологией; при $n=1$ получается выше-названный результат.

Вначале предположим, что каждое A_i — элементарная формула или отрицание элементарной формулы. Мы утверждаем, что $A_1 \vee \dots \vee A_n$ — тавтология тогда и только тогда, когда некоторое A_j есть отрицание некоторого A_i . Если это условие выполняется, то для каждой истинностной оценки V или $V(A_i) = И$, или $V(A_j) = И$; таким образом, $V(A_1 \vee \dots \vee A_n) = И$. Предположим, что данное условие не выполняется. Определим истинностную оценку V , положив $V(A) = И$ тогда и только тогда, когда $\neg A$ есть некоторое A_i . Легко видеть, что $V(A_i) = Л$ для всех i ; таким образом, $V(A_1 \vee \dots \vee A_n) = Л$.

Предположим, что некоторое A_i не является элементарной формулой и не является отрицанием элементарной формулы. Поскольку

$$V(A_1 \vee \dots \vee A_n) = V(A_i \vee \dots \vee A_n \vee A_1 \vee \dots \vee A_{i-1})$$

для всех истинностных оценок V , то $A_1 \vee \dots \vee A_n$ — тавтология тогда и только тогда, когда

$$A_i \vee \dots \vee A_n \vee A_1 \vee \dots \vee A_{i-1}$$

является тавтологией. Следовательно, мы могли бы сразу предположить, что A_1 не является ни элементарной формулой, ни отрицанием элементарной формулы. Тогда A_1 есть или дизъюнкция или отрицание; а в последнем случае A_1 есть отрицание отрицания или отрицание дизъюнкции. Предположим, что A_1 есть $B \vee C$. Поскольку

$$V(A_1 \vee \dots \vee A_n) = V(B \vee C \vee A_2 \vee \dots \vee A_n)$$

для каждой истинностной оценки V , то $A_1 \vee \dots \vee A_n$ — тавтология тогда и только тогда, когда

$$B \vee C \vee A_2 \vee \dots \vee A_n$$

является тавтологией. Итак, достаточно определить, будет ли $B \vee C \vee A_2 \vee \dots \vee A_n$ тавтологией; а это может быть сделано по индуктивному предположению.

Предположим, что A_1 есть $\neg \neg B$. Тогда для каждой истинностной оценки V имеем $V(A_1) = V(B)$ и, следовательно, $V(A_1 \vee \dots \vee A_n) = V(B \vee A_2 \vee \dots \vee A_n)$. Отсюда следует, что достаточно определить, будет ли $B \vee A_2 \vee \dots \vee A_n$ тавтологией; а это может быть сделано по индуктивному предположению.

Предположим, что A_1 есть $\neg(B \vee C)$. Тогда для каждой истинностной оценки V имеем

$$V(A_1) = И \text{ тогда и только тогда, когда}$$

$$V(\neg B) = V(\neg C) = И;$$

таким образом,

$$V(A_1 \vee \dots \vee A_n) = И$$

тогда и только тогда, когда

$$V(\neg B \vee A_2 \vee \dots \vee A_n) = V(\neg C \vee A_2 \vee \dots \vee A_n) = И.$$

Поэтому достаточно определить, будут ли

$$\neg B \vee A_2 \vee \dots \vee A_n \text{ и } \neg C \vee A_2 \vee \dots \vee A_n$$

тавтологиями; а это может быть сделано по индуктивному предположению.

Обратимся к основному результату этого параграфа.

Теорема тавтологии (Пост). Если B — тавтологическое следствие $A_1, \dots, A_n$ и $\vdash A_1, \dots, \vdash A_n$, то $\vdash B$.

Следствие. Каждая тавтология является теоремой.

Наш первый шаг — свести теорему к следствию.

Лемма 1. Если $\vdash A \vee B$, то $\vdash B \vee A$.

Доказательство. Поскольку $\neg A \vee A$ — пропозициональная аксиома, то $\vdash \neg A \vee B$ и $\vdash \neg A \vee A$. Следовательно, $\vdash B \vee A$ по правилу сечения.

Правило отделения. Если $\vdash A$ и $\vdash A \rightarrow B$, то $\vdash B$.

Доказательство. Из $\vdash A$ мы получаем $\vdash B \vee A$ по правилу расширения и, значит, $\vdash A \vee B$ по лемме 1. Из $\vdash A \vee B$ и $\vdash A \rightarrow B$ мы получаем $\vdash B \vee B$ по

правилу сечения (и определению $\rightarrow$); следовательно, $\vdash B$ по правилу сокращения.

Следствие. Если $\vdash A_1, \dots, \vdash A_n$ и $\vdash A_1 \rightarrow \dots \rightarrow A_n \rightarrow B$, то $\vdash B$.

Доказательство. Индукцией по n .

Ясно, что теорема тавтологии следует из следствия к теореме тавтологии и следствия к правилу отделения. Таким образом, осталось лишь доказать, что каждая тавтология есть теорема. $V(A \vee A) = V(A)$ для каждой истинностной оценки V ; таким образом, если A — тавтология, то $A \vee A$ — тавтология. С другой стороны, из $\vdash A \vee A$ следует $\vdash A$ по правилу сокращения. Следовательно, нам нужно только показать, что если $A \vee A$ — тавтология, то $A \vee A$ — теорема. Это есть частный случай следующего результата.

Лемма 2. Если $n \geq 2$ и $A_1 \vee \dots \vee A_n$ есть тавтология, то $\vdash A_1 \vee \dots \vee A_n$.

Наше доказательство леммы 2 ведется индукцией по сумме длин A_i и параллельно методом, описанным выше. В процессе доказательства мы будем отмечать результаты, в которых мы нуждаемся, и позднее их докажем.

Сначала предположим, что каждая A_i является элементарной формулой или отрицанием элементарной формулы. С помощью метода, описанного выше, получаем, что некоторое A_j является отрицанием некоторого A_i . Тогда $\vdash A_j \vee A_i$ по пропозициональной аксиоме. Тогда получаем $\vdash A_1 \vee \dots \vee A_n$ по

(А) Если $n \geq 1$, $m \geq 1$, числа $i_1, \dots, i_m$ находятся среди чисел $1, \dots, n$ и

$$\vdash A_{i_1} \vee \dots \vee A_{i_m},$$

то

$$\vdash A_1 \vee \dots \vee A_n.$$

Теперь предположим, что некоторое A_i не является элементарной формулой и не является отрицанием элементарной формулы. По (А) $\vdash A_1 \vee \dots \vee A_n$ тогда и только тогда, когда $\vdash A_i \vee \dots \vee A_n \vee A_1 \vee \dots \vee A_{i-1}$. Поэтому так же, как и раньше, можно предполагать, что A_1 не является элементарной формулой и не является отрицанием элементарной формулы. Как и раньше, это разбивается на три случая.

Предположим, что A_1 есть $B \vee C$. Тогда $B \vee C \vee \dots \vee A_2 \vee \dots \vee A_n$ — тавтология и, следовательно, по индуктивному предположению — теорема. Поэтому $\vdash A_1 \vee \dots \vee A_n$ по правилу ассоциативности.

Предположим, что A_1 есть $\neg \neg B$. Тогда $B \vee A_2 \vee \dots \vee A_n$ — тавтология и, следовательно, по индуктивному предположению — теорема. Тогда мы получаем $\vdash A_1 \vee \dots \vee A_n$ по

(Б) Если $\vdash A \vee B$, то $\vdash \neg \neg A \vee B$.

Наконец, предположим, что A_1 есть $\neg(B \vee C)$. Тогда

$$\neg B \vee A_2 \vee \dots \vee A_n \quad \text{и} \quad \neg C \vee A_2 \vee \dots \vee A_n$$

— тавтологии и, следовательно, по индуктивному предположению — теоремы. Тогда получаем $\vdash A_1 \vee \dots \vee A_n$ по

(В) Если $\vdash \neg A \vee C$ и $\vdash \neg B \vee C$, то $\vdash \neg(A \vee B) \vee C$.

Теперь докажем (А) индукцией по m . Вначале предположим, что $m \geq 3$. Пусть A есть $A_1 \vee \dots \vee A_n$. Из посылок (А) и ассоциативного закона имеем

$$\vdash (A_{i_1} \vee A_{i_2}) \vee A_{i_3} \vee \dots \vee A_{i_m}.$$

Следовательно, $\vdash (A_{i_1} \vee A_{i_2}) \vee A$ по индуктивному предположению. Применяя лемму 1 и ассоциативный закон, получаем $\vdash (A \vee A_{i_1}) \vee A_{i_2}$; таким образом, $\vdash (A \vee A_{i_1}) \vee A$ по индуктивному предположению. Снова применяя лемму 1 и ассоциативный закон, получаем $\vdash (A \vee A) \vee A_{i_1}$; таким образом, по индуктивному предположению имеем $\vdash (A \vee A) \vee (A \vee A)$. Теперь два применения правила сокращения дают $\vdash A$.

Теперь предположим, что $m = 1$, и пишем i вместо i_1 . По правилу расширения получаем

$$\vdash (A_{i+1} \vee \dots \vee A_n) \vee A_i$$

таким образом, по лемме 1 имеем $\vdash A_i \vee \dots \vee A_n$. Применяя $i - 1$ раз правило расширения, получаем $\vdash A_1 \vee \dots \vee A_n$.

Остается случай, когда $m = 2$. Если $i_1 = i_2$, то $\vdash A_{i_1} \vee A_{i_2}$ дает $\vdash A_{i_1}$ по правилу сокращения, и мы возвращаемся к случаю, когда $m = 1$. Случай $i_1 > i_2$ сводится к случаю $i_1 < i_2$ по лемме 1. Итак, остается доказать

(А') Если $1 \leq i < j \leq n$ и $\vdash A_i \vee A_j$, то $\vdash A_1 \vee \dots \vee A_n$.

Докажем (А') индукцией по n . Если $n = 2$, то доказывать нечего; поэтому предположим, что $n \geq 3$. Положим

B вместо $A_3 \vee \dots \vee A_n$, тогда доказываемый результат будет $\vdash A_1 \vee A_2 \vee B$.

Если $i \geq 2$, то $\vdash A_2 \vee B$ по индуктивному предположению; таким образом, $\vdash A_1 \vee A_2 \vee B$ по правилу расширения.

Если $i=1$ и $j \geq 3$, то $\vdash A_1 \vee B$ по индуктивному предположению. По лемме 1 и правилу расширения получаем $\vdash A_2 \vee B \vee A_1$. По правилу ассоциативности и лемме 1 получаем $\vdash A_1 \vee A_2 \vee B$. Если $i=1$ и $j=2$, то $\vdash A_1 \vee A_2$ по предположению. Следовательно, $\vdash B \vee A_1 \vee A_2$ по правилу расширения. Применяя правило ассоциативности и лемму 1, имеем $\vdash A_2 \vee B \vee A_1$. Применение правила ассоциативности и леммы 1 снова дает $\vdash A_1 \vee A_2 \vee B$.

Теперь докажем (Б). Так как $\neg\neg A \vee \neg A$ — пропозициональная аксиома, то $\vdash \neg A \vee \neg\neg A$ получаем по лемме 1. Из $\vdash A \vee B$ и $\vdash \neg A \vee \neg\neg A$ по правилу сечения получаем $\vdash B \vee \neg\neg A$. Следовательно, $\vdash \neg\neg A \vee B$ по лемме 1.

Теперь докажем (В). Так как $\neg(A \vee B) \vee A \vee B$ — пропозициональная аксиома, то $\vdash A \vee B \vee \neg(A \vee B)$ получаем по (А). Отсюда и из $\vdash \neg A \vee C$ по правилу сечения получаем $\vdash (B \vee \neg(A \vee B)) \vee C$. Отсюда по лемме 1 получаем $\vdash C \vee B \vee \neg(A \vee B)$; таким образом, $\vdash B \vee C \vee \neg(A \vee B)$ по (А). Отсюда и из $\vdash \neg B \vee C$ по правилу сечения получаем $\vdash (C \vee \neg(A \vee B)) \vee C$. Применение леммы 1 дает $\vdash C \vee C \vee \neg(A \vee B)$; таким образом, $\vdash \neg(A \vee B) \vee C$ по (А). Это завершает доказательство теоремы тавтологии.

Когда мы будем утверждать, что некоторая формула есть тавтологическое следствие других формул или что некоторая формула есть тавтология, мы обычно будем оставлять доказательство этого читателю. Как правило, он быстрее будет находить не прямое доказательство. Так, чтобы показать, что $A \& B \rightarrow A$ — тавтология, предположим, что существует истинностная оценка V такая, что $V(A \& B \rightarrow A) = \text{Л}$. Тогда $V(A \& B) = \text{И}$ и $V(A) = \text{Л}$. Из первого имеем $V(A) = V(B) = \text{И}$. Поскольку имеется два разных значения для $V(A)$, то мы получаем противоречие. С накоплением опыта читатель будет все больше убеждаться в том, что как только он может увидеть, что B истинна (или является следствием $A_1, \dots, A_n$) лишь

по смыслу $\neg, \vee, \rightarrow, \&$ и $\leftrightarrow$, то B является тавтологией (или тавтологическим следствием $A_1, \dots, A_n$).

Замечание. Предположим, что с каждой формулой A мы связали формулу A^* так, что $(\neg A)^*$ есть $\neg A^*$ и $(A \vee B)^*$ есть $A^* \vee B^*$. Если B — тавтологическое следствие $A_1, \dots, A_n$, то B^* — тавтологическое следствие $A_1^*, \dots, A_n^*$. Чтобы убедиться в этом, предположим, что V — некоторая истинностная оценка. Определим новую истинностную оценку V' так: $V'(A) = V(A^*)$ для элементарных формул A . Тогда легко проверить, что $V'(A) = V(A^*)$ для всех A . Следовательно, если

$$V(A_1^*) = \dots = V(A_n^*) = \text{И},$$

то

$$V'(A_1) = \dots = V'(A_n) = \text{И};$$

таким образом, $V'(B) = \text{И}$; следовательно, $V(B^*) = \text{И}$.

Выпишем часто применяемые случаи теоремы тавтологии (отличные от правила отделения):

(i) Если $\vdash A \leftrightarrow B$, то $\vdash A$ тогда и только тогда, когда $\vdash B$.

(ii) Если $\vdash A \rightarrow B$ и $\vdash B \rightarrow C$, то $\vdash A \rightarrow C$.

(iii) Если $\vdash A \leftrightarrow B$ и $\vdash B \leftrightarrow C$, то $\vdash A \leftrightarrow C$.

(iv) $\vdash A \& B$ тогда и только тогда, когда $\vdash A$ и $\vdash B$.

(v) $\vdash A \leftrightarrow B$ тогда и только тогда, когда $\vdash A \rightarrow B$ и $\vdash B \rightarrow A$.

(vi) $\vdash A \rightarrow B$ тогда и только тогда, когда $\vdash \neg B \rightarrow \neg A$.

Кроме того, теорема тавтологии может заменить применение пропозициональных аксиом и правил расширения, сокращения, ассоциативности и сечения. Другими словами, мы можем определить теоремы теории T с помощью следующего обобщенного индуктивного определения:

(i) каждая аксиома подстановки, аксиома тождества, аксиома равенства и нелогическая аксиома является теоремой;

(ii) если $A_1, \dots, A_n$ ($n \geq 0$) — теоремы и B — тавтологическое следствие $A_1, \dots, A_n$, то B — теорема;

(iii) если A — теорема и B может быть выведена из A с помощью правила $\exists$ -введения, то B — теорема.

Это приводит нас к доказательству индукцией, которое мы также называем *доказательством индукцией по*

теоремам. По этому методу мы доказываем, что каждая теорема имеет свойство P , доказывая, что:

(i) каждая аксиома подстановки, аксиома тождества, аксиома равенства и нелогическая аксиома имеют свойство P ;

(ii) если $A_1, \dots, A_n$ имеют свойство P и B — тавтологическое следствие $A_1, \dots, A_n$, то B имеет свойство P ;

(iii) если A имеет свойство P и B может быть выведена из A с помощью правила $\exists$ -введения, то B имеет свойство P .

3.2. Результаты о кванторах

Теперь выведем некоторые правила для оперирования с кванторами.

Правило $\forall$ -введения. Если $\vdash A \rightarrow B$ и x не является свободной в A , то $\vdash A \rightarrow \forall x B$.

Доказательство. Из $\vdash A \rightarrow B$ с помощью теоремы тавтологии получаем $\vdash \neg B \rightarrow \neg A$. Тогда $\vdash \exists x \neg B \rightarrow \neg A$ по правилу $\exists$ -введения; следовательно, $\vdash A \rightarrow \neg \exists x \neg B$ по теореме тавтологии. По определению $\forall$ это есть $\vdash A \rightarrow \forall x B$.

Правило обобщения. Если $\vdash A$, то $\vdash \forall x A$.

Доказательство. Из $\vdash A$ по теореме тавтологии имеем $\vdash \neg \forall x A \rightarrow A$. Тогда по правилу $\forall$ -введения получаем $\vdash \neg \forall x A \rightarrow \forall x A$; следовательно, $\vdash \forall x A$ по теореме тавтологии.

Скажем, что A' есть частный случай формулы A , если A' имеет вид $A_{x_1, \dots, x_n} [a_1, \dots, a_n]$.

Правило подстановки. Если $\vdash A$ и A' — частный случай формулы A , то $\vdash A'$.

Доказательство. Вначале предположим, что A' есть $A_x [a]$. Из $\vdash A$ по правилу обобщения получаем $\vdash \forall x A$, то есть $\vdash \neg \exists x \neg A$. По аксиоме подстановки получаем $\vdash \neg A_x [a] \rightarrow \exists x \neg A$. Следовательно, $\vdash A_x [a]$ по теореме тавтологии.

Теперь предположим, что A' есть $A_{x_1, \dots, x_n} [a_1, \dots, a_n]$. Пусть $y_1, \dots, y_n$ — n новых переменных (т. е. переменных, которые не входят в A или A'). Применяя первую часть доказательства, мы последовательно получаем $\vdash A_{x_1} [y_1]$, $\vdash A_{x_1, x_2} [y_1, y_2]$, $\dots$, $\vdash A_{x_1, \dots, x_n} [y_1, \dots, y_n]$.

Начиная с последнего и снова применяя первую часть доказательства, последовательно получаем, что

$$\begin{aligned} &\vdash A_{x_1, \dots, x_n} [a_1, y_2, \dots, y_n]^*, \\ &\vdash A_{x_1, \dots, x_n} [a_1, a_2, \dots, y_n], \\ &\vdots \\ &\vdash A_{x_1, \dots, x_n} [a_1, a_2, \dots, a_n]. \end{aligned}$$

(Читатель должен заметить, что применение y_i в вышеприведенном доказательстве действительно необходимо. Начиная с A , мы могли бы получить $A_{x_1} [a_1]$, но мы не смогли бы тогда получить $A_{x_1, x_2} [a_1, a_2]$, если бы x_2 входило в a_1 .)

Теорема подстановки.

$$(a) \vdash A_{x_1, \dots, x_n} [a_1, \dots, a_n] \rightarrow \exists x_1 \dots \exists x_n A;$$

$$(b) \vdash \forall x_1 \dots \forall x_n A \rightarrow A_{x_1, \dots, x_n} [a_1, \dots, a_n].$$

Доказательство. По аксиомам подстановки получаем

$$\vdash C \rightarrow \exists x C \quad (1)$$

и $\vdash \neg C \rightarrow \exists x \neg C$. Из последней формулы с помощью теоремы тавтологии и определения $\forall$ получаем

$$\vdash \forall x C \rightarrow C. \quad (2)$$

Ввиду (1)

$$\vdash \exists x_{i+1} \dots \exists x_n A \rightarrow \exists x_i \exists x_{i+1} \dots \exists x_n A$$

для $i = 1, \dots, n$. Отсюда с помощью теоремы тавтологии получаем $\vdash A \rightarrow \exists x_1 \dots \exists x_n A$, а из последней формулы мы получаем (a) по правилу подстановки.

Аналогично, мы можем применить (2) для получения $\vdash \forall x_1 \dots \forall x_n A \rightarrow A$ и затем получить (b) по правилу подстановки.

Правило дистрибутивности. Если $\vdash A \rightarrow B$, то $\vdash \exists x A \rightarrow \exists x B$ и $\vdash \forall x A \rightarrow \forall x B$.

Доказательство. По аксиоме подстановки получаем $\vdash B \rightarrow \exists x B$. Отсюда и из $\vdash A \rightarrow B$ получаем $\vdash A \rightarrow \exists x B$ по теореме тавтологии; таким образом, $\vdash \exists x A \rightarrow \exists x B$ по правилу $\exists$ -введения.

*) Заметим, что имеет место $A_{x_1, \dots, x_n} [a_1, y_2, \dots, y_n] = A_{x_1, \dots, x_n} [y_1, y_2, \dots, y_n]_{y_1 [a_1]}$. — Прим. ред.

По теореме подстановки получаем $\vdash \forall x A \rightarrow A$. Отсюда и из $\vdash A \rightarrow B$ получаем $\vdash \forall x A \rightarrow B$ по теореме тавтологии; таким образом, $\vdash \forall x A \rightarrow \forall x B$ по правилу $\forall$ -введения.

Пусть A — формула и $x_1, \dots, x_n$ — переменные, перечисленные в алфавитном порядке, которые свободны в A . Формула $\forall x_1 \dots \forall x_n A$ называется *замыканием* формулы A . Ясно, что замыкание формулы A замкнуто и что если A замкнута, то замыкание формулы A есть A .

Теорема замыкания. Если A' — замыкание формулы A , то $\vdash A'$ тогда и только тогда, когда $\vdash A$.

Доказательство. Если $\vdash A$, то $\vdash A'$ по правилу обобщения. По теореме подстановки получаем $\vdash A' \rightarrow A$; следовательно, если $\vdash A'$, то $\vdash A$ по правилу отделения.

Следствие. Если A' — замыкание формулы A , то A является истинной в структуре $\mathcal{A}$ тогда и только тогда, когда A' является истинной в $\mathcal{A}$.

Доказательство. Предположим, что A является истинной в $\mathcal{A}$. Если T имеет формулу A в качестве своей единственной нелогической аксиомы, то $\mathcal{A}$ — модель теории T . По теореме замыкания получаем $\vdash_T A'$; следовательно, A' является истинной в $\mathcal{A}$ по теореме истинности. Обратное доказывается аналогично.

3.3. Теорема дедукции

Если математик желает доказать утверждение *если* P , *то* Q , то он обычно предполагает P и затем доказывает Q . Мы покажем, что в теориях существует подобный метод доказательства теорем.

Обозначим теорию, полученную из T добавлением $A_1, \dots, A_n$ в качестве новых нелогических аксиом, через $T[A_1, \dots, A_n]$. Тогда аналогом вышеописанного метода для теорий будет следующее: если мы желаем доказать $A \rightarrow B$ в T , то мы стараемся доказать B в $T[A]$. Покажем, что если мы добьемся этого и если A замкнута, то $A \rightarrow B$ действительно является теоремой теории T .

Теорема дедукции. Пусть A — замкнутая формула теории T . Для каждой формулы B теории T имеем $\vdash_T A \rightarrow B$ тогда и только тогда, когда B является теоремой теории $T[A]$.

Доказательство. Если $\vdash_T A \rightarrow B$, то A и $A \rightarrow B$ являются теоремами теории $T[A]$; следовательно, B — теорема теории $T[A]$ по правилу отделения. Докажем теперь, что $\vdash_T A \rightarrow B$ для каждой теоремы B теории $T[A]$, применяя индукцию по теоремам (в форме, описанной в § 3.1).

Предположим, что B — аксиома теории $T[A]$. Если B есть A , то $A \rightarrow B$ есть тавтология и, следовательно, теорема теории T . В противном случае B есть аксиома теории T ; поэтому $\vdash B$; тогда $\vdash_T A \rightarrow B$ по теореме тавтологии.

Предположим, что B — тавтологическое следствие формул $C_1, \dots, C_n$. Тогда $A \rightarrow B$ — тавтологическое следствие $A \rightarrow C_1, \dots, A \rightarrow C_n$. По индуктивному предположению $\vdash_T A \rightarrow C_1, \dots, \vdash_T A \rightarrow C_n$; следовательно, $\vdash_T A \rightarrow B$ по теореме тавтологии.

Предположим, что B выведена по правилу $\exists$ -введения; например, B есть $\exists x C \rightarrow D$ и выводится из $C \rightarrow D$, где x не является свободной в D . По индуктивному предположению $\vdash_T A \rightarrow C \rightarrow D$; следовательно, по теореме тавтологии имеем $\vdash_T C \rightarrow A \rightarrow D$. Так как x не является свободной ни в A , ни в D , то $\vdash_T \exists x C \rightarrow A \rightarrow D$ по правилу $\exists$ -введения; следовательно, $\vdash_T A \rightarrow B$ по теореме тавтологии.

Следствие. Пусть $A_1, \dots, A_n$ — замкнутые формулы теории T . Для каждой формулы B теории T имеем $\vdash_T A_1 \rightarrow \dots \rightarrow A_n \rightarrow B$ тогда и только тогда, когда B — теорема теории $T[A_1, \dots, A_n]$.

Доказательство. Индукцией по n .

Теорема дедукции ложна, если не требовать, чтобы A была замкнутой. Так, если мы добавим $x=0$ в качестве аксиомы к N , то мы можем доказать $y=0$ по правилу подстановки. Но $x=0 \rightarrow y=0$ не является теоремой N , так как она не является истинной в модели $\mathcal{A}$. Чтобы обойти эту трудность, докажем теорему, которая позволит нам заменять $A \rightarrow B$ на импликацию с замкнутой посылкой.

Теорема о константах. Пусть T' получена из T добавлением новых констант (но не новых нелогических аксиом). Для каждой формулы A теории T и каждой последовательности $e_1, \dots, e_n$ различных новых констант имеем $\vdash_T A$ тогда и только тогда, когда $\vdash_{T'} A[e_1, \dots, e_n]$.

Доказательство. Если $\vdash_T A$, то $\vdash_{T'} A$; следовательно, $\vdash_{T'} A[e_1, \dots, e_n]$ по правилу подстановки. Теперь предположим, что мы имеем доказательство $A[e_1, \dots, e_n]$ в T' . Мы выберем n переменных $y_1, \dots, y_n$, не встречающихся ни в доказательстве, ни в A , и заменим $e_1, \dots, e_n$ во всем доказательстве на $y_1, \dots, y_n$. Это не затронет нелогических аксиом (которые не содержат никаких новых констант). Легко видеть, что каждая другая аксиома становится аксиомой того же типа, а каждое применение правила становится новым применением того же правила. Отсюда следует, что мы получим доказательство $A[y_1, \dots, y_n]$ в T . Таким образом,

$$\vdash_T A[y_1, \dots, y_n];$$

следовательно, $\vdash_T A$ по правилу подстановки.

Теперь возвратимся к проблеме доказательства $A \rightarrow B$ в T . Пусть $x_1, \dots, x_n$ — переменные, свободные в A . Строим T' из T добавлением новых констант $e_1, \dots, e_n$. По теореме о константах имеем

$$\begin{aligned} \vdash_T A \rightarrow B \text{ тогда и только тогда, когда} \\ \vdash_{T'} A[e_1, \dots, e_n] \rightarrow B[e_1, \dots, e_n]. \end{aligned}$$

Так как $A[e_1, \dots, e_n]$ замкнута, то теорема дедукции показывает, что для этого достаточно доказать $B[e_1, \dots, e_n]$ в $T' [A[e_1, \dots, e_n]]$.

3.4. Теоремы эквивалентности и равенства

Результаты этого параграфа могут быть приблизительно сформулированы как следующие: эквивалентные формулы и равные термы взаимозаменяемы.

Теорема эквивалентности. Пусть A' получена из A заменой некоторых вхождений $B_1, \dots, B_n$ на $B'_1, \dots, B'_n$ соответственно. Если

$$\vdash B_1 \leftrightarrow B'_1, \dots, \vdash B_n \leftrightarrow B'_n,$$

то

$$\vdash A \leftrightarrow A'.$$

Доказательство. Рассмотрим вначале один специальный случай: существует только одно такое вхождение и оно есть всё A . Тогда A есть B_i и A' есть B'_i для некоторого i ; следовательно, $\vdash A \leftrightarrow A'$ по предположению.

Докажем теперь теорему индукцией по длине A . Если A — атомная формула, то любое вхождение формулы в A есть всё A по теореме о вхождении. Следовательно, если это не специальный случай, то никакое вхождение не заменяется и A' есть A . Тогда $\vdash A \leftrightarrow A'$ по теореме тавтологии.

Предположим, что A есть $\neg C$. По теореме о вхождении любое вхождение формулы в A или есть всё A или целиком содержится в C . Отсюда следует, что если это не специальный случай, то A' есть $\neg C'$, где C' получается заменами из C так, как описано в теореме. По индуктивному предположению $\vdash C \leftrightarrow C'$; следовательно, $\vdash A \leftrightarrow A'$ по теореме тавтологии.

Если A есть $C \vee D$, то доказательство аналогично. Теперь предположим, что A есть $\exists x C$. Если это не специальный случай, то A' есть $\exists x C'$, где $\vdash C \leftrightarrow C'$ по индуктивному предположению. Тогда $\vdash C \rightarrow C'$ и $\vdash C' \rightarrow C$ по теореме тавтологии. По правилу дистрибутивности имеем $\vdash A \rightarrow A'$ и $\vdash A' \rightarrow A$; следовательно, $\vdash A \leftrightarrow A'$ по теореме тавтологии.

Мы уже замечали, что формула не меняет своего значения, если связанную переменную заменить другой переменной. Как применение теоремы эквивалентности докажем теперь синтаксический вариант этого замечания.

Скажем, что A' — *вариант* формулы A , если A' может быть получена из A с помощью последовательных замен следующего типа: заменяем часть $\exists x B$ на $\exists y B_x[y]$, где y — переменная, не являющаяся свободной в B .

Теорема о варианте. Если A' — вариант формулы A , то $\vdash A \leftrightarrow A'$.

Доказательство. Ввиду теоремы эквивалентности и теоремы тавтологии нам нужно лишь показать, что в обозначениях предыдущего определения $\vdash \exists x B \leftrightarrow \exists y B_x[y]$. Пусть B' есть $B_x[y]$. По теореме подстановки $\vdash B' \rightarrow \exists x B$; следовательно, по правилу $\exists$ -введения

$$\vdash \exists y B' \rightarrow \exists x B. \quad (1)$$

Учитывая то, что y не является свободной в B , видим, что $B'_y[x]$ есть B . Следовательно, по теореме подстановки $\vdash B \rightarrow \exists y B'$; таким образом, $\vdash \exists x B \rightarrow \exists y B'$ по правилу $\exists$ -введения. Отсюда и из (1) получаем $\vdash \exists x B \leftrightarrow \exists y B'$ по теореме тавтологии.

Варианты применяются, когда у нас имеются трудности, связанные с тем, что терм a не является допустимым для подстановки вместо x в A . Мы можем тогда найти вариант A' формулы A , в котором ни одна переменная из a не является связанной. Тогда a будет допустимым для подстановки вместо x в A' , и мы можем заменить A на A' .

Теорема симметрии. $\vdash a=b \leftrightarrow b=a$.

Доказательство. По аксиоме равенства имеем

$$\vdash x=y \rightarrow x=x \rightarrow x=x \rightarrow y=x.$$

Таким образом, по аксиомам тождества и теореме тавтологии $\vdash x=y \rightarrow y=x$. По правилу подстановки $\vdash a = b \rightarrow b=a$ и $\vdash b=a \rightarrow a=b$; следовательно, $\vdash a=b \leftrightarrow b=a$ по теореме тавтологии.

Теорема равенства. Пусть b' получен из b заменой некоторых вхождений $a_1, \dots, a_n$ на $a'_1, \dots, a'_n$ соответственно, и пусть A' получена из A заменой некоторых вхождений $a_1, \dots, a_n$ на $a'_1, \dots, a'_n$ соответственно. Если $\vdash a_1 = a'_1, \dots, \vdash a_n = a'_n$, то $\vdash b=b'$ и $\vdash A \leftrightarrow A'$.

Доказательство. Вначале докажем, что $\vdash b=b'$. Если единственное заменяемое вхождение есть всё b , то для некоторого i терм b есть a_i и терм b' есть a'_i ; следовательно, $\vdash b=b'$ по предположению. Мы исключаем теперь этот специальный случай и проведем индукцию по длине b . Если b — переменная, то нет вхождений, которые можно заменить (так как специальный случай исключен). Следовательно, b' есть b и $\vdash b=b'$ по аксиоме тождества и правилу подстановки. Теперь предположим, что b есть $fc_1 \dots c_k$. Тогда b' есть $fc'_1 \dots c'_k$, где $\vdash c_i = c'_i$ для $i=1, \dots, k$ по индуктивному предположению. По аксиомам равенства и правилу подстановки имеем

$$\vdash c_1 = c'_1 \rightarrow \dots \rightarrow c_k = c'_k \rightarrow b=b'.$$

Следовательно, $\vdash b=b'$ по правилу отделения.

Докажем теперь, что $\vdash A \leftrightarrow A'$, индукцией по длине A . Если A — атомная формула $pc_1 \dots c_k$, то по первой части доказательства A' есть $pc'_1 \dots c'_k$, где $\vdash c_i = c'_i$ для $i=1, \dots, k$. По теореме симметрии $\vdash c'_i = c_i$ для $i=1, \dots, k$. По аксиомам равенства и правилу подстановки

$$\vdash c_1 = c'_1 \rightarrow \dots \rightarrow c_k = c'_k \rightarrow A \rightarrow A'$$

и

$$\vdash c'_1 = c_1 \rightarrow \dots \rightarrow c'_k = c_k \rightarrow A' \rightarrow A.$$

Следовательно, $\vdash A \leftrightarrow A'$ по теореме тавтологии. Оставшиеся случаи рассматриваются так же, как и в доказательстве теоремы эквивалентности.

Следствие 1. $\vdash a_1 = a'_1 \rightarrow \dots \rightarrow a_n = a'_n \rightarrow b[a_1, \dots, a_n] = b[a'_1, \dots, a'_n]$.

Доказательство. Заменяем каждую переменную, входящую в a_i или в a'_i , новой константой. Предположим, что a_i, a'_i и b превращаются в c_i, c'_i и d . Формулой, которую надо доказать, является

$$c_1 = c'_1 \rightarrow \dots \rightarrow c_n = c'_n \rightarrow d[c_1, \dots, c_n] = d[c'_1, \dots, c'_n].$$

Ввиду результатов последнего параграфа достаточно добавить $c_i = c'_i$ в качестве аксиом и доказать $d[c_1, \dots, c_n] = d[c'_1, \dots, c'_n]$. Это можно сделать с помощью теоремы равенства.

Следствие 2. $\vdash a_1 = a'_1 \rightarrow \dots \rightarrow a_n = a'_n \rightarrow (A[a_1, \dots, a_n] \leftrightarrow A[a'_1, \dots, a'_n])$.

Доказательство. Аналогично доказательству следствия 1.

В приложениях теорема и оба следствия будут называться просто теоремой равенства.

Следствие 3. Если x не входит в a , то

$$\vdash A_x[a] \leftrightarrow \exists x (x=a \& A).$$

Доказательство. По теореме равенства

$$\vdash x=a \rightarrow (A \leftrightarrow A_x[a]);$$

следовательно, по теореме тавтологии и правилу $\exists$ -введения

$$\vdash \exists x (x=a \& A) \rightarrow A_x[a]. \quad (2)$$

По теореме подстановки

$$\vdash (a=a \& A_x[a]) \rightarrow \exists x (x=a \& A). \quad (3)$$

По аксиомам тождества и правилу подстановки

$$\vdash a=a. \quad (4)$$

По теореме тавтологии следствие получается из (2), (3) и (4).

3.5. Пренексная форма

Теперь покажем, что каждая формула эквивалентна формуле, находящейся в некоторой специальной форме.

Формула называется *открытой*, если она не содержит кванторов. Формула A находится в *пренексной форме*, если она имеет вид $Qx_1 \dots Qx_n B$, где каждое Qx_i есть или $\exists x_i$ или $\forall x_i$; $x_1, \dots, x_n$ различны и B открыта. В этом случае $Qx_1 \dots Qx_n$ называем *приставкой*, а B — *матрицей* для A . Мы допускаем случай, когда приставка пуста, другими словами, считаем, что открытая формула также находится в пренексной форме.

Наше определение пренексной формы содержит определяемый символ $\forall$. Как и во всех таких случаях, в определении, на самом деле, упоминаются формулы, полученные устранением определяемых символов. Однако, имея дело с пренексной формой, вообще лучше не предполагать определяемый символ $\forall$ устраненным.

Введем теперь некоторые операции, называемые *пренексными операциями*. Это операции, которые могут быть произведены над формулой A , возможно, содержащей определяемый символ $\forall$; результатом операции является другая такая формула. Пренексными операциями являются:

- (а) замена A некоторым вариантом;
- (б) замена части $\neg Qx B$ в A на $Q'x \neg B$, где $Q'x$ есть $\forall x$, если Qx есть $\exists x$, и $Q'x$ есть $\exists x$, если Qx есть $\forall x$;
- (в) замена части $Qx B \vee C$ в A на $Qx (B \vee C)$ при условии, что x не является свободной в C ;
- (г) замена части $B \vee Qx C$ в A на $Qx (B \vee C)$ при условии, что x не является свободной в B .

Вначале покажем, что если A' — результат, полученный из A при помощи некоторой пренексной операции, то $\vdash A \leftrightarrow A'$. Для (а) это следует из теоремы о варианте. Для (б) достаточно, имея в виду теорему эквивалентности, показать, что $\vdash \neg Qx B \leftrightarrow Q'x \neg B$. Таким образом, мы должны показать, что

$$\neg \exists x B \leftrightarrow \forall x \neg B$$

и

$$\neg \forall x B \leftrightarrow \exists x \neg B$$

являются теоремами. Если устранить $\forall$, то получим

$$\neg \exists x B \leftrightarrow \neg \exists x \neg \neg B \quad \text{и} \quad \neg \neg \exists x \neg B \leftrightarrow \exists x \neg B.$$

Они следуют из теоремы эквивалентности и теоремы тавтологии.

Обращаясь к (в), достаточно доказать, что $\vdash Qx B \vee C \leftrightarrow Qx (B \vee C)$. Это будет следовать из теоремы тавтологии, если мы докажем

$$\vdash Qx B \rightarrow Qx (B \vee C), \quad (1)$$

$$\vdash C \rightarrow Qx (B \vee C), \quad (2)$$

$$\vdash Qx (B \vee C) \rightarrow Qx B \vee C. \quad (3)$$

Мы получаем (1) из тавтологии $B \rightarrow B \vee C$ по правилу дистрибутивности. Если Qx есть $\exists x$, мы получаем (2) из аксиомы подстановки $B \vee C \rightarrow \exists x (B \vee C)$ по теореме тавтологии. Если Qx есть $\forall x$, мы получаем (2) из тавтологии $C \rightarrow B \vee C$ по правилу $\forall$ -введения. Теперь из аксиомы подстановки $B \rightarrow \exists x B$ мы получаем $\vdash B \vee C \rightarrow \exists x B \vee C$ по теореме тавтологии; следовательно, $\vdash \exists x (B \vee C) \rightarrow \exists x B \vee C$ по правилу $\exists$ -введения. Это есть (3), когда Qx есть $\exists x$. По теореме подстановки имеем $\vdash \forall x (B \vee C) \rightarrow B \vee C$; следовательно, по теореме тавтологии и правилу $\forall$ -введения имеем

$$\vdash \forall x (B \vee C) \rightarrow \forall x B.$$

Отсюда по теореме тавтологии получаем $\vdash \forall x (B \vee C) \rightarrow \forall x B \vee C$, которое есть (3), когда Qx есть $\forall x$.

Обращаясь к (г), достаточно показать, что $\vdash B \vee Qx C \leftrightarrow Qx (B \vee C)$, если x не является свободной в B . По сказанному выше имеем $\vdash Qx C \vee B \leftrightarrow Qx (C \vee B)$, и желаемый результат следует по теореме эквивалентности и теореме тавтологии.

Теперь покажем, что каждая формула может быть преобразована в формулу в пренексной форме с помощью применения пренексных операций. Доказательство ведется индукцией по длине A . Если A — атомная формула, то она уже в пренексной форме. Предположим, что A есть $\neg B$. По индуктивным предположениям мы можем преобразовать B в формулу B' в пренексной форме с помощью пренексных операций. Те же операции преобразуют A в $\neg B'$. Но ясно, что $\neg B'$ может быть преобразована в

формулу в пренексной форме последовательным применением операции (б).

Теперь предположим, что A есть $B \vee C$. По индуктивному предположению мы можем преобразовать B и C в формулы B' и C' в пренексной форме. Имея в виду операцию (а), мы можем далее предполагать, что переменные в приставке B' отличны от переменных в приставке C' и что переменные в обеих приставках отличны от переменных, свободных в B' и C' . Мы можем тогда преобразовать A в $B' \vee C'$; с помощью операций (в) и (г) мы можем преобразовать $B' \vee C'$ в формулу в пренексной форме.

Наконец, предположим, что A есть $\exists x B$. Мы можем преобразовать B в формулу B' в пренексной форме; мы можем предполагать, что переменные в приставке B' отличны от x . Тогда A может быть преобразована в $\exists x B'$, которая находится в пренексной форме.

Под пренексной формой формулы A мы понимаем формулу в пренексной форме, в которую A может быть преобразована с помощью пренексных операций. Мы уже видели, что каждая формула имеет пренексную форму и что если A' — пренексная форма A , то $\vdash A \leftrightarrow A'$. Заметим, что пренексные операции не зависят от теории, в которой мы работаем.

Наш метод получения пренексной формы формулы A требует от нас устранения определяемых символов, отличных от $\forall$. Мы можем избежать устранения $\rightarrow$ и $\&$ с помощью введения следующих дополнительных пренексных операций:

(д) замена части $\exists x B \rightarrow C$ в A на $\exists x' (B \rightarrow C)$, где $\exists x'$ означает то же, что и в (б), при условии, что x не является свободной в C ;

(е) замена части $B \rightarrow \exists x C$ в A на $\exists x (B \rightarrow C)$ при условии, что x не является свободной в B ;

(ж) замена части $\exists x B \& C$ в A на $\exists x (B \& C)$ при условии, что x не является свободной в C ;

(з) замена части $B \& \exists x C$ в A на $\exists x (B \& C)$ при условии, что x не является свободной в B .

Можно видеть, как и раньше, что этих операций достаточно, чтобы преобразовать любую формулу, содержащую $\rightarrow$ и $\&$, в пренексную форму. Чтобы убедиться, что формула, полученная в результате этих операций, эквивалентна формуле, над которой операции производи-

лись, заметим, что каждая операция по устранении определяемого символа становится некоторой последовательностью операций (б), (в) и (г). Например, предположим, что мы используем (д) для замены $\exists x B \rightarrow C$ на $\forall x (B \rightarrow C)$. Устраняя $\rightarrow$, видим, что мы заменили $\neg \exists x B \vee C$ на $\forall x (\neg B \vee C)$. Это можно сделать, вначале применяя (б) и затем применяя (в). Мы не можем получить подобного правила для $\leftrightarrow$; если мы устраним $\leftrightarrow$ и применим (а) — (з), то обнаружим, что не можем вернуться к $\leftrightarrow$.

В заключение приведем пример шагов преобразования формулы из N в пренексную форму:

$$\begin{aligned} \exists x (x = y) &\rightarrow \exists x (x = 0 \vee \neg \exists y (y < 0)), \\ \exists x (x = y) &\rightarrow \exists z (z = 0 \vee \neg \exists w (w < 0)), \\ \exists x (x = y) &\rightarrow \exists z (z = 0 \vee \forall w \neg (w < 0)), \\ \exists x (x = y) &\rightarrow \exists z \forall w (z = 0 \vee \neg (w < 0)), \\ \forall x \exists z \forall w (x = y \rightarrow z = 0 \vee \neg (w < 0)). \end{aligned}$$

Задачи

1. Показать, что если A — формула, доказуемая без использования аксиом подстановки, нелогических аксиом, аксиом тождества, аксиом равенства и правила $\exists$ -введения, то A — тавтология.

2. Пусть T — теория без нелогических аксиом. Для каждой формулы A теории T пусть A^* — формула, полученная из A опусканием всех кванторов и заменой всех термов новой константой e . Показать, что если $\vdash_T A$, то A^* — тавтологическое следствие формул вида $a = a$. Вывести, что не существует формулы A такой, что $\vdash_T A$ и $\vdash_T \neg A$.

$$3. (a) \vdash \forall x (A \rightarrow B) \rightarrow \exists x A \rightarrow \forall x B.$$

$$(b) \vdash \exists x (A \rightarrow B) \rightarrow \forall x A \rightarrow \exists x B.$$

$$4. (a) \vdash \exists x (A \vee B) \leftrightarrow \exists x A \vee \exists x B.$$

$$(b) \vdash \forall x (A \& B) \leftrightarrow \forall x A \& \forall x B.$$

$$(v) \vdash \exists x (A \& B) \rightarrow \exists x A \& \exists x B.$$

$$(r) \vdash \forall x A \vee \forall x B \rightarrow \forall x (A \vee B).$$

(д) Привести примеры формул из N вида

$$\forall x (A \vee B) \rightarrow \forall x A \vee \forall x B \text{ и } \exists x A \& \exists x B \rightarrow \exists x (A \& B),$$

которые не являются истинными в $\mathcal{N}$.

5. Показать, что если x не является свободной в A , то $\vdash \exists x A \leftrightarrow A$ и $\vdash \forall x A \leftrightarrow A$.

$$6. (a) \vdash \exists x \exists y A \leftrightarrow \exists y \exists x A.$$

$$(b) \vdash \forall x \forall y A \leftrightarrow \forall y \forall x A.$$

$$(v) \vdash \exists x \forall y A \rightarrow \forall y \exists x A.$$

(г) Привести пример формулы из N вида $\forall x \exists y A \rightarrow \exists y \forall x A$, которая не является истинной в $\mathcal{N}$.

7. (а) Пусть A' получена из A заменой некоторых вхождений B на B' . Пусть $x_1, \dots, x_n$ включают в себя все те переменные, которые имеют вхождение внутри этих вхождений B и B' , свободное в B или B' и связанное в A или A' .

Показать, что

$$\vdash \forall x_1 \dots \forall x_n (B \leftrightarrow B') \rightarrow (A \leftrightarrow A').$$

[Использовать метод из § 3.3 и теорему эквивалентности.]

(б) Привести пример формул A, A', B и B' из N , удовлетворяющих условию (а) таких, что $(B \leftrightarrow B') \rightarrow (A \leftrightarrow A')$ не является истинной в $\mathcal{N}$.

8. (а) Пусть A' получена из A заменой некоторых вхождений a , не находящихся в областях действия кванторов, на a' . Пусть $x_1, \dots, x_n$ включают в себя все те переменные, которые имеют вхождение внутри этих вхождений a и a' , связанное в A или A' . Показать, что

$$\vdash \forall x_1 \dots \forall x_n (a = a') \rightarrow (A \leftrightarrow A').$$

[Подобно 7 (а).]

(б) Привести пример термов a и a' и формул A и A' из N , удовлетворяющих условию (а), таких, что $a = a' \rightarrow (A \leftrightarrow A')$ не является истинной в $\mathcal{N}$.

9. Пусть T — теория. Пусть T' — формальная система, полученная из T опусканием аксиом равенства и добавлением в качестве новых аксиом всех формул $x = y \rightarrow A \rightarrow A_x[y]$ для атомных формул A . Показать, что T и T' имеют одни и те же теоремы.

10. (а) Показать, что если x не входит в a , то

$$\vdash A_x[a] \leftrightarrow \forall x (x = a \rightarrow A).$$

(б) Привести примеры формул из N вида

$$A_x[a] \leftrightarrow \exists x (x = a \ \& \ A) \quad \text{и} \quad A_x[a] \leftrightarrow \forall x (x = a \rightarrow A),$$

которые не являются истинными в $\mathcal{N}$.

11. (а) Формула находится в *дизъюнктивной форме*, если эта формула есть дизъюнкция конъюнкций формул, которые являются элементарными формулами или отрицаниями элементарных формул. Показать, что для каждой формулы A существует формула A' , находящаяся в дизъюнктивной форме, такая, что $A \leftrightarrow A'$ — тавтология.

(б) Формула находится в *конъюнктивной форме*, если эта формула есть конъюнкция дизъюнкций формул, которые являются элементарными формулами или отрицаниями элементарных формул. Показать, что для каждой формулы A существует формула A' , находящаяся в конъюнктивной форме, такая, что $A \leftrightarrow A'$ — тавтология. [Начать с формулы B в дизъюнктивной форме такой, что $\neg A \leftrightarrow B$ является тавтологией.]

12. Пусть A — формула, возможно, содержащая определяемые символы $\&$ и $\vee$. Пусть A^0 получена из A следующим образом: для каждого вхождения атомной формулы B в A , если B непосредственно следует за $\neg$, то опускаем $\neg$; в противном случае вставляем $\neg$ перед B . Пусть A^* получена из A^0 заменой всех $\vee, \&, \exists$ и $\forall$ на $\&, \vee, \forall$ и $\exists$ соответственно. Показать, что $\vdash A^* \leftrightarrow \neg A$. [Использовать индукцию по длине A .]

ПРОБЛЕМА ХАРАКТЕРИЗАЦИИ

4.1. Теорема редукции

Главная цель формальной системы — служить основой для доказательства теорем. Поэтому особенно важной проблемой для любой формальной системы F является следующая: найти необходимые и достаточные условия того, чтобы формула системы F была теоремой системы F . Эта проблема называется *проблемой характеристики* для F . Мы предполагаем изучить проблему характеристики для теорий.

Имеется тривиальное решение проблемы характеристики для любой теории T : формула является теоремой тогда и только тогда, когда эта формула имеет доказательство. Такое решение проблемы является неудовлетворительным, потому что условие, что A — теорема, зависит от всех формул, которые могут встретиться в доказательстве формулы A . При удовлетворительном решении условия должны зависеть только от A и формул, тесно связанных с A .

Если мы ищем решение проблемы характеристики, подходящее для всех теорий, мы должны немного изменить это требование. Будет ли A теоремой теории T или нет, очевидно, сильно зависит от нелогических аксиом теории T . Поэтому мы должны ожидать, что условие, согласно которому A — теорема теории T , будет учитывать не только A , но также и нелогические аксиомы теории T . Если эти нелогические аксиомы достаточно просты, то это не должно создавать каких-либо неудобств. Для теорий со сложными нелогическими аксиомами необходимо отказаться от общих решений и искать решение, приспособленное к частной теории.

Существуют несколько простых результатов, относящихся к проблеме характеристики для различных теорий. Чтобы рассмотреть их, введем некоторые понятия, которые часто применяются при изучении теорий.

Язык первого порядка L' называется *расширением* языка первого порядка L , если каждый нелогический символ из L является нелогическим символом из L' . (Учитывается соглашение из § 2.4 относительно применения нелогических символов в двух различных языках.) Теория T' называется *расширением* теории T , если $L(T')$ — расширение языка $L(T)$ и каждая теорема теории T является теоремой теории T' . Ясно, что для последнего необходимо и достаточно, чтобы каждая нелогическая аксиома теории T была теоремой теории T' , но не обязательно, чтобы каждая нелогическая аксиома теории T была нелогической аксиомой теории T' .

Консервативным расширением теории T называется расширение T' теории T такое, что каждая формула теории T , являющаяся теоремой теории T' , также является теоремой теории T . Например, если мы получаем T' из T добавлением некоторых новых констант, то по теореме о константах T' является консервативным расширением теории T .

Теории T и T' называются *эквивалентными*, если каждая из них есть расширение другой, т. е. если они имеют одинаковый язык и одинаковые теоремы. Отсюда следует, что эти теории являются консервативными расширениями одна другой. Если T' является (консервативным) расширением теории T , то любая теория, эквивалентная T' , является (консервативным) расширением любой теории, эквивалентной T .

Если T' — консервативное расширение теории T , то формула теории T является теоремой теории T тогда и только тогда, когда она является теоремой теории T' ; таким образом, решение проблемы характеристики для T' дает решение аналогичной проблемы для T . В частности, если T и T' эквивалентны, то проблемы характеристики для T и T' эквивалентны.

Если Γ — множество формул теории T , то пусть $T[\Gamma]$ — теория, полученная из T добавлением всех формул из Γ в качестве новых нелогических аксиом.

Теорема редукции. Пусть Γ — какое-то множество формул теории T и A — некоторая формула теории T . Тогда A является теоремой теории $T[\Gamma]$ тогда и только тогда, когда существует теорема теории T вида $B_1 \rightarrow \dots \rightarrow B_n \rightarrow A$, где каждое B_i есть замыкание некоторой формулы из Γ .

Доказательство. Если такая теорема теории T существует, то по теореме замыкания $B_1, \dots, B_n$ и $B_1 \rightarrow \dots \rightarrow B_n \rightarrow A$ являются теоремами теории $T[\Gamma]$; таким образом, по правилу отделения A — теорема теории $T[\Gamma]$. Теперь предположим, что A имеет доказательство в $T[\Gamma]$, и пусть $B_1, \dots, B_n$ — замыкания тех формул из Γ , которые используются в доказательстве в качестве нелогических аксиом. Применяя снова теорему замыкания, получим, что A — теорема теории $T[B_1, \dots, B_n]$; следовательно, по теореме дедукции $B_1 \rightarrow \dots \rightarrow B_n \rightarrow A$ — теорема теории T .

Теорема редукции сводит проблему характеристики для $T[\Gamma]$ к проблеме характеристики для T . Далее, любая теория T' есть $T[\Gamma]$, где T получена из T' опусканием всех нелогических аксиом, а Γ — множество нелогических аксиом теории T' . Поэтому для того, чтобы решить проблему характеристики для всех теорий, достаточно решить ее для теорий, у которых нет нелогических аксиом. Конечно, тогда решение для T' зависит от нелогических аксиом теории T' ; но мы уже видели, что это неизбежно.

Теория T называется *противоречивой*, если каждая формула теории T является теоремой теории T ; в противном случае T называется *непротиворечивой*. Проблема, будет T непротиворечивой или нет, является специальным случаем проблемы характеристики для T . Это важно потому, что, как мы увидим в следующем параграфе, T непротиворечива тогда и только тогда, когда она имеет модель.

Если для некоторой формулы A обе формулы A и $\neg A$ являются теоремами теории T , то T противоречива; действительно, каждая формула есть тавтологическое следствие формул A и $\neg A$. Мы часто будем молчаливо использовать этот факт в рассуждениях о непротиворечивости.

Если T' — расширение теории T и T' непротиворечива, то T непротиворечива; действительно, если A — любая формула теории T , то одна из формул A и $\neg A$ не является теоремой теории T' и, следовательно, не является теоремой теории T . Если T' — консервативное расширение теории T , то T' непротиворечива тогда и только тогда, когда T непротиворечива. Действительно, если T непротиворечива и A — формула теории T , то одна из формул A или $\neg A$ не является теоремой теории T и, следовательно, не является теоремой теории T' .

Теперь переформулируем теорему редукции применительно к непротиворечивости.

Теорема редукции для непротиворечивости. Пусть Γ — непустое множество формул теории T . Тогда $T[\Gamma]$ противоречива тогда и только тогда, когда существует теорема теории T , которая есть дизъюнкция отрицаний замыканий различных формул из Γ .

Доказательство. Если такая формула $\neg A_1 \vee \dots \vee \neg A_n$ существует, то каждая из $A_1, \dots, A_n, \neg A_1 \vee \dots \vee \neg A_n$ является теоремой теории $T[\Gamma]$; следовательно, по теореме тавтологии каждая формула есть теорема теории $T[\Gamma]$. Теперь предположим, что $T[\Gamma]$ противоречива, и пусть B — любая формула теории T . Тогда $B \& \neg B$ — теорема теории $T[\Gamma]$; следовательно, по теореме редукции $\vdash_T A_1 \rightarrow \dots \rightarrow A_n \rightarrow B \& \neg B$, где каждое A_i является замыканием некоторой формулы из Γ . Ясно, что можно предполагать, что $n > 0$ и что A_i различны. По теореме тавтологии имеем $\vdash_T \neg A_1 \vee \dots \vee \neg A_n$.

Следствие. Пусть A' — замыкание формулы A . Тогда A является теоремой теории T тогда и только тогда, когда $T[\neg A']$ противоречива.

Доказательство. По теореме $T[\neg A']$ противоречива тогда и только тогда, когда $\vdash_T \neg \neg A'$. По теореме тавтологии и теореме замыкания это выполняется тогда и только тогда, когда $\vdash_T A$.

4.2. Теорема полноты

Нашим первым решением проблемы характеристики является результат, уже упоминавшийся в главе 2.

Теорема полноты, первая форма (Гёдель). Формула A теории T является теоремой теории T тогда и только тогда, когда A является истинной в T .

Эта теорема имеет вторую форму, относящуюся к непротиворечивости.

Теорема полноты, вторая форма. Теория T непротиворечива тогда и только тогда, когда она имеет модель.

Вначале покажем, что из второй формы теоремы полноты следует первая. Ввиду теоремы замыкания и ее следствия достаточно доказать первую форму для замкнутой формулы A . По следствию к теореме редукции для

непротиворечивости A есть теорема теории T тогда и только тогда, когда $T[\neg A]$ противоречива. По второй форме теоремы полноты это выполняется тогда и только тогда, когда $T[\neg A]$ не имеет модели. Далее, так как A замкнута, то модель для $T[\neg A]$ есть просто модель для T , в которой A не является истинной. Следовательно, A является теоремой теории T тогда и только тогда, когда A является истинной в каждой модели теории T .

Одна часть второй формы теоремы полноты следует из теоремы истинности. Предположим, что T имеет модель $\mathcal{A}$. Если A — замкнутая формула теории T , то $\mathcal{A}(A \& \neg A) = \mathbf{J}$; таким образом, $A \& \neg A$ не является истинной в $\mathcal{A}$ и, следовательно, не является теоремой теории T . Таким образом, T непротиворечива.

Дадим теперь доказательство Генкина другой части второй формы теоремы полноты. Начнем с некоторых замечаний о структурах и расширениях.

Предположим, что язык первого порядка L' является расширением языка первого порядка L , и пусть $\mathcal{A}'$ — структура для L' . Опуская некоторые функции и предикаты из $\mathcal{A}'$, мы получим структуру $\mathcal{A}$ для L . Мы называем структуру $\mathcal{A}$ *обеднением* структуры $\mathcal{A}'$ до L и обозначаем $\mathcal{A}$ через $\mathcal{A}'|L$. Мы также говорим, что структура $\mathcal{A}'$ является *обогащением* структуры $\mathcal{A}$ до L' .

Если $\mathcal{A}'$ является обогащением структуры $\mathcal{A}$ до L' , то $\mathcal{A}$ и $\mathcal{A}'$ имеют одни и те же индивиды. Поэтому мы используем одну и ту же константу в качестве имени индивида a в $L(\mathcal{A})$ и $L'(\mathcal{A}')$. Легко проверить, что $\mathcal{A}(A) = \mathcal{A}'(A)$ для каждой замкнутой формулы A языка $L(\mathcal{A})$. Отсюда и по следствию к теореме замыкания получаем, что одни и те же формулы языка L являются истинными как в $\mathcal{A}$, так и в $\mathcal{A}'$. Отсюда и по теореме истинности мы получаем следующий результат.

Лемма 1. Если T' — расширение теории T и $\mathcal{A}'$ — модель для T' , то обеднение $\mathcal{A}'$ до $L(T)$ является моделью теории T .

Возвращаясь к теореме полноты, мы сталкиваемся со следующей проблемой: как мы найдем модель для данной непротиворечивой теории T ? Поскольку дана только теория, то мы должны строить нашу модель из синтаксических материалов. Далее, выражения теории T , которые обозначают отдельные индивиды, являются терминами, сво-

бодными от переменных. Основная идея — взять эти термы в качестве индивидов, и пусть теоремы говорят нам, что будет истинным для этих индивидов. Фактически индивидами будут множества термов, свободных от переменных; это необходимо, потому что теоремы теории могут вынуждать два терма, свободных от переменных, представлять один и тот же индивид.

Пусть T — теория, содержащая константы. Определим структуру $\mathcal{A}$, которую мы называем *канонической структурой* для T . Если a и b — термы теории T , свободные от переменных, то мы определяем $a \sim b$, означающее $\vdash_T a = b$. Имеем $\vdash_T a = a$ и

$$\vdash_T a = b \rightarrow (a = c \leftrightarrow b = c)$$

по аксиомам тождества и теореме равенства. Следовательно,

$$a \sim a \text{ и } a \sim b \rightarrow (a \sim c \leftrightarrow b \sim c).$$

Полагая c равным a в последнем выражении и используя первое выражение, получаем

$$a \sim b \rightarrow b \sim a.$$

Итак, $\sim$ является отношением эквивалентности.

Пусть $|\mathcal{A}|$ — множество всех классов эквивалентности по $\sim$. Класс эквивалентности, содержащий терм a , обозначим через a^0 . Мы полностью определяем структуру $\mathcal{A}$, полагая

$$f_{\mathcal{A}}(a_1^0, \dots, a_n^0) = (fa_1 \dots a_n)^0,$$

$p_{\mathcal{A}}(a_1^0, \dots, a_n^0)$ тогда и только тогда, когда $\vdash_T pa_1 \dots a_n$. Мы должны показать, что правые части зависят только от a_i^0 , а не от a_i . Для этого предположим, что $a_i^0 = b_i^0$ для $i = 1, \dots, n$. Тогда $\vdash_T a_i = b_i$; следовательно, по теореме равенства имеем

$$\begin{aligned} \vdash_T fa_1 \dots a_n &= fb_1 \dots b_n, \\ \vdash_T pa_1 \dots a_n &\leftrightarrow pb_1 \dots b_n. \end{aligned}$$

Итак,

$$(fa_1 \dots a_n)^0 = (fb_1 \dots b_n)^0$$

и

$$\vdash_T pa_1 \dots a_n \text{ тогда и только тогда, когда } \vdash_T pb_1 \dots b_n.$$

А это как раз то, что мы хотели доказать.

Теперь покажем, что

$$\mathcal{A}(a) = a^0 \quad (1)$$

для каждого терма a теории T , свободного от переменных. Используем индукцию по длине a . Поскольку a свободен от переменных, он должен иметь вид $fa_1 \dots a_n$. Следовательно, применяя индуктивное предположение, получаем

$$\begin{aligned} \mathcal{A}(a) &= f_{\mathcal{A}}(\mathcal{A}(a_1), \dots, \mathcal{A}(a_n)) \\ &= f_{\mathcal{A}}(a_1^0, \dots, a_n^0) = a^0. \end{aligned}$$

Отсюда следует, что если A — атомная формула, свободная от переменных, то $\mathcal{A}(A) = \mathbf{I}$ тогда и только тогда, когда $\vdash_T A$. Действительно, для этого предположим, что A есть $pa_1 \dots a_n$, где p отлично от $=$. Тогда

$$\begin{aligned} \mathcal{A}(A) = \mathbf{I} &\leftrightarrow p_{\mathcal{A}}(\mathcal{A}(a_1), \dots, \mathcal{A}(a_n)) \\ &\leftrightarrow p_{\mathcal{A}}(a_1^0, \dots, a_n^0) \\ &\leftrightarrow \vdash_T A. \end{aligned}$$

Теперь предположим, что A есть $a = b$. Тогда

$$\begin{aligned} \mathcal{A}(A) = \mathbf{I} &\leftrightarrow \mathcal{A}(a) = \mathcal{A}(b) \\ &\leftrightarrow a^0 = b^0 \\ &\leftrightarrow a \sim b \\ &\leftrightarrow \vdash_T A. \end{aligned}$$

Мы показали, что атомная формула, свободная от переменных, истинна в $\mathcal{A}$ тогда и только тогда, когда она является теоремой. Это не обязательно верно для всех замкнутых формул по двум причинам. Во-первых, может оказаться, что термов, свободных от переменных, недостаточно; может быть, существует теорема, которая утверждает, что какой-то индивид имеет некоторое свойство и не существует терма, свободного от переменных, представляющего такой индивид. Во-вторых, теоремы могут не определять истинность или ложность всех замкнутых формул; может быть, существует замкнутая формула A такая, что ни A , ни $\neg A$ не являются теоремами. Теперь мы введем некоторые допущения о теории T , которые устраняют эти трудности.

Теория T называется *теорией Генкина*, если для каждого замкнутого утверждения $\exists x A$ теории T существует константа e такая, что $\vdash_T \exists x A \rightarrow A_x[e]$.

Формула A теории T называется *неразрешимой* в T , если ни A , ни $\neg A$ не являются теоремами теории T ; в противном случае A называется *разрешимой* в T . Теория T называется *полной*, если она непротиворечива и каждая замкнутая формула теории T разрешима в T . Это можно переформулировать так: T — полная теория, если для каждой замкнутой формулы A теории T в точности одна из формул A и $\neg A$ является теоремой теории T .

Позднее мы изучим в деталях полные теории. Заметим только, что неразумно требовать, чтобы каждая формула была разрешимой. Например, ни $x=0$, ни $x \neq 0$ не являются истинными для всех значений переменных; следовательно, мы не должны надеяться, чтобы какая-нибудь из них была теоремой.

Лемма 2. Пусть T — полная теория Генкина, $\mathcal{A}$ — каноническая структура для T , A — замкнутая формула теории T . Тогда $\mathcal{A}(A) = \mathbf{I}$ тогда и только тогда, когда A является теоремой теории T .

Доказательство. Используем индукцию по высоте A . Для атомных формул A результат уже был доказан. Предположим, что A есть $\neg B$. Тогда $\mathcal{A}(A) = \mathbf{I}$ тогда и только тогда, когда $\mathcal{A}(B) = \mathbf{J}$; следовательно, по индуктивному предположению тогда и только тогда, когда B не является теоремой теории T . Так как T полная, то это выполняется тогда и только тогда, когда A является теоремой теории T .

Предположим, что A есть $B \vee C$. Если $\mathcal{A}(A) = \mathbf{I}$, то $\mathcal{A}(B) = \mathbf{I}$ или $\mathcal{A}(C) = \mathbf{I}$; следовательно, по индуктивному предположению одна из формул B или C является теоремой теории T . По теореме тавтологии A — теорема теории T . Теперь предположим, что $\mathcal{A}(A) = \mathbf{J}$. Тогда

$$\mathcal{A}(B) = \mathcal{A}(C) = \mathbf{J};$$

следовательно, ни B , ни C не являются теоремами теории T . Ввиду полноты имеем $\vdash_T \neg B$ и $\vdash_T \neg C$; следовательно, $\vdash_T \neg A$ по теореме тавтологии. Ввиду непротиворечивости теории T формула A не является теоремой теории T .

Предположим, что A есть $\exists x B$. Тогда $\mathcal{A}(A) = \mathbf{I}$ тогда и только тогда, когда $\mathcal{A}(B_x[i]) = \mathbf{I}$ для некоторого i . Каждое i есть имя индивида a^0 . Так как $\mathcal{A}(a) = a^0$, то по лемме из § 2.5 следует, что $\mathcal{A}(B_x[i]) =$

$= \mathcal{A}(B_x[a])$. Следовательно, $\mathcal{A}(A) = \mathbf{I}$ тогда и только тогда, когда $\mathcal{A}(B_x[a]) = \mathbf{I}$ для некоторого терма a , свободного от переменных. По индуктивному предположению это выполняется тогда и только тогда, когда $\vdash_T B_x[a]$ для некоторого терма a , свободного от переменных. Поэтому мы должны доказать, что это последнее условие эквивалентно $\vdash_T A$. $B_x[a] \rightarrow A$ есть аксиома подстановки; следовательно, если $\vdash_T B_x[a]$ для некоторого a , то $\vdash_T A$ по правилу отделения. Теперь предположим, что $\vdash_T A$. Так как T — теория Генкина, то существует e такое, что $\vdash_T A \rightarrow B_x[e]$; следовательно, $\vdash_T B_x[e]$ по правилу отделения.

Следствие. Если T является полной теорией Генкина, то каноническая структура для T является моделью теории T .

Доказательство. Пусть A — нелогическая аксиома теории T , и пусть A' — замыкание формулы A . Тогда $\vdash_T A'$; следовательно, A' является истинной в $\mathcal{A}$ по лемме; поэтому A является истинной в $\mathcal{A}$.

Наша следующая проблема — посмотреть, как получать теории Генкина. Для этого введем некоторые определения.

Пусть L — язык первого порядка. Определим *специальные константы уровня n* индукцией по n . Предположим, что специальные константы всех уровней, меньших n , уже определены. Пусть $\exists x A$ — замкнутое подтверждение, образованное из этих констант и символов языка L . Если $n > 0$, то предположим также, что $\exists x A$ содержит по крайней мере одну специальную константу уровня $n-1$. Тогда символ, состоящий из буквы s с нижним индексом $\exists x A$, есть специальная константа уровня n , называемая специальной константой для $\exists x A$.

Язык, полученный из L добавлением всех специальных констант всех уровней, обозначим через L_c . Если $\exists x A$ — замкнутое подтверждение языка L_c , то в L_c существует единственная специальная константа для $\exists x A$; ее уровень есть наименьшее натуральное число, большее уровней всех специальных констант, входящих в $\exists x A$. Мы используем r, s и t в качестве синтаксических переменных, областью изменения которых являются специальные константы. Если r — специальная константа для $\exists x A$, то формула $\exists x A \rightarrow A_x[r]$ называется *специальной аксиомой для r* .

Пусть T — теория языка L . Обозначим через T_c теорию, язык которой есть L_c и нелогическими аксиомами которой являются нелогические аксиомы теории T и специальные аксиомы для специальных констант из L_c . Очевидно, что T_c есть теория Генкина.

Лемма 3. T_c является консервативным расширением теории T .

Доказательство. Пусть T' получается из T добавлением специальных констант (но не новых аксиом). По теореме о константах T' является консервативным расширением теории T ; таким образом, достаточно будет показать, что каждая формула A теории T , являющаяся теоремой теории T_c , есть теорема теории T . По теореме редукции получаем, что $\vdash_{T'} B_1 \rightarrow \dots \rightarrow B_k \rightarrow A$, где $B_1, \dots, B_k$ — различные специальные аксиомы. Теперь применим индукцию по k . Если $k=0$, то нечего доказывать. Пусть $k>0$. Можно считать, что уровень специальной константы r , для которой B_1 есть специальная аксиома, по крайней мере такой же большой, как уровни специальных констант, для которых $B_2, \dots, B_k$ являются специальными аксиомами. Тогда r не входит в $B_2, \dots, B_k$ и, конечно, в A . Отсюда по теореме о константах следует, что если B_1 есть $\exists x C \rightarrow C_x[r]$ и y — новая переменная, то

$$\vdash_{T'} (\exists x C \rightarrow C_x[y]) \rightarrow B_2 \rightarrow \dots \rightarrow B_k \rightarrow A.$$

Следовательно, по правилу $\exists$ -введения

$$\vdash_{T'} \exists y (\exists x C \rightarrow C_x[y]) \rightarrow B_2 \rightarrow \dots \rightarrow B_k \rightarrow A.$$

Теперь по теореме о варианте $\vdash_{T'} \exists x C \rightarrow \exists y C_x[y]$; таким образом, с помощью пренексных операций получаем $\vdash_{T'} \exists y (\exists x C \rightarrow C_x[y])$. Следовательно, $\vdash_{T'} B_2 \rightarrow \dots \rightarrow B_k \rightarrow A$ по правилу отделения; таким образом, $\vdash_{T'} A$ по индуктивному предположению.

Теперь нам нужен метод для получения полных теорий. Для этого нам будет нужен один результат из теории множеств, который мы приведем без доказательства. (Набросок доказательства см. в задаче 4 главы 9.)

Пусть E — множество и пусть J — какой-то класс подмножеств множества E . Скажем, что J имеет *конечный характер*, если для каждого подмножества A множества E множество A принадлежит J тогда и только тогда, когда

каждое конечное подмножество множества A принадлежит J . Множество A в J называется *максимальным элементом* из J , если A не является подмножеством никакого другого множества из J .

Лемма Тейхмюллера — Тьюки. Если J — непустой класс подмножеств множества E , имеющий конечный характер, то J содержит максимальный элемент.

Расширение T' теории T называется *простым* расширением, если T и T' имеют один и тот же язык.

Теорема Линденбаума. Если T — непротиворечивая теория, то T имеет полное простое расширение.

Доказательство. Пусть E — множество формул теории T . Пусть J — класс всех подмножеств A множества E таких, что $T[A]$ непротиворечива. Покажем, что J имеет конечный характер. Если A принадлежит J , то каждое подмножество A' множества A находится в J , так как $T[A]$ является расширением теории $T[A']$.

Предположим, что A не принадлежит J , так что $T[A]$ противоречива. Выберем формулу A теории T и доказательства формул A и $\neg A$ в $T[A]$. Пусть A' — множество формул из A , которые используются как нелогические аксиомы в этих доказательствах. Тогда A' — конечное подмножество из A и, значит, $T[A']$ противоречива; следовательно, A' не принадлежит J .

Пустое множество находится в J ; следовательно, по лемме Тейхмюллера — Тьюки существует максимальный элемент A из J . Ясно, что $T[A]$ — непротиворечивое простое расширение теории T ; покажем, что оно полное. Мы должны показать, что если A — замкнутая формула теории T , которая не является теоремой теории $T[A]$, то $\neg A$ — теорема теории $T[A]$. Пусть A' получается добавлением $\neg A$ к A . По следствию к теореме редукции для непротиворечивости получаем, что $T[A']$ непротиворечива; следовательно, A' принадлежит J . Ввиду максимальной A отсюда следует, что $A = A'$; таким образом, $\neg A$ принадлежит A . Следовательно, $\neg A$ — теорема теории $T[A]$.

Теперь легко доказать теорему полноты. Предположим, что T — непротиворечивая теория. Тогда по лемме 3 T_c — непротиворечивая теория. По теореме Линденбаума существует полное простое расширение U теории T_c . Так как U — простое расширение теории T_c , то U сама является теорией Генкина. Следовательно, по следствию

к лемме 2 U имеет модель. Так как U — расширение теории T , то T имеет модель по лемме 1.

Комбинируя наши леммы, можно также получить один результат, который будет полезен позднее.

Лемма 4. Пусть T — теория и U — непротиворечивое простое расширение теории T_c . Тогда U имеет модель $\mathcal{A}$ такую, что каждый индивид из $\mathcal{A}$ есть $\mathcal{A}(r)$ для бесконечного множества специальных констант r .

Доказательство. По теореме Линденбаума существует полное простое расширение U' теории U . Поскольку U' — теория Генкина, то каноническая структура $\mathcal{A}$ для U' есть модель теории U' и, следовательно, по лемме 1 модель для U . По (1) каждый индивид a из $\mathcal{A}$ есть $\mathcal{A}(a)$ для некоторого терма a , свободного от переменных. По аксиомам тождества и теореме подстановки получаем $\vdash_U \exists x (x = a)$; таким образом, если r — специальная константа для $\exists x (x = a)$, то $\vdash_U r = a$. Отсюда следует, что $\mathcal{A}(r) = \mathcal{A}(a) = a$. Заменяя x другими переменными, мы можем найти бесконечно много других специальных констант с тем же свойством.

Каждая форма теоремы полноты устанавливает эквивалентность между некоторым синтаксическим понятием и некоторым семантическим понятием. Из них можно получить много других таких же эквивалентностей. Дадим один пример.

Следствие. Пусть T и T' — теории с одним и тем же языком. Тогда T есть расширение теории T' тогда и только тогда, когда каждая модель для T' есть модель для T . Следовательно, T и T' эквивалентны тогда и только тогда, когда они имеют одни и те же модели.

Доказательство. Условие необходимо ввиду леммы 1. Если условие выполняется, то каждая формула, истинная в T , является истинной и в T' ; таким образом, каждая теорема теории T есть теорема теории T' по первой форме теоремы полноты.

Укажем одно применение этого следствия. Как хорошо известно, существует большое количество множеств аксиом для групп, отличных от тех, которые мы формализовали в G . Предположим, что мы формализуем одно из этих множеств в теории G' с тем же языком, что и у G . Тогда G и G' имеют одни и те же модели (а именно, группы) и, следовательно, являются эквивалентными.

4.3. Теорема непротиворечивости

Проблема характеристики имеет дело только с конкретными объектами. Решение проблемы характеристики, данное с помощью теоремы полноты, использует, однако, модели, которые являются абстрактными объектами. Поэтому естественно поискать финитное решение проблемы характеристики для теорий. Мы дадим такое решение в этом и следующем параграфе.

Теория называется *открытой*, если все ее нелогические аксиомы открыты. В этом параграфе мы рассмотрим специальный случай проблемы характеристики для теорий, а именно, проблему непротиворечивости для открытых теорий.

Пусть r — специальная константа для $\exists x A$. Формула относится к r , если она является специальной аксиомой языка $L(T_c)$ для r или замкнутой аксиомой подстановки вида $A_x[a] \rightarrow \exists x A$. Обозначим через $\Delta(T)$ множество всех формул теории T_c , которые относятся к специальным константам или являются замкнутыми частными случаями аксиом тождества, аксиом равенства или нелогических аксиом теории T .

Лемма 1. Если $\vdash_T A$ и A' — замкнутый частный случай формулы A языка $L(T_c)$, то A' есть тавтологическое следствие формул из $\Delta(T)$.

Доказательство. Используем индукцию по теоремам (в форме, описанной в § 3.1). Если A — аксиома подстановки, то A' — замкнутая аксиома подстановки и, следовательно, принадлежит $\Delta(T)$. Если A является аксиомой тождества, аксиомой равенства или нелогической аксиомой, то ясно, что A' принадлежит $\Delta(T)$. Если A — тавтологическое следствие $B_1, \dots, B_n$, то A' — тавтологическое следствие замкнутых частных случаев $B'_1, \dots, B'_n$ формул $B_1, \dots, B_n$ соответственно. По индуктивному предположению $B'_1, \dots, B'_n$ — тавтологические следствия формул из $\Delta(T)$; следовательно, такова же и A' . Наконец, предположим, что A есть $\exists x B \rightarrow C$ и A выводится из $B \rightarrow C$ по правилу $\exists$ -введения. Тогда A' есть $\exists x B' \rightarrow C'$. Если r — специальная константа для $\exists x B'$, то $B'_x[r] \rightarrow C'$ — замкнутый частный случай формулы $B \rightarrow C$, и, следовательно, по индуктивному предположению, есть тавтологическое следствие формул из $\Delta(T)$. Поскольку

A' — тавтологическое следствие $B'_x[r] \rightarrow C'$ и специальной аксиомы $\exists x B' \rightarrow B'_x[r]$, то A' есть тавтологическое следствие формул из $\Delta(T)$.

Формула называется *квазитавтологией*, если она есть тавтологическое следствие некоторых частных случаев аксиом тождества и аксиом равенства.

Теорема непротиворечивости (Гильберт — Аккерман). *Открытая теория T является противоречивой тогда и только тогда, когда существует квазитавтология, которая представляет собой дизъюнкцию отрицаний некоторых частных случаев нелогических аксиом теории T .*

Доказательство. Предположим, что $\bigvee \bigwedge A_n$ является такой квазитавтологией. Тогда все $A_1, \dots, A_n$ и $\bigwedge A_1 \vee \dots \vee \bigwedge A_n$ являются теоремами теории T ; следовательно, по теореме тавтологии T противоречива.

Теперь предположим, что T противоречива. Пусть r — любая специальная константа в T_c . Тогда $r \neq r$ есть частный случай теоремы $x \neq x$ теории T ; следовательно, по лемме 1 существуют формулы $A_1, \dots, A_k$ из $\Delta(T)$ такие, что формула $A_1 \rightarrow \dots \rightarrow A_k \rightarrow r \neq r$ является тавтологией. Поскольку $r = r$ принадлежит $\Delta(T)$, можно предположить, что это есть одна из A_i . Тогда $\bigwedge A_1 \vee \dots \vee \bigwedge A_k$ — тавтология.

Рангом специальной константы для $\exists x A$ называется число вхождений $\exists$ в формулу $\exists x A$; ранг по крайней мере равен 1. Пусть $\Delta_n(T)$ — множество, полученное из $\Delta(T)$ опусканием формул, относящихся к специальным константам ранга, большего n . Таким образом, $\Delta_0(T)$ состоит из свободных от переменных частных случаев аксиом тождества, аксиом равенства и нелогических аксиом теории T в языке $L(T_c)$.

Мы называем $A_1, \dots, A_k$ *специальной последовательностью*, если $\bigwedge A_1 \vee \dots \vee \bigwedge A_k$ — тавтология; т. е. если не существует истинностной оценки V такой, что $V(A_i) = \text{И}$ для всех i . Мы уже видели, что существует специальная последовательность, все формулы которой принадлежат $\Delta(T)$ и, следовательно, все принадлежат $\Delta_n(T)$ для некоторого n . Предположим, что мы имеем специальную последовательность формул из $\Delta_0(T)$. Заменяя каждую специальную константу новой переменной, мы получаем специальную последовательность, формулы которой являются

частными случаями аксиом тождества, аксиом равенства и нелогических аксиом теории T в языке $L(T)$. Если $A_1, \dots, A_k$ — все частные случаи нелогических аксиом, входящих в эту последовательность, то ясно, что $\bigwedge A_1 \vee \dots \vee \bigwedge A_k$ является квазитавтологией. Отсюда следует, что доказательство сводится к доказательству следующей леммы.

Лемма 2. *Если $n > 0$ и существует специальная последовательность, состоящая из формул, принадлежащих $\Delta_n(T)$, то существует специальная последовательность, состоящая из формул, принадлежащих $\Delta_{n-1}(T)$.*

Доказательство. По предположению существует специальная последовательность, состоящая из формул, принадлежащих $\Delta_{n-1}(T)$, и формул, относящихся к специальным константам ранга n . Докажем заключение леммы индукцией по числу этих констант ранга n . Если таких констант нет, то доказывать нечего; поэтому мы предположим, что существует по крайней мере одна такая константа. Пусть r — та константа, которая имеет наивысший из возможных уровней, и пусть $r_1, \dots, r_s$ — остальные константы ранга n . Мы построим специальную последовательность, состоящую из формул, принадлежащих $\Delta_{n-1}(T)$, и формул, относящихся к $r_1, \dots, r_s$; ввиду индуктивного предположения доказательство теоремы будет завершено.

Пусть $A_1, \dots, A_r$ — все формулы из данной специальной последовательности, которые принадлежат $\Delta_{n-1}(T)$ или относятся к одной из констант $r_1, \dots, r_s$. Пусть остальными формулами из данной специальной последовательности будут специальная аксиома $\exists x B \rightarrow B_x[r]$ для r и формулы

$$B_x[a_i] \rightarrow \exists x B, \quad i = 1, \dots, p.$$

Покажем, что среди A_i нет формулы, содержащей вхождения $\exists x B$. Это сразу ясно в случае, когда A_i является частным случаем аксиомы тождества, аксиомы равенства или нелогической аксиомы, так как тогда A_i открыта. Предположим, что A_i является формулой $\exists y C \rightarrow C_y[s]$ или $C_y[a] \rightarrow \exists y C$, относящейся к s . Поскольку ранг r не меньше ранга s , то $\exists x B$ содержит не меньше вхождений символа $\exists$, чем $\exists y C$. Следовательно, $\exists x B$ не может входить в $C_y[s]$ или в $C_y[a]$. $\exists x B$ не может входить

в $\exists yC$, кроме случая, когда $\exists yC$ есть $\exists xB$. Но это невозможно, так как s отлично от r .

Если в нашей данной специальной последовательности мы заменим каждое вхождение $\exists xB$ на $B_x[r]$, то мы получим новую специальную последовательность. (Это следует из замечания в § 3.1.) Эти замены не затронут A_i . При них $\exists xB \rightarrow B_x[r]$ перейдет в тавтологию $B_x[r] \rightarrow B_x[r]$, а $B_x[a_i] \rightarrow \exists xB$ — в $B_x[a_i] \rightarrow B_x[r]$. Отсюда следует, что

$$A_1, \dots, A_r, B_x[a_1] \rightarrow B_x[r], \dots, B_x[a_p] \rightarrow B_x[r] \quad (1)$$

является специальной последовательностью.

Пусть для каждого выражения u языка $L(T_c)$ выражение $u^{(i)}$ получается из u заменой r везде (в том числе и внутри нижних индексов у специальных констант) на a_i . Если $C_1, \dots, C_k$ — специальная последовательность, то такова же и $C_1^{(i)}, \dots, C_k^{(i)}$ (по тому же замечанию из § 3.1). Применяя это к (1) и замечая, что $B_x[r]^{(i)}$ есть $B_x[a_i]$, потому что r не встречается в B , получаем специальную последовательность

$$A_1^{(i)}, \dots, A_r^{(i)}, B_x[a_1]^{(i)} \rightarrow B_x[a_i], \dots, B_x[a_p]^{(i)} \rightarrow B_x[a_i]. \quad (2)$$

Теперь мы утверждаем, что последовательность, состоящая из всех A_i и всех $A_i^{(j)}$ ($i=1, \dots, r; j=1, \dots, p$) является специальной последовательностью. Для этого предположим, что существует истинностная оценка V , дающая значение $\mathbf{I}$ для всех этих формул. Согласно (2) для каждого i оценка V будет давать значение $\mathbf{I}$ некоторой формуле $B_x[a_j]^{(i)} \rightarrow B_x[a_i]$. Таким образом, $V(B_x[a_i]) = \mathbf{I}$ для всех i ; следовательно, V дает значение $\mathbf{I}$ каждой формуле $B_x[a_i] \rightarrow B_x[r]$. Это невозможно по (1).

Теперь достаточно показать, что каждая $A_i^{(j)}$ либо принадлежит $\Delta_{n-1}(T)$, либо относится к одной из констант $r_1, \dots, r_s$. Если A — частный случай аксиомы тождества, аксиомы равенства или нелогической аксиомы теории T , то такова же $A_i^{(j)}$. Теперь предположим, что A_i — предложение $\exists yC \rightarrow C_y[s]$ или $C_y[a] \rightarrow \exists yC$, относящееся к s . Тогда $A_i^{(j)}$ есть

$$\exists yC^{(j)} \rightarrow C_y^{(j)}[s^{(j)}]$$

или

$$C_y^{(j)}[a^{(j)}] \rightarrow \exists yC^{(j)}.$$

Поскольку s отлично от r , то ясно, что $s^{(j)}$ — специальная константа для $\exists yC^{(j)}$. Следовательно, $A_i^{(j)}$ — предложение, относящееся к $s^{(j)}$. Ясно, что s и $s^{(j)}$ имеют одинаковый ранг. Следовательно, если A_i относится к $\Delta_{n-1}(T)$, то такова же и $A_i^{(j)}$. Предположим, что s есть одно из $r_1, \dots, r_s$. Поскольку уровень r не меньше уровня s , то r не входит в $\exists yC$ и, следовательно, не входит в s . Значит, $s^{(j)}$ есть s и $A_i^{(j)}$ относится к одной из констант $r_1, \dots, r_s$.

Комбинируя то, что $\mathcal{N}$ есть модель для теории N , с теоремой полноты, получаем доказательство непротиворечивости теории N . Теперь укажем, как можно превратить это доказательство в финитное доказательство непротиворечивости теории N . Сначала заменим все индивиды из $\mathcal{N}$ конкретными объектами. Для этого достаточно заменить натуральное число n выражением, состоящим из n черточек. Затем замечаем, что если даются свободные от переменных терм a или формула A , то мы в действительности можем вычислить $\mathcal{N}(a)$ или $\mathcal{N}(A)$. Отсюда следует, что в некоторых случаях можно дать финитное доказательство того, что некоторая открытая формула A языка $L(N)$ истинна в $\mathcal{N}$. В частности, можно доказать, что каждый частный случай нелогической аксиомы теории N является истинной формулой в $\mathcal{N}$ и каждая открытая квазитавтология является истинной в $\mathcal{N}$. Теперь ясно, что невозможно найти открытые формулы $A_1, \dots, A_n$ такие, что все $A_1, \dots, A_n$ и $\neg A_1 \vee \dots \vee \neg A_n$ являются истинными в $\mathcal{N}$; следовательно, по теореме непротиворечивости теория N непротиворечива.

Итак, мы имеем два доказательства непротиворечивости теории N : одно финитное и одно нефинитное. Так как финитное доказательство более длинное, то естественно спросить: какие дополнительные выгоды мы можем извлечь из финитного доказательства?

Прежде всего, как упоминалось ранее, финитные доказательства могут пролить свет на природу конкретного и абстрактного. Например, финитное доказательство непротиворечивости теории N показывает, что точка зрения Гильберта на абстрактную математику, обсуждавшаяся

в § 1.2, подходит для N . Можно считать, что формулы теории N , свободные от переменных, выражают конкретные результаты, а кванторы являются абстрактными понятиями, введенными для доказательства конкретных результатов. Тогда наше доказательство непротиворечивости показывает, что любой такой конкретный результат является правильным, т. е. что любая формула A , свободная от переменных и доказуемая в N , является истинной в $\mathcal{N}$. В противном случае $\neg A$ должна быть истинной в $\mathcal{N}$, и вышеприведенное доказательство показывало бы, что $N[\neg A]$ непротиворечива, что противоречит следствию к теореме редукции для непротиворечивости.

Далее, финитное доказательство часто дает больше информации, чем абстрактное доказательство, просто потому, что ограничение финитными методами часто заставляет нас доказывать больше, чем нужно для того, чтобы получить требуемый результат. Например, наше абстрактное доказательство непротиворечивости теории N основано на доказательстве того, что каждая теорема теории N является истинной. Так как истинность формулы теории N не является финитным понятием, финитное доказательство должно доказывать нечто более сильное о теоремах теории N . Если мы более внимательно проанализируем доказательство, то найдем, что можно действительно построить формулу, которая является истинной, но не имеет этого более сильного свойства. Таким образом, мы получаем истинную формулу теории N , которая не является теоремой теории N . Мы не будем сейчас рассматривать эту конструкцию, так как подобный результат про другую теорию будет рассмотрен в главе 8.

4.4. Теорема Эрбрана

Перейдем теперь к финитному решению проблемы характеристики для теорий. Так как доказательство теоремы редукции финитно, достаточно дать решение этой проблемы для теорий, у которых нет нелогических аксиом. Ввиду результатов из § 3.5 достаточно дать решение для формул в пренексной форме. Мы даже можем ограничиться замкнутыми формулами в пренексной форме; это следует из теоремы замыкания и того, что замыкание

формулы в пренексной форме находится в пренексной форме.

Формула в пренексной форме называется *экзистенциальной*, если все кванторы в ее приставке являются кванторами существования. Начнем с решения проблемы характеристики для замкнутых экзистенциальных формул.

Лемма 1. Пусть T — теория, не имеющая нелогических аксиом. Замкнутая экзистенциальная формула A является теоремой теории T тогда и только тогда, когда существует квазитавтология, являющаяся дизъюнкцией частных случаев матрицы формулы A .

Доказательство. Предположим, что A есть $\exists x_1 \dots \exists x_n B$, где B — открытая формула. По следствию к теореме редукции для непротиворечивости A является теоремой тогда и только тогда, когда теория $T[\neg A]$ является противоречивой. Применяя пренексные операции и теорему замыкания, получаем, что теория $T[\neg A]$ эквивалентна теории $T[\neg B]$. Следовательно, A является теоремой тогда и только тогда, когда теория $T[\neg B]$ противоречива. По теореме непротиворечивости это выполняется тогда и только тогда, когда существует квазитавтология $\neg \neg B_1 \vee \dots \vee \neg \neg B_n$, где каждое B_i есть некоторый частный случай формулы B . Поскольку $\neg \neg B_1 \vee \dots \vee \neg \neg B_n$ — квазитавтология тогда и только тогда, когда формула $B_1 \vee \dots \vee B_n$ является квазитавтологией, мы получаем доказательство леммы.

Перед тем как дать полное решение проблемы характеристики, мы вводим одно расширение T'_c теории T_c . Под *специальной аксиомой равенства* мы понимаем формулу

$$\forall x (A \leftrightarrow B) \rightarrow r = s,$$

где r и s являются специальными константами для $\exists x A$ и $\exists x B$ соответственно. Мы получаем теорию T'_c из теории T_c добавлением всех специальных аксиом равенства в качестве новых нелогических аксиом.

Лемма 2. Теория T'_c является консервативным расширением теории T .

Доказательство. Допустим, что $T[r_1, \dots, r_n]$ — теория, полученная из T добавлением констант $r_1, \dots, r_n$, специальных аксиом и специальных аксиом равенства, которые содержат только эти специальные константы. Как и в доказательстве леммы 3 из § 4.2, всё сводится к

доказательству следующего: если уровень r_i не превосходит уровня r для $i=1, \dots, n$, то $T[r_1, \dots, r_n, r]$ является консервативным расширением теории $T[r_1, \dots, r_n]$. Покажем, что если формула A теории $T[r_1, \dots, r_n]$ имеет доказательство в теории $T[r_1, \dots, r_n, r]$, то формула A имеет такое доказательство, которое не использует специальных аксиом равенства, содержащих r ; тогда мы можем завершить доказательство леммы так же, как и в лемме 3 из § 4.2.

Заметим, что для каждой специальной константы, встречающейся в левой части специальной аксиомы равенства, существует специальная константа более высокого уровня, встречающаяся в правой части. Отсюда следует, что специальная аксиома равенства в нашем данном доказательстве формулы A может содержать r только в правой части. Можно предполагать, что все эти аксиомы имеют вид $\forall x (B \leftrightarrow C) \rightarrow r = s$; действительно, $\forall x (C \leftrightarrow B) \rightarrow s = r$ можно вывести из $\forall x (B \leftrightarrow C) \rightarrow r = s$ по теореме эквивалентности. Можно также предполагать, что ни одна из этих аксиом не имеет правую часть вида $r = r$; такую аксиому можно было бы вывести из аксиом тождества.

Пусть $\forall x (B \leftrightarrow C) \rightarrow r = s$ является одной из этих специальных аксиом равенства в данном доказательстве формулы A . Пусть T' — теория, полученная из $T[r_1, \dots, r_n]$ добавлением константы r и двух аксиом $r = s$ и $\forall x (B \leftrightarrow C)$. Покажем, что A является теоремой теории T' . Для этого достаточно доказать в T' все те нелогические аксиомы из данного доказательства формулы A , которые содержат r . Прежде всего мы можем вывести $B \leftrightarrow C$ и, следовательно, $B_x[r] \leftrightarrow C_x[r]$ из аксиомы $\forall x (B \leftrightarrow C)$. Из $B_x[r] \leftrightarrow C_x[r]$ и $r = s$ мы выводим по теореме равенства $B_x[r] \leftrightarrow C_x[s]$. Затем мы можем по теореме эквивалентности вывести специальную аксиому $\exists x B \rightarrow B_x[r]$ для r из специальной аксиомы $\exists x C \rightarrow C_x[s]$ для s . Теперь рассмотрим специальную аксиому равенства $\forall x (B \leftrightarrow D) \rightarrow r = t$, входящую в данное доказательство формулы A . Мы можем вывести ее по теоремам эквивалентности и равенства из специальной аксиомы равенства $\forall x (C \leftrightarrow D) \rightarrow s = t$ (которая не содержит r).

Так как $\vdash_{T'} A$, то по теореме дедукции и теореме о константах следует, что формула

$$y = s \rightarrow \forall x (B \leftrightarrow C) \rightarrow A$$

является теоремой теории $T[r_1, \dots, r_n]$. Подставляя s вместо y и используя аксиомы тождества, получаем, что формула $\forall x (B \leftrightarrow C) \rightarrow A$ является теоремой теории $T[r_1, \dots, r_n]$. По теореме тавтологии отсюда следует, что $\vdash (\forall x (B \leftrightarrow C) \rightarrow r = s) \rightarrow A$ доказуемо в $T[r_1, \dots, r_n, r]$ без применения нелогических аксиом, содержащих r .

Теперь пусть $D_1, \dots, D_k$ — специальные аксиомы равенства, содержащие r и используемые в данном доказательстве формулы A . По теореме дедукции формула $D_1 \rightarrow \dots \rightarrow D_k \rightarrow A$ имеет доказательство, не использующее специальные аксиомы равенства, содержащие r . Мы только что показали, что каждая формула $\vdash D_i \rightarrow A$ также имеет такое же доказательство. Таким образом, по теореме тавтологии и A имеет такое же доказательство.

Сделаем следующее замечание о теории T'_c . Пусть r — специальная константа для формулы $\exists x \neg A$. Тогда $\exists x \neg A \rightarrow \neg A_x[r]$ — аксиома теории T'_c . Приводя левую часть к пренексной форме и используя теорему тавтологии, получаем

$$\vdash_{T'_c} A_x[r] \rightarrow \forall x A. \quad (1)$$

Теперь возвратимся к проблеме характеристики. Мы свяжем некоторую замкнутую экзистенциальную формулу A_H с каждой замкнутой формулой A , находящейся в пренексной форме. Если A — экзистенциальная формула, то A_H есть A . В противном случае A имеет вид $\exists x_1 \dots \exists x_n \forall y B$ ($n \geq 0$). Вводим новый n -арный функциональный символ f , и пусть A^* будет $\exists x_1 \dots \exists x_n B_y[f x_1 \dots x_n]$. Тогда A^* имеет на один квантор всеобщности меньше, чем A . Если A^* — не экзистенциальная формула, то строим A^{**} , A^{***} и т. д., пока не придем к экзистенциальной формуле. Эта экзистенциальная формула и есть A_H .

Теорема Эрбрана. Пусть T — теория, не имеющая нелогических аксиом и A — замкнутая формула теории T , находящаяся в пренексной форме. Тогда A является теоремой теории T тогда и только тогда, когда существует квазитавтология, являющаяся дизъюнкцией частных случаев матрицы формулы A_H .

Доказательство. Пусть T' получена из T добавлением новых функциональных символов из A_H . Покажем, что $\vdash_{T'} A$ тогда и только тогда, когда $\vdash_{T'} A_H$; тогда по лемме 1 будет сразу следовать теорема.

Применяя обозначения, используемые при определении A_H , по теореме подстановки получаем $\vdash_T \forall y B \rightarrow B_y [fx_1 \dots x_n]$ и, следовательно, по правилу дистрибутивности $\vdash_T A \rightarrow A^*$. Аналогично получаем $\vdash_T A^* \rightarrow A^{**}$, $\vdash_T A^{**} \rightarrow A^{***}$ и т. д.; следовательно, $\vdash_T A \rightarrow A_H$. Если $\vdash_T A$, то $\vdash_T A$; следовательно, по правилу отделения $\vdash_T A_H$.

Доказывая обратное утверждение, для простоты предположим, что A есть $\exists x \forall y \exists z \forall w B$ с открытой формулой B . (Однако метод доказательства будет совершенно общим.) Когда B записывается с квадратными скобками, то подразумевается, что переменными в этих скобках являются x, y, z, w . Поэтому можно A переписать в виде

$$\exists x \forall y \exists z \forall w B[x, y, z, w],$$

а формулой A_H будет

$$\exists x \exists z B[x, fx, z, g(x, z)].$$

Введем теперь следующее обозначение: если a и b — термы теории T'_c , свободные от переменных, тогда $r(a)$ — специальная константа для

$$\exists y \neg \exists z \forall w B[a, y, z, w]$$

и $s(a, b)$ — специальная константа для

$$\exists w \neg B[a, r(a), b, w].$$

Из (1) и теоремы подстановки получаем в T'_c :

$$\begin{aligned} &\vdash B[a, r(a), b, s(a, b)] \rightarrow \forall w B[a, r(a), b, w], \\ &\vdash \forall w B[a, r(a), b, w] \rightarrow \exists z \forall w B[a, r(a), z, w], \\ &\vdash \exists z \forall w B[a, r(a), z, w] \rightarrow \forall y \exists z \forall w B[a, y, z, w], \\ &\vdash \forall y \exists z \forall w B[a, y, z, w] \rightarrow \exists x \forall y \exists z \forall w B[x, y, z, w]. \end{aligned}$$

Следовательно,

$$\vdash B[a, r(a), b, s(a, b)] \rightarrow A. \quad (2)$$

Имеем также

$$\vdash a = a' \rightarrow r(a) = r(a') \quad (3)$$

и

$$\vdash a = a' \rightarrow b = b' \rightarrow s(a, b) = s(a', b'). \quad (4)$$

Чтобы доказать (3), используем специальную аксиому

равенства

$$\forall y (\neg \exists z \forall w B[a, y, z, w] \leftrightarrow \neg \exists z \forall w B[a', y, z, w]) \rightarrow \rightarrow r(a) = r(a')$$

и теорему равенства. Чтобы доказать (4), используем (3), специальную аксиому равенства

$$\forall w (\neg B[a, r(a), b, w] \leftrightarrow \neg B[a', r(a'), b', w]) \rightarrow \rightarrow s(a, b) = s(a', b')$$

и теорему равенства.

Теперь предположим, что $\vdash_T A_H$. По лемме 1 существует квазитавтология

$$B[a_1, fa_1, b_1, ga_1b_1] \vee \dots \vee B[a_n, fa_n, b_n, ga_nb_n], \quad (5)$$

где a_i и b_i — термы языка $L(T')$. Теперь изменим (5) следующим образом. Во-первых, заменим каждую переменную некоторой специальной константой. Затем выберем часть вида fa или gab , где a и b не содержат f или g . Если выбранная часть есть fa , то заменим ее везде на $r(a)$; если выбранная часть есть gab , заменяем ее везде на $s(a, b)$. Продолжаем делать такие замены до тех пор, пока мы не устраним все вхождения f и g . Получим окончательную формулу

$$B[a'_1, r(a'_1), b'_1, s(a'_1, b'_1)] \vee \dots \vee B[a'_n, r(a'_n), b'_n, s(a'_n, b'_n)] \quad (6)$$

теории T'_c . Покажем, что (6) является теоремой теории T'_c . Тогда по (2) и теореме тавтологии получим, что A является теоремой теории T'_c и, следовательно, по лемме 2 теоремой теории T .

Формула (5) является тавтологическим следствием частных случаев $C_1, \dots, C_r$ аксиом тождества и равенства. Если мы проделаем те же преобразования над $C_1, \dots, C_r$, которые мы делали, чтобы получить (6) из (5), мы получим формулы $C'_1, \dots, C'_r$. По замечанию из § 3.1 формула (6) является тавтологическим следствием формул $C'_1, \dots, C'_r$; следовательно, нам нужно лишь доказать формулу C'_i в теории T'_c . Но C'_i — снова частный случай аксиомы тождества или равенства, если только C_i не является частным случаем аксиомы равенства.

$x = x' \rightarrow fx = fx'$ или $x = x' \rightarrow y = y' \rightarrow gxy = gx'y'$. В этом случае C'_i является теоремой по (3) и (4). Это завершает доказательство теоремы Эрбрана.

4.5. Добавление функциональных символов

Существует такой тип рассуждений, часто используемый в математике, который мы еще не рассматривали. Для его иллюстрации допустим, что мы рассматриваем натуральные числа, и доказали, что для каждого числа x существует простое число y такое, что $y > x$. В ходе более позднего доказательства мы могли сказать: пусть y будет простым числом таким, что $y > x$. В оставшейся части доказательства мы должны помнить, что y зависит от x . Если мы желаем указать эту зависимость с помощью какого-то обозначения, то вместо этого мы могли бы сказать: для каждого x пусть $f(x)$ будет простое число, большее x . Конечно, f должен быть новым символом, не встречающимся в том утверждении, которое мы хотим доказать. Наш следующий результат показывает, что аналогичный метод, примененный к теории T , не приводит нас к утверждениям, которые не могут быть доказаны в T .

Теорема о функциональных расширениях. Пусть $x, y_1, \dots, y_n$ — различные переменные и $\exists x A$ — теорема теории T , в которой нет свободных переменных, отличных от $y_1, \dots, y_n$. Пусть T' — теория, полученная из T добавлением нового n -арного функционального символа f и новой нелогической аксиомы $A_x[fy_1 \dots y_n]$. Тогда теория T' является консервативным расширением теории T .

Доказательство. Ввиду теоремы замыкания достаточно доказать, что каждая замкнутая формула B теории T , являющаяся теоремой теории T' , является теоремой теории T . По теореме редукции существует доказательство (не использующее нелогических аксиом) формулы

$$\forall y_1 \dots \forall y_n A_x[fy_1 \dots y_n] \rightarrow C_1 \rightarrow \dots \rightarrow C_k \rightarrow B, \quad (1)$$

где каждое C_i есть замыкание некоторой нелогической аксиомы теории T . Пусть C является пренексной формой формулы $A \rightarrow C_1 \rightarrow \dots \rightarrow C_k \rightarrow B$. Тогда формула $\exists y_1 \dots \exists y_n C_x[fy_1 \dots y_n]$ является пренексной формой формулы (1), и следовательно, эта формула доказуема без нелогических аксиом.

Пусть D — формула $\exists y_1 \dots \exists y_n \forall x C$. Тогда D не содержит f . Если мы используем f в качестве нового

функционального символа при образовании D^* , как это делалось в последнем параграфе, то D^* есть

$$\exists y_1 \dots \exists y_n C_x[fy_1 \dots y_n];$$

таким образом, D^* доказуема без нелогических аксиом. Так как D_H — то же самое, что и D_H^* , то из теоремы Эрбрана следует, что D также доказуема без нелогических аксиом и, следовательно, есть теорема теории T . Отсюда и из теоремы эквивалентности получаем

$$\vdash_T \exists y_1 \dots \exists y_n \forall x (A \rightarrow C_1 \rightarrow \dots \rightarrow C_k \rightarrow B).$$

Поэтому с помощью пренексных операций получаем

$$\vdash_T \forall y_1 \dots \forall y_n \exists x A \rightarrow C_1 \rightarrow \dots \rightarrow C_k \rightarrow B.$$

Поскольку $\forall y_1 \dots \forall y_n \exists x A, C_1, \dots, C_k$ — теоремы теории T , то по правилу отделения получаем, что B — теорема теории T .

Формула называется универсальной, если она находится в пренексной форме и все кванторы в ее приставке являются кванторами всеобщности. Мы свяжем некоторую замкнутую универсальную формулу A_S с каждой замкнутой формулой A , находящейся в пренексной форме. Если A — универсальная формула, то A_S есть A . В противном случае A имеет вид $\forall x_1 \dots \forall x_n \exists y B$ ($n \geq 0$). Вводим новый n -арный функциональный символ f , и пусть A° будет $\forall x_1 \dots \forall x_n B_y[f x_1 \dots x_n]$. Тогда A° имеет на один квантор существования меньше, чем A . Если A° — не универсальная формула, то строим $A^{\circ\circ}, A^{\circ\circ\circ}$ и т. д. до тех пор, пока не придем к универсальной формуле. Это универсальная формула и есть A_S .

Применяя несколько раз теорему о функциональных расширениях, получаем, что если A — замкнутая формула в пренексной форме, являющаяся теоремой теории T , и если T' получена из T добавлением функциональных символов из формулы A_S и новой нелогической аксиомы A_S , то теория T' является консервативным расширением теории T . Заметим также, что формула $A_S \rightarrow A$ доказуема без нелогических аксиом. Очевидно, для этого достаточно показать, что так может быть доказана

формула $A^\circ \rightarrow A$. Теперь в вышеприведенных обозначениях $B_y[fx_1 \dots x_n] \rightarrow \exists y B$ является аксиомой подстановки; следовательно, по правилу дистрибутивности получаем $A^\circ \rightarrow A$.

Теорема Скулема. *Каждая теория имеет открытое консервативное расширение.*

Доказательство. Пусть T — теория. Пусть T_1 получена из T заменой каждой нелогической аксиомы на замыкание одной из ее пренексных форм. По § 3.5 и теореме замыкания T_1 эквивалентна T . Далее, получаем T_2 из T_1 следующим образом: для каждой нелогической аксиомы A теории T_1 добавим функциональные символы из A_S и добавим A_S в качестве новой аксиомы. Применяя предыдущие результаты и то, что любое доказательство в T_2 может использовать только конечное число новых функциональных символов и аксиом, видим, что теория T_2 является консервативным расширением теории T_1 . Далее, получаем T_3 из T_2 , отбрасывая нелогические аксиомы теории T_1 . Поскольку $A_S \rightarrow A$ доказуема без нелогических аксиом, эти отброшенные аксиомы доказуемы в T_3 ; следовательно, T_3 эквивалентна T_2 . Нелогические аксиомы теории T_3 являются универсальными формулами. Затем получаем T_4 из T_3 заменой каждой нелогической аксиомы ее матрицей. Тогда T_4 — открытая теория и по теореме замыкания T_4 эквивалентна T_3 , а следовательно, теория T_4 является консервативным расширением теории T .

Одним из приложений теоремы Скулема является получение финитного доказательства непротиворечивости для теорий, не являющихся открытыми. Для такой теории T строим консервативное открытое расширение T' теории T и затем доказываем, что T' является непротиворечивой теорией, с помощью метода из § 4.3. Если нелогические аксиомы теории T достаточно просты, этот метод вполне эффективен. Однако если теория T имеет сложные нелогические аксиомы, то теория T' может быть так сложна, что не существует модели теории T' , которую можно описать финитным образом; может случиться также, что все такие модели так сложны, что обращаться с ними неудобно.

4.6. Расширения с помощью определений

Теперь перейдем к проблеме определения в теории новых функциональных и предикатных символов. Для иллюстрации проблемы предположим, что мы хотим ввести $\leq$ в N . Мы можем сделать это с помощью соглашения, что $a \leq b$ является сокращением для $a < b \vee a = b$. Имеется одна трудность, которая состоит в том, что тогда $\leq$ является определяемым символом и поэтому не является предикатным символом.

Более удовлетворительная процедура состоит в образовании расширения N' из N добавлением нового бинарного предикатного символа $\leq$ и новой аксиомы

$$x \leq y \leftrightarrow x < y \vee x = y.$$

Из этой новой аксиомы можно доказать

$$a \leq b \leftrightarrow a < b \vee a = b$$

по правилу подстановки, а затем мы можем применять теорему эквивалентности для замены $a \leq b$ на $a < b \vee a = b$ и наоборот.

Мы хотим показать, что переход от N к N' является не более чем введением определяемого символа $\leq$ в N . Чтобы сделать это строго, допустим, что A — формула теории N' . Если мы считаем $\leq$ определяемым символом в N , то A — определяемая формула теории N , которая сокращает некоторую формулу A^* теории N . Мы хотим показать, что $\vdash_{N'} A$ тогда и только тогда, когда $\vdash_N A^*$.

Теперь рассмотрим общую ситуацию. Мы имеем теорию T , различные переменные $x_1, \dots, x_n$ и формулу D теории T , в которой нет свободных переменных, отличных от $x_1, \dots, x_n$. Образует T' из T добавлением нового n -арного предикатного символа p и новой нелогической аксиомы $px_1 \dots x_n \leftrightarrow D$, которую мы называем *определяющей аксиомой* для p .

Для данной формулы A теории T' мы получаем формулу A^* теории T , называемую *переводом A в T* , следующим образом. Выбираем вариант D' формулы D , в котором никакая переменная из A не является связанной, и заменяем каждую часть $pa_1 \dots a_n$ из A на

$$D'_{x_1, \dots, x_n}[a_1, \dots, a_n].$$

Некоторый произвол при выборе не страшен; при разных выборах D' получаются различные ответы для A^* , но эти ответы являются вариантами один другого.

Покажем теперь, что $\vdash_T A$ тогда и только тогда, когда $\vdash_{T'} A^*$. Для этого достаточно доказать, что

(i) $\vdash_{T'} A \leftrightarrow A^*$;

(ii) T' является консервативным расширением теории T . Действительно, тогда по (i) $\vdash_{T'} A$ в том и только в том случае, когда $\vdash_T A^*$, и $\vdash_{T'} A^*$ в том и только в том случае, когда $\vdash_T A^*$ по (ii).

Сначала докажем (i). Ввиду теоремы эквивалентности достаточно показать, что (при вышеприведенных обозначениях)

$$\vdash_{T'} p a_1 \dots a_n \leftrightarrow D'_{x_1, \dots, x_n} [a_1, \dots, a_n].$$

Это следует из определяющей аксиомы для p по теореме о варианте и правилу подстановки.

Если A — формула теории T , то A^* есть A . Поэтому для доказательства (ii) достаточно показать, что $\vdash_T A^*$ для каждой теоремы A теории T' . Докажем это индукцией по теоремам (в форме, описанной в § 3.1).

Предположим, что A — аксиома подстановки $B_x[a] \rightarrow \exists x B$. Легко доказать индукцией по длине B , что $B_x[a]^*$ есть $B_x^*[a]$. Значит, A^* — аксиома подстановки $B_x^*[a] \rightarrow \exists x B^*$. Если A — аксиома тождества или аксиома равенства, не содержащая p , то A^* есть A . Если A — аксиома равенства

$$y_1 = y'_1 \rightarrow \dots \rightarrow y_n = y'_n \rightarrow p y_1 \dots y_n \rightarrow p y'_1 \dots y'_n,$$

то A^* есть

$$y_1 = y'_1 \rightarrow \dots \rightarrow y_n = y'_n \rightarrow D' [y_1, \dots, y_n] \rightarrow D' [y'_1, \dots, y'_n].$$

Она следует из следствия 2 к теореме равенства. Если A — нелогическая аксиома теории T , то A^* есть A . Если A — определяющая аксиома для p , то A^* есть $D' \leftrightarrow D$, которая является теоремой по теореме о варианте.

Если A — тавтологическое следствие $B_1, \dots, B_n$, то A^* — тавтологическое следствие $B_1^*, \dots, B_n^*$; поэтому A^* является теоремой по индуктивному предположению и теореме тавтологии. Если A есть $\exists x B \rightarrow C$ и выводится из $B \rightarrow C$ по правилу $\exists$ -введения, то A^* есть $\exists x B^* \rightarrow C^*$. По индуктивному предположению имеем $\vdash B^* \rightarrow C^*$, и

поскольку x не является свободной в C , то x не является свободной в C^* . Значит, $\vdash \exists x B^* \rightarrow C^*$ по правилу $\exists$ -введения.

Теперь допустим, что мы рассматриваем аналогичную проблему для функциональных символов. Например, предположим, что мы рассматриваем теорию, содержащую $\cdot$, индивиды которой являются положительными действительными числами, и мы хотим определить функцию извлечения квадратного корня $\sqrt{}$. Мы могли бы добавить $\sqrt{}$ в качестве нового унарного функционального символа и добавить новую аксиому

$$y = \sqrt{x} \leftrightarrow y \cdot y = x.$$

Перед тем, как это сделать, мы могли бы доказать в нашей теории, что каждый индивид имеет один и только один квадратный корень, т. е. мы могли бы доказать

$$\exists y (y \cdot y = x)$$

и

$$y \cdot y = x \ \& \ y' \cdot y' = x \rightarrow y = y'.$$

Допустим, что все это сделано. Как можно перевести формулу $\dots \sqrt{x} \dots$, содержащую новый символ, в первоначальную теорию? Один путь — перевести эту формулу следующим образом:

$$\exists y (y \cdot y = x \ \& \ \dots y \dots).$$

Теперь можно описать общую ситуацию. Мы имеем теорию T , различные переменные $x_1, \dots, x_n, y, y'$ и формулу D , в которой нет свободных переменных, отличных от $x_1, \dots, x_n, y$. Имеем

$$\vdash_T \exists y D \quad (1)$$

и

$$\vdash_T D \ \& \ D_y[y'] \rightarrow y = y'. \quad (2)$$

Образуем T' из T добавлением нового n -арного функционального символа f и новой нелогической аксиомы $y = f x_1 \dots x_n \leftrightarrow D$, которую мы называем *определяющей аксиомой* для f . Мы называем (1) *условием существования* и (2) *условием единственности* для f .

Теперь определяем формулу A^* теории T , соответствующую формуле A теории T' . Сделаем это только для

атомных формул A ; в общем случае A^* получается заменой каждой атомной части B формулы A на B^* . Наше определение дается индукцией по числу вхождений f в A . Если таких вхождений не существует, то A^* есть A . В противном случае A может быть записано как $B_x[fa_1 \dots a_n]$, где $a_1, \dots, a_n$ не содержат f и B — атомная формула, содержащая на одно вхождение f меньше, чем A . Выбираем вариант D' формулы D , в котором никакая переменная из A не является связанной, и пусть A^* будет

$$\exists z (D'_{x_1, \dots, x_n, y}[a_1, \dots, a_n, z] \& B^*).$$

Мы снова хотим показать, что $\vdash_{T'} A$ тогда и только тогда, когда $\vdash_T A^*$. Снова достаточно доказать, что

(i) $\vdash_{T'} A \leftrightarrow A^*$;

(ii) теория T' является консервативным расширением теории T .

Достаточно доказать (i) для атомных A . Сделаем это индукцией по числу вхождений f в A . Если таких вхождений нет, то $A \leftrightarrow A^*$ является тавтологией $A \leftrightarrow A$. Теперь предположим, что f входит в A , и применим вышеприведенные обозначения. Из определяющей аксиомы для f , теоремы о варианте и правилу подстановки получаем

$$\vdash z = fa_1 \dots a_n \leftrightarrow D'[a_1, \dots, a_n, z].$$

Следовательно, по теореме эквивалентности имеем

$$\vdash \exists z (z = fa_1 \dots a_n \& B^*) \leftrightarrow A^*.$$

Поскольку по индуктивному предположению $\vdash B \leftrightarrow B^*$, то

$$\vdash \exists z (z = fa_1 \dots a_n \& B) \leftrightarrow A^*;$$

следовательно, по следствию 3 к теореме равенства получаем

$$\vdash B_z[fa_1 \dots a_n] \leftrightarrow A^*,$$

т. е. $\vdash A \leftrightarrow A^*$.

Доказывая (ii), допустим, что T'' получена из T добавлением f и новой аксиомы

$$D_y[fx_1 \dots x_n]. \quad (3)$$

По (1) и теореме о функциональных расширениях теория T'' является консервативным расширением теории T . Поэтому достаточно доказать, что T' и T'' эквивалентны.

Можно доказать (3) в T' , подставляя $fx_1 \dots x_n$ вместо y в определяющей аксиоме для f и применяя аксиомы тождества. Теперь по теореме равенства получаем

$$\vdash_{T'} y = fx_1 \dots x_n \rightarrow (D \leftrightarrow D_y[fx_1 \dots x_n]), \quad (4)$$

в то время как по (2) и правилу подстановки имеем

$$\vdash_{T'} D \& D_y[fx_1 \dots x_n] \rightarrow y = fx_1 \dots x_n. \quad (5)$$

Из (3), (4) и (5) мы можем получить определяющую аксиому для f по теореме тавтологии.

З а м е ч а н и е. Эквивалентность теорий T' и T'' показывает, что мы могли бы с тем же успехом принять (3) в качестве новой аксиомы. Поэтому мы иногда называем (3) также *определяющей аксиомой для f* .

Особым случаем, часто встречающимся, является случай, когда D есть $y = a$, где a — терм, не содержащий переменной, отличной от $x_1, \dots, x_n$. Определяющая аксиома для f (в виде (3)) тогда становится формулой $fx_1 \dots x_n = a$. В этом случае условия существования и единственности всегда доказуемы. Условие существования $\exists y (y = a)$ следует из $a = a$ и аксиомы подстановки; условие единственности

$$= a \& y' = a \rightarrow y = y'$$

следует из

$$y' = a \rightarrow (y = y' \leftrightarrow y = a),$$

а это есть один из случаев теоремы равенства.

Скажем, что теория T' является *расширением* теории T с помощью определений, если T' получается из T с помощью конечного числа расширений двух описанных типов. В этом случае мы имеем для каждой формулы A теории T' формулу A^* теории T (перевод A в T) такую, что $\vdash_{T'} A$ тогда и только тогда, когда $\vdash_T A^*$. Кроме того, теория T' является консервативным расширением теории T ; следовательно, T' непротиворечива тогда и только тогда, когда T непротиворечива.

Теперь предположим, что теория T' является расширением теории T с помощью определений и $\mathcal{A}$ — модель теории T . Мы утверждаем, что существует единственное обогащение $\mathcal{A}'$ модели $\mathcal{A}$, являющееся моделью теории T' . Ясно, что достаточно это проверить, когда T' содержит только один нелогический символ, не содержащийся

в T . Если этот символ есть предикатный символ p с определяющей аксиомой

$$px_1 \dots x_n \leftrightarrow D,$$

то

$$p_{\mathcal{A}'}(a_1, \dots, a_n) \leftrightarrow \mathcal{A}'(D_{x_1, \dots, x_n}[i_1, \dots, i_n]) = \mathbf{И},$$

где $i_1, \dots, i_n$ — имена для $a_1, \dots, a_n$. Если новый символ есть функциональный символ f с определяющей аксиомой $fx_1 \dots x_n = y \leftrightarrow D$, то $f_{\mathcal{A}'}(a_1, \dots, a_n)$ есть единственное b такое, что

$$\mathcal{A}'(D_{x_1, \dots, x_n, y}[i_1, \dots, i_n, j]) = \mathbf{И},$$

где $i_1, \dots, i_n, j$ — имена для $a_1, \dots, a_n, b$. То, что такое b существует и единственно, следует из того, что условия существования и единственности для f являются истинными в $\mathcal{A}$.

4.7. Интерпретации

До сих пор все структуры описывались на русском языке. Мы могли бы, конечно, перевести целиком всё описание на любой язык, в котором существует достаточная теоретико-множественная система обозначений для рассмотрения функций, предикатов и т. д.

Однако если мы хотим изучать лишь какую-нибудь частную структуру $\mathcal{A}$ для L , то необязательно иметь такой богатый язык. Достаточно иметь язык L' , который имеет какой-то символ для универсума $\mathcal{A}$ и какие-то символы для каждой функции и предиката из $\mathcal{A}$. Это приводит к одной незначительной трудности: функции и предикаты, обозначенные символами из L' , используют все индивиды из L' в качестве своих значений аргументов, хотя функции и предикаты из $\mathcal{A}$ используют в качестве значений своих аргументов только индивиды из $\mathcal{A}$. Эта трудность преодолевается, если разрешить символу из L' обозначать любую функцию (или предикат), которая (ый) является расширением функции (или предиката) из $\mathcal{A}$.

Пусть L и L' — языки первого порядка. *Интерпретация* I языка L в языке L' состоит из

(i) унарного предикатного символа U_I из L' , называемого *универсумом* для I ;

(ii) n -арного функционального символа f_I из L' для каждого n -арного функционального символа f из L ;

(iii) n -арного предикатного символа p_I из L' для каждого n -арного предикатного символа p из L , отличного от $=$.

Интерпретацией языка L в теории T' называется интерпретация I языка L в языке $L(T')$ такая, что

$$\vdash_{T'} \exists x U_I x \quad (1)$$

и

$$\vdash_{T'} U_I x_1 \rightarrow \dots \rightarrow U_I x_n \rightarrow U_I f_I x_1 \dots x_n \quad (2)$$

для каждого f из L . Первое условие требует, чтобы универсум был непустым; второе условие требует, чтобы f_I представляло функцию, ограничение которой до универсума для I принимает значения в универсуме для I . (Оба условия (1) и (2) выполняются при любом наборе переменных; ясно, что если (1) выполняется для одного x и если для каждого f выполняется (2) для одного набора $x_1, \dots, x_n$ различных переменных, то (1) и (2) выполняются при любом выборе переменных.)

Пусть I — интерпретация языка L в языке L' . Будем определять для каждой формулы A языка L формулу $A^{(I)}$ языка L' , называемую *интерпретацией* формулы A с помощью I , означающую, что A является истинной в рассматриваемой структуре. Допустим, что A_I — формула языка L' , полученная из A с помощью двух следующих шагов:

(а) заменяем каждый нелогический символ u на u_I ;

(б) заменяем каждую часть $\exists x B$ на $\exists x (U_I x \& B)$.

Тогда $A^{(I)}$ есть

$$U_I x_1 \rightarrow \dots \rightarrow U_I x_n \rightarrow A_I,$$

где $x_1, \dots, x_n$ — все переменные, свободные в A (и, значит, в A_I), взятые в алфавитном порядке. Если a — терм языка L , то пусть a_I обозначает терм, полученный из a с помощью правила (а), данного выше.

Теперь можно определить понятие, в данной ситуации соответствующее модели. *Интерпретацией* теории T в теории T' называется интерпретация I языка $L(T)$ в теории T' такая, что $\vdash_{T'} A^{(I)}$ для каждой нелогической аксиомы A теории T .

Наш следующий результат является аналогом теоремы истинности в данной ситуации.

Теорема об интерпретации. Если I является интерпретацией теории T в теории T' , то $\vdash_{T'} A^{(I)}$ для каждой теоремы A теории T .

Доказательство. Нам нужны два предварительных результата. Во-первых, если a — терм теории T и $x_1, \dots, x_n$ — все переменные из a , то

$$\vdash U_I x_1 \rightarrow \dots \rightarrow U_I x_n \rightarrow U_I a_I. \quad (3)$$

(Здесь и в последующем $\vdash$ означает $\vdash_{T'}$.) Доказательство (3) проводится индукцией по длине a с использованием (2). Оставляем детали читателю.

Второй предварительный результат состоит в том, что если среди $x_1, \dots, x_n$ имеются все переменные, свободные в A , и если

$$\vdash U_I x_1 \rightarrow \dots \rightarrow U_I x_n \rightarrow A_I, \quad (4)$$

то $\vdash A^{(I)}$. Из (4) по теореме тавтологии получаем

$$\vdash U_I y_1 \rightarrow \dots \rightarrow U_I y_k \rightarrow A^{(I)}, \quad (5)$$

где $y_1, \dots, y_k$ — различные переменные, не свободные в A , и, значит, не свободные в $A^{(I)}$. Применяя правило $\exists$ -введения к (5) и затем используя (1) и правило отделения, получаем

$$\vdash U_I y_2 \rightarrow \dots \rightarrow U_I y_k \rightarrow A^{(I)}.$$

Далее просто повторяем этот шаг $k-1$ раз.

Докажем теперь теорему об интерпретации индукцией по теоремам теории T (в виде, описанном в § 3.1). Предположим, что A — аксиома подстановки $B_x[a] \rightarrow \exists x B$ и $y_1, \dots, y_k$ — переменные, отличные от x , свободные в B и a . По (3) имеем

$$\vdash U_I y_1 \rightarrow \dots \rightarrow U_I y_n \rightarrow U_I a_I.$$

По теореме подстановки получаем

$$\vdash (U_I a_I \& (B_I)_x[a_I]) \rightarrow \exists x (U_I x \& B_I).$$

Из этих результатов по теореме тавтологии получаем

$$\vdash U_I y_1 \rightarrow \dots \rightarrow U_I y_n \rightarrow (B_I)_x[a_I] \rightarrow \exists x (U_I x \& B_I),$$

т. е.

$$\vdash U_I y_1 \rightarrow \dots \rightarrow U_I y_n \rightarrow A_I.$$

Следовательно, $\vdash A^{(I)}$ по второму предварительному результату.

Если A — аксиома тождества или равенства, то такова же и A_I ; следовательно, $\vdash A_I$ и, значит, $\vdash A^{(I)}$. Если A — нелогическая аксиома, то $\vdash A^{(I)}$ по предположению.

Предположим, что A — тавтологическое следствие формул $B_1, \dots, B_k$. По замечанию из § 3.1 A_I — тавтологическое следствие формул $(B_1)_I, \dots, (B_k)_I$. Отсюда следует, что если $x_1, \dots, x_n$ — все переменные, свободные в A , $B_1, \dots, B_k$, то (4) есть тавтологическое следствие формул $B_1^{(I)}, \dots, B_k^{(I)}$. Следовательно, $\vdash A^{(I)}$ по индуктивному предположению, теореме тавтологии и второму предварительному результату.

Предположим, что A есть $\exists x B \rightarrow C$ и выведено из $B \rightarrow C$ по правилу $\exists$ -введения. Пусть $x_1, \dots, x_n$ — все переменные, свободные в A . Тогда x отлично от x_i . По индуктивному предположению и теореме тавтологии получаем

$$\vdash U_I x_1 \rightarrow \dots \rightarrow U_I x_n \rightarrow U_I x \rightarrow B_I \rightarrow C_I.$$

Следовательно, по теореме тавтологии и правилу $\exists$ -введения получаем

$$\vdash \exists x (U_I x \& B_I) \rightarrow U_I x_1 \rightarrow \dots \rightarrow U_I x_n \rightarrow C_I,$$

из которой по теореме тавтологии следует $\vdash A^{(I)}$.

Следствие. Если I — интерпретация теории T в теории T' и T' является непротиворечивой, то T является непротиворечивой.

Доказательство. Предположим, что T является противоречивой, и пусть A — некоторая замкнутая формула теории T . Тогда $\vdash_T A$ и $\vdash_T \neg A$. Поскольку $(\neg A)^{(I)}$ есть $\neg A^{(I)}$, то $A^{(I)}$ и $\neg A^{(I)}$ являются теоремами теории T' , что противоречит непротиворечивости теории T' .

Так как доказательство теоремы об интерпретации финитно, то мы можем использовать это следствие для финитных доказательств непротиворечивости.

При образовании A_I и $A^{(I)}$ мы предполагали, что определяемые символы устранены. Однако ясно, что необязательно устранять $\rightarrow$, $\&$ и $\leftrightarrow$. Если A содержит часть $\forall x B$, то она превращается в $\neg \exists x \neg B$ при устранении $\forall$ и, значит, дает часть

$$\neg \exists x (U_I x \& \neg B)$$

в A_I и $A^{(1)}$. По теореме тавтологии и теореме эквивалентности эта часть эквивалентна

$$\neg \exists x \neg (U_I x \rightarrow B),$$

т. е. $\forall x (U_I x \rightarrow B)$. Следовательно, мы можем просто заменить часть $\forall x B$ на $\forall x (U_I x \rightarrow B)$.

Пусть I — интерпретация теории T в теории T' и U — расширение теории T с помощью определений. Мы собираемся показать, что при подходящих предположениях I может быть расширена до интерпретации теории U в расширении теории T' с помощью определений.

Сначала предположим, что U получается из T добавлением нового предикатного символа p с определяющей аксиомой

$$p x_1 \dots x_n \leftrightarrow D. \quad (6)$$

Строим расширение U' теории T' с помощью определений, добавляя новый предикатный символ p' с определяющей аксиомой

$$p' x_1 \dots x_n \leftrightarrow D_I. \quad (7)$$

Затем расширяем I , полагая, что p_I есть p' . Чтобы убедиться, что I является интерпретацией теории U в теории U' , мы должны доказать, что интерпретация формулы (6) выводима в U' . Эта интерпретация есть формула

$$U_I x_1 \rightarrow \dots \rightarrow U_I x_n \rightarrow (p' x_1 \dots x_n \leftrightarrow D_I)$$

и, значит, выводима из (7).

Когда мы действуем с функциональными символами, появляется одна новая проблема. Если f есть новый функциональный символ в расширении теории T с помощью определений, то f обозначает единственную функцию на универсуме нашей модели, и мы должны расширить эту функцию до универсума теории T' . Наше решение этой проблемы состоит в том, что мы выбираем индивид из T' и считаем его значением функции для всех новых множеств аргументов.

Поэтому предположим, что некоторая константа e в T' фиксирована. Пусть U получена из T добавлением нового функционального символа f с определяющей аксиомой

$$f x_1 \dots x_n = y \leftrightarrow D. \quad (8)$$

Строим расширение U' теории T' с помощью определений, добавляя новый функциональный символ f' с определяющей аксиомой

$$f' x_1 \dots x_n = y \leftrightarrow (U_I x_1 \& \dots \& U_I x_n \& D_I \& U_I y) \vee (\neg (U_I x_1 \& \dots \& U_I x_n) \& y = e). \quad (9)$$

Легко проверить, что условия существования и единственности для f' следуют из интерпретаций условий существования и единственности для f . Мы снова расширяем I , полагая, что f_I будет f' . Мы должны тогда доказать

$$U_I x_1 \rightarrow \dots \rightarrow U_I x_n \rightarrow U_I f' x_1 \dots x_n.$$

Это следует из (9). Интерпретация формулы (8) есть формула

$$U_I x_1 \rightarrow \dots \rightarrow U_I x_n \rightarrow U_I y \rightarrow (f' x_1 \dots x_n = y \leftrightarrow D_I),$$

которая также следует из (9).

Скажем, что T интерпретируема в T' , если существует интерпретация I теории T в некотором расширении теории T' с помощью определений. Из следствия к теореме об интерпретации мы видим, что если T интерпретируема в T' и T' является непротиворечивой, то T является непротиворечивой. (Доказательство этого факта полностью финитно.) Ввиду вышеприведенного рассуждения мы видим, что если теория T интерпретируема в теории T' и если в T' или в расширении теории T' с помощью определений существует некоторая константа, то каждое расширение теории T с помощью определений интерпретируемо в теории T' .

Задачи

1. Доказать теорему Линденбаума для теории T , имеющей только счетное число нелогических символов, не применяя лемму Тейхмюллера — Тьюки. [Показать, что существует только счетное число формул теории T . Если $A_1, A_2, \dots$ — все замкнутые формулы, выберем B_i индуктивно так, что B_i есть либо A_i , либо $\neg A_i$ и $T[B_1, \dots, B_i]$ непротиворечива. Добавим все B_i к T в качестве новых аксиом.]

2. Пусть L — язык первого порядка, содержащий константу. Множество Γ формул языка L свободных от переменных, называется тавтологически противоречивым, если существует квазитавтология, которая представляет собой дизъюнкцию отрицаний предложений из Γ ; в противном случае Γ называется тавтологически непротиворечивым. Если Γ является тавтологически непротиворечивым и для

каждой формулы A , свободной от переменных, либо A , либо $\neg A$ принадлежит Γ , то Γ называется *тавтологически полным*.

(а) Показать, что каждое тавтологически непротиворечивое множество является подмножеством тавтологически полного множества. [Показать, что любое максимальное тавтологически непротиворечивое множество является тавтологически полным, и использовать лемму Тейхмюллера—Тьюки.]

(б) Показать, что если Γ является тавтологически полным, то существует структура $\mathcal{A}$ для L такая, что каждая открытая формула A является истинной в $\mathcal{A}$ тогда и только тогда, когда каждый частный случай формулы A , свободный от переменных, принадлежит Γ . [Выбрать $\mathcal{A}$ подобно канонической структуре для теории, заменив множество теорем теории множеством Γ .]

(в) Используя (а), (б) и теорему Скулема, дать новое доказательство теоремы полноты.

(г) Используя (а), (б) и теорему полноты, дать новое доказательство теоремы непротиворечивости.

3. (а) Пусть язык $L(T')$ является расширением языка $L(T)$. Показать, что теория T' является расширением теории T тогда и только тогда, когда обеднение до $L(T)$ каждой модели теории T' является моделью теории T .

(б) Показать, что если теория T' является расширением теории T и каждая модель теории T имеет обогащение, являющееся моделью теории T' , то теория T' является консервативным расширением теории T .

4. (а) Доказать теорему о функциональных расширениях посредством моделей. [Использовать 3(б).]

(б) Используя лемму 1 из § 4.4 и (а), дать новое доказательство теоремы Эрбрана.

5. Пусть Γ —множество формул языка L и $\mathfrak{X}(\Gamma)$ —множество отображений из Γ в множество истинностных значений. Мы рассматриваем $\mathfrak{X}(\Gamma)$ как произведение пространств $\prod_{A \in \Gamma} T_A$, где каждое T_A

есть множество истинностных значений. Если мы наделяем каждое T_A дискретной топологией, то по теореме Тихонова $\mathfrak{X}(\Gamma)$ становится компактным хаусдорфовым пространством. Пусть $\mathfrak{X}\mathfrak{B}(\Gamma)$ —множество таких V из $\mathfrak{X}(\Gamma)$, что $V(\neg A) = H_{\neg}(V(A))$, как только A и $\neg A$ принадлежат Γ , и $V(A \vee B) = H_{\vee}(V(A), V(B))$, как только A, B и $A \vee B$ принадлежат Γ .

(а) Показать, что для любой формулы A из Γ множество таких V из $\mathfrak{X}(\Gamma)$, что $V(A) = \text{И}$, является открытым и замкнутым.

(б) Показать, что пространство $\mathfrak{X}\mathfrak{B}(\Gamma)$ является замкнутым в $\mathfrak{X}(\Gamma)$ и, следовательно, компактным. [Использовать (а).]

(в) Используя (а) и (б), дать новое решение задачи 2(а). [Использовать свойство центрируемости.]

6. Дизъюнкты формулы A определяются индукцией по длине A следующим образом: если A не является дизъюнкцией, то единственным дизъюнктом формулы A является сама A ; если A есть $B \vee C$, то дизъюнктами формулы A являются дизъюнкты формулы B и дизъюнкты формулы C .

Пусть T —некоторая теория, и пусть T' будет следующей формальной теорией. Языком теории T' является язык теории T . Аксио-

мами теории T' являются аксиомы тождества, аксиомы равенства, нелогические аксиомы теории T и все формулы $\neg A \vee A$, где A —атомная формула. Правилами теории T' являются:

(i) $\vee$ -правило: B следует из A , если каждый дизъюнкт формулы A является дизъюнктом формулы B ;

(ii) $\neg\neg$ -правило: $\neg\neg A \vee B$ следует из $A \vee B$;

(iii) $\neg\vee$ -правило: $\neg(A \vee B) \vee C$ следует из $\neg B \vee C$ и $\neg A \vee C$;

(iv) $\exists$ -правило: $\exists x A \vee B$ следует из $A_x[a] \vee B$;

(v) $\neg\exists$ -правило: $\neg\exists x A \vee B$ следует из $\neg A \vee B$ при условии, что x не является свободной в B ;

(vi) правило сечения.

Показать, что теории T и T' имеют одни и те же теоремы.

7. Пусть теории T и T' такие же, как в задаче 6. Пусть L' будет языком, полученным из языка L добавлением бесконечного числа новых констант. Пусть U будет следующей формальной системой. Язык системы U есть L' . Аксиомы системы U являются замкнутыми частными случаями языка L' аксиом теории T' . Правила системы U те же, что и правила теории T' , за исключением того, что в каждом правиле требуется, чтобы посылки и заключение были замкнутыми формулами, а также $\neg\exists$ -правило исправлено следующим образом: $\neg\exists x A \vee B$ следует из $\neg A_x[e] \vee B$ при условии, что e есть новая константа, которая не встречается в $\neg\exists x A \vee B$. Показать, что каждый замкнутый частный случай языка L' теоремы теории T есть теорема системы U .

8. Пусть T —открытая теория, а U такая же, как в задаче 7. Систему U' получаем из системы U заменой правила сечения на *слабое правило сечения*: $B \vee C$ следует из $A \vee B$ и $\neg A \vee C$ при условии, что A свободна от переменных (а B и C замкнуты). Формула A системы U' называется *секущей* формулой, если для каждой пары замкнутых формул B и C таких, что $\vdash_{U'} A \vee B$ и $\vdash_{U'} \neg A \vee C$, мы имеем $\vdash_{U'} B \vee C$.

(а) Показать, что если $\vdash_{U'} A$ и $e_1, \dots, e_n$ —новые константы, то существует доказательство A в U' такое, что

(i) каждая формула в доказательстве, за исключением последней, используется ровно один раз в качестве посылки правила для вывода последующей формулы;

(ii) если $\neg\exists$ -правило используется для вывода $\neg\exists x B \vee C$ из $\neg B_x[e] \vee C$, то e не является одной из $e_1, \dots, e_n$.

(б) Показать, что если $\vdash_{U'} A$ и A' получается из A заменой везде новой константы e термом a , свободным от переменных, то $\vdash_{U'} A'$. [Использовать (а).]

(в) Показать, что если формула A не является свободной от переменных и $\vdash_{U'} \neg\neg A \vee B$, то $\vdash_{U'} A \vee B$. [Начать с доказательства $\neg\neg A \vee B$, данного по (а). В каждой формуле этого доказательства заменить $\neg\neg A$ в некоторых местах, где эта формула встречается как дизъюнкт, на A .] Затем показать, что если A —секущая формула, то и $\neg A$ —секущая формула.

(г) Показать, что если $A \vee B$ не является свободной от переменных и $\vdash_{U'} \neg(A \vee B) \vee C$, то $\vdash_{U'} \neg A \vee C$ и $\vdash_{U'} \neg B \vee C$. [Подобно

(в.) Вывести, что если A и B являются секущими формулами, то $A \vee B$ — секущая формула.

(д) Показать, что если $\vdash_{U'} \neg \exists x A \vee C$ и e — новая константа, не встречающаяся в $\exists x A \vee C$, то $\vdash_{U'} \neg A_x[e] \vee C$. [Подобно (в).]

(е) Показать, что если $A_x[a]$ является секущей формулой для каждого термина a , свободного от переменных, то $\exists x A$ является секущей формулой. [Предположим, что $\vdash_{U'} \exists x A \vee B$ и $\vdash_{U'} \neg \exists x A \vee C$. Начать с доказательства $\exists x A \vee B$, как описано в (а), и заменить подходящие вхождения $\exists x A$ на C . Использовать, что если $\vdash_{U'} A_x[a] \vee D$, то $\vdash_{U'} C \vee D$ по (д) и (б).]

(ж) Показать, что каждая теорема системы U есть теорема системы U' . [Использовать (в), (г) и (е) для доказательства того, что каждая замкнутая формула является секущей формулой.]

(з) Используя (ж) и задачу 7, дать новое доказательство теоремы непротиворечивости. [Заметим, что доказательство формулы системы U' , свободной от переменных, удовлетворяющее (а), может не содержать кванторов.]

9. Пусть T — открытая теория и A — формула теории T , находящаяся в пренексной форме. Показать, что $\vdash_T A$ тогда и только тогда, когда существует дизъюнкция частных случаев матрицы, которая является тавтологическим следствием частных случаев аксиом тождества, аксиом равенства и нелогических аксиом теории T . [Использовать теорему редукции и теорему Эрбрана.]

10. Показать, что если A есть теорема теории T , то существует доказательство формулы A , в котором не встречаются нелогические символы, за исключением тех, которые есть в A и в нелогических аксиомах теории T . [Использовать теорему редукции и теорему Эрбрана.]

11. Пусть A — открытая формула и n — число термов, входящих в A . Показать, что A является квазитавтологией тогда и только тогда, когда A является истинной в каждой структуре, имеющей не более n индивидов. [Показать, что мы можем предполагать, что A свободна от переменных. Если A не является квазитавтологией, то получить структуру $\mathcal{A}$, в которой A не является истинной, с помощью конструкции, подобной той, которая применяется для построения канонической структуры для теории, заменяя теоремы теории на формулы, которые имеют значение И при подходящей истинностной оценке.]

12. Теории T и T' называются *слабо эквивалентными*, если некоторое расширение теории T с помощью определений эквивалентно некоторому расширению теории T' с помощью определений.

(а) Показать, что для каждой теории T существует теория T' , не содержащая функциональных символов, слабо эквивалентная теории T . [Получить расширение U теории T с помощью определений, добавляя для каждого f в T предикатный символ p с определяющей аксиомой $px_1 \dots x_n u \leftrightarrow fx_1 \dots x_n = u$. Выбрать теорию T' так, чтобы $u = fx_1 \dots x_n \leftrightarrow px_1 \dots x_n u$ могло быть использовано как определяющая аксиома для f .]

(б) Показать, что если T является открытой теорией, то существует теория T' , слабо эквивалентная теории T , такая, что T' не содержит функциональных символов и нелогические аксиомы тео-

рии T' являются экзистенциальными. [Подобно (а).] Если T имеет только одну нелогическую аксиому, то показать, что T' может быть выбрана так, что она имеет только одну аксиому.

(в) Формула A называется *выполнимой* в A , если A является истинной в некоторой модели, имеющей A своим универсумом. Формула находится в *скулемовской форме*, если она находится в пренексной форме, не содержит функциональных символов и все ее кванторы всеобщности предшествуют кванторам существования. Показать, что для данной формулы A можно построить замкнутую формулу B в скулемовской форме такую, что A выполнима в A для каждого A тогда и только тогда, когда B выполнима в A . [Использовать (б).]

13. Пусть L — язык первого порядка.

(а) Пусть $\mathcal{A}$ — структура для L , имеющая конечное число индивидов, и Q — конечное множество нелогических символов языка L . Предположим, что нам дано $\mathcal{A}(a)$ для каждого термина a вида $fi_1 \dots i_n$, где f принадлежит Q , и $\mathcal{A}(A)$ для каждой формулы A вида $pi_1 \dots i_n$, где p принадлежит Q . Показать, что можно вычислять $\mathcal{A}(A)$ для каждой замкнутой формулы языка $L(A)$, все нелогические символы которой принадлежат Q .

(б) Показать, что для данной формулы A языка L и любого числа n можно решить, будет ли A истинной в каждой структуре для L , имеющей n индивидов.

(в) Предположим, что A — экзистенциальная формула языка, не содержащая функциональных символов, отличных от констант. Показать, что если A не является логически истинной, то существует структура, в которой A не является истинной, имеющая не более n индивидов, где n — число переменных и констант в A .

(г) Показать, что для данной экзистенциальной формулы A , не содержащей функциональных символов, отличных от констант, можно решить, будет A логически истинной или нет. [Использовать (б) и (в).]

ТЕОРИЯ МОДЕЛЕЙ

5.1. Теорема компактности

Цель теоремы полноты — показать, что каждое логическое следствие множества нелогических аксиом может быть выведено из этих нелогических аксиом посредством логических аксиом и правил. Однако может показаться, что следствия теоремы зависят от нашего выбора логических аксиом и правил, и следовательно, эта теорема ничего не говорит нам про природу моделей. Это не так, потому что логические аксиомы и правила, которые мы выбрали, имеют два простых свойства, а то, что множества логических аксиом и правил с этими свойствами достаточно для получения всех логических следствий каждого множества нелогических аксиом, имеет важные следствия.

Первое свойство выражается в следующем утверждении: если мы имеем метод для решения, будет ли формула нелогической аксиомой или нет, то мы имеем и метод для решения, будет ли последовательность формул доказательством или нет. Мы изучим это свойство и его следствия в следующей главе.

Второе свойство состоит в том, что логические правила являются конечными. Мы собираемся вывести одно важное следствие из этого.

Теория T называется *частью* теории T' , если T и T' имеют один и тот же язык и каждая нелогическая аксиома теории T является нелогической аксиомой теории T' . Теория T называется *конечно аксиоматизируемой*, если она имеет только конечное число нелогических аксиом.

Теорема компактности. *Формула A теории T является истинной в T тогда и только тогда, когда A является истинной в некоторой конечно аксиоматизируемой части теории T .*

Доказательство. Ввиду теоремы полноты нам нужно показать лишь, что формула есть теорема теории T тогда и только тогда, когда эта формула есть теорема

в некоторой конечно аксиоматизируемой части теории T . Это очевидно, так как в любом доказательстве может использоваться лишь конечное число нелогических аксиом.

Следствие. *Теория T имеет модель тогда и только тогда, когда каждая конечно аксиоматизируемая часть теории T имеет модель.*

Доказательство. Беря в качестве теоремы формулу $x \neq x$, замечаем, что $x \neq x$ в любой структуре не является истинной.

Теорема компактности не зависит от логических аксиом и правил, так как в ней ничего не говорится про них. Возможно, это будет яснее, если мы сформулируем эту теорему в несколько другой форме: формула A является логическим следствием множества формул Γ тогда и только тогда, когда A является логическим следствием некоторого конечного подмножества множества Γ . Можно дать доказательство, которое не использует логических аксиом и правил (см. задачу 30), но такое доказательство не будет тривиальным.

Дадим некоторые применения теоремы компактности к *элементарной теории полей*. Эта теория, которую мы обозначаем через FL, имеет в качестве нелогических символов 0, 1 и -1 и бинарные функциональные символы $+$ и $\cdot$. Нелогическими аксиомами FL являются:

$$\text{FL1. } (x + y) + z = x + (y + z).$$

$$\text{FL2. } x + 0 = x.$$

$$\text{FL3. } x + (-1 \cdot x) = 0.$$

$$\text{FL4. } x + y = y + x.$$

$$\text{FL5. } (x \cdot y) \cdot z = x \cdot (y \cdot z).$$

$$\text{FL6. } x \cdot 1 = x.$$

$$\text{FL7. } x \neq 0 \rightarrow \exists y (x \cdot y = 1).$$

$$\text{FL8. } x \cdot y = y \cdot x.$$

$$\text{FL9. } x(y + z) = (x \cdot y) + (x \cdot z).$$

$$\text{FL10. } 0 \neq 1.$$

Теория FL имеет такое же отношение к полям, как и теория G к группам. Говоря коротко, моделями FL являются в точности поля.

Можно получать элементарные теории некоторых специальных типов полей, добавляя дополнительные нелогические аксиомы. Так, пусть A_n есть формула

$$1 + 1 + \dots + 1 = 0,$$

где имеется n вхождений 1 в левую часть (и мы используем соглашение правого сочетания скобок). Добавляя нелогические аксиомы

$$\neg A_2, \neg A_3, \dots, \neg A_{n-1}, A_n,$$

получаем элементарную теорию FL(n) полей характеристики n ($n \geq 2$). Чтобы получить элементарную теорию FL(0) полей характеристики 0, добавляем все формулы $\neg A_n$ в качестве нелогических аксиом. Так как каждое поле имеет характеристикой 0 или простое число, то, как следует из теоремы полноты, теория FL(n) является противоречивой, если n составное.

Покажем теперь, что если A является истинной в FL(0), то существует n_0 такое, что A является истинной в FL(n) для каждого $n \geq n_0$. По теореме компактности A является истинной в некоторой конечной части T теории FL(0), и мы должны лишь выбрать n_0 , большее всех n таких, что $\neg A_n$ является нелогической аксиомой теории T . Следствием этого результата является то, что мы не можем заменить бесконечное число аксиом, добавленных к FL, чтобы получить FL(0), некоторым конечным числом этих аксиом. Если бы мы это могли сделать, то конъюнкция этих аксиом была бы истинной в поле нулевой характеристики, но не в других полях. Выбирая, как и раньше, n_0 , мы должны были бы заключить, что не существует полей характеристики больше n_0 , что является абсурдным.

Можно было бы попытаться построить элементарную теорию конечных полей, т. е. можно было бы поискать простое расширение T теории FL, моделями которого являются в точности конечные поля. Однако это сделать нельзя. Чтобы убедиться в этом, допустим, что B_n есть формула, которая утверждает, что существуют по крайней мере n индивидов. (Например, B_3 есть

$$\exists x \exists y \exists z (x \neq y \& x \neq z \& y \neq z).$$

Предположим, что мы имеем такую теорию T , и пусть T' получается из T добавлением всех B_n в качестве нелогических аксиом. Тогда T' не имеет модели; таким образом, некоторая конечно аксиоматизируемая часть T' теории T не имеет модели. Выбираем n_0 большим любого

n такого, что B_n является нелогической аксиомой теории T' , и выбираем конечное поле $\mathcal{A}$, имеющее более n_0 элементов. Тогда $\mathcal{A}$ является моделью теории T' , что противоречит выбору T' .

5.2. Изоморфизмы и подструктуры

Пусть $\mathcal{A}$ — некоторая структура. Можно получать структуры, подобные $\mathcal{A}$, с помощью следующего процесса: заменяем каждый индивид из $\mathcal{A}$ новым индивидом (различные индивиды заменяются различными индивидами), но во всем остальном оставляя функции и предикаты $\mathcal{A}$ неизменными. Опишем теперь этот процесс точнее.

Пусть φ — некоторое отображение из A в B . Мы говорим, что φ *инъективно* (или *1-1-отображение*), если для каждого a и a' из A из $\varphi(a) = \varphi(a')$ следует $a = a'$. Мы говорим, что φ *сюръективно* (или *отображение на*), если для каждого b из B существует a из A такое, что $\varphi(a) = b$. Мы говорим, что φ *биективно* (или *взаимно однозначно*), если оно инъективно и сюръективно.

Теперь пусть $\mathcal{A}$ — некоторая структура для L и φ — некоторое биективное отображение $|\mathcal{A}|$ в B . Определяем структуру $\mathcal{B}$ для L с универсумом B следующим образом. Если $b_1, \dots, b_n$ принадлежат B , то существуют однозначно определенные индивиды $a_1, \dots, a_n$, принадлежащие $\mathcal{A}$, такие, что $\varphi(a_1) = b_1, \dots, \varphi(a_n) = b_n$. Положим

$$f_{\mathcal{B}}(b_1, \dots, b_n) = \varphi(f_{\mathcal{A}}(a_1, \dots, a_n)),$$

$$p_{\mathcal{B}}(b_1, \dots, b_n) \leftrightarrow p_{\mathcal{A}}(a_1, \dots, a_n).$$

Если $\mathcal{B}$ строится из $\mathcal{A}$ описанным выше способом, то мы говорим, что $\mathcal{A}$ *изоморфно* $\mathcal{B}$ и φ является *изоморфизмом* между $\mathcal{A}$ и $\mathcal{B}$. Другими словами, изоморфизм между $\mathcal{A}$ и $\mathcal{B}$ есть биективное отображение φ из $|\mathcal{A}|$ в $|\mathcal{B}|$ такое, что для $a_1, \dots, a_n$, принадлежащих $|\mathcal{A}|$, имеем

$$f_{\mathcal{B}}(\varphi(a_1), \dots, \varphi(a_n)) = \varphi(f_{\mathcal{A}}(a_1, \dots, a_n)) \quad (1)$$

и

$$p_{\mathcal{B}}(\varphi(a_1), \dots, \varphi(a_n)) \leftrightarrow p_{\mathcal{A}}(a_1, \dots, a_n). \quad (2)$$

Пример. Если $\mathcal{A}$ и $\mathcal{B}$ — группы, рассматриваемые как модели теории G , то изоморфизм между $\mathcal{A}$ и $\mathcal{B}$ в

описанном выше смысле является изоморфизмом между $\mathcal{A}$ и $\mathcal{B}$ в обычном теоретико-групповом смысле.

Тождественное отображение из $|\mathcal{A}|$ в $|\mathcal{A}|$ (т. е. отображение φ такое, что $\varphi(a) = a$ для всех a , принадлежащих $|\mathcal{A}|$) является изоморфизмом между $\mathcal{A}$ и $\mathcal{A}$. Если φ — изоморфизм между $\mathcal{A}$ и $\mathcal{B}$, то обратное отображение для φ является изоморфизмом между $\mathcal{B}$ и $\mathcal{A}$. Если φ — изоморфизм между $\mathcal{A}$ и $\mathcal{B}$, а ψ — изоморфизм между $\mathcal{B}$ и $\mathcal{C}$, то композиция отображений $\psi\varphi$ является изоморфизмом между $\mathcal{A}$ и $\mathcal{C}$. Из этих утверждений следует, что изоморфизм является отношением эквивалентности на структурах для L .

Пусть $\mathcal{A}$ и $\mathcal{B}$ — некоторые структуры для L и φ — некоторое отображение из $|\mathcal{A}|$ в $|\mathcal{B}|$. Если i — имя индивида a из структуры $\mathcal{A}$, то мы используем i^φ для обозначения имени индивида $\varphi(a)$ из структуры $\mathcal{B}$. Если u — выражение языка $L(\mathcal{A})$, то u^φ — выражение, полученное из u заменой каждого имени i на i^φ .

Лемма 1. Пусть φ — некоторый изоморфизм между $\mathcal{A}$ и $\mathcal{B}$. Тогда $\varphi(\mathcal{A}(a)) = \mathcal{B}(a^\varphi)$ для каждого свободного от переменных терма a языка $L(\mathcal{A})$ и $\mathcal{A}(A) = \mathcal{B}(A^\varphi)$ для каждой замкнутой формулы A языка $L(\mathcal{A})$.

Доказательство. Докажем первую часть индукцией по длине a . Если a — имя, то результат очевиден. В противном случае a есть $fa_1 \dots a_n$, где f принадлежит L . Используя (1) и индуктивное предположение, получаем

$$\begin{aligned}\varphi(\mathcal{A}(a)) &= \varphi(f_{\mathcal{A}}(\mathcal{A}(a_1), \dots, \mathcal{A}(a_n))) \\ &= f_{\mathcal{B}}(\varphi(\mathcal{A}(a_1)), \dots, \varphi(\mathcal{A}(a_n))) \\ &= f_{\mathcal{B}}(\mathcal{B}(a_1^\varphi), \dots, \mathcal{B}(a_n^\varphi)) = \mathcal{B}(a^\varphi).\end{aligned}$$

Теперь докажем вторую часть индукцией по длине A . Если A — атомная формула $pa_1 \dots a_n$, где p отлично от $=$, то по (2) и первой части получаем

$$\begin{aligned}\mathcal{A}(A) = \mathbf{I} &\leftrightarrow p_{\mathcal{A}}(\mathcal{A}(a_1), \dots, \mathcal{A}(a_n)) \\ &\leftrightarrow p_{\mathcal{B}}(\varphi(\mathcal{A}(a_1)), \dots, \varphi(\mathcal{A}(a_n))) \\ &\leftrightarrow p_{\mathcal{B}}(\mathcal{B}(a_1^\varphi), \dots, \mathcal{B}(a_n^\varphi)) \\ &\leftrightarrow \mathcal{B}(A^\varphi) = \mathbf{I}.\end{aligned}$$

Если A есть $a=b$, то так как φ является инъективным,

имеем

$$\begin{aligned}\mathcal{A}(A) = \mathbf{I} &\leftrightarrow \mathcal{A}(a) = \mathcal{A}(b) \\ &\leftrightarrow \varphi(\mathcal{A}(a)) = \varphi(\mathcal{A}(b)) \\ &\leftrightarrow \mathcal{B}(a^\varphi) = \mathcal{B}(b^\varphi) \\ &\leftrightarrow \mathcal{B}(A^\varphi) = \mathbf{I}.\end{aligned}$$

Если A есть отрицание или дизъюнкция, то результат легко следует из индуктивного предположения. Теперь предположим, что A есть $\exists x B$. Так как φ является сюръективным, то каждое j из $L(\mathcal{B})$ есть i^φ для некоторого i из $L(\mathcal{A})$. Следовательно, по индуктивному предположению имеем

$$\begin{aligned}\mathcal{A}(A) = \mathbf{I} &\leftrightarrow \mathcal{A}(B_x[i]) = \mathbf{I} \text{ для некоторого } i \text{ из } L(\mathcal{A}) \\ &\leftrightarrow \mathcal{B}(B_x^\varphi[i^\varphi]) = \mathbf{I} \text{ для некоторого } i \text{ из } L(\mathcal{A}) \\ &\leftrightarrow \mathcal{B}(B_x^\varphi[j]) = \mathbf{I} \text{ для некоторого } j \text{ из } L(\mathcal{B}) \\ &\leftrightarrow \mathcal{B}(A^\varphi) = \mathbf{I}.\end{aligned}$$

Две структуры $\mathcal{A}$ и $\mathcal{B}$ для L называются *элементарно эквивалентными*, если одни и те же формулы языка L являются истинными в $\mathcal{A}$ и $\mathcal{B}$. Очевидно, отсюда следует, что $\mathcal{A}$ и $\mathcal{B}$ являются моделями для одних и тех же теорий.

Следствие к теореме замыкания показывает, что если одни и те же замкнутые формулы истинны в $\mathcal{A}$ и $\mathcal{B}$, то $\mathcal{A}$ и $\mathcal{B}$ являются элементарно эквивалентными. Следовательно, по лемме 1 изоморфные структуры являются элементарно эквивалентными.

Пусть $\mathcal{A}$ и $\mathcal{B}$ — некоторые структуры для L . Вложением $\mathcal{A}$ в $\mathcal{B}$ называется инъективное отображение φ из $|\mathcal{A}|$ в $|\mathcal{B}|$ такое, что (1) и (2) выполняются для всех нелогических символов f и p из L и для всех $a_1, \dots, a_n$ из $|\mathcal{A}|$. Если $|\mathcal{A}|$ — подмножество множества $|\mathcal{B}|$ и тождественное отображение из $|\mathcal{A}|$ в $|\mathcal{B}|$ является вложением $\mathcal{A}$ в $\mathcal{B}$, то $\mathcal{A}$ называется *подструктурой* структуры $\mathcal{B}$, а $\mathcal{B}$ — *расширением* структуры $\mathcal{A}$. В этом случае (1) и (2) превращаются в

$$f_{\mathcal{A}}(a_1, \dots, a_n) = f_{\mathcal{B}}(a_1, \dots, a_n), \quad (3)$$

$$p_{\mathcal{A}}(a_1, \dots, a_n) \leftrightarrow p_{\mathcal{B}}(a_1, \dots, a_n). \quad (4)$$

Если $\mathcal{A}$ и $\mathcal{B}$ являются моделями некоторой теории, то мы иногда говорим *подмодель* вместо подструктуры.

Пример. Если $\mathcal{A}$ и $\mathcal{B}$ являются группами (рассматриваемыми в качестве моделей теории G), то $\mathcal{A}$ является подмоделью модели $\mathcal{B}$ тогда и только тогда, когда $\mathcal{A}$ является подгруппой группы $\mathcal{B}$.

Пусть $\mathcal{B}$ — некоторая структура для L и A — непустое подмножество множества $|\mathcal{B}|$. Если существует подструктура $\mathcal{A}$ структуры $\mathcal{B}$ с универсумом A , то она единственна, так как она определяется с помощью (3) и (4). Ясно, что (3) и (4) определяют структуру $\mathcal{A}$ тогда и только тогда, когда A удовлетворяет следующему условию: если $a_1, \dots, a_n$ принадлежат A и f — функциональный символ из L , то $f_{\mathcal{A}}(a_1, \dots, a_n)$ принадлежит A .

Пусть $\mathcal{A}$ и $\mathcal{B}$ — структуры для L такие, что $|\mathcal{A}|$ — подмножество множества $|\mathcal{B}|$. Если a — индивид из $\mathcal{A}$, то мы используем одно и то же имя для a в $L(\mathcal{A})$ и $L(\mathcal{B})$. Следовательно, язык $L(\mathcal{B})$ является расширением языка $L(\mathcal{A})$.

Лемма 2. Пусть $\mathcal{A}$ и $\mathcal{B}$ — некоторые структуры для L и φ — некоторое отображение из $|\mathcal{A}|$ в $|\mathcal{B}|$. Тогда φ является вложением $\mathcal{A}$ в $\mathcal{B}$ тогда и только тогда, когда $\mathcal{A}(A) = \mathcal{B}(A^\varphi)$ для каждой свободной от переменных формулы A языка $L(\mathcal{A})$.

Доказательство. Доказательство того, что данное условие выполняется, если φ — вложение, в точности такое же, как и доказательство в лемме 1. Теперь предположим, что данное условие выполняется. Пусть $a_1, \dots, a_n$ — индивиды структуры $\mathcal{A}$ и $i_1, \dots, i_n$ — имена индивидов $a_1, \dots, a_n$ соответственно. Тогда $\mathcal{A}(pi_1 \dots i_n) = \mathcal{B}(pi_1^\varphi \dots i_n^\varphi)$. Отсюда следует (2). Если j — имя индивида $f_{\mathcal{A}}(a_1, \dots, a_n)$, то

$$\mathcal{B}(fi_1^\varphi \dots i_n^\varphi = j^\varphi) = \mathcal{A}(fi_1 \dots i_n = j) = \mathbf{I}.$$

Отсюда следует (1). Наконец, если $\varphi(a_1) = \varphi(a_2)$, то

$$\mathcal{A}(i_1 = i_2) = \mathcal{B}(i_1^\varphi = i_2^\varphi) = \mathbf{I};$$

следовательно, $a_1 = a_2$. Таким образом, φ инъективно.

Следствие. Пусть $\mathcal{A}$ и $\mathcal{B}$ — структуры для L такие, что $|\mathcal{A}|$ — подмножество множества $|\mathcal{B}|$. Тогда $\mathcal{A}$ является подструктурой структуры $\mathcal{B}$ тогда и только тогда, когда $\mathcal{A}(A) = \mathcal{B}(A)$ для каждой свободной от переменных формулы A языка $L(\mathcal{A})$.

Пусть Γ — множество формул языка L и $\mathcal{A}$ — структура для L . Тогда через $\Gamma(\mathcal{A})$ будем обозначать множество $\mathcal{A}$ -частных случаев для формул из Γ . Таким образом, если Γ есть множество всех открытых формул языка L , то $\Gamma(\mathcal{A})$ есть множество всех свободных от переменных формул языка $L(\mathcal{A})$, а если Γ есть множество всех формул языка L , то $\Gamma(\mathcal{A})$ есть множество всех замкнутых формул языка $L(\mathcal{A})$.

Пусть $\mathcal{A}$ и $\mathcal{B}$ — структуры для L такие, что $|\mathcal{A}|$ является подмножеством множества $|\mathcal{B}|$, и Γ — некоторое множество формул языка L . Мы говорим, что $\mathcal{A}$ есть Γ -подструктура структуры $\mathcal{B}$, а $\mathcal{B}$ есть Γ -расширение структуры $\mathcal{A}$, если для каждой формулы A из $\Gamma(\mathcal{A})$ из $\mathcal{A}(A) = \mathbf{I}$ следует $\mathcal{B}(A) = \mathbf{I}$.

Если отрицание каждой формулы из Γ принадлежит Γ , то это же самое справедливо и для $\Gamma(\mathcal{A})$. Отсюда следует, что если $\mathcal{A}$ — Γ -подструктура структуры $\mathcal{B}$, то $\mathcal{A}(A) = \mathcal{B}(A)$ для каждой формулы A из $\Gamma(\mathcal{A})$. Действительно, если $\mathcal{A}(A) = \mathbf{I}$, то $\mathcal{A}(\neg A) = \mathbf{I}$; следовательно, $\mathcal{B}(\neg A) = \mathbf{I}$; таким образом, $\mathcal{B}(A) = \mathbf{I}$.

Из только что сделанного замечания и следствия к лемме 2 мы видим, что если Γ есть множество открытых формул языка L , то любая Γ -подструктура есть просто подструктура, а любое Γ -расширение есть просто расширение. Если Γ — множество всех формул языка L , то мы говорим об элементарной подструктуре вместо Γ -подструктуры и элементарном расширении вместо Γ -расширения. Далее, если $\mathcal{A}$ — элементарная подструктура структуры $\mathcal{B}$, то мы имеем $\mathcal{A}(A) = \mathcal{B}(A)$ для каждой замкнутой формулы A языка L ; следовательно, $\mathcal{A}$ и $\mathcal{B}$ элементарно эквивалентны.

Если $\mathcal{A}$ есть произвольная Γ -подструктура структуры $\mathcal{B}$, то $\mathcal{A}$ является Δ -подструктурой структуры $\mathcal{B}$ для каждого подмножества Δ множества Γ . Если подмножество Δ состоит из формул языка L' , имеющего L своим расширением, то $\mathcal{A}|L'$ есть Δ -подструктура структуры $\mathcal{B}|L'$.

Лемма 3. Если в Γ имеется формула $x=e$ и $\mathcal{A}$ — некоторая Γ -подструктура структуры $\mathcal{B}$, то $\mathcal{A}(e) = \mathcal{B}(e)$.

Доказательство. Если i — имя индивида $\mathcal{A}(e)$, то в $\Gamma(\mathcal{A})$ имеется формула $i=e$ и $\mathcal{A}(i=e) = \mathbf{I}$.

Следовательно, $\mathcal{B}(i=e)=\mathbf{I}$; таким образом, $\mathcal{B}(e)=\mathcal{B}(i)=\mathcal{A}(i)=\mathcal{A}(e)$.

Пусть $\mathcal{A}$ и $\mathcal{B}$ — структуры для L такие, что $|\mathcal{A}|$ является подмножеством множества $|\mathcal{B}|$. Обогащаем $\mathcal{B}$ до структуры $\mathcal{B}_{\mathcal{A}}$ для $L(\mathcal{A})$ следующим образом: если i — имя индивида a из $\mathcal{A}$, то значением символа i в структуре $\mathcal{B}_{\mathcal{A}}$ является a .

Пусть $L'=L(\mathcal{A})$ — язык для $\mathcal{B}_{\mathcal{A}}$, тогда имя i в L' играет в $L'(\mathcal{B}_{\mathcal{A}})$ двойную роль; это какая-то константа из L' и имя некоторого индивида из $\mathcal{B}_{\mathcal{A}}$. Мы утверждаем, что по крайней мере для получения истинностных значений $\mathcal{B}_{\mathcal{A}}(A)$ это различие не играет никакой роли. Чтобы убедиться в этом, допустим, что мы временно считаем любое такое имя i константой из L' и используем i' в качестве имени соответствующего индивида из $\mathcal{B}_{\mathcal{A}}$. Тогда i' — имя индивида $\mathcal{B}_{\mathcal{A}}(i)$. Если A' получается заменой i на i' из A , то $\mathcal{B}_{\mathcal{A}}(A)=\mathcal{B}_{\mathcal{A}}(A')$ по лемме из § 2.5.

Пусть Γ — множество формул языка L и $\mathcal{A}$ — структура для L . Γ -диаграммой структуры $\mathcal{A}$, обозначаемой через $D_{\Gamma}(\mathcal{A})$, называется теория, язык которой есть $L(\mathcal{A})$, а нелогическими аксиомами являются формулы A из $\Gamma(\mathcal{A})$ такие, что $\mathcal{A}(A)=\mathbf{I}$. Если Γ — множество открытых формул, то мы пишем $D(\mathcal{A})$ вместо $D_{\Gamma}(\mathcal{A})$; если Γ — множество всех формул, то мы пишем $D_e(\mathcal{A})$ вместо $D_{\Gamma}(\mathcal{A})$.

Лемма о диаграмме. Пусть Γ — множество формул языка L , а $\mathcal{A}$ и $\mathcal{B}$ — структуры для L такие, что $|\mathcal{A}|$ является подмножеством множества $|\mathcal{B}|$. Тогда $\mathcal{A}$ является Γ -подструктурой структуры $\mathcal{B}$ тогда и только тогда, когда $\mathcal{B}_{\mathcal{A}}$ является моделью теории $D_{\Gamma}(\mathcal{A})$.

Доказательство. Для замкнутых формул A языка $L(\mathcal{A})$ имеем $\mathcal{B}_{\mathcal{A}}(A)=\mathcal{B}(A)$, потому что $\mathcal{B}_{\mathcal{A}}$ является обогащением структуры $\mathcal{B}$. Лемма следует тогда из определений Γ -подструктуры и Γ -диаграммы.

Множество формул Γ языка L называется *регулярным*, если каждая формула вида $x=u$ или $x \neq u$ принадлежит Γ и для каждой формулы A из Γ каждая формула вида $A[x_1, \dots, x_n]$ принадлежит Γ .

Теорема о расширении модели (Кислер). Пусть $\mathcal{A}$ — структура для L , T — теория языка L , Γ — некоторое регулярное множество формул языка L . Тогда

$\mathcal{A}$ имеет Γ -расширение, являющееся моделью теории T , тогда и только тогда, когда каждая теорема теории T , являющаяся дизъюнкцией отрицаний некоторых формул из Γ , является истинной в $\mathcal{A}$.

Доказательство. Предположим, что такое Γ -расширение $\mathcal{B}$ существует. Мы должны показать, что если

$$\vdash \neg \bigvee A_1 \vee \dots \vee \neg A_n,$$

где каждое A_i принадлежит Γ , то $\bigvee A_1 \vee \dots \vee \neg A_n$ является истинной в $\mathcal{A}$. Если это не так, то существует $\mathcal{A}$ -частный случай $\bigvee A'_1 \vee \dots \vee \neg A'_n$ формулы $\bigvee A_1 \vee \dots \vee \neg A_n$ такой, что $\mathcal{A}(A'_i)=\mathbf{I}$ для $i=1, \dots, n$. Поскольку $\mathcal{B}$ является Γ -расширением структуры $\mathcal{A}$ и A'_i принадлежит $\Gamma(\mathcal{A})$, то $\mathcal{B}(A'_i)=\mathbf{I}$. Следовательно, $\mathcal{B}(\bigvee A'_1 \vee \dots \vee \neg A'_n)=\mathbf{I}$. Это невозможно, так как $\bigvee A'_1 \vee \dots \vee \neg A'_n$ является $\mathcal{B}$ -частным случаем некоторой теоремы теории T и $\mathcal{B}$ является моделью теории T .

Теперь предположим, что условие выполнено. Образует T' из T добавлением всех имен языка $L(\mathcal{A})$ в качестве новых констант; образуем T'' из T' добавлением всех нелогических аксиом теории $D_{\Gamma}(\mathcal{A})$ в качестве новых аксиом. Покажем, что T'' является непротиворечивой. Если это не так, то по теореме редукции для непротиворечивости мы имеем

$$\vdash_{T'} \neg A'_1 \vee \dots \vee \neg A'_n,$$

где каждая A'_i есть формула из $\Gamma(\mathcal{A})$ такая, что $\mathcal{A}(A'_i)=\mathbf{I}$. Следовательно, по теореме о константах имеем

$$\vdash \neg A_1 \vee \dots \vee \neg A_n,$$

где A_i получается из A'_i заменой имен новыми переменными. Тогда A_i получается из некоторой формулы, принадлежащей Γ , подстановкой переменных и, следовательно, ввиду регулярности Γ , принадлежит Γ . Следовательно, по предположению $\bigvee A_1 \vee \dots \vee \neg A_n$ является истинной в $\mathcal{A}$. Отсюда следует, что $\mathcal{A}(\bigvee A'_1 \vee \dots \vee \neg A'_n)=\mathbf{I}$; таким образом, $\mathcal{A}(A'_i)=\mathbf{I}$ для некоторого i ; получили противоречие.

По теореме полноты T'' имеет модель $\mathcal{B}'$. Если i и j — имена различных индивидов из $\mathcal{A}$, то $i \neq j$ является формулой из $\Gamma(\mathcal{A})$ (так как множество Γ регулярное) и $D(i \neq j)=\mathbf{I}$. Следовательно, $i \neq j$ является аксиомой теории $D_{\Gamma}(\mathcal{A})$; таким образом, $\mathcal{B}'(i \neq j)=\mathbf{I}$ и, значит,

$\mathcal{B}'(i) \neq \mathcal{B}'(j)$. Заменяя $\mathcal{B}'$ на изоморфную структуру, легко заметить, что мы можем предполагать, что для каждого имени i языка $L(\mathcal{A})$ $\mathcal{B}'(i)$ является индивидом, именем которого является i . Это означает, что если $\mathcal{B}$ есть обеднение структуры $\mathcal{B}'$ до L , то $\mathcal{B}_{\mathcal{A}} = \mathcal{B}'$. Так как $\mathcal{B}'$ есть модель теории $D_{\Gamma}(\mathcal{A})$, то, как следует из леммы о диаграмме, $\mathcal{B}$ есть Γ -расширение структуры $\mathcal{A}$, в то время как $\mathcal{B}$ есть модель теории T по лемме 1 из § 4.2.

Следствие. Пусть Γ — регулярное множество формул языка L и Δ — множество формул, содержащее каждую формулу $\forall x_1 \dots \forall x_n A$, где A — дизъюнкция отрицаний некоторых формул из Γ . Если $\mathcal{A}$ — структура для L и $\mathcal{B}$ — Δ -расширение структуры $\mathcal{A}$, то существует Γ -расширение $\mathcal{C}$ структуры $\mathcal{B}$, которое является элементарным расширением структуры $\mathcal{A}$.

Доказательство. Пусть Γ' — множество формул $A[i_1, \dots, i_k]$, где A из Γ и $i_1, \dots, i_k$ — имена языка $L(\mathcal{A})$. Покажем, что существует Γ' -расширение структуры $\mathcal{B}_{\mathcal{A}}$, которое является моделью теории $D_{\mathcal{C}}(\mathcal{A})$. По теореме нам нужно лишь показать, что если $A_1, \dots, A_n$ из Γ' и $\neg A_1 \vee \dots \vee \neg A_n$ является теоремой теории $D_{\mathcal{C}}(\mathcal{A})$, то $\neg A_1 \vee \dots \vee \neg A_n$ является истинной в $\mathcal{B}_{\mathcal{A}}$. Замыкание B формулы $\neg A_1 \vee \dots \vee \neg A_n$ является теоремой теории $D_{\mathcal{C}}(\mathcal{A})$; таким образом, по лемме о диаграмме $\mathcal{A}(B) = \mathcal{A}_{\mathcal{A}}(B) = \mathbf{I}$. Поскольку B принадлежит $\Delta(\mathcal{A})$, то она является аксиомой теории $D_{\Delta}(\mathcal{A})$; таким образом, по лемме о диаграмме снова имеем $\mathcal{B}_{\mathcal{A}}(B) = \mathbf{I}$. Следовательно, $\neg A_1 \vee \dots \vee \neg A_n$ является истинной в $\mathcal{B}_{\mathcal{A}}$.

Пусть $\mathcal{C}'$ — Γ' -расширение структуры $\mathcal{B}_{\mathcal{A}}$, которое представляет собой модель теории $D_{\mathcal{C}}(\mathcal{A})$, и пусть $\mathcal{C} = \mathcal{C}' \upharpoonright L$. Поскольку Γ является подмножеством множества Γ' , то $\mathcal{C}$ есть Γ -расширение структуры $\mathcal{B}$. Если i — имя индивида a из $\mathcal{A}$, то $\mathcal{C}'(i) = \mathcal{B}_{\mathcal{A}}(i) = a$ по лемме 3. Отсюда следует, что $\mathcal{C}' = \mathcal{C}_{\mathcal{A}}$; следовательно, по лемме о диаграмме $\mathcal{C}$ — элементарное расширение структуры $\mathcal{A}$.

Применим наши результаты для решения следующей проблемы: каким условиям должны удовлетворять модели теории T , чтобы T была эквивалентна теории, нелогические аксиомы которой принадлежат Γ ? Мы решим эту проблему в том случае, когда Γ — множество открытых формул и когда Γ — множество экзистенциальных формул.

Лемма 4. Пусть Γ — множество формул языка $L(T)$ и Γ' — множество всех тех формул из Γ , которые являются теоремами теории T . Если каждая структура для $L(T)$, в которой все формулы из Γ' являются истинными, является моделью теории T , то T эквивалентна теории, нелогические аксиомы которой принадлежат Γ .

Доказательство. Пусть T' — теория языка $L(T)$, нелогические аксиомы которой являются формулами из Γ' . Ясно, что теория T — расширение теории T' . По предположению каждая модель теории T' представляет собой модель теории T ; поэтому по следствию к теореме полноты теория T' является расширением теории T . Значит, T эквивалентна T' .

Теорема Лося — Тарского. Теория T эквивалентна открытой теории тогда и только тогда, когда каждая подструктура произвольной модели теории T является моделью теории T .

Доказательство. Предположим, что T эквивалентна открытой теории T' . По следствию к теореме полноты достаточно показать, что каждая подструктура $\mathcal{A}$ произвольной модели $\mathcal{B}$ теории T' является моделью теории T' . По следствию к лемме 2 каждая открытая формула, истинная в $\mathcal{B}$, является истинной в $\mathcal{A}$; следовательно, $\mathcal{A}$ является моделью теории T' .

Предположим, что условие теоремы выполняется. По лемме 4 достаточно показать, что если каждая открытая теорема теории T является истинной в $\mathcal{A}$, то $\mathcal{A}$ — модель теории T . По теореме о расширении модели $\mathcal{A}$ имеет расширение, являющееся моделью теории T ; следовательно, по условию теоремы $\mathcal{A}$ — модель теории T .

Последовательность $\mathcal{A}_1, \mathcal{A}_2, \dots$ структур для L называется *цепью*, если для каждого n структура $\mathcal{A}_{n+1}$ является расширением $\mathcal{A}_n$. Для каждой такой цепи мы определяем структуру $\mathcal{A}$, которую мы называем *объединением* цепи. Универсумом структуры $\mathcal{A}$ является объединение универсумов структур $\mathcal{A}_n$. Если $a_1, \dots, a_k$ принадлежат этому объединению, то существует n такое, что все $a_1, \dots, a_k$ — индивиды структуры $\mathcal{A}_n$. Положим

$$f_{\mathcal{A}}(a_1, \dots, a_k) = f_{\mathcal{A}_n}(a_1, \dots, a_k),$$

$$p_{\mathcal{A}}(a_1, \dots, a_k) \leftrightarrow p_{\mathcal{A}_n}(a_1, \dots, a_k).$$

Используя определение цепи, легко заметить, что это определение не зависит от выбора n , а также, что $\mathcal{A}$ является расширением каждой структуры $\mathcal{A}_n$.

Элементарной цепью называется цепь $\mathcal{A}_1, \mathcal{A}_2, \dots$ такая, что для каждого n структура $\mathcal{A}_{n+1}$ является элементарным расширением структуры $\mathcal{A}_n$.

Лемма Тарского. Если $\mathcal{A}_1, \mathcal{A}_2, \dots$ — элементарная цепь, то объединение $\mathcal{A}$ цепи является элементарным расширением каждой структуры $\mathcal{A}_n$.

Доказательство. Мы должны показать, что если A — замкнутая формула языка $L(\mathcal{A}_n)$, то $\mathcal{A}_n(A) = \mathcal{A}(A)$. Используем индукцию по длине A . Если A — атомная, то $\mathcal{A}_n(A) = \mathcal{A}(A)$ по следствию к лемме 2. Если A — отрицание или дизъюнкция, то результат непосредственно следует из индуктивного предположения. Теперь предположим, что A есть $\exists x B$. Если $\mathcal{A}(A) = \text{Л}$, то $\mathcal{A}(B_x[i]) = \text{Л}$ для всех i из $L(\mathcal{A})$. По индуктивному предположению $\mathcal{A}_n(B_x[i]) = \text{Л}$ для всех i из $L(\mathcal{A}_n)$; следовательно, $\mathcal{A}_n(A) = \text{Л}$. Если $\mathcal{A}(A) = \text{И}$, то $\mathcal{A}(B_x[i]) = \text{И}$ для некоторого i из $L(\mathcal{A})$. Выберем k так, чтобы $k > n$ и i являлось именем из $L(\mathcal{A}_k)$. По индуктивному предположению $\mathcal{A}_k(B_x[i]) = \text{И}$; следовательно, $\mathcal{A}_k(A) = \text{И}$. Поскольку $\mathcal{A}_k$ — элементарное расширение $\mathcal{A}_n$, то отсюда следует, что $\mathcal{A}_n(A) = \text{И}$.

Теорема Чжана — Лося — Сушко. Теория T эквивалентна теории, нелогические аксиомы которой экзистенциальны, тогда и только тогда, когда для каждой цепи моделей теории T объединение этой цепи является моделью теории T .

Доказательство. Предположим, что теория T эквивалентна теории T' , нелогические аксиомы которой экзистенциальны. По следствию к теореме полноты достаточно доказать, что объединение $\mathcal{A}$ цепи $\mathcal{A}_1, \mathcal{A}_2, \dots$ моделей теории T' является моделью теории T' . Пусть $\exists x_1 \dots \exists x_n A$ — $\mathcal{A}$ -частный случай некоторой нелогической аксиомы теории T' . Для достаточно большого k $\exists x_1 \dots \exists x_n A$ является $\mathcal{A}_k$ -частным случаем этой аксиомы; следовательно, $\mathcal{A}_k(\exists x_1 \dots \exists x_n A) = \text{И}$. Отсюда следует, что

$$\mathcal{A}_k(A[i_1, \dots, i_n]) = \text{И}$$

для некоторых $i_1, \dots, i_n$ из $L(\mathcal{A}_k)$. По следствию

к лемме 2 получаем

$$\mathcal{A}(A[i_1, \dots, i_n]) = \text{И};$$

следовательно,

$$\mathcal{A}(\exists x_1 \dots \exists x_n A) = \text{И}.$$

Итак, мы показали, что $\mathcal{A}$ является моделью теории T' .

Теперь предположим, что для каждой цепи моделей теории T объединение этой цепи является моделью теории T . По лемме 4 достаточно показать, что если $\mathcal{A}$ — структура, в которой каждая экзистенциальная теорема теории T является истинной, то $\mathcal{A}$ является моделью теории T . Построим цепь $\mathcal{A}_1, \mathcal{A}_2, \dots$ такую, что $\mathcal{A}_1 = \mathcal{A}$, $\mathcal{A}_{2n}$ является моделью теории T , а $\mathcal{A}_{2n+1}$ является элементарным расширением структуры $\mathcal{A}_{2n+1}$. Предположим, что это уже сделано, и пусть $\mathcal{B}$ — объединение этой цепи. Тогда $\mathcal{B}$ — объединение цепи $\mathcal{A}_2, \mathcal{A}_4, \dots$ моделей теории T и, следовательно, является моделью теории T . Но $\mathcal{B}$ также есть объединение элементарной цепи $\mathcal{A}_1, \mathcal{A}_3, \dots$. Следовательно, по лемме Тарского $\mathcal{B}$ — элементарное расширение структуры $\mathcal{A}_1 = \mathcal{A}$ и, значит, элементарно эквивалентна $\mathcal{A}$. Отсюда следует, что $\mathcal{A}$ — модель теории T .

Теперь определим $\mathcal{A}_n$. Предположим, что $\mathcal{A}_{2n-1}$ уже определена и $\mathcal{A}_{2n-1}$ является элементарным расширением структуры $\mathcal{A}_1 = \mathcal{A}$; строим $\mathcal{A}_{2n}$ и $\mathcal{A}_{2n+1}$. Пусть Γ — множество универсальных формул языка L ; покажем, что существует Γ -расширение $\mathcal{A}_{2n}$ структуры $\mathcal{A}_{2n-1}$, которое является моделью теории T . По теореме о расширении модели достаточно показать, что если $\vdash_T A$, где A — дизъюнкция отрицаний некоторых универсальных предложений, то A является истинной в $\mathcal{A}_{2n-1}$. Пусть A имеет экзистенциальную пренексную форму B . По предположению B является истинной в $\mathcal{A}$ и, следовательно, в $\mathcal{A}_{2n-1}$. Значит, $\mathcal{A}_{2n-1}$ является моделью теории, у которой B — единственная нелогическая аксиома. Так как A — теорема этой теории, то A истинна в $\mathcal{A}_{2n-1}$.

Так как каждая открытая формула принадлежит Γ , то $\mathcal{A}_{2n}$ — расширение структуры $\mathcal{A}_{2n-1}$. По следствию к теореме о расширении модели существует расширение $\mathcal{A}_{2n+1}$ структуры $\mathcal{A}_{2n}$, которое является элементарным расширением $\mathcal{A}_{2n-1}$. Это завершает доказательство теоремы.

Если мы применим эту теорему к теории G и используем хорошо известный факт, что объединение цепи групп есть группа, то мы выводим отсюда, что G эквивалентна теории, у которой нелогические аксиомы экзистенциальны. Аксиомы такой теории также хорошо известны: они состоят из ассоциативного закона и аксиом $\exists x(x \cdot y = z)$ и $\exists x(y \cdot x = z)$.

5.3. Мощность моделей

В этом параграфе мы предполагаем известными некоторые элементарные результаты о мощностях. Доказательства можно найти в главе 9 или в любом учебнике по теории множеств.

Под *мощностью* структуры $\mathcal{A}$ мы понимаем мощность ее универсума $|\mathcal{A}|$ (*). Мы будем говорить, что $\mathcal{A}$ конечна или бесконечна, счетна или несчетна, если $|\mathcal{A}|$ имеет соответствующее свойство.

Пусть m — произвольная бесконечная мощность. Язык первого порядка L называется *m-языком*, если мощность множества нелогических символов языка L не превосходит m . Теория T называется *m-теорией*, если $L(T)$ — m -язык. Мы говорим *счетный язык* и *счетная теория* вместо $\aleph_0$ -языка и $\aleph_0$ -теории.

Лемма. Если m — бесконечная мощность и L — m -язык, то L_c содержит самое большее m специальных констант.

Доказательство. Покажем индукцией по n , что существует самое большее m специальных констант уровня n ; отсюда будет следовать, что существует самое большее $\aleph_0 \cdot m = m$ специальных констант. Так как L содержит только счетное число логических символов, то L содержит самое большее $\aleph_0 + m = m$ символов. Если Q — множество всех символов языка L и всех специальных констант уровня, меньшего n , то по индуктивному предположению мощность Q не превосходит $m + nm = m$. Следовательно, для каждого k число выражений длины k , образуемых с помощью символов из Q , не больше $m^k = m$; таким образом, число всех выражений, образуемых с помощью символов из Q , не превосходит $\aleph_0 \cdot m = m$. Отсюда немедленно

*) В главе 9 мы вместо «мощность множества» говорим «кардинал множества». — Прим. перев.

следует, что число специальных констант уровня n не больше m .

Теорема о мощности (Тарский). Пусть m — бесконечная мощность и T — m -теория, имеющая бесконечную модель. Тогда T имеет модель мощности m .

Доказательство. Строим U из T следующим образом: добавляем множество новых констант мощности m и, если e и e' — различные новые константы, добавляем аксиому $e \neq e'$. Покажем, что U имеет модель. Ввиду следствия к теореме компактности достаточно показать, что каждая конечная часть U' теории U имеет модель. Пусть $e_1, \dots, e_k$ — новые константы, встречающиеся в нелогических аксиомах теории U' . Пусть $\mathcal{A}$ — бесконечная модель теории T и $a_1, \dots, a_k$ — различные индивиды модели $\mathcal{A}$. Обогатим $\mathcal{A}$ до структуры $\mathcal{A}'$ для U' , придавая e_i значение a_i и новым константам, отличным от $e_1, \dots, e_k$, произвольные значения. Ясно, что $\mathcal{A}'$ является моделью для U' .

Число нелогических констант в U не превосходит $m + m = m$; следовательно, U — m -теория. По лемме U_c содержит самое большее m специальных констант. Из сказанного выше и леммы 3 из § 4.2 получаем, что U_c непротиворечива. Следовательно, по лемме 4 из § 4.2 U_c имеет модель $\mathcal{A}$, мощность которой не больше m . Аксиомы теории U гарантируют, что $\mathcal{A}(e) \neq \mathcal{A}(e')$, если e и e' — различные новые константы; следовательно, мощность $\mathcal{A}$ в точности равна m . Обеднение структуры $\mathcal{A}$ до $L(T)$ является моделью теории T мощности m .

Следствие (Лёвенгейм—Скулем). Если T — счетная теория, имеющая модель, то T имеет конечную или счетную модель.

Существуют несколько парадоксов, впервые указанных Скулемом, получающихся из теоремы о мощности и теоремы Лёвенгейма—Скулема. Мы наверняка можем формализовать достаточно большую часть математики в счетной теории, чтобы доказать, что множество действительных чисел несчетно. Как же может такая теория иметь счетную модель? Объясним это. Множество действительных чисел в модели на самом деле счетно, и, значит, существует биективное отображение этого множества в множество натуральных чисел. Но это отображение не находится в этой модели; поэтому теорема теории, утверждающая,

что не существует биективного отображения множества действительных чисел в множество натуральных чисел, не опровергается.

Другой парадокс возникает из аксиом Пеано. Имеется хорошо известное доказательство того, что любое множество объектов, удовлетворяющее этим аксиомам, изоморфно множеству натуральных чисел и поэтому счетно. Если же мы формализуем аксиомы Пеано в $L(N)$, то теорема о мощности показывает, что полученная теория имеет несчетные модели. Трудность здесь состоит в том, что мы не можем полностью выразить аксиому индукции (являющуюся одной из аксиом Пеано) в $L(N)$. Мы обсудим эту ситуацию более подробно в главе 8.

5.4. Совместная непротиворечивость

Пусть T и T' — некоторые теории. Объединением теорий T и T' , обозначаемым через $T \cup T'$, называется теория, нелогическими символами которой являются нелогические символы теории T и нелогические символы теории T' , а нелогическими аксиомами которой являются нелогические аксиомы теории T и нелогические аксиомы теории T' .

Теория $T \cup T'$ может быть противоречивой, даже если теории T и T' обе непротиворечивы; действительно, может существовать формула A такая, что $\vdash_T A$ и $\vdash_{T'} \neg A$. Мы покажем, что если не существует такой формулы A , то $T \cup T'$ непротиворечива. Это показывает, что любое противоречие в $T \cup T'$ может быть «локализовано» в формуле A , являющейся формулой обеих теорий T и T' .

Теорема о совместной непротиворечивости (Крейг—Робинсон). Пусть T и T' — некоторые теории. Тогда $T \cup T'$ противоречива тогда и только тогда, когда существует замкнутая формула A такая, что $\vdash_T A$ и $\vdash_{T'} \neg A$.

Доказательство. Если такая формула A существует, то A и $\neg A$ — теоремы теории $T \cup T'$; таким образом, $T \cup T'$ противоречива. Предположим, что такой формулы A не существует, и докажем, что $T \cup T'$ непротиворечива.

Пусть Γ — множество замкнутых формул языка $L(T)$, которые являются теоремами теории T' . Тогда $T[\Gamma]$ не-

противоречива. Действительно, в противном случае, как следует из теоремы редукции для непротиворечивости, существует формула A теории T , являющаяся дизъюнкцией отрицаний некоторых замкнутых теорем теории T' . Тогда $\vdash_T A$ и $\vdash_{T'} \neg A$, что противоречит нашему предположению.

Пусть L — язык первого порядка, нелогические символы которого являются нелогическими символами, общими для $L(T)$ и $L(T')$. Будем строить элементарную цепь $\mathcal{A}_1, \mathcal{A}_2, \dots$ моделей теории T и элементарную цепь $\mathcal{A}'_1, \mathcal{A}'_2, \dots$ моделей теории T' таких, что $\mathcal{A}_1|L, \mathcal{A}'_1|L, \mathcal{A}_2|L, \mathcal{A}'_2|L, \dots$ является элементарной цепью.

Пусть $\mathcal{A}_1$ — произвольная модель теории $T[\Gamma]$. Пусть Δ — множество всех формул языка L . Тогда Δ регулярно. Пусть $\mathcal{B}$ — обогащение структуры $\mathcal{A}_1|L$ до $L(T')$. Тогда одни и те же формулы языка L истинны в $\mathcal{A}_1$ и $\mathcal{B}$. Если формула языка L является теоремой теории T' , то ее замыкание принадлежит Γ и, следовательно, является истинным в $\mathcal{A}_1$; значит, сама формула истинна в $\mathcal{A}_1$, а следовательно, и в $\mathcal{B}$. Как следует из теоремы о расширении модели, существует модель $\mathcal{A}'_1$ теории T' , которая является Δ -расширением структуры $\mathcal{B}$. Тогда $\mathcal{A}'_1|L$ — элементарное расширение структуры $\mathcal{B}|L = \mathcal{A}_1|L$.

Опишем теперь конструкцию для $\mathcal{A}_n$ при $n > 1$; конструкция для $\mathcal{A}'_n$ аналогична. Пусть $\mathcal{C}$ — обогащение структуры $\mathcal{A}'_{n-1}|L$ до $L(T)$. Тогда $\mathcal{C}|L$ — элементарное расширение структуры $\mathcal{A}_{n-1}|L$; следовательно, $\mathcal{C}$ есть Δ -расширение структуры $\mathcal{A}_{n-1}$. Ввиду следствия к теореме о расширении модели существует Δ -расширение $\mathcal{A}_n$ структуры $\mathcal{C}$, являющееся элементарным расширением структуры $\mathcal{A}_{n-1}$. Тогда $\mathcal{A}_n$ является элементарным расширением структуры $\mathcal{A}_1$ и, следовательно, моделью теории T . Очевидно, что $\mathcal{A}_n|L$ — элементарное расширение структуры $\mathcal{C}|L = \mathcal{A}'_{n-1}|L$.

Пусть $\mathcal{A}$ — объединение цепи $\mathcal{A}_1, \mathcal{A}_2, \dots$ и $\mathcal{A}'$ — объединение цепи $\mathcal{A}'_1, \mathcal{A}'_2, \dots$. По лемме Тарского структура $\mathcal{A}$ является элементарным расширением структуры $\mathcal{A}_1$ и, значит, моделью теории T . Аналогично, структура $\mathcal{A}'$ является моделью теории T' . Теперь $\mathcal{A}|L = \mathcal{A}'|L$, так как они обе являются объединением цепи $\mathcal{A}_1|L, \mathcal{A}'_1|L, \mathcal{A}_2|L, \mathcal{A}'_2|L, \dots$. Из этого сразу

видно, что существует структура $\mathcal{B}$ для $T \cup T'$ такая, что $\mathcal{B} \models L(T) = \mathcal{A}$ и $\mathcal{B} \models L(T') = \mathcal{A}'$. Тогда $\mathcal{B}$ — модель теории $T \cup T'$; таким образом, $T \cup T'$ непротиворечива.

Следствие (интерполяционная лемма Крейга). Пусть T и T' — некоторые теории и $A \rightarrow B$ является теоремой теории $T \cup T'$ такой, что A — формула теории T а B — формула теории T' . Тогда существует формула такая, что $\vdash_T A \rightarrow C$ и $\vdash_{T'} C \rightarrow B$.

Доказательство. Вначале предположим, что A и B замкнуты. В теории $T[A] \cup T'[\neg B]$ мы можем доказать $A \wedge \neg B$ и $A \rightarrow B$; следовательно, по теореме тавтологии теории $T[A] \cup T'[\neg B]$ противоречива. По теореме Крейга — Робинсона существует замкнутая формула C такая, что C является теоремой теории $T[A]$, а $\neg C$ является теоремой теории $T'[\neg B]$. По теореме дедукции $\vdash_T A \rightarrow C$ и $\vdash_{T'} \neg B \rightarrow \neg C$; следовательно, по теореме тавтологии $\vdash_{T'} C \rightarrow B$.

В общем случае, подставляя новую константу вместо каждой переменной, свободной в A или B , получим формулы A' и B' . Из сказанного выше следует, что для подходящей формулы C' имеем $\vdash_U A' \rightarrow C'$ и $\vdash_{U'} C' \rightarrow B'$, где теории U и U' получены соответственно из теорий T и T' добавлением констант. По теореме о варианте C' может быть выбрана так, чтобы ни одна из переменных, связанных в C' , не была свободной в A или B . Заменяя новые константы первоначальными переменными, получим формулу C , обладающую ввиду теоремы о константах требуемыми свойствами.

Укажем одно применение интерполяционной леммы. Пусть Q — некоторое множество нелогических символов теории T . Предикатный символ p , не принадлежащий Q называется *определимым в терминах Q в T* , если существует формула A , не содержащая нелогических символов не принадлежащих Q , такая, что $\vdash_T p x_1 \dots x_n \leftrightarrow A$ (где $x_1, \dots, x_n$ различны). Функциональный символ f , не принадлежащий Q , называется *определимым в терминах Q в T* если существует формула A , не содержащая нелогических символов, не принадлежащих Q , такая, что $\vdash_T y = f x_1 \dots x_n \leftrightarrow A$ (где $x_1, \dots, x_n, y$ различны).

Пусть $\mathcal{A}$ и $\mathcal{B}$ — структуры для L , μ — нелогический символ языка L , а φ — биективное отображение из $|\mathcal{A}|$ в $|\mathcal{B}|$. Мы говорим, что φ есть μ -изоморфизм между $\mathcal{A}$ и $\mathcal{B}$,

если φ — изоморфизм между объединениями структур $\mathcal{A}$ и $\mathcal{B}$ до языка с единственным нелогическим символом μ .

Теорема определимости (Бет). Пусть Q — некоторое множество нелогических символов теории T , а μ — нелогический символ теории T , которого нет в Q . Тогда μ определим в терминах Q в T тогда и только тогда, когда для каждой пары моделей $\mathcal{A}$ и $\mathcal{B}$ теории T и каждого биективного отображения φ из $|\mathcal{A}|$ в $|\mathcal{B}|$, которое является ν -изоморфизмом для каждого ν из Q , отображение φ является μ -изоморфизмом.

Доказательство. Предположим, что μ — предикатный символ p ; если μ — функциональный символ, то доказательство по существу такое же. Предположим, что мы имеем $\vdash_T p x_1 \dots x_n \leftrightarrow A$, где A не содержит нелогических символов, не принадлежащих Q . Пусть $\mathcal{A}$, $\mathcal{B}$ и φ таковы, как в условии теоремы. Если $i_1, \dots, i_n$ — имена языка $L(\mathcal{A})$ и B есть $A_{x_1, \dots, x_n}[i_1, \dots, i_n]$, то

$$\begin{aligned}\mathcal{A}(p i_1 \dots i_n \leftrightarrow B) &= \text{И}, \\ \mathcal{B}(p i_1^\varphi \dots i_n^\varphi \leftrightarrow B^\varphi) &= \text{И}, \\ \mathcal{A}(B) &= \mathcal{B}(B^\varphi).\end{aligned}$$

Поэтому

$$\mathcal{A}(p i_1 \dots i_n) = \mathcal{B}(p i_1^\varphi \dots i_n^\varphi).$$

Отсюда следует, что

$$p_{\mathcal{A}}(a_1, \dots, a_n) \leftrightarrow p_{\mathcal{B}}(\varphi(a_1), \dots, \varphi(a_n))$$

для $a_1, \dots, a_n$ из $|\mathcal{A}|$; следовательно, φ есть p -изоморфизм.

Теперь предположим, что условие теоремы выполняется. Для каждого n -арного функционального или предикатного символа ν из T , которого нет в Q , вводим новый n -арный функциональный или предикатный символ ν' . Мы получаем T' из T , заменяя каждое ν на ν' (оставляя символы из Q неизменными). Покажем, что $p x_1 \dots x_n \rightarrow p' x_1 \dots x_n$ является теоремой теории $T \cup T'$. По теореме полноты нам нужно лишь показать, что эта формула является истинной в каждой модели $\mathcal{A}$ теории $T \cup T'$. $\mathcal{A} \models L(T)$ и $\mathcal{A} \models L(T')$ являются моделями теорий T и T' соответственно. Строим структуру $\mathcal{B}$ для $L(T)$, беря $|\mathcal{B}| = |\mathcal{A}|$, $\nu_{\mathcal{B}} = \nu_{\mathcal{A}}$ для ν из Q и $\nu_{\mathcal{B}} = \nu'_{\mathcal{A}}$ для ν , которого нет в Q . Так как $\mathcal{A} \models L(T')$ есть модель теории T' ,

то очевидно, что $\mathcal{B}$ есть модель теории T . Ясно также, что тождественное отображение из $\mathcal{A} \mid L(T)$ в $\mathcal{B}$ есть v -изоморфизм для v из Q ; следовательно, это отображение есть p -изоморфизм. Отсюда получаем, что $p_A = p_B = p'_A$; а из последнего равенства следует, что $px_1 \dots x_n \rightarrow p'_x_1 \dots x_n$ является истинной в $\mathcal{A}$.

Применим интерполяционную лемму Крейга к теореме

$$px_1 \dots x_n \rightarrow p'_x_1 \dots x_n$$

теории $T \cup T'$. Получим формулу A такую, что

$$\vdash_T px_1 \dots x_n \rightarrow A \text{ и } \vdash_{T'} A \rightarrow p'_x_1 \dots x_n.$$

Так как A принадлежит как T , так и T' , то она не содержит нелогических констант, не принадлежащих Q . По выбору T' из

$$\vdash_{T'} A \rightarrow p'_x_1 \dots x_n$$

следует

$$\vdash_T A \rightarrow px_1 \dots x_n;$$

поэтому имеем

$$\vdash_T px_1 \dots x_n \leftrightarrow A$$

по теореме тавтологии.

5.5. Полные теории

Мы уже использовали понятие полной теории при доказательстве теоремы полноты. Кроме этого, существует несколько других важных приложений полных теорий.

Для первого приложения предположим, что нам дана структура $\mathcal{A}$ для L . Теорией структуры $\mathcal{A}$, обозначаемой через $\text{Th}(\mathcal{A})$, называется теория, язык которой есть L , а нелогические аксиомы которой являются формулами языка L , истинными в $\mathcal{A}$. Ясно, что $\mathcal{A}$ — модель для $\text{Th}(\mathcal{A})$; следовательно, по теореме истинности теоремами теории $\text{Th}(\mathcal{A})$ являются в точности те формулы, которые истинны в $\mathcal{A}$.

Теория $\text{Th}(\mathcal{A})$ обычно трудно поддается изучению, потому что нам неизвестны ее нелогические аксиомы. Поэтому желательно найти простую аксиоматизацию теории $\text{Th}(\mathcal{A})$, т. е. найти теорию T , эквивалентную $\text{Th}(\mathcal{A})$, нелогические аксиомы которой просты. Мы будем, конечно, рассматривать только аксиомы, являющиеся истинными

в $\mathcal{A}$, т. е., мы будем рассматривать только теории T , имеющие $\mathcal{A}$ своей моделью. Следующая лемма показывает, что всякая такая теория, являющаяся полной, эквивалентна теории $\text{Th}(\mathcal{A})$.

Лемма 1. Для непротиворечивой теории T следующие условия эквивалентны:

(а) T — полная теория;

(б) каждые две модели теории T элементарно эквивалентны;

(в) для каждой модели $\mathcal{A}$ теории T теория T эквивалентна теории $\text{Th}(\mathcal{A})$.

Доказательство. Вначале покажем, что из (а) следует (б). Мы должны доказать, что если $\mathcal{A}$ и $\mathcal{B}$ — модели теории T , то каждая замкнутая формула A либо является истинной и в $\mathcal{A}$, и в $\mathcal{B}$, либо не является истинной ни в $\mathcal{A}$, ни в $\mathcal{B}$. Но первое выполняется, если $\vdash_T A$, а последнее выполняется, если $\vdash_T \neg A$; следовательно, одно или другое выполняется по (а).

Покажем теперь, что из (б) следует (в). Ясно, что теория $\text{Th}(\mathcal{A})$ — расширение теории T . По (б) каждая модель теории T элементарно эквивалентна $\mathcal{A}$ и, следовательно, есть модель теории $\text{Th}(\mathcal{A})$; таким образом, по следствию к теореме полноты теория T — расширение теории $\text{Th}(\mathcal{A})$.

Покажем теперь, что из (в) следует (а). Пусть $\mathcal{A}$ — некоторая модель теории T . Если A — замкнутая формула, то либо A , либо $\neg A$ истинна в $\mathcal{A}$ и, следовательно, является теоремой теории $\text{Th}(\mathcal{A})$. Таким образом, $\text{Th}(\mathcal{A})$ — полная теория; следовательно, по (в) T — полная теория.

Второе наше приложение также связано с леммой 1. Предположим, что T — полная теория, и допустим, что мы уже показали, что A выполняется в некоторой модели теории T . Согласно (б) из леммы 1 мы можем заключить, что A выполняется в каждой модели теории T .

Третье приложение полных теорий будет рассматриваться в главе 6. Эти приложения показывают важность нахождения методов доказательства того, что некоторые специальные теории полны. Мы даем один такой метод, другой будет дан в следующем параграфе.

Скажем, что формула A эквивалентна формуле B в T , если $\vdash_T A \leftrightarrow B$. Мы скажем, что теория T допускает

элиминацию кванторов, если каждая формула теории T эквивалентна в T некоторой открытой формуле. Ясно, что если T допускает элиминацию кванторов, то тем же свойством обладает и каждое простое расширение теории T .

Лемма 2. *Предположим, что теория T непротиворечива, T допускает элиминацию кванторов, T содержит какую-то константу и каждая формула теории T , свободная от переменных, разрешима в T . Тогда T полна.*

Доказательство. Если A — замкнутая формула теории T , то $\vdash_T A \leftrightarrow B$ для некоторой открытой формулы B . Так как мы можем подставить константу вместо переменных, свободных в B , то можно предполагать, что B свободна от переменных. Тогда B разрешима в T ; таким образом, A разрешима в T .

Практически трудно проверить в посылке леммы 2, что T допускает элиминацию кванторов. Мы докажем теорему, дающую достаточные условия для этого случая. Формула называется *простой экзистенциальной*, если она имеет вид $\exists x A$, где A — открытая формула.

Лемма 3. *Если каждая простая экзистенциальная формула эквивалентна в T открытой формуле, то T допускает элиминацию кванторов.*

Доказательство. Докажем индукцией по длине A , что A эквивалентна открытой формуле. Если A — атомная формула, то все ясно. Если A — отрицание или дизъюнкция, то результат следует из индуктивного предположения и теоремы эквивалентности. Теперь предположим, что A есть $\exists x B$. По индуктивному предположению B эквивалентна некоторой открытой формуле B' ; следовательно, по теореме эквивалентности A эквивалентна простой экзистенциальной формуле $\exists x B'$. Так как $\exists x B'$ эквивалентна открытой формуле, то такова же и A .

Лемма 4. *Пусть A — замкнутая формула теории T . Предположим, что T содержит какую-то константу и для каждой двух моделей $\mathcal{A}$ и $\mathcal{A}'$ теории T таких, что $\mathcal{A}(B) = \mathcal{A}'(B)$ для каждой свободной от переменных формулы B теории T , имеем $\mathcal{A}(A) = \mathcal{A}'(A)$. Тогда A эквивалентна в T формуле, свободной от переменных.*

Доказательство. Пусть Γ — множество теорем теории $T[A]$, свободных от переменных. Достаточно показать, что A — теорема теории $T[\Gamma]$. Действительно, отсюда по теореме редукции следует, что $\vdash_T B_1 \rightarrow \dots \rightarrow B_n \rightarrow A$,

где каждая B_i принадлежит Γ . Так как B_i принадлежит T , то теорема дедукции показывает, что $\vdash_T A \rightarrow B_i$. Тогда ввиду теоремы тавтологии имеем

$$\vdash_T A \leftrightarrow (B_1 \& \dots \& B_n)$$

и формула $B_1 \& \dots \& B_n$ свободна от переменных.

Предположим, что A не является теоремой теории $T[\Gamma]$. По теореме полноты существует модель $\mathcal{A}$ теории $T[\Gamma]$ такая, что $\mathcal{A}(A) = \text{Л}$. Пусть Δ — множество формул, свободных от переменных, которые истинны в $\mathcal{A}$. Пусть $\mathcal{A}'$ — любая модель теории $T[\Delta]$. Для каждой формулы B , свободной от переменных, имеем $\mathcal{A}(B) = \mathcal{A}'(B)$. Действительно, если $\mathcal{A}(B) = \text{И}$, то B принадлежит Δ и, следовательно, $\mathcal{A}'(B) = \text{И}$; если же $\mathcal{A}(B) = \text{Л}$, то $\neg B$ принадлежит Δ и, следовательно, $\mathcal{A}'(B) = \text{Л}$. Отсюда следует, что $\mathcal{A}'(A) = \mathcal{A}(A) = \text{Л}$; таким образом, $\mathcal{A}'(\neg A) = \text{И}$. Мы показали, что $\neg A$ истинна в $T[\Delta]$. По теореме полноты $\neg A$ — теорема теории $T[\Delta]$; таким образом, по теореме дедукции

$$\vdash_T C_1 \rightarrow \dots \rightarrow C_m \rightarrow \neg A,$$

где $C_1, \dots, C_m$ принадлежат Δ . Тогда по теореме тавтологии

$$\vdash_T A \rightarrow \neg(C_1 \& \dots \& C_m);$$

таким образом, $\neg(C_1 \& \dots \& C_m)$ принадлежит Γ . Поэтому заключаем, что все формулы

$$C_1, \dots, C_m \text{ и } \neg(C_1 \& \dots \& C_m)$$

истинны в $\mathcal{A}$, а это невозможно.

Скажем, что T удовлетворяет *условию изоморфизма*, если для любых двух моделей $\mathcal{A}$ и $\mathcal{A}'$ теории T и каждого изоморфизма φ подструктуры модели $\mathcal{A}$ и подструктуры модели $\mathcal{A}'$ существует расширение изоморфизма φ , которое является изоморфизмом между моделью модели $\mathcal{A}$ и подмоделью модели $\mathcal{A}'$. Скажем, что T удовлетворяет *подмодельному условию*, если для каждой модели $\mathcal{B}$ теории T , каждой подмодели $\mathcal{A}$ модели $\mathcal{B}$ и каждой замкнутой простой экзистенциальной формулы A языка $L(\mathcal{A})$ имеем $\mathcal{A}(A) = \mathcal{B}(A)$.

Лемма 5. *Пусть T' получается из T добавлением новой константы e . Если T удовлетворяет условию изоморфизма (подмодельному условию), то такова же и T' .*

Доказательство. Предположим, что T удовлетворяет условию изоморфизма. Пусть $\mathcal{A}$ и $\mathcal{A}'$ — модели теории T , и пусть φ — некоторый изоморфизм между подструктурой $\mathcal{B}$ модели $\mathcal{A}$ и подструктурой $\mathcal{B}'$ модели $\mathcal{A}'$. Тогда φ можно расширить до изоморфизма φ' между подмоделью $\mathcal{C}$ модели $\mathcal{A} \upharpoonright L(T)$ и подмоделью $\mathcal{C}'$ модели $\mathcal{A}' \upharpoonright L(T)$. Обогащаем $\mathcal{C}$ до структуры для $L(T')$, полагая $e_{\mathcal{C}} = e_{\mathcal{A}}$; это даст нам подмодель модели $\mathcal{A}$. Подобным же образом получаем подмодель модели $\mathcal{A}'$. Так как $\varphi(e_{\mathcal{A}}) = e_{\mathcal{A}'}$, то φ' — изоморфизм между этими подмоделями.

Предположим, что T удовлетворяет подмодельному условию. Пусть $\mathcal{B}$ — модель теории T , $\mathcal{A}$ — подмодель модели $\mathcal{B}$ и A — замкнутая простая экзистенциальная формула языка $L(\mathcal{A})$. Пусть A' получается из A подстановкой имени индивида $\mathcal{A}(e)$ вместо e . По лемме из § 2.5 имеем

$$\mathcal{A}(A') = \mathcal{A}(A) \quad \text{и} \quad \mathcal{B}(A') = \mathcal{B}(A).$$

Применяя подмодельное условие для T к $\mathcal{A} \upharpoonright L(T)$ и $\mathcal{B} \upharpoonright L(T)$, находим, что $\mathcal{A}(A') = \mathcal{B}(A')$; таким образом, $\mathcal{A}(A) = \mathcal{B}(A)$.

Лемма 6. Если T удовлетворяет условию изоморфизма и подмодельному условию и содержит некоторую константу, то каждая замкнутая простая экзистенциальная формула теории T эквивалентна в T формуле, свободной от переменных.

Доказательство. Пусть A — замкнутая простая экзистенциальная формула. По лемме 4 достаточно проверить, что если $\mathcal{A}$ и $\mathcal{A}'$ — модели теории T такие, что $\mathcal{A}(B) = \mathcal{A}'(B)$ для каждой B , свободной от переменных, то $\mathcal{A}(A) = \mathcal{A}'(A)$. Пусть B — множество всех $\mathcal{A}(a)$ для термов a , свободных от переменных. Так как T содержит константу, то B непусто; ясно, что $f_{\mathcal{A}}(a_1, \dots, a_n)$ принадлежит B , если $a_1, \dots, a_n$ принадлежат B . Отсюда следует, что B — универсум подструктуры $\mathcal{B}$ модели $\mathcal{A}$.

Пусть $\mathcal{B}'$ — соответствующая подструктура модели $\mathcal{A}'$. Мы утверждаем, что существует изоморфизм φ между $\mathcal{B}$ и $\mathcal{B}'$, определенный так: $\varphi(\mathcal{A}(a)) = \mathcal{A}'(a)$. То, что отображение φ корректно определено и биективно, следует из равенства $\mathcal{A}(a=b) = \mathcal{A}'(a=b)$. Тогда то, что

φ — изоморфизм, следует из равенств

$$\begin{aligned} \mathcal{A}(fa_1 \dots a_n = b) &= \mathcal{A}'(fa_1 \dots a_n = b) \quad \text{и} \\ \mathcal{A}(pa_1 \dots a_n) &= \mathcal{A}'(pa_1 \dots a_n). \end{aligned}$$

По условию изоморфизма φ можно расширить до изоморфизма между подмоделью $\mathcal{C}$ модели $\mathcal{A}$ и подмоделью $\mathcal{C}'$ модели $\mathcal{A}'$. Так как A — простая экзистенциальная формула, то из подмодельного условия следует, что $\mathcal{A}(A) = \mathcal{C}(A)$ и $\mathcal{A}'(A) = \mathcal{C}'(A)$. Но $\mathcal{C}(A) = \mathcal{C}'(A)$, так как $\mathcal{C}$ и $\mathcal{C}'$ изоморфны; таким образом, $\mathcal{A}(A) = \mathcal{A}'(A)$.

Теорема об элиминации кванторов. Если T удовлетворяет условию изоморфизма и подмодельному условию, то T допускает элиминацию кванторов.

Доказательство. Ввиду леммы 3 достаточно доказать, что каждая простая экзистенциальная формула A теории T эквивалентна в T открытой формуле. Пусть A' получается из A заменой каждой свободной в A переменной на новую константу; пусть T' получается из T добавлением этих констант (или добавлением одной новой константы, если A замкнута). По леммам 5 и 6 A' эквивалентна в T' формуле, свободной от переменных; следовательно, по теореме о константах A эквивалентна в T открытой формуле.

Чтобы проверить, что T удовлетворяет подмодельному условию, достаточно проверить, что следующее условие выполняется для каждой модели $\mathcal{B}$ теории T и каждой подмодели $\mathcal{A}$ модели $\mathcal{B}$: если $A_1, \dots, A_n$ — атомные формулы языка $L(\mathcal{A})$, в которых нет свободных переменных, за исключением x , а j — имя языка $L(\mathcal{B})$, то существует имя i языка $L(\mathcal{A})$ такое, что

$$\mathcal{B}(A_i[i]) = \mathcal{B}(A_i[j]) \quad \text{для} \quad i=1, \dots, n.$$

Пусть это проверено, и пусть $\exists x A$ — замкнутая простая экзистенциальная формула языка $L(\mathcal{A})$. Очевидно, что из $\mathcal{A}(\exists x A) = \mathbf{И}$ следует $\mathcal{B}(\exists x A) = \mathbf{И}$; мы должны доказать обратное. Предположим, что $\mathcal{B}(\exists x A) = \mathbf{И}$, и выберем имя j языка $L(\mathcal{B})$, так, чтобы $\mathcal{B}(A_x[j]) = \mathbf{И}$. Выберем, как и выше, i , где $A_1, \dots, A_n$ — атомные формулы, входящие в A . Тогда

$$\mathcal{A}(A[i]) = \mathcal{B}(A[i]) = \mathcal{B}(A[j]) = \mathbf{И};$$

таким образом,

$$\mathcal{A}(\exists x A) = \mathbf{И}.$$

Применим наши результаты для нахождения систем аксиом для поля комплексных чисел и поля действительных чисел. (Эти системы аксиом найдены Тарским.)

Поле комплексных чисел *алгебраически замкнуто*, т. е. каждый многочлен, отличный от константы, с коэффициентами из поля имеет корень в этом поле. Мы получаем элементарную теорию ACF алгебраически замкнутых полей из теории FL добавлением для каждого $n \geq 1$ аксиомы, утверждающей, что каждый многочлен степени n имеет корень. Например, аксиомой для $n=2$ является

$$y \neq 0 \rightarrow \exists x (y \cdot x \cdot x + z \cdot x + w = 0).$$

Используем теперь теорему об элиминации кванторов, чтобы показать, что ACF допускает элиминацию кванторов. Любая подструктура поля содержит 0, 1 и -1 и замкнута относительно сложения и умножения; таким образом, она есть подкольцо, содержащее 1. Следовательно, условие изоморфизма для ACF сводится к следующему: если $\mathcal{A}$ и $\mathcal{A}'$ — алгебраически замкнутые поля и φ — изоморфизм между подкольцом поля $\mathcal{A}$, содержащим 1, и подкольцом поля $\mathcal{A}'$, содержащим 1, то φ можно расширить до изоморфизма между алгебраически замкнутым подполем поля $\mathcal{A}$ и алгебраически замкнутым подполем поля $\mathcal{A}'$. Чтобы получить это расширение, вначале расширяем φ до изоморфизма между наименьшими подполями полей $\mathcal{A}$ и $\mathcal{A}'$, включающими эти подкольца, а затем полученный изоморфизм расширяем до изоморфизма между наименьшими алгебраически замкнутыми подполями, включающими эти подполя. То, что такие два расширения могут быть сделаны, доказывается в стандартных учебниках алгебры.

Предположим, что $\mathcal{A}$ — поле и a — терм языка $L(\mathcal{A})$, не содержащий переменных, отличных от x . Тогда существует многочлен p_a с коэффициентами из $\mathcal{A}$, который представляет a в следующем смысле: если $\mathcal{B}$ — расширение поля $\mathcal{A}$ и j — имя индивида b из $\mathcal{B}$, то $\mathcal{B}(a_x[j]) = p_a(b)$. Доказательство проводится индукцией по длине a ; детали оставляются читателю. Теперь предположим, что b — другой такой терм, и пусть $r = p_a - p_b$. Если A — атомная формула $a = b$, то $\mathcal{B}(A_x[j]) = \text{И}$ тогда и только тогда, когда $r(b) = 0$.

Если мы скомбинируем эти замечания с замечаниями, данными после теоремы об элиминации кванторов, то мы увидим, что для того, чтобы доказать, что ACF удовлетворяет подмодельному условию, достаточно доказать следующий результат: если $\mathcal{B}$ — алгебраически замкнутое поле, $\mathcal{A}$ — алгебраически замкнутое подполе поля $\mathcal{B}$, $r_1, \dots, r_n$ — многочлены с коэффициентами из $\mathcal{A}$ и b принадлежит $\mathcal{B}$, то существует a из $\mathcal{A}$ такое, что $r_i(a) = 0 \leftrightarrow r_i(b) = 0$ для всех i . Мы можем предполагать, что ни один из r_i не является постоянным многочленом 0, так как такое r_i можно выбросить из списка. Если некоторое $r_i(b)$ есть 0, то b — алгебраический элемент над $\mathcal{A}$ и, следовательно, принадлежит $\mathcal{A}$; таким образом, мы можем взять $a = b$. В противном случае мы находим a из $\mathcal{A}$ такое, что $r_i(a) \neq 0$ для всех i . Так как многочлен имеет только конечное число корней, то достаточно показать, что $\mathcal{A}$ бесконечно. Но если бы $a_1, \dots, a_k$ были всеми элементами из $\mathcal{A}$, то многочлен

$$(X - a_1) \cdot \dots \cdot (X - a_k) + 1$$

не имел бы корней в $\mathcal{A}$.

Пусть $\text{ACF}(n)$ — теория $\text{ACF} \cup \text{FL}(n)$. Покажем, что если n равно 0 или простому числу, то $\text{ACF}(n)$ полна. Так как теория $\text{ACF}(n)$ имеет модель, то она непротиворечива, а так как она есть простое расширение теории ACF, то она допускает элиминацию кванторов. Следовательно, по лемме 2 нам нужно лишь доказать, что каждая формула теории $\text{ACF}(n)$, свободная от переменных, разрешима в $\text{ACF}(n)$. Ввиду теоремы полноты для этого достаточно доказать, что если A — формула теории $\text{ACF}(n)$, свободная от переменных, то истинностное значение $\mathcal{A}(A)$ одинаково для всех моделей $\mathcal{A}$ теории $\text{ACF}(n)$. Если $n=0$, то пусть $\mathcal{B}$ — поле рациональных чисел; если n — простое число, то пусть $\mathcal{B}$ — поле целых чисел по модулю n . Каждая модель $\mathcal{A}$ теории $\text{ACF}(n)$ имеет подструктуру, изоморфную $\mathcal{B}$; таким образом, $\mathcal{A}(A) = \mathcal{B}(A)$ для всех моделей $\mathcal{A}$ теории $\text{ACF}(n)$ по следствию к лемме 2 из § 5.2.

Отсюда следует, что $\text{ACF}(0)$ эквивалентна теории поля комплексных чисел. Ввиду нашего второго приложения полных теорий отсюда следует, что каждая формула теории FL, истинная в поле комплексных чисел, является

истинной в каждом алгебраически замкнутом поле характеристики 0. Значение этого состоит в том, что мы имеем много средств, не пригодных в других полях (таких, как интегрирование по контуру), для того, чтобы доказывать, что некоторая формула является истинной в поле комплексных чисел.

Имея дело с полем действительных чисел, лучше рассматривать предикат $<$. Поэтому мы вводим теорию OF упорядоченных полей. Она получается из FL добавлением предикатного символа $<$ и аксиом

$$\text{OF1. } \neg(x < x).$$

$$\text{OF2. } x < y \rightarrow y < z \rightarrow x < z.$$

$$\text{OF3. } x < y \vee x = y \vee y < x.$$

$$\text{OF4. } x < y \rightarrow x + z < y + z.$$

$$\text{OF5. } 0 < x \rightarrow 0 < y \rightarrow 0 < x \cdot y.$$

В дальнейшем изложении будем предполагать известными основы теории упорядоченных полей.

Упорядоченное поле действительных чисел является *вещественно замкнутым*. Это означает, что из каждого положительного элемента извлекается квадратный корень и каждый многочлен нечетной степени имеет корень. Мы получаем элементарную теорию RCF вещественно замкнутых полей из теории OF добавлением аксиомы

$$0 < x \rightarrow \exists y (y \cdot y = x)$$

и для каждого нечетного n такой же аксиомы, как мы добавляли, чтобы получить ACF.

Теперь применяем теорему об элиминации кванторов для того, чтобы показать, что RCF допускает элиминацию кванторов. Условие изоморфизма теперь говорит следующее: если $\mathcal{A}$ и $\mathcal{A}'$ — вещественно замкнутые поля и φ — изоморфизм между подкольцом поля $\mathcal{A}$, содержащим 1, и подкольцом поля $\mathcal{A}'$, содержащим 1, то φ можно расширить до изоморфизма между вещественно замкнутым подполем поля $\mathcal{A}$ и вещественно замкнутым подполем поля $\mathcal{A}'$. (Конечно, этот изоморфизм должен сохранять порядок.) Опять-таки мы вначале расширяем φ до изоморфизма между наименьшими подполями, включающими эти подкольца, а затем полученный изоморфизм до изоморфизма между наименьшими вещественно замкнутыми подполями, включающими эти подполя.

Мы видим, как и ранее, что проверка подмодельного условия сводится к доказательству следующего: если $\mathcal{B}$ — вещественно замкнутое поле, $\mathcal{A}$ — вещественно замкнутое подполе поля $\mathcal{B}$, $r_1, \dots, r_n$ — многочлены с коэффициентами из $\mathcal{A}$, b принадлежит $\mathcal{B}$, то существует a из $\mathcal{A}$ такое, что

$$r_i(a) = 0 \leftrightarrow r_i(b) = 0 \quad \text{и} \quad r_i(a) < 0 \leftrightarrow r_i(b) < 0.$$

Снова мы можем предполагать, что ни один из r_i не является постоянным многочленом 0. Если $r_i(b) = 0$, то b — алгебраический элемент над $\mathcal{A}$ и, следовательно, принадлежит $\mathcal{A}$; таким образом, мы могли бы взять $a = b$. Поэтому мы можем предполагать, что $r_i(b) \neq 0$ для всех i .

Предположим вначале, что существует корень c некоторого многочлена r_i и корень d некоторого многочлена r_j такие, что $c < b < d$. Так как многочлен имеет только конечное число корней, то можно предполагать, что ни один из многочленов $r_1, \dots, r_n$ не имеет корней между c и d . Тогда каждый из многочленов $r_1, \dots, r_n$ имеет один и тот же знак в каждой точке из $\mathcal{B}$ между c и d . (Это происходит потому, что многочлен в вещественно замкнутом поле, положительный в некоторой точке и отрицательный в некоторой другой точке, имеет корень между этими точками.) Ввиду сказанного выше c и d принадлежат $\mathcal{A}$; таким образом, мы можем взять $a = \frac{1}{2}(c + d)$.

Теперь предположим, что никакой корень каждого многочлена r_i не превосходит b . Тогда знак многочлена r_i во всех точках, больших b , такой же, как его знак в точке b . Знак многочлена r_i при больших значениях аргумента определяется по знаку коэффициента многочлена r_i при высшей степени и, следовательно, один и тот же в $\mathcal{A}$ и в $\mathcal{B}$. Таким образом, если мы выберем a из $\mathcal{A}$ достаточно большим, то каждое $r_i(a)$ будет иметь тот же знак, что и $r_i(b)$. Подобное доказательство можно провести и в том случае, когда ни один корень любого многочлена r_i не меньше b .

Так как упорядоченное поле всегда имеет упорядоченное подполе, изоморфное упорядоченному полю рациональных чисел, то можно, как и раньше, показать, что каждая формула теории RCF, свободная от переменных,

разрешима в RCF; следовательно, теория RCF полна. Таким образом, RCF эквивалентна теории упорядоченного поля действительных чисел. Из этого легко можно получить аксиомы для поля действительных чисел (см. задачу 17).

5.6. Категоричность

Скажем, что теория T *категорична*, если любые две модели теории T изоморфны. Например, пусть T — теория без нелогических символов и с единственной нелогической аксиомой $x = y$. Тогда каждая модель теории T содержит только один индивид, и легко видеть, что любые две такие модели изоморфны.

Можно дать и более сложные примеры, чем этот; но все эти примеры имеют только конечные модели. Действительно, если T имеет бесконечную модель, то теорема о мощности показывает, что T имеет модели многих разных мощностей, а две модели с различными мощностями не могут быть изоморфными.

Это приводит нас к обобщению нашего определения. Пусть m — некоторая бесконечная мощность. Теория T называется *m -категоричной* (или *категоричной в мощности m*), если каждые две модели теории T мощности m изоморфны. Тогда мы имеем следующие возможности:

(i) T является m -категоричной для каждой m . Примером служит теория без нелогических символов и без нелогических аксиом.

(ii) T не m -категорична ни для какой m . Примером служит теория без нелогических аксиом и только с одним унарным предикатным символом в качестве нелогического символа. Известно также, что этим свойством обладает теория RCF.

(iii) T является $\aleph_0$ -категоричной, но не m -категоричной ни для какой несчетной m . Например, пусть единственным нелогическим символом теории T является унарный предикатный символ P . Пусть нелогические аксиомы теории T утверждают, что для каждого натурального числа k существуют по крайней мере k индивидов, принадлежащих множеству P , и по крайней мере k индивидов, не принадлежащих множеству P . Другой пример приводится в задаче 23.

(iv) T является m -категоричной для несчетной m , но не $\aleph_0$ -категоричной. Например, пусть нелогическими символами теории T будет бесконечная последовательность констант $e_1, e_2, \dots$, а нелогическими аксиомами будут $e_i \neq e_j$ для $i \neq j$. Известно также, что этим свойством обладает теория ACF.

Для счетных теорий имеются только эти возможности, так как *теорема Морли* утверждает, что если счетная теория m -категорична для какой-то несчетной m , то она m -категорична для всех несчетных m . Так как доказательство этой теоремы довольно длинное, то оно здесь не приводится.

Полезность понятия категоричности показывает следующая

Теорема Лося—Воота. Пусть m — некоторая бесконечная мощность. Если T — непротиворечивая m -теория, имеющая только бесконечные модели, и T является m -категоричной, то T полна.

Доказательство. Предположим, что существует замкнутая формула A , которая неразрешима в T . По следствию к теореме о редукции для непротиворечивости обе теории $T[\neg A]$ и $T[\neg\neg A]$ непротиворечивы. Поэтому обе эти теории имеют модели и эти модели бесконечны, потому что каждая модель теории T бесконечна. По теореме о мощности существует модель $\mathcal{A}$ теории $T[\neg A]$ мощности m и модель $\mathcal{B}$ теории $T[\neg\neg A]$ мощности m . Так как T является m -категоричной, то $\mathcal{A}$ и $\mathcal{B}$ изоморфны. Это невозможно, так как $\mathcal{A}(A) = \text{Л}$ и $\mathcal{B}(A) = \text{И}$.

Вместе с результатом, упомянутым в (iv), эта теорема дает новое доказательство полноты теории ACF.

Теперь будем исследовать $\aleph_0$ -категоричность. В оставшейся части этого параграфа $z_1, z_2, \dots$ будут означать переменные, расположенные в алфавитном порядке. Пишем $A[a_1, \dots, a_n]$ вместо $A_{z_1, \dots, z_n}[a_1, \dots, a_n]$. Обозначим через $S_n(L)$ множество формул языка L , в которых нет свободных переменных, отличных от $z_1, \dots, z_n$.

Пусть $\mathcal{A}$ — некоторая структура для L и $a_1, \dots, a_n$ — некоторые индивиды из $\mathcal{A}$. Типом n -ки $(a_1, \dots, a_n)$ называется множество всех формул A из $S_n(L)$ таких, что

$$\mathcal{A}(A[i_1, \dots, i_n]) = \text{И},$$

где $i_1, \dots, i_n$ — имена индивидов $a_1, \dots, a_n$ соответст-

венно. n -типом в $\mathcal{A}$ называется тип некоторой n -ки индивидов из $\mathcal{A}$. Так, единственным 0-типом в $\mathcal{A}$ является множество замкнутых формул, истинных в $\mathcal{A}$. Если T — теория, то мы пишем $S_n(T)$ вместо $S_n(L(T))$ и каждый n -тип в модели теории T называем n -типом в T .

Отметим несколько простых фактов про типы. Если Γ есть n -тип в структуре для L и A принадлежит $S_n(L)$, то в точности одна из формул A или $\neg A$ принадлежит Γ . Отсюда следует, что если один n -тип включается в другой, то эти два n -типа совпадают. Если

$$\vdash_T A_1 \vee \dots \vee A_k,$$

где $A_1, \dots, A_k$ принадлежат $S_n(T)$, то каждый n -тип в T содержит по крайней мере одну из формул A_i . Если $\vdash_T A_1 \rightarrow \dots \rightarrow A_k \rightarrow B$, где формулы $A_1, \dots, A_k, B$ принадлежат $S_n(T)$, то отсюда следует, что каждый n -тип в T , содержащий $A_1, \dots, A_k$, также содержит и B .

Лемма. Пусть T — счетная теория и Γ — непустое множество формул из $S_n(T)$ такое, что никакая дизъюнкция отрицаний формул из Γ не является теоремой теории T . Тогда существует n -тип в конечной или счетной модели T , содержащий Γ .

Доказательство. Образует T' из T добавлением n новых констант $e_1, \dots, e_n$ и добавлением $A[e_1, \dots, e_n]$ в качестве аксиомы для каждой A из Γ . По предположению, по теореме редукции для непротиворечивости и по теореме о константах теория T' непротиворечива. По теореме полноты и по теореме Лёвенгейма — Скулема T' имеет конечную или счетную модель $\mathcal{A}$. Пусть $a_i = \mathcal{A}(e_i)$. Тогда $\mathcal{A} \models L(T)$ является конечной или счетной моделью теории T и тип n -ки $(a_1, \dots, a_n)$ в этой модели содержит Γ .

Следствие. Если T — счетная теория и Γ есть n -тип в T , то Γ есть n -тип в конечной или счетной модели теории T .

Доказательство. Если $A_1, \dots, A_k$ принадлежат Γ , то не может выполняться $\vdash_T \neg A_1 \vee \dots \vee \neg A_k$; отсюда следовало бы, что некоторая $\neg A_i$ принадлежит Γ . По лемме некоторый n -тип в конечной или счетной модели теории T содержит Γ и, следовательно, равен Γ .

Пусть Γ — некоторое множество формул из $S_n(T)$. Формула A из $S_n(T)$ называется образующей для Γ , если $\neg A$

не является теоремой теории T и $\vdash_T A \rightarrow B$ для каждой формулы B из Γ . Если Γ имеет какую-то образующую, то назовем множество Γ *главным*.

Если A — образующая для n -типа Γ , то A принадлежит Γ . Иначе $\neg A$ принадлежала бы Γ ; поэтому $\vdash_T A \rightarrow \neg A$; следовательно, по теореме тавтологии $\vdash_T \neg A$. Отсюда следует, что Γ — множество всех формул B из $S_n(T)$ таких, что $\vdash_T A \rightarrow B$. Это показывает, что главный n -тип определяется любой своей образующей.

Теорема Эренфойхта. Пусть T — счетная непротиворечивая теория и Γ — некоторое подмножество множества $S_n(T)$, не являющееся главным. Тогда существует не более чем счетная модель $\mathcal{A}$ теории T такая, что никакой n -тип в $\mathcal{A}$ не содержит Γ .

Доказательство. По лемме из § 5.3 T_c содержит только счетное число специальных констант. Поэтому мы можем расположить множество n -ок различных специальных констант из T_c в последовательность.

Определим индуктивно последовательности $A_1, A_2, \dots$ замкнутых формул из T_c так, что

(а) $T_k = T_c[A_1, \dots, A_k]$ непротиворечива;

(б) A_k есть $\neg A[r_1, \dots, r_n]$, где A принадлежит Γ и $(r_1, \dots, r_n)$ — k -я по порядку n -ка в вышеуказанной последовательности. Прежде всего T непротиворечива; следовательно, $T_0 = T_c$ непротиворечива по лемме 3 из § 4.2.

Теперь предположим, что $A_1, \dots, A_{k-1}$ уже выбраны, и пусть Δ — множество формул A из $S_n(T)$ таких, что $A[r_1, \dots, r_n]$ — теорема теории T_{k-1} . Для любой такой A формула

$$A_1 \rightarrow \dots \rightarrow A_{k-1} \rightarrow A[r_1, \dots, r_n]$$

по теореме дедукции является теоремой теории T_c . Из доказательства леммы 3 из § 4.2 мы видим, что эта формула имеет доказательство в T_c , которое использует специальные аксиомы только для $r_1, \dots, r_n$ и специальных констант, входящих в $A_1, \dots, A_{k-1}$. Отсюда следует, что если B — конъюнкция этих специальных аксиом и $A_1, \dots, A_{k-1}$, то $B \rightarrow A[r_1, \dots, r_n]$ выводима в T_c без специальных аксиом для каждой A из Δ .

Можно записать B как $C[r_1, \dots, r_m]$, где $m \geq n$, $r_1, \dots, r_m$ различны и формула C принадлежит $S_m(T)$. По теореме о константах $\vdash_T C \rightarrow A$ для каждой A из Δ .

Если C' — формула $\exists z_{n+1} \dots \exists z_m C$, принадлежащая $S_n(T)$, то по правилу $\exists$ -введения $\vdash_T C' \rightarrow A$ для каждой A из Δ .

Так как $C[r_1, \dots, r_m]$ — теорема теории T_{k-1} , то по теореме подстановки и правилу отделения $C'[r_1, \dots, r_n]$ — теорема теории T_{k-1} . Так как T_{k-1} непротиворечива, то $\neg C'[r_1, \dots, r_n]$ не является теоремой теории T_{k-1} ; таким образом, $\neg C'$ не является теоремой теории T . Но C' не является образующей для Γ ; таким образом, должна существовать формула A в Γ такая, что $C' \rightarrow A$ не является теоремой теории T . Тогда A не принадлежит Δ . Пусть A_k есть $\neg A[r_1, \dots, r_n]$. Тогда по следствию к теореме редукции для непротиворечивости T_k непротиворечива.

Образуем T' , добавляя все $A_1, A_2, \dots$ в качестве новых аксиом к теории T_c . Каждая конечная часть теории T' имеет некоторую T_k в качестве своего расширения и поэтому непротиворечива. Следовательно, по теореме компактности и теореме полноты теория T' непротиворечива. Как следует из леммы 4 из § 4.2 T' имеет модель $\mathcal{A}$ такую, что каждый индивид из $\mathcal{A}$ есть $\mathcal{A}(r)$ для бесконечно многих r . Такая модель, конечно, не более чем счетна.

Пусть $a_1, \dots, a_n$ — индивиды из $\mathcal{A}$. Тогда можно найти различные специальные константы $r_1, \dots, r_n$ такие, что $\mathcal{A}(r_1) = a_1, \dots, \mathcal{A}(r_n) = a_n$. Для некоторой A из Γ формула $\neg A[r_1, \dots, r_n]$ является аксиомой теории T' и, следовательно, истинной в $\mathcal{A}$. Применяя лемму из § 2.5, заключаем, что $\neg A$ находится в типе n -ки $(a_1, \dots, a_n)$; таким образом, Γ не содержится в типе n -ки $(a_1, \dots, a_n)$. Это показывает, что Γ не содержится в n -типе в $\mathcal{A}$.

Теорема Рылль-Нардзевского. Пусть T — полная счетная теория, имеющая только бесконечные модели. Тогда следующие условия эквивалентны:

- (а) T является $\aleph_0$ -категоричной;
- (б) для каждого n теория T имеет лишь конечное число n -типов;
- (в) для каждого n каждый n -тип в T главный.

Доказательство. Предположим, что T имеет n -тип Γ , не являющийся главным; покажем, что тогда (а) и (б) ложны. По теореме Эренфойхта существует счетная модель $\mathcal{A}$ теории T , в которой Γ не является n -типом, в то время как по следствию к лемме существует счетная модель $\mathcal{B}$ теории T , в которой Γ является n -типом. Так как $\mathcal{A}$ и $\mathcal{B}$ не изоморфны, то (а) ложно.

Теперь покажем, что (б) ложно. Так как n -тип Γ не главный и так как конъюнкция формул из Γ принадлежит Γ , то по индукции можно выбрать формулы $A_1, A_2, \dots$ теории T такие, что для каждого k формула $(A_1 \& \dots \& A_{k-1}) \rightarrow A_k$ не является теоремой теории T . Тогда формула $\neg A_1 \vee \dots \vee \neg A_{k-1} \vee \neg A_k$ не является теоремой теории T . Следовательно, по лемме существует n -тип Γ_k в T , который содержит $A_1, \dots, A_{k-1}, \neg A_k$. Ясно, что n -типы Γ_k различны.

Теперь предположим, что (в) верно и докажем (а) и (б). Начнем с (б). Фиксируем n . Для каждого n -типа в T выберем образующую, и пусть эти образующие будут $A_1, A_2, \dots$. Тогда никакой n -тип не может содержать все формулы $\neg A_1, \neg A_2, \dots$. Следовательно, по лемме 2 и теореме тавтологии существует k такое, что $A_1 \vee \dots \vee A_k$ является теоремой теории T . Тогда каждый n -тип в T содержит A_i . Но если некоторый n -тип содержит A_i , то он содержит и n -тип с образующей A_i и, следовательно, совпадает с этим n -типом. Таким образом, n -типами являются лишь n -типы с образующими $A_1, \dots, A_k$.

Теперь докажем (а). Пусть $\mathcal{A}$ и $\mathcal{B}$ — модели теории T мощности $\aleph_0$. Расположим все элементы множеств $|\mathcal{A}|$ и $|\mathcal{B}|$ в последовательности различных элементов. Будем располагать их в новые последовательности $a_1, a_2, \dots$ и $b_1, b_2, \dots$ так, чтобы для каждого n $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ имели одинаковый тип. Вначале мы должны показать, что это выполняется для $n=0$, т. е. что пустая последовательность имеет одинаковый тип и в $\mathcal{A}$, и в $\mathcal{B}$. Это означает, что одинаковые замкнутые формулы истинны в $\mathcal{A}$ и $\mathcal{B}$, а это выполняется по лемме 1 из § 5.5.

Теперь предположим, что элементы $a_1, \dots, a_{n-1}, b_1, \dots, b_{n-1}$ уже выбраны. Сперва предположим, что n четное. Пусть a_n — первый индивид в старой последовательности индивидов из $\mathcal{A}$, которого нет среди $a_1, \dots, a_{n-1}$. Пусть Γ — тип n -ки $(a_1, \dots, a_n)$, а A — образующая для Γ . Тогда $\exists z_n A$ принадлежит типу $n-1$ -ки $(a_1, \dots, a_{n-1})$ и, следовательно, типу $n-1$ -ки $(b_1, \dots, b_{n-1})$. Отсюда следует, что мы можем выбрать b_n в $|\mathcal{B}|$ так, что A принадлежит типу n -ки $(b_1, \dots, b_n)$. Тогда тип n -ки $(b_1, \dots, b_n)$ включает Γ и поэтому должен быть равен Γ . Более того, $b_n \neq b_i$ для $i < n$; действительно, $a_n \neq a_i$ и, следовательно, формула $z_n \neq z_i$ принадлежит Γ .

Если n нечетно, то пусть b_n — первый индивид из старой последовательности индивидов из $\mathcal{B}$, которого нет среди $b_1, \dots, b_{n-1}$. Мы можем тогда выбрать a_n , как и выше. Первые n членов старой последовательности элементов из $\mathcal{A}$ встречаются среди $a_1, \dots, a_{2n}$; таким образом, каждый индивид из $\mathcal{A}$ есть a_i . Аналогично, каждый индивид из $\mathcal{B}$ есть b_i . Поэтому мы можем определить биективное отображение φ из $|\mathcal{A}|$ в $|\mathcal{B}|$ следующим образом: $\varphi(a_i) = b_i$. По лемме 2 из § 5.2 φ — изоморфизм.

В качестве приложения теоремы Рылль-Нардзевског покажем, что $\text{Th}(\mathcal{N})$ не является $\aleph_0$ -категоричной. В действительности легко видеть, что если i и j — различные натуральные числа, то тип i отличается от типа j . Таким образом, $\text{Th}(\mathcal{N})$ имеет счетные модели, не изоморфные $\mathcal{N}$.

Задачи

1. Пусть Γ — множество замкнутых формул языка L . Пусть $\mathfrak{I}(\Gamma)$ — такое же множество, как и в задаче 5 из главы 4, и пусть $\mathfrak{I}\mathfrak{E}(\Gamma)$ — множество таких V , принадлежащих $\mathfrak{I}(\Gamma)$, что для некоторой структуры $\mathcal{A}$ для L имеем $V(\mathcal{A}) = \mathfrak{I}(\mathcal{A})$ для всех A из Γ . Показать, что $\mathfrak{I}\mathfrak{E}(\Gamma)$ замкнуто в $\mathfrak{I}(\Gamma)$ и, следовательно, компактно. [Применить теорему компактности.]

2. Пусть $\mathfrak{Z}$ — класс структур для L . Если существует формула A языка L такая, что $\mathfrak{Z}$ — класс всех структур, в которых A является истинной, то $\mathfrak{Z}$ называется *элементарным классом*. Если существует теория T языка L такая, что $\mathfrak{Z}$ — класс всех моделей теории T , то $\mathfrak{Z}$ называется *обобщенно элементарным классом* *).

(а) Показать, что класс структур для L является элементарным классом тогда и только тогда, когда он является классом всех моделей некоторой конечно аксиоматизируемой теории языка L .

(б) Показать, что класс структур для L есть обобщенно элементарный класс тогда и только тогда, когда он является пересечением некоторого семейства элементарных классов.

(в) Пусть A — некоторое семейство обобщенно элементарных классов и $\mathfrak{Z}$ — элементарный класс, содержащий пересечение всех элементов из A . Показать, что существует конечное подсемейство A' семейства A такое, что $\mathfrak{Z}$ содержит пересечение всех элементов из A' . [Применить теорему компактности.]

(г) Пусть $\mathfrak{Z}_1, \mathfrak{Z}_2, \dots$ — последовательность элементарных классов таких, что, для всех n класс $\mathfrak{Z}_{n+1}$ есть собственный подкласс класса $\mathfrak{Z}_n$. Показать, что пересечение всех $\mathfrak{Z}_n$ не является элементарным классом. [Применить (в).]

*) В советской литературе принят термин *аксиоматизируемый класс*. — Прим. ред.

(д) Пусть $\mathfrak{Z}$ — обобщенно элементарный класс, $\mathfrak{Z}'$ — класс структур для L , которые не принадлежат $\mathfrak{Z}$. Показать, что $\mathfrak{Z}$ — элементарный класс тогда и только тогда, когда $\mathfrak{Z}'$ является обобщенно элементарным классом. [Применить (б), (в) и (а).]

3. (а) Пусть $\mathcal{A}$ — структура для L и B — непустое подмножество множества $|\mathcal{A}|$. Показать, что существует наименьшее подмножество C множества $|\mathcal{A}|$, включающее B и являющееся универсумом некоторой подструктуры структуры $\mathcal{A}$. Подструктуру с универсумом C мы называем подструктурой, порожденной множеством B .

(б) Пусть $\mathcal{B}$ — подструктура структуры $\mathcal{A}$, порожденная множеством B . Показать, что если m — наибольшая из следующих мощностей: $\aleph_0$, мощность множества B и мощность множества функциональных символов языка L , — то мощность структуры $\mathcal{B}$ не превосходит m . В частности, если L — счетный язык и множество B счетно, то структура $\mathcal{B}$ счетная.

(в) Структура $\mathcal{A}$ называется *конечно порожденной*, если существует конечное подмножество B множества $|\mathcal{A}|$ такое, что подструктура структуры $\mathcal{A}$, порожденная множеством B , совпадает с $\mathcal{A}$. Показать, что структура $\mathcal{A}$ имеет расширение, являющееся моделью теории T , тогда и только тогда, когда каждая конечно порожденная подструктура структуры $\mathcal{A}$ имеет расширение, являющееся моделью теории T . [Если $\mathcal{A}$ не имеет такого расширения, то по теореме о расширении модели существует открытая теорема A теории T , не являющаяся истинной в $\mathcal{A}$. Показать, что A не является истинной в некоторой конечно порожденной подструктуре структуры $\mathcal{A}$.]

(г) Показать, что структура $\mathcal{A}$ для открытой теории T является моделью теории T тогда и только тогда, когда каждая конечно порожденная подструктура структуры $\mathcal{A}$ является моделью теории T . [Применить (в) и теорему Лоса — Тарского.]

(д) Группа $\mathcal{A}$ называется *полной*, если для каждого положительного целого числа n и каждого индивида a из $\mathcal{A}$ существует индивид b из $\mathcal{A}$ такой, что $b^n = a$. Показать, что каждая абелева группа изоморфна подгруппе некоторой полной абелевой группы. [Всякая циклическая группа изоморфна некоторой подгруппе мультипликативной группы отличных от нуля комплексных чисел, а эта группа является полной. Обобщить результат на конечно порожденные абелевы группы и затем применить (в).]

4. (а) Пусть Γ — регулярное множество формул языка L и $\mathcal{A}, \mathcal{B}$ — структуры для L такие, что каждая дизъюнкция отрицаний формул из Γ , истинных в $\mathcal{A}$, является истинной в $\mathcal{B}$. Показать, что существует Γ -расширение структуры $\mathcal{B}$, изоморфное некоторому элементарному расширению структуры $\mathcal{A}$. [Обогатить $\mathcal{B}$ до структуры $\mathcal{B}'$ для $L(\mathcal{A})$. Найти Γ -расширение структуры $\mathcal{B}'$, являющееся моделью теории $D_e(\mathcal{A})$.]

(б) Показать, что если $\mathcal{A}$ и $\mathcal{B}$ — структуры для L , то $\mathcal{A}$ и $\mathcal{B}$ элементарно эквивалентны тогда и только тогда, когда они имеют изоморфные элементарные расширения. [Применить (а).]

5. Пусть $\mathcal{A}$ и $\mathcal{B}$ — структуры для L и Γ — некоторое множество формул языка L . Γ -морфизмом из $\mathcal{A}$ в $\mathcal{B}$ называется отображение φ из $|\mathcal{A}|$ в $|\mathcal{B}|$ такое, что для каждой формулы A , принадлежащей $\Gamma(\mathcal{A})$, из $\mathcal{A}(A) = \text{И}$ следует $\mathcal{B}(A^\varphi) = \text{И}$.

(а) Показать, что если $|\mathcal{A}|$ — подмножество множества $|\mathcal{B}|$, то $\mathcal{A}$ есть Γ -подструктура структуры $\mathcal{B}$ тогда и только тогда, когда тождественное отображение из $|\mathcal{A}|$ в $|\mathcal{B}|$ является Γ -морфизмом.

(б) Показать, что если $x=e$ принадлежит Γ и φ — Γ -морфизм из $\mathcal{A}$ в $\mathcal{B}$, то $\varphi(\mathcal{A}(e)) = \mathcal{B}(e)$.

(в) Если φ — отображение из $|\mathcal{A}|$ в $|\mathcal{B}|$, то мы обогащаем $\mathcal{B}$ до структуры $\mathcal{B}_\varphi$ для $L(\mathcal{A})$, придавая значение $\varphi(a)$ имени индивида a . Показать, что φ является Γ -морфизмом тогда и только тогда, когда $\mathcal{B}_\varphi$ является моделью теории $D_\Gamma(\mathcal{A})$. [Вначале показать, что $\mathcal{B}_\varphi(A) = \mathcal{B}_\varphi(A^\varphi) = \mathcal{B}(A^\varphi)$ для любой замкнутой формулы A языка $L(\mathcal{A})$.]

(г) Множество формул Γ называется *инвариантным*, если для каждой формулы A из Γ каждая формула $A[x_1, \dots, x_n]$ принадлежит Γ . Показать, что если Γ инвариантно и $L(T) = L$, то Γ -морфизм из $\mathcal{A}$ в некоторую модель теории T существует тогда и только тогда, когда каждая теорема теории T , являющаяся дизъюнкцией отрицаний формул из Γ , является истинной в $\mathcal{A}$. [Аналогично доказательству теоремы о расширении модели.]

(д) Пусть Γ — инвариантное множество формул, содержащее $x=y$; Δ — множество формул, содержащее каждую формулу $\forall x_1 \dots \forall x_n A$, где A — дизъюнкция отрицаний некоторых формул из Γ , φ — Δ -морфизм из $\mathcal{A}$ в $\mathcal{B}$. Показать, что существует Γ -морфизм ψ из $\mathcal{B}$ в некоторое элементарное расширение $\mathcal{C}$ структуры $\mathcal{A}$ такой, что $\psi\varphi$ есть тождественное отображение из $|\mathcal{A}|$ в $|\mathcal{C}|$. [Аналогично доказательству следствия к теореме о расширении модели.]

6. Формула называется *позитивной*, если она находится в префиксной форме и ее матрица построена из атомных формул с помощью нескольких применений дизъюнкций и конъюнкций. Формула называется *негативной*, если она есть отрицание позитивной формулы. Если Γ — множество атомных (позитивных, негативных) формул, то вместо Γ -морфизма мы будем говорить о *гомоморфизме* (позитивном гомоморфизме, негативном гомоморфизме).

(а) Показать, что отображение φ из $|\mathcal{A}|$ в $|\mathcal{B}|$ является гомоморфизмом тогда и только тогда, когда для всех нелогических символов f и p и для всех $a_1, \dots, a_n$ из $|\mathcal{A}|$

$$\varphi(f_{\mathcal{A}}(a_1, \dots, a_n)) = f_{\mathcal{B}}(\varphi(a_1), \dots, \varphi(a_n))$$

и

$$p_{\mathcal{A}}(a_1, \dots, a_n) \rightarrow p_{\mathcal{B}}(\varphi(a_1), \dots, \varphi(a_n)).$$

Показать, что в этом случае $\varphi(\mathcal{A}(a)) = \mathcal{B}(\varphi(a))$ для каждого свободного от переменных термина a языка $L(\mathcal{A})$.

(б) Показать, что сюръективный гомоморфизм является позитивным гомоморфизмом.

(в) Показать, что если φ — негативный гомоморфизм из $\mathcal{A}$ в $\mathcal{B}$, то существует позитивный гомоморфизм ψ из $\mathcal{B}$ в некоторое элементарное расширение $\mathcal{C}$ структуры $\mathcal{A}$ такой, что $\psi\varphi$ является тождественным отображением $|\mathcal{A}|$ в $|\mathcal{C}|$. [Применить 5 (д).]

(г) Пусть φ — позитивный гомоморфизм из $\mathcal{A}$ в $\mathcal{B}$. Показать, что существует элементарное расширение $\mathcal{A}'$ структуры $\mathcal{A}$ и негативный гомоморфизм ψ из $\mathcal{B}_\varphi$ в $\mathcal{A}'$. [Применить 5 (г) для по-

лучения негативного гомоморфизма из $\mathcal{B}_\varphi$ в некоторую модель теории $D_e(\mathcal{A})$.]

(д) Пусть φ — позитивный гомоморфизм из $\mathcal{A}$ в $\mathcal{B}$. Показать, что существуют элементарные расширения $\mathcal{A}'$ и $\mathcal{B}'$ структур $\mathcal{A}$ и $\mathcal{B}$ соответственно и позитивный гомоморфизм φ' из $\mathcal{A}'$ в $\mathcal{B}'$, являющийся расширением гомоморфизма φ , такие, что $\varphi'(\mathcal{A}')$ включает $|\mathcal{B}|$. [Выбрать $\mathcal{A}'$, как в (г), и использовать (в) для нахождения позитивного гомоморфизма φ' из $\mathcal{A}'$ в некоторое элементарное расширение $\mathcal{C}$ структуры $\mathcal{B}_\varphi$. Положить $\mathcal{B}' = \mathcal{C}[L]$.]

(е) Скажем, что структура $\mathcal{B}$ есть *гомоморфный образ* структуры $\mathcal{A}$, если существует сюръективный гомоморфизм из $\mathcal{A}$ в $\mathcal{B}$. Показать, что если существует позитивный гомоморфизм из $\mathcal{A}'$ в $\mathcal{B}'$, то некоторое элементарное расширение $\mathcal{B}$ структуры $\mathcal{B}'$ является гомоморфным образом некоторого элементарного расширения $\mathcal{A}$ структуры $\mathcal{A}'$. [Взять $\mathcal{A}$ и $\mathcal{B}$ как объединения элементарных цепей, построенных с использованием (д).]

(ж) Показать, что теория T эквивалентна теории, нелогические аксиомы которой позитивны тогда и только тогда, когда каждый гомоморфный образ модели теории T является моделью теории T . [Для доказательства части «только тогда» использовать (б).] Предположим, что $\mathcal{B}$ — структура, в которой каждая позитивная теорема теории T является истинной. Показать, что если Γ — множество негативных формул, истинных в $\mathcal{B}$, то теория $T[\Gamma]$ непротиворечива. Пользуясь 5 (г), найти позитивный гомоморфизм из модели $\mathcal{A}$ теории $T[\Gamma]$ в некоторое элементарное расширение структуры $\mathcal{B}$. Затем применить (е), чтобы показать, что $\mathcal{B}$ — модель теории T .]

7. Пусть $\mathcal{A}_i$ будет структурой для L для каждого i из непустого множества I . Прямым произведением $\mathcal{A} = \prod_{i \in I} \mathcal{A}_i$ называется

структура для L , определенная следующим образом. Универсум структуры $\mathcal{A}$ есть множество $\prod_{i \in I} |\mathcal{A}_i|$ и

$$(f_{\mathcal{A}}(a_1, \dots, a_n))_i = f_{\mathcal{A}_i}((a_1)_i, \dots, (a_n)_i),$$

$$p_{\mathcal{A}}(a_1, \dots, a_n) \leftrightarrow p_{\mathcal{A}_i}((a_1)_i, \dots, (a_n)_i) \text{ для всех } i.$$

(а) Пусть $\pi_i(a) = (a)_i$ для a из $|\mathcal{A}|$. Показать, что π_i — сюръективный гомоморфизм из $\mathcal{A}$ в $\mathcal{A}_i$.

(б) Показать, что если A — формула языка $L(\mathcal{A})$, свободная от переменных, то $\mathcal{A}(A) = \mathbf{I}$ тогда и только тогда, когда $\mathcal{A}_i(A^{\pi_i}) = \mathbf{I}$ для всех i из I . [Применить (а) и 6 (а).]

(в) Назовем формулу формулой Маккинси, если она представляет собой дизъюнкцию формул, каждая из которых является либо атомной, либо отрицанием атомной формулы, и самое большее одна из этих формул атомная. Показать, что если A — замкнутая формула

Маккинси языка $L(\mathcal{A})$ такая, что $\mathcal{A}_i(A^{\pi_i}) = \mathbf{I}$ для всех i из I , то $\mathcal{A}(A) = \mathbf{I}$. [Предположить, что $\mathcal{A}(A) = \mathbf{J}$, и применить (б).]

(г) Назовем формулу формулой Хорна, если она находится в префиксной форме и ее матрица есть конъюнкция формул Маккинси. Показать, что результат из (в) обобщается на формулы Хорна.

[Применить индукцию по числу кванторов.] Вывести, что если формула Хорна является истинной в каждой структуре $\mathcal{A}_i$, то она является истинной и в $\mathcal{A}$.

(д) Пусть T — теория такая, что каждое прямое произведение моделей теории T есть снова модель теории T . Пусть $\neg A_1 \vee \dots \vee \neg A_n \vee B_1 \vee \dots \vee B_m$ — теорема теории T , где $m > 0$, а A_i и B_j — атомные. Показать, что для некоторого j формула $\neg A_1 \vee \dots \vee \neg A_n \vee B_j$ является теоремой теории T . [Предположить, что такого j не существует. Найти модель $\mathcal{A}_i$ теории T такую, что $\neg A_1 \vee \dots \vee \neg A_n \vee B_i$ не является истинной в $\mathcal{A}_i$, и показать, что $\neg A_1 \vee \dots \vee \neg A_n \vee B_1 \vee \dots \vee B_n$ не является истинной в прямом произведении структур $\mathcal{A}_i$.]

(е) Показать, что теория T эквивалентна теории, у которой аксиомы являются формулами Маккинси, тогда и только тогда, когда каждая подструктура модели теории T является моделью теории T и каждое прямое произведение моделей теории T является моделью теории T . [Применить теорему Лоса — Тарского, (в), задачу 11 (б) из главы 3 и (д).]

8. Класс $\mathfrak{Z}$ структур для L называется *замкнутым*, если каждая подструктура структуры из $\mathfrak{Z}$ находится в $\mathfrak{Z}$, каждый гомоморфный образ структуры из $\mathfrak{Z}$ находится в $\mathfrak{Z}$ и каждое прямое произведение структур из $\mathfrak{Z}$ находится в $\mathfrak{Z}$. Обозначим через $\text{At}(\mathfrak{Z})$ множество атомных формул, которые являются истинными в каждой структуре из $\mathfrak{Z}$.

(а) Пусть $\mathfrak{Z}$ — замкнутый класс структур для L , L' получается из L добавлением непустого множества новых констант и $\mathfrak{Z}'$ — множество обогащений до L' структур из $\mathfrak{Z}$. Показать, что $\mathfrak{Z}'$ замкнут и $\text{At}(\mathfrak{Z})$ — подмножество множества $\text{At}(\mathfrak{Z}')$.

(б) Пусть обозначения такие же, как и в (а), и пусть A — формула языка L' , свободная от переменных, не являющаяся частным случаем формулы из $\text{At}(\mathfrak{Z})$. Показать, что существует $\mathcal{A}$ из $\mathfrak{Z}'$ такая, что $\mathcal{A}(A) = \perp$, и такая, что каждый индивид из $\mathcal{A}$ есть $\mathcal{A}(a)$ для некоторого свободного от переменных терма a языка L' . [Выбрать структуру $\mathcal{B}$ в $\mathfrak{Z}'$ так, чтобы $\mathcal{B}(A) = \perp$, и взять любую подструктуру.]

(в) Пусть обозначения такие же, как и в (а). Показать, что существует структура $\mathcal{A}$ из $\mathfrak{Z}'$ такая, что

(i) каждая атомная формула языка L' , свободная от переменных, истинная в $\mathcal{A}$, есть частный случай некоторой формулы из $\text{At}(\mathfrak{Z})$;

(ii) каждый индивид из $\mathcal{A}$ есть $\mathcal{A}(a)$ для некоторого свободного от переменных терма a языка L' . [Применить (б) и 7 (б).]

(г) Пусть $\mathfrak{Z}$ — некоторый замкнутый класс структур для L . Показать, что если $\mathcal{B}$ — структура для L , в которой каждая формула из $\text{At}(\mathfrak{Z})$ является истинной, то $\mathcal{B}$ принадлежит $\mathfrak{Z}$. [Пусть L' будет $L(\mathcal{B})$ и $\mathcal{A}$ такая же, как в (в). Если A — атомная формула языка L' , свободная от переменных, то из $\mathcal{A}(A) = \perp$ следует $\mathcal{B}(A) = \perp$. Определим сюръективный гомоморфизм φ из $\mathcal{A}$ в $\mathcal{B}$, полагая $\varphi(\mathcal{A}(a)) = \mathcal{B}(a)$.]

(д) Показать, что класс $\mathfrak{Z}$ структур для L замкнут тогда и только тогда, когда этот класс является классом всех моделей теории языка L , нелогические аксиомы которой атомные. [Для доказательства части «только тогда» применить (г).]

9. Если T — теория, язык которой есть расширение языка L , то *обеднением* теории T до L назовем теорию, язык которой есть L и нелогические аксиомы которой представляют собой формулы языка L , являющиеся теоремами теории T .

(а) Пусть T — обеднение теории T' до L . Показать, что структура $\mathcal{A}$ для L является моделью теории T тогда и только тогда, когда какое-то обогащение некоторого элементарного расширения структуры $\mathcal{A}$ является моделью теории T' . [Пусть $\mathcal{A}$ — модель теории T ; применить теорему о совместной непротиворечивости, чтобы показать, что $T' \cup D_e(\mathcal{A})$ непротиворечива.]

(б) Привести пример теории T' , обеднения T теории T' и модели $\mathcal{A}$ теории T , не имеющей обогащения, являющегося моделью теории T' . [Пусть T' имеет в качестве нелогических символов константы $e_1, e_2, \dots$ и в качестве нелогических аксиом все формулы $e_i \neq e_j$ для $i \neq j$. Получить T отбрасыванием e_1 .]

(в) Пусть T' — расширение теории T . Показать, что T' является консервативным расширением теории T тогда и только тогда, когда для каждой модели $\mathcal{A}$ теории T какое-то обогащение некоторого элементарного расширения модели $\mathcal{A}$ является моделью теории T' . [Применить (а).]

(г) Пусть T — теория, язык которой есть расширение языка L и $\mathfrak{Z}$ — класс обеднений моделей теории T до L . Предположим, что каждая подструктура произвольной структуры из $\mathfrak{Z}$ находится в $\mathfrak{Z}$. Показать, что $\mathfrak{Z}$ есть множество всех моделей обеднения T' теории T до L и что T' эквивалентна открытой теории. [Применить (а) и теорему Лоса — Тарского.]

(д) Пусть T — открытая теория, язык которой получается из L добавлением предикатных символов. Пусть $\mathcal{A}$ — структура для L . Показать, что $\mathcal{A}$ имеет обогащение, являющееся моделью теории T , тогда и только тогда, когда каждая конечно порожденная подструктура структуры $\mathcal{A}$ имеет обогащение, являющееся моделью теории T . [Пусть $\mathfrak{Z}$ такое же, как в (г); показать, что каждая подструктура структуры из $\mathfrak{Z}$ находится в $\mathfrak{Z}$. Затем применить (г) и 3 (в).]

(е) *Гипотеза четырех красок* утверждает, что любую карту можно раскрасить четырьмя красками так, что никакие две соседние страны не будут иметь одинаковый цвет. Показать, что если гипотеза четырех красок справедлива для карт с конечным числом стран, то она справедлива для всех карт. [Будем рассматривать карту как структуру, индивидами которой являются страны, и с бинарным предикатом *быть соседней страной к стране*. Показать, что карту можно раскрасить четырьмя красками тогда и только тогда, когда эта карта имеет обогащение до модели подходящей открытой теории, содержащей четыре унарных предиката. Затем применить (д).]

10. Обозначим через $\Sigma\Gamma$ множество всех формул $\exists x_1 \dots \exists x_n A$, где A из Γ , и через $\forall\Gamma$ множество всех формул $\forall x_1 \dots \forall x_n A$, где A из Γ . Определим Σ_n и $\forall_n$ индуктивно следующим образом: Σ_0 и $\forall_0$ — множество всех открытых формул, $\Sigma_{n+1} = \exists \forall_n$, $\forall_{n+1} = \forall \Sigma_n$. Пусть B_n — множество формул, полученных из формул в Σ_n и $\forall_n$ с помощью применения отрицаний и дизъюнкций.

(а) Пусть Γ — некоторое множество формул языка L , $\mathcal{B}$ — структура для L , $\mathcal{A}$ — подструктура структуры $\mathcal{B}$. Показать, что если

некоторое элементарное расширение структуры $\mathcal{A}$ есть Γ -расширение структуры $\mathcal{B}$, то $\mathcal{B}$ есть $\forall\Gamma$ -расширение структуры $\mathcal{A}$, где Γ — множество отрицаний формул из Γ .

(б) Показать, что каждая формула из B_n имеет пренексную форму, находящуюся в $\exists_{n+1}$, и пренексную форму, находящуюся в $\forall_{n+1}$. Показать, что отрицание формулы из $\exists_n$ ($\forall_n$) имеет пренексную форму, находящуюся в $\forall_n$ ($\exists_n$).

(в) n -сэндвичем для L называется последовательность $\mathcal{A}_0, \dots, \mathcal{A}_n$ структур для L таких, что $\mathcal{A}_{i+1}$ — расширение структуры $\mathcal{A}_i$ для $i < n$ и $\mathcal{A}_{i+2}$ — элементарное расширение структуры $\mathcal{A}_i$ для $i < n-1$. Пусть $\mathcal{B}$ — расширение структуры $\mathcal{A}$. Показать, что $\mathcal{B}$ есть $\forall_n$ -расширение структуры $\mathcal{A}$ тогда и только тогда, когда существует $(n+1)$ -сэндвич, первыми двумя структурами которого являются $\mathcal{A}$ и $\mathcal{B}$. [Применить (а), (б) и следствие к теореме о расширении модели.]

(г) Показать, что теория T эквивалентна теории, нелогические аксиомы которой находятся в $\exists_n$, тогда и только тогда, когда для каждого $(n+1)$ -сэндвича для $L(T)$, если вторая структура в сэндвиче — модель теории T , то первая структура в сэндвиче — модель теории T . [Для доказательства части «только тогда» применить (в) и (б). Пусть условие выполняется и $\mathcal{A}$ — структура, в которой все теоремы теории T из $\exists_n$ являются истинными; использовать (б) и теорему о расширении модели для получения $\forall_n$ -расширения для $\mathcal{A}$, являющегося моделью теории T . Затем применить (в).]

11. (а) Пусть $\mathcal{A}_1, \mathcal{A}_2, \dots$ — цепь структур для L такая, что для каждого k структура $\mathcal{A}_{k+1}$ есть $\forall_n$ -расширение структуры $\mathcal{A}_k$. Показать, что объединение цепи $\mathcal{A}$ есть $\forall_n$ -расширение каждой структуры $\mathcal{A}_k$. [Аналогично доказательству леммы Тарского.]

(б) Пусть T и T' — теории одного и того же языка, нелогические аксиомы которых находятся в $\exists_n$. Показать, что для $n \geq 1$ теория $T \cup T'$ противоречива тогда и только тогда, когда существует замкнутая формула A из B_n такая, что $\vdash_T A$ и $\vdash_{T'} \neg A$. [Предположим, что такой формулы A не существует. Пусть Γ — множество замкнутых формул из B_n , являющихся теоремами теории T ; определим Γ' подобным же образом. Показать, что $T[\Gamma']$ и $T'[\Gamma]$ непротиворечивы и что одни и те же формулы из B_{n-1} являются доказуемыми в $T[\Gamma']$ и в $T'[\Gamma]$. Используя теорему о расширении модели, найти цепь $\mathcal{A}_1, \mathcal{A}_2, \dots$ такую, что $\mathcal{A}_{k+1} \vdash B_{n-1}$ — расширение структуры $\mathcal{A}_k$, $\mathcal{A}_{2k+1}$ — модель теории $T[\Gamma']$ и $\mathcal{A}_{2k}$ — модель теории $T'[\Gamma]$. Использовать (а), чтобы показать, что объединение цепи есть $\forall_n$ -расширение каждой структуры $\mathcal{A}_k$ и, следовательно, модель теории $T \cup T'$.] Если $n=0$, то это же утверждение справедливо при условии, что мы отказываемся от требования, чтобы A была замкнутой. [Применить теорему о непротиворечивости.]

(в) Пусть $\vdash_T A \rightarrow B$, где A из $\forall_{n+1}$, а B из $\exists_{n+1}$. Предположим, что все нелогические аксиомы теории T принадлежат $\exists_n$. Показать, что существует формула C из B_n такая, что $\vdash_T A \rightarrow C$ и $\vdash_T C \rightarrow B$. [Доказывать аналогично интерполяционной лемме Крейга, используя (б).]

(г) Пусть T — теория, нелогические аксиомы которой находятся в $\exists_n$. Показать, что если A эквивалентна в T формуле из $\exists_{n+1}$ и

эквивалентна в T формуле из $\forall_{n+1}$, то A эквивалентна в T формуле из B_n . [Применить (в).]

12. (а) Пусть $\mathcal{B}$ — такое расширение структуры $\mathcal{A}$, что для каждой замкнутой формулы $\exists x A$ языка $L(\mathcal{A})$ такой, что $\mathcal{B}(\exists x A) = \text{И}$, существует такое i в $L(\mathcal{A})$, что $\mathcal{B}(A_x[i]) = \text{И}$. Показать, что $\mathcal{B}$ — элементарное расширение структуры $\mathcal{A}$.

(б) Пусть m — бесконечная мощность, L — m -язык. $\mathcal{A}$ — структура для L мощности $\geq m$ и B — подмножество множества $|\mathcal{A}|$ мощности $\leq m$. Показать, что существует элементарная подструктура $\mathcal{B}$ структуры $\mathcal{A}$, имеющая мощность m , такая, что B — подмножество множества $|\mathcal{B}|$. [Определить индуктивно последовательность $B_0, B_1, \dots$ подмножеств множества $|\mathcal{A}|$ таких, что (i) $B_0 = B$; (ii) если $a_1, \dots, a_n$ принадлежат B_k , то $f_{\mathcal{A}}(a_1, \dots, a_n)$ принадлежит B_{k+1} для всех f ; (iii) если $\mathcal{A}(\exists x A[i_1, \dots, i_n]) = \text{И}$, где A — формула языка L и $i_1, \dots, i_n$ — имена индивидов из B_k , то $\mathcal{A}(A[j, i_1, \dots, i_n]) = \text{И}$ для некоторого имени j индивида из B_{k+1} ; (iv) B_k имеет мощность m для $k > 0$. Взять в качестве $|\mathcal{B}|$ объединение множеств B_k и применить (а).]

(в) Пусть m — бесконечная мощность, L — m -язык и $\mathcal{A}$ — бесконечная структура для L мощности, не превосходящей m . Показать, что $\mathcal{A}$ имеет элементарное расширение мощности m . [Применить теорему о мощности к $D_e(\mathcal{A})$.]

13. Пусть $\mathcal{A}$ — структура для L , A_1 и A_2 — подмножества множества $|\mathcal{A}|$. Изоморфизмом между A_1 и A_2 в $\mathcal{A}$ называется биективное отображение ϕ из A_1 в A_2 такое, что $\mathcal{A}(A) = \mathcal{A}(\phi A)$ для каждой замкнутой формулы A языка $L(\mathcal{A})$ такой, что все имена из A являются именами некоторых индивидов из A_1 . Автоморфизмом структуры $\mathcal{A}$ называется изоморфизм между $\mathcal{A}$ и $\mathcal{A}$.

(а) Показать, что биективное отображение из $|\mathcal{A}|$ в $|\mathcal{A}|$ является автоморфизмом структуры $\mathcal{A}$ тогда и только тогда, когда это отображение является изоморфизмом между $|\mathcal{A}|$ и $|\mathcal{A}|$ в $\mathcal{A}$.

(б) Пусть ϕ — изоморфизм между A_1 и A_2 в $\mathcal{A}$. Показать, что существует элементарное расширение $\mathcal{B}$ структуры $\mathcal{A}$ и изоморфизм ϕ' между $|\mathcal{A}|$ и некоторым подмножеством множества $|\mathcal{B}|$ в $\mathcal{B}$, расширяющий ϕ . [Для каждого имени i языка $L(\mathcal{A})$ ввести новое имя i' ; для каждой формулы A языка $L(\mathcal{A})$ пусть A' получается из A заменой каждого i на i' . Получить T' из $D_e(\mathcal{A})$ заменой каждого i на i' . Получить T из $D_e(\mathcal{A})$ следующим путем: если i — имя индивида из A_1 , то добавить константу i' и аксиому $i' = i^\phi$. Обогащить $\mathcal{A}$ до структуры $\mathcal{A}'$ теории T , полагая $\mathcal{A}'(i') = \mathcal{A}(i^\phi)$. Показать, что $\mathcal{A}'$ — модель теории T и что если A' — замкнутая формула теории T , то

$$\mathcal{A}'(A') = \mathcal{A}'(A^\phi) = \mathcal{A}(A).$$

Вывести, что если $\vdash_T A'$, то A истинна в $\mathcal{A}$. Использовать это и теорему о совместной непротиворечивости, чтобы показать, что $T \cup T'$ непротиворечива. Пусть $\mathcal{C}$ — модель теории $T \cup T'$ такая, что $\mathcal{C}(i) = \mathcal{A}(i)$ для имени i языка $L(\mathcal{A})$. Пусть $\mathcal{B}$ будет $\mathcal{C} \upharpoonright L$, и пусть $\phi'(i) = \mathcal{C}(i')$.]

(в) Пусть ϕ — изоморфизм между A_1 и A_2 в $\mathcal{A}$. Показать, что существует элементарное расширение $\mathcal{B}$ структуры $\mathcal{A}$ и изоморфизм ϕ' между некоторым подмножеством множества $|\mathcal{B}|$ и множе-

ством $|\mathcal{A}|$ в $\mathcal{B}$, который расширяет φ . [Применить (б) для получения обратного отображения для φ .]

(г) Показать, что каждый изоморфизм между подмножествами множества $|\mathcal{A}|$ в $\mathcal{A}$ может быть расширен до автоморфизма некоторого элементарного расширения структуры $\mathcal{A}$. [Образовать элементарную цепь, начинающуюся с $\mathcal{A}$, в которой элементы получаются попеременно по (б) и (в).]

(д) Показать, что если T имеет бесконечную модель, то T имеет модель, в которой существуют два различных индивида, имеющие одинаковый тип. [Достаточно доказать непротиворечивость теории T' , полученной из T добавлением двух констант e и e' , аксиомы $e \neq e'$ и аксиомы $A[e] \rightarrow A[e']$ для каждой A из $S_1(T)$. Если T' противоречива, то

$$\vdash_T (A_1 \leftrightarrow A_1[y]) \rightarrow \dots \rightarrow (A_n \leftrightarrow A_n[y]) \rightarrow z_1 = y,$$

где $A_1, \dots, A_n$ из $S_1(T)$. Вывести, что никакая модель теории T не имеет более 2^n индивидов.]

(е) Показать, что если T имеет бесконечную модель, то T имеет модель, в которой есть автоморфизм, отличный от тождественного отображения. [Применить (д) и (г).]

14. Пусть T — теория, p — предикатный символ теории T и Q — некоторое множество нелогических символов из T , не содержащее p . Скажем, что p *дизъюнктивно определим* в терминах Q в T , если существует теорема теории T , которая представляет собой дизъюнкцию замыканий формул вида $px_1 \dots x_n \leftrightarrow A$, где $x_1, \dots, x_n$ различны и A не содержит нелогических символов, не принадлежащих Q .

(а) Показать, что если p не является дизъюнктивно определяемым в терминах Q , то существует модель $\mathcal{A}$ теории T такая, что для каждой формулы A , не содержащей нелогических символов, не принадлежащих Q , формула $px_1 \dots x_n \leftrightarrow A$ не является истинной в $\mathcal{A}$. [Пусть Γ — множество отрицаний замыканий таких формул; показать, что $T[\Gamma]$ непротиворечива.]

(б) Показать, что p дизъюнктивно определим в терминах Q тогда и только тогда, когда для каждой модели $\mathcal{A}$ теории T и каждого биективного отображения φ из $|\mathcal{A}|$ в $|\mathcal{A}|$, являющегося u -изоморфизмом для каждого u из Q , φ является p -изоморфизмом. [Если p не является дизъюнктивно определяемым в терминах Q , то берем $\mathcal{A}$ такую же, как и в (а), и применяем теорему об определмости, чтобы получить модели $\mathcal{B}$ и $\mathcal{C}$ теории $\text{Th}(\mathcal{A})$ и биективное отображение φ из $|\mathcal{B}|$ в $|\mathcal{C}|$, являющееся u -изоморфизмом для всех u из Q , но не являющееся p -изоморфизмом. После замены $\mathcal{B}$ на изоморфную модель применить 4 (б), чтобы получить общее элементарное расширение для $\mathcal{B}$ и $\mathcal{C}$, и применить 13 (г).]

(в) Обобщить результаты этой задачи на функциональные символы.

15. Будем предполагать известной следующую теорему: если $\mathcal{A}$ — поле и p — многочлен, отличный от константы, с коэффициентами из $\mathcal{A}$, то существует расширение поля $\mathcal{A}$, являющееся полем, в котором p имеет корень.

(а) Показать, что для каждого поля $\mathcal{A}$ существует расширение $\mathcal{B}$ поля $\mathcal{A}$, являющееся полем, в котором каждый многочлен, отлич-

ный от константы, с коэффициентами из $\mathcal{A}$ имеет корень. [Получить T из $\text{FL} \cup D(\mathcal{A})$ добавлением для каждого многочлена p , отличного от константы, с коэффициентами из $\mathcal{A}$ аксиому, утверждающую, что p имеет корень. Применить теорему компактности, чтобы показать, что T имеет модель.]

(б) Показать, что каждое поле $\mathcal{A}$ является подполем некоторого алгебраически замкнутого поля. [Построить по (а) цепь полей, начинающуюся с $\mathcal{A}$, и применить теорему Чжана — Лося — Сушко.]

16. Теория T называется *модельно полной*, если для каждой модели $\mathcal{B}$ теории T каждая подмодель модели $\mathcal{B}$ является элементарной подмоделью модели $\mathcal{B}$.

(а) Показать, что если T допускает элиминацию кванторов, то T модельно полна. Показать, что если T — модельно полная открытая теория, то T допускает элиминацию кванторов. [Применить теорему об элиминации кванторов.]

(б) Предположим, что для каждой модели $\mathcal{B}$ теории T каждая подмодель модели $\mathcal{B}$ есть V_1 -подмодель модели $\mathcal{B}$. Показать, что T модельно полна. [Пусть $\mathcal{A}$ — подмодель модели $\mathcal{B}$. Применяя индукцию по n и 10 (в), показать, что существует n -сэндвич, двумя первыми структурами которого являются $\mathcal{A}$ и $\mathcal{B}$. Затем снова использовать 10 (в).]

(в) Показать, что если $\mathcal{A}$ и $\mathcal{B}$ — структуры для L такие, что $|\mathcal{A}|$ — подмножество множества $|\mathcal{B}|$, то $\mathcal{A}$ — элементарная подструктура структуры $\mathcal{B}$ тогда и только тогда, когда $\mathcal{A} \equiv \mathcal{A}$ элементарно эквивалентна $\mathcal{B}$.

(г) Показать, что теория T модельно полна тогда и только тогда, когда для каждой модели $\mathcal{A}$ теории T теория $T \cup D(\mathcal{A})$ полна. [Применить (в), лемму о диаграмме и лемму 1 из § 5.5.]

(д) Модель $\mathcal{A}$ теории T называется *простой*, если каждая модель теории T имеет подмодель, изоморфную $\mathcal{A}$. Показать, что если T модельно полна и имеет простую модель, то T полна.

17. Пусть T получается из FL добавлением аксиом

$$\exists y (y \cdot y = x \vee y \cdot y = -x),$$

$$x \cdot x \neq -1,$$

$$\exists z (z \cdot z = x \cdot x + y \cdot y)$$

и для каждого нечетного n аксиомы, утверждающей, что каждый многочлен степени n имеет корень.

(а) Показать, что если $\mathcal{A}$ — модель теории T и для a и b из $|\mathcal{A}|$ формула $a < b$ означает, что $a = b + c^2$ для некоторого ненулевого c из $|\mathcal{A}|$, то $\mathcal{A}$ становится вещественно замкнутым полем.

(б) Показать, что некоторое расширение теории T с помощью определений эквивалентно RCF. [Применить (а), следствие к теореме компактности и полноту RCF.] Вывести, что T полна и, следовательно, эквивалентна теории поля действительных чисел.

(в) Показать, что T не допускает элиминации кванторов. [Показать, что если A — открытая формула теории T , в которой нет свободных переменных, за исключением x , P — множество действительных чисел a таких, что A является истинной, когда x принимает значение a , то либо P конечно, либо все действительные числа, за исключением конечного числа, принадлежат P . Вывести, что $\exists x (x = y \cdot y)$ не эквивалентна в T никакой открытой формуле.]

18. Пусть $\mathcal{A}$ — поле и $\mathcal{B}$ — кольцо многочленов от n неизвестных с коэффициентами из $\mathcal{A}$.

(а) Пусть $f_1, \dots, f_k$ — многочлены из $\mathcal{B}$, одновременно обращающиеся в нуль для некоторого набора аргументов в некотором расширении поля $\mathcal{A}$. Показать, что $f_1, \dots, f_k$ одновременно обращаются в нуль для некоторого множества аргументов в каждом алгебраически замкнутом расширении поля $\mathcal{A}$. [Применить 16 (а) и 16 (г), чтобы показать, что $\text{ACF} \cup D(\mathcal{A})$ полна *); затем применить лемму 1 из § 5.5 и лемму о диаграмме.]

(б) Показать, что если I — собственный идеал кольца $\mathcal{B}$, то все многочлены из I одновременно обращаются в нуль для некоторого набора аргументов в некотором поле $\mathcal{C}$, являющемся расширением поля $\mathcal{A}$. [Применить лемму Цорна, чтобы найти максимальный идеал J , включающий I . Заметить, что $\mathcal{B}/J$ — поле и естественное отображение из $\mathcal{B}$ в $\mathcal{B}/J$ есть изоморфизм на $\mathcal{A}$. Взять $\mathcal{C}$ изоморфным $\mathcal{B}/J$.]

(в) Пусть $\mathcal{C}$ — алгебраически замкнутое поле, являющееся расширением поля $\mathcal{A}$, и пусть $f_1, \dots, f_k$ — многочлены из $\mathcal{B}$, одновременно не обращающиеся в нуль для любого набора аргументов из $\mathcal{C}$. Показать, что идеал кольца $\mathcal{B}$, порожденный многочленами $f_1, \dots, f_k$, есть $\mathcal{B}$. [Применить (а) и (б).]

(г) Пусть $f, g_1, \dots, g_k$ — многочлены из $\mathcal{B}$. Предположим, что существует алгебраически замкнутое поле $\mathcal{C}$, являющееся расширением поля $\mathcal{A}$, такое, что все общие корни многочленов $g_1, \dots, g_k$ в $\mathcal{C}$ являются корнями многочлена f . Показать, что некоторая степень многочлена f принадлежит идеалу кольца $\mathcal{B}$, порожденному многочленами $g_1, \dots, g_k$ (теорема Гильберта о корнях). [Пусть Z — новая неизвестная. Вывести из (в), что $1 = h_1 g_1 + \dots + h_k g_k + h(1 - Zf)$ для подходящих многочленов $h_1, \dots, h_k, h$. Подставить $\frac{1}{f}$ вместо Z и освободиться от дробей.]

(д) Если $f, g_1, \dots, g_k$ такие же, как и в (г), то $f^m = h_1 g_1 + \dots + h_k g_k$ для подходящих $m, h_1, \dots, h_k$. Показать, что существуют границы для m и степеней многочленов h_i , которые зависят только от n и степеней многочленов f и g_i . [Для данного n и степеней многочленов $f, g_1, \dots, g_k$ построить формулу A теории FL такую, что если $x_1, \dots, x_s$ — данные значения коэффициентов многочленов $f, g_1, \dots, g_k$, то A является истинной в некотором расширении $\mathcal{C}$ поля $\mathcal{A}$ тогда и только тогда, когда все общие корни многочленов $g_1, \dots, g_k$ в $\mathcal{C}$ являются корнями многочлена f . Пусть B — открытая формула, эквивалентная формуле A в ACF. Пусть C_r — формула, которая при тех же значениях $x_1, \dots, x_s$ является истинной тогда и только тогда, когда

$$f^m = h_1 g_1 + \dots + h_k g_k$$

для некоторого $m \leq r$ и некоторых многочленов $h_1, \dots, h_k$ степеней $\leq r$. Тогда если $e_1, \dots, e_s$ — новые константы, то $\neg B[e_1, \dots, e_s]$ —

*) 16 (г) здесь неприменимо, так как $\mathcal{A}$ не является, вообще говоря, моделью ACF. Нужно применить 16 (д) и теорему о существовании и единственности алгебраического замыкания. — Прим. ред.

логическое следствие нелогических аксиом теории FL и формулы $\neg C_r[e_1, \dots, e_s]$. Применить теорему компактности.]

19. Пусть $\mathcal{A}$ — упорядоченное поле.

(а) Пусть $f_1, \dots, f_k$ — многочлены от n неизвестных с коэффициентами из $\mathcal{A}$, которые одновременно обращаются в нуль для некоторого множества аргументов упорядоченного поля, являющегося расширением поля $\mathcal{A}$. Показать, что $f_1, \dots, f_k$ одновременно обращаются в нуль для некоторого множества аргументов в каждом вещественно замкнутом расширении поля $\mathcal{A}$. [Подобно 18 (а).]

(б) Многочлен f от n неизвестных с коэффициентами из $\mathcal{A}$ положителен в расширении $\mathcal{B}$ для $\mathcal{A}$, если f принимает только неотрицательные значения для аргументов из $\mathcal{B}$. Показать, что если f положителен в некотором вещественно замкнутом расширении поля $\mathcal{A}$, то f положителен в каждом вещественно замкнутом расширении поля $\mathcal{A}$. [Подобно 18 (а).]

(в) Теорема Артина — Шрайера утверждает, что если $\mathcal{B}$ — расширение поля $\mathcal{A}$ и b — индивид из $\mathcal{B}$, который не может быть представлен в виде $c_1 a_1^2 + \dots + c_k a_k^2$, где c_i — положительные индивиды из $\mathcal{A}$, то существует упорядочение $\mathcal{B}$, превращающее $\mathcal{B}$ в упорядоченное поле, расширяющее порядок поля $\mathcal{A}$ и такое, что $b < 0$. Предполагая, что это верно, доказать следующую теорему Артина. Пусть f — многочлен от n неизвестных с коэффициентами из $\mathcal{A}$, положительный в некотором вещественно замкнутом расширении поля $\mathcal{A}$. Тогда $f = c_1 g_1^2 + \dots + c_k g_k^2$, где c_i — положительные элементы из $\mathcal{A}$, а g_i — рациональные функции с коэффициентами из $\mathcal{A}$. Более того, если $\mathcal{A}$ — вещественно замкнутое поле или поле рациональных чисел, то вместо c_i могут быть взяты 1. [Предположим, что f не может быть записан в такой форме. Применяя теорему Артина — Шрайера, упорядочить поле рациональных функций так, чтобы $f < 0$, и показать, что это противоречит (б).]

(г) Показать, что в теореме Артина существует граница для k и для степеней числителей и знаменателей функций g_i , которая зависит только от n и степени f . [Подобно 18 (д).]

20. Пусть $\mathcal{A}$ и $\mathcal{B}$ — структуры для $L, a_1, \dots, a_n$ — индивиды из $\mathcal{A}$, а $b_1, \dots, b_n$ — индивиды из $\mathcal{B}$. Определим m -эквивалентность $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ индукцией по m следующим образом. Скажем, что n -ки $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ являются 0-эквивалентными, если типы n -ок $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ содержат одни и те же атомные формулы. Скажем, что n -ки $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ являются $(m+1)$ -эквивалентными, если для каждого a из $|\mathcal{A}|$ существует b из $|\mathcal{B}|$ такое, что n -ки $(a_1, \dots, a_n, a)$ и $(b_1, \dots, b_n, b)$ будут m -эквивалентными, и для каждого b из $|\mathcal{B}|$ существует a из $|\mathcal{A}|$ такое, что n -ки $(a_1, \dots, a_n, a)$ и $(b_1, \dots, b_n, b)$ будут m -эквивалентными. Показать, что если n -ки $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ являются m -эквивалентными, то типы n -ок $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ содержат одни и те же формулы высоты m . [Использовать индукцию по m .] Вывести, что если n -ки $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ являются m -эквивалентными для каждого m , то они имеют одинаковые типы.

21. Пусть EQ — теория, у которой единственным нелогическим символом является бинарный предикатный символ $\sim$, а нелогическими

аксиомами являются

$$\begin{aligned} x &\sim x, \\ x &\sim y \rightarrow y \sim x, \\ x &\sim y \rightarrow y \sim z \rightarrow x \sim z. \end{aligned}$$

Тогда всякая модель $\mathcal{A}$ теории EQ состоит из непустого множества $|\mathcal{A}|$ и отношения эквивалентности $\sim_{\mathcal{A}}$ на $|\mathcal{A}|$.

(а) Для каждого m и n показать, что существует замкнутая формула $A_{m,n}$, которая истинна в модели $\mathcal{A}$ теории EQ тогда и только тогда, когда $\mathcal{A}$ имеет по крайней мере m классов эквивалентности, содержащих n элементов, и замкнутая формула $B_{m,n}$, которая истинна в модели $\mathcal{A}$ теории EQ тогда и только тогда, когда $\mathcal{A}$ имеет по крайней мере m классов эквивалентности, содержащих по крайней мере n элементов.

(б) Если $\mathcal{A}$ и $\mathcal{B}$ — модели теории EQ, то мы пишем $\mathcal{A} \equiv \mathcal{B}$, когда

$$\mathcal{A}(A_{m,n}) = \mathcal{B}(A_{m,n}) \text{ и } \mathcal{A}(B_{m,n}) = \mathcal{B}(B_{m,n}) \text{ для всех } m \text{ и } n.$$

Предположим, что $\mathcal{A} \equiv \mathcal{B}$, $(a_1, \dots, a_n)$ — n -ка из $|\mathcal{A}|$, 0-эквивалентная n -ке $(b_1, \dots, b_n)$ из $|\mathcal{B}|$, и что для $i=1, \dots, n$ либо классы эквивалентности для a_i и b_i имеют одно и то же число элементов, либо оба эти класса эквивалентности имеют больше $m+n$ элементов. Показать, что n -ка $(a_1, \dots, a_n)$ будет m -эквивалентна n -ке $(b_1, \dots, b_n)$. [Применить индукцию по m .]

(в) Показать, что если $\mathcal{A}$ и $\mathcal{B}$ — модели теории EQ, то $\mathcal{A} \equiv \mathcal{B}$ тогда и только тогда, когда $\mathcal{A}$ элементарно эквивалентна $\mathcal{B}$. [Использовать (б) и задачу 20.]

22. Пусть L — язык, нелогическими символами которого являются лишь унарные предикатные символы $p_1, \dots, p_n$.

(а) Показать, что для каждого подмножества I множества $\{1, \dots, n\}$ и каждого m существует замкнутая формула $A_{I,m}$, истинная в структуре $\mathcal{A}$ для L тогда и только тогда, когда существуют по крайней мере m индивидов a из $\mathcal{A}$ таких, что $[i | (p_i)_{\mathcal{A}}(a)] = I$.

(б) Если $\mathcal{A}$ и $\mathcal{B}$ — структуры для L , то мы пишем $\mathcal{A} \equiv \mathcal{B}$, если $\mathcal{A}(A_{I,m}) = \mathcal{B}(A_{I,m})$ для всех I и m . Покажем, что если $\mathcal{A} \equiv \mathcal{B}$, то любая n -ка из $\mathcal{A}$ и любая n -ка из $\mathcal{B}$, которые 0-эквивалентны, являются m -эквивалентными для всех m . Вывести, что $\mathcal{A} \equiv \mathcal{B}$ тогда и только тогда, когда $\mathcal{A}$ и $\mathcal{B}$ элементарно эквивалентны. [Использовать задачу 20.]

23. Пусть DO — теория, единственным нелогическим символом которой является $<$, а нелогическими аксиомами — аксиомы OF1 — OF3 теории OF и

$$\begin{aligned} x &< y \rightarrow \exists z (x < z \ \& \ z < y), \\ \exists x (x &< y), \\ \exists x (y &< x). \end{aligned}$$

(а) Пусть $\mathcal{A}$ и $\mathcal{B}$ — модели теории DO и $(a_1, \dots, a_n)$ — n -ка из $|\mathcal{A}|$, которая 0-эквивалентна n -ке $(b_1, \dots, b_n)$ из $|\mathcal{B}|$. Показать, что $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ имеют одинаковый тип. [Показать, что они m -эквивалентны для каждого m , и использовать задачу 20.]

(б) Показать, что DO полна. [Использовать (а) и лемму 1 из § 5.5.]

(в) Показать, что DO является $\aleph_0$ -категоричной. [Использовать (а), (б) и теорему Рылль-Нардзевского.]

(г) Доказать (в), не применяя (а) или (б). [Для данных моделей $\mathcal{A}$ и $\mathcal{B}$ мощности $\aleph_0$ выбрать последовательности $a_1, a_2, \dots$ и $b_1, b_2, \dots$, как в доказательстве теоремы Рылль-Нардзевского так, чтобы $a_i < a_j$ тогда и только тогда, когда $b_i < b_j$.] Получить новое доказательство (б).

(д) Показать, что если m — мощность множества действительных чисел, то DO не является m -категоричной. [Построить модель теории DO, начав с рациональных чисел и заменяя каждый элемент линейно упорядоченным множеством, изоморфным множеству действительных чисел *]. Показать, что эта модель не изоморфна множеству действительных чисел.]

24. Пусть нелогическими символами теории T являются унарный предикатный символ p и две бесконечные последовательности констант $e_1, e_2, \dots$ и $e'_1, e'_2, \dots$. Пусть нелогическими аксиомами теории T будут $p(e_i)$ и $\neg p(e'_i)$ и все $e \neq e'$ для различных констант e и e' . Показать, что T — полная теория, не являющаяся m -категоричной для любой бесконечной мощности m . [Использовать метод из § 5.5.]

25. Показать, что если T — полная теория и T имеет конечную модель, то T категорична. [Предположим, что $\mathcal{A}$ — конечная модель и $\mathcal{B}$ — модель, не изоморфная $\mathcal{A}$. Пусть $i_1, \dots, i_n$ — имена индивидов из $\mathcal{A}$. Если φ — биективное отображение $|\mathcal{A}|$ в $|\mathcal{B}|$, то существует формула A_{φ} из $S_n(T)$ такая, что

$$\mathcal{A}(A_{\varphi}[i_1, \dots, i_n]) = \text{И} \text{ и } \mathcal{B}(A_{\varphi}[i_1^{\varphi}, \dots, i_n^{\varphi}]) = \text{Л}.$$

Пусть B — конъюнкция формул A_{φ} , формул $z_i \neq z_j$ для $1 \leq i < j \leq n$ и формулы

$$\forall z_{n+1} (z_{n+1} = z_1 \vee \dots \vee z_{n+1} = z_n).$$

Тогда $\mathcal{A}(\exists z_1 \dots \exists z_n B) = \text{И}$ и $\mathcal{B}(\exists z_1 \dots \exists z_n B) = \text{Л}$.]

26. Пусть T — счетная полная теория, имеющая только бесконечные модели, и $\mathcal{A}$ — счетная модель теории T . Скажем, что $\mathcal{A}$ слабо насыщена, если для каждого n каждый n -тип в T есть n -тип в $\mathcal{A}$. Скажем, что $\mathcal{A}$ насыщена, если для каждого $a_1, \dots, a_{n-1}$ из $|\mathcal{A}|$ и каждого n -типа Γ в T , содержащего тип $(n-1)$ -ки $(a_1, \dots, a_{n-1})$, существует a_n из $|\mathcal{A}|$ такое, что Γ — тип n -ки $(a_1, \dots, a_n)$. Скажем, что $\mathcal{A}$ однородна, если, как только $a_1, \dots, a_n, b_1, \dots, b_n$ являются индивидами из $\mathcal{A}$ такими, что типы n -ок $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ одинаковы, существует автоморфизм φ структуры $\mathcal{A}$ такой, что $\varphi(a_i) = b_i, \dots, \varphi(a_n) = b_n$. Скажем, что $\mathcal{A}$ универсальна, если каждая счетная модель теории T изоморфна некоторой элементарной подструктуре структуры $\mathcal{A}$.

(а) Показать, что всякая насыщенная модель $\mathcal{A}$ теории T универсальна. [Пусть $\mathcal{B}$ — счетная модель с индивидами $b_1, b_2, \dots$. Выберем индивиды $a_1, a_2, \dots$ из $\mathcal{A}$ индуктивно так, чтобы n -ки $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ имели одинаковые типы. Показать, что a_i являются

* Проще заменить только один элемент. — Прим. ред.

индивидами некоторой элементарной подструктуры структуры $\mathcal{A}$, изоморфной $\mathcal{B}$.]

(б) Пусть $\mathcal{A}$ и $\mathcal{B}$ — насыщенные модели теории T . Пусть, $a_1, \dots, a_n$ — индивиды из $\mathcal{A}$ и $b_1, \dots, b_n$ — индивиды из $\mathcal{B}$ такие, что n -ки $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ имеют одинаковые типы. Показать, что существует изоморфизм φ между $\mathcal{A}$ и $\mathcal{B}$ такой, что

$$\varphi(a_1) = b_1, \dots, \varphi(a_n) = b_n.$$

[Подобно доказательству теоремы Рылль-Нардзевского.] Вывести, что любые две насыщенные модели теории T изоморфны и что всякая насыщенная модель однородна.

(в) Показать, что всякая универсальная модель слабо насыщена. [Использовать лемму из § 5.6.]

(г) Показать, что всякая слабо насыщенная однородная модель насыщена.

(д) Пусть $\mathcal{A}$ — счетная модель теории T , $a_1, \dots, a_{n-1}$ — индивиды из $\mathcal{A}$, Γ — n -тип в T , включающий тип $(n-1)$ -ки $(a_1, \dots, a_{n-1})$. Показать, что существует счетное элементарное расширение $\mathcal{B}$ модели $\mathcal{A}$ и элемент a_n из $\mathcal{B}$ такой, что Γ — тип n -ки $(a_1, \dots, a_n)$. [Пусть $i_1, \dots, i_{n-1}$ — имена индивидов $a_1, \dots, a_{n-1}$. Получить T' из $D_e(\mathcal{A})$ добавлением новой константы e и для каждой формулы A из Γ новой аксиомы $A[i_1, \dots, i_{n-1}, e]$.]

Если $A_1, \dots, A_k$ принадлежат Γ , то $\exists z_n (A_1 \& \dots \& A_k)$ принадлежит типу $(n-1)$ -ки $(a_1, \dots, a_{n-1})$, так как ее отрицание не может принадлежать этому типу. Вывести, что T' непротиворечива, и взять в качестве $\mathcal{B}$ обединение некоторой модели теории T' .]

(е) Допустим, что для каждого n теория T имеет только счетное число n -типов. Показать, что T имеет насыщенную модель. [Пусть $\mathcal{A}$ — любая счетная модель; применить (д) и лемму Тарского, чтобы получить элементарное расширение $\mathcal{B}$ модели $\mathcal{A}$ такое, что заключение (д) выполняется для каждого выбора Γ и $a_1, \dots, a_{n-1}$. Скомбинировать этот результат с леммой Тарского.]

(ж) Показать, что следующие условия эквивалентны:

- (i) для каждого n теория T имеет только счетное число n -типов;
- (ii) T имеет насыщенную модель;
- (iii) T имеет универсальную модель;
- (iv) T имеет слабо насыщенную модель.

[Применить (е), (а) и (в).]

27. Пусть T — некоторая счетная полная теория. Используя обозначения задачи 5 из главы 4, отождествим каждое подмножество Γ из $S_n(T)$ с элементом V из $\mathfrak{X}(S_n(T))$ так, что $V(A) = \mathbf{I}$ тогда и только тогда, когда A принадлежит Γ . Множество n -типов в T является тогда подпространством пространства $\mathfrak{X}(S_n(T))$; обозначим это подпространство через $\mathfrak{X}_n(T)$.

(а) Показать, что элемент V из $\mathfrak{X}(S_n(T))$ принадлежит $\mathfrak{X}_n(T)$ тогда и только тогда, когда V принадлежит $\mathfrak{X}\mathfrak{B}(S_n(T))$ и $V(A) = \mathbf{I}$ для каждой формулы A из $S_n(T)$, являющейся теоремой теории T . [Использовать лемму из § 5.6.] Вывести, что $\mathfrak{X}_n(T)$ замкнуто в $\mathfrak{X}\mathfrak{B}(S_n(T))$ и, следовательно, компактно.

(б) Для формулы A из $S_n(T)$ пусть Φ_A будет множеством элементов V из $\mathfrak{X}_n(T)$ таких, что $V(A) = \mathbf{I}$. Показать, что Φ_A обра-

зует базу для $\mathfrak{X}_n(T)$ и что Φ_A непусто тогда и только тогда, когда $\vdash_T \exists z_1 \dots \exists z_n A$.

(в) Пусть $\Gamma \subset S_n(T)$, и пусть Φ будет множеством всех n -типов в T , включающих Γ . Показать, что формула A из $S_n(T)$ является образующей для Γ тогда и только тогда, когда Φ_A — непустое подмножество множества Φ . Вывести, что n -тип является главным тогда и только тогда, когда этот тип является изолированной точкой пространства $\mathfrak{X}_n(T)$.

(г) Показать, что если $\mathcal{A}$ — модель теории T , то n -типы в $\mathcal{A}$ образуют плотное подмножество пространства $\mathfrak{X}_n(T)$. [Использовать (б).] Вывести, что n -тип в T является главным тогда и только тогда, когда этот тип есть n -тип в каждой модели теории T . [Использовать (в) и теорему Эренфойхта.]

(д) Пусть R — множество типов в T таких, что для каждого n $R \cap \mathfrak{X}_n(T)$ нигде не плотно в $\mathfrak{X}_n(T)$. Показать, что существует счетная модель $\mathcal{A}$ теории T такая, что никакой тип в $\mathcal{A}$ не находится в R . [Аналогично теореме Эренфойхта, используя (в).]

(е) Допустим, что $\mathcal{A}$ и $\mathcal{B}$ — счетные бесконечные модели теории T , и предположим, что каждый n -тип в $\mathcal{A}$ является главным. Показать, что $\mathcal{A}$ изоморфна некоторой элементарной подмодели модели $\mathcal{B}$. [Пусть $a_1, a_2, \dots$ — индивиды из $\mathcal{A}$. Как и в доказательстве теоремы Рылль-Нардзевского, выбрать индивиды $b_1, b_2, \dots$ из $\mathcal{B}$ так, чтобы n -ки $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ для каждого n имели одинаковый тип. Затем действовать, как в 26 (а).] Кроме того, показать, что если каждый тип в $\mathcal{B}$ является главным, то $\mathcal{A}$ и $\mathcal{B}$ изоморфны. [Аналогично теореме Рылль-Нардзевского.]

(ж) Модель $\mathcal{A}$ теории T называется *элементарно простой*, если каждая модель теории T изоморфна некоторому элементарному расширению модели $\mathcal{A}$. Показать, что модель $\mathcal{A}$ теории T является элементарно простой тогда и только тогда, когда $\mathcal{A}$ счетна и каждый тип в $\mathcal{A}$ главный. [Использовать теорему Лёвенгейма—Скулема, теорему Эренфойхта, задачу 25 и (е).]

(з) Показать, что любые две элементарно простые модели теории T изоморфны. [Использовать (е) и (ж).]

(и) Показать, что T имеет элементарно простую модель тогда и только тогда, когда для каждого n множество главных n -типов является плотным в $\mathfrak{X}_n(T)$. [Использовать (ж), (г), (д) и (в).]

28. Пусть $\mathcal{U}$ — класс подмножеств некоторого непустого пространства I . Скажем, что $\mathcal{U}$ — *ультрафильтр* над I , если

(i) $\mathcal{U}$ является центрированным классом *);

(ii) для каждого подмножества J пространства I либо J , либо J^c (дополнение J в I) принадлежит $\mathcal{U}$.

(а) Показать, что если $\mathcal{U}$ — центрированный класс подмножеств пространства I , то $\mathcal{U}$ содержится в некотором ультрафильтре над I . [Использовать лемму Тейхмюллера—Тьюки.]

(б) Пусть $\mathcal{U}$ — ультрафильтр над I . Показать, что если $J \in \mathcal{U}$ и $J \subset K$, то $K \in \mathcal{U}$. Показать, что пересечение любых двух элементов из $\mathcal{U}$ есть элемент из $\mathcal{U}$.

*) Напомним, что класс множеств называется *центрированным*, если пересечение любого конечного числа множеств из этого класса непусто. — Прим. перев.

29. Пусть $\mathfrak{U}$ — ультрафильтр над непустым пространством I . Для каждого i из I пусть $\mathcal{A}_i$ будет структурой для L , и пусть $\mathcal{B} = \prod_{i \in I} \mathcal{A}_i$. Для a и b из $|\mathcal{B}|$ пусть $a \sim b$ означает, что $[i | (a)_i = (b)_i] \in \mathfrak{U}$.

(а) Показать, что $\sim$ — отношение эквивалентности.

(б) Пусть A — множество классов эквивалентности по $\sim$ и $\varphi(b)$ — класс эквивалентности, содержащий b . Показать, что мы можем определить структуру $\mathcal{A}$ с универсумом A следующим образом:

$$f_{\mathcal{A}}(\varphi(a_1), \dots, \varphi(a_n)) = \varphi(f_{\mathcal{B}}(a_1, \dots, a_n)),$$

$$P_{\mathcal{A}}(\varphi(a_1), \dots, \varphi(a_n)) \leftrightarrow [i | P_{\mathcal{A}_i}((a_1)_i, \dots, (a_n)_i)] \in \mathfrak{U}.$$

Мы называем $\mathcal{A}$ ультрапроизведением структур $\mathcal{A}_i$ и обозначаем через $\prod_{i \in I} \mathcal{A}_i / \mathfrak{U}$.

(в) Пусть a — терм языка $L(\mathcal{B})$, свободный от переменных; показать, что $\mathcal{A}(a^{\varphi}) = \varphi(\mathcal{B}(a))$.

(г) Пусть A — замкнутая формула языка $L(\mathcal{B})$ и π_i определяется так: $\pi_i(b) = (b)_i$; показать, что $\mathcal{A}(A^{\varphi}) = \mathbf{I}$ тогда и только тогда, когда $[i | \mathcal{A}_i(A^{\pi_i}) = \mathbf{I}] \in \mathfrak{U}$. [Использовать индукцию по длине A и 28 (б).] В частности, замкнутая формула A языка L является истинной в $\mathcal{A}$ тогда и только тогда, когда $[i | \mathcal{A}_i(A) = \mathbf{I}] \in \mathfrak{U}$. Вывести, что если каждая структура $\mathcal{A}_i$ есть модель теории T , то $\mathcal{A}$ есть модель теории T .

(д) Если все структуры $\mathcal{A}_i$ равны $\mathcal{C}$, то $\mathcal{A}$ называется ультрастепенью структуры $\mathcal{C}$. Показать, что в этом случае структура $\mathcal{C}$ изоморфна некоторой элементарной подструктуре структуры $\mathcal{A}$. [Отобразить индивид c из $\mathcal{C}$ на класс эквивалентности, содержащий b из $|\mathcal{B}|$, для которого $(b)_i = c$ для всех i , и использовать (г).]

30. (а) Использовать ультрапроизведения, чтобы доказать теорему компактности, не применяя теоремы полноты. [Предположим, что замкнутая формула A не является истинной в никакой конечно аксиоматизированной части теории T . Пусть I — класс формул $\neg A \& A_1 \& \dots \& A_n$, где $A_1, \dots, A_n$ — нелогические аксиомы теории T . Для B из I пусть $\mathcal{A}_B$ — структура, в которой B является истинной, и пусть J_B — множество всех B' из I таких, что B является истинной в $\mathcal{A}_{B'}$. Используя 28 (а), найти ультрафильтр $\mathfrak{U}$ над I , содержащий каждое J_B . По 29 (г) каждая B из I является истинной в $\prod \mathcal{A}_B / \mathfrak{U}$.]

(б) Пусть $\mathcal{A}$ и $\mathcal{B}$ — структуры для L . Показать, что $\mathcal{A}$ элементарно эквивалентна $\mathcal{B}$ тогда и только тогда, когда $\mathcal{A}$ изоморфна некоторой элементарной подструктуре некоторой ультрастепени структуры $\mathcal{B}$. [Часть «тогда» следует из 29 (д). Предположим, что $\mathcal{A}$ и $\mathcal{B}$ элементарно эквивалентны. Пусть I — множество замкнутых формул A языка $L(\mathcal{A})$ таких, что $\mathcal{A}(A) = \mathbf{I}$. Если A принадлежит I , то мы можем определить отображение φ_A из $|\mathcal{A}|$ в $|\mathcal{B}|$ так, что $\mathcal{B}(A^{\varphi_A}) = \mathbf{I}$. Пусть $J_A = \{B | \mathcal{B}(A^{\varphi_B}) = \mathbf{I}\}$. Найдем ультрафильтр $\mathfrak{U}$, содержащий все J_A . Пусть $\mathcal{B}_A = \mathcal{B}$, $\mathcal{C} = \prod \mathcal{B}_A / \mathfrak{U}$. Для a

из $|\mathcal{A}|$ пусть $\varphi(a)$ — класс эквивалентности из $|\mathcal{C}|$, содержащий элемент b такой, что $b_A = \varphi_A(a)$ для A из I . Использовать 29 (г), чтобы показать, что $\mathcal{C}(A^{\varphi}) = \mathbf{I}$ для A из I .]

(в) Показать, что класс $\mathfrak{Z}$ структур для L является обобщенно элементарным классом тогда и только тогда, когда каждое ультрапроизведение структур из $\mathfrak{Z}$ принадлежит $\mathfrak{Z}$ и каждая структура, элементарно эквивалентная структуре из $\mathfrak{Z}$, принадлежит $\mathfrak{Z}$. [Для доказательства части «только тогда» использовать 29 (г). Предположим, что условия выполняются. Пусть нелогические аксиомы теории T являются замкнутыми формулами, истинными в каждой структуре из $\mathfrak{Z}$. Пусть $\mathcal{A}$ — модель теории T и I — класс замкнутых формул, истинных в $\mathcal{A}$. Для каждой A из I выберем $\mathcal{B}_A$ из $\mathfrak{Z}$ так, чтобы $\mathcal{B}_A(A) = \mathbf{I}$. Пусть Q_A — множество B из I таких, что $\mathcal{B}_B(A) = \mathbf{I}$, и $\mathfrak{U}$ — ультрафильтр, содержащий все Q_A . Показать, что $\mathcal{A}$ элементарно эквивалентна $\prod \mathcal{B}_B / \mathfrak{U}$.]

НЕПОЛНОТА И НЕРАЗРЕШИМОСТЬ

6.1. Вычислимость

Разрешающим методом для формальной системы F называется такой метод, с помощью которого для любой данной формулы из F мы можем за конечное число шагов решить, будет она теоремой из F или нет. *Проблема разрешимости* *) для F состоит в следующем: найти разрешающий метод для F или доказать, что такого метода не существует.

Хотя решение проблемы разрешимости для F дает решение проблемы характеристики, обратное утверждение не всегда верно. Например, если T — теория, в которой нет нелогических аксиом, то теорема Эрбрана не дает решения проблемы разрешимости. Решая с помощью теоремы Эрбрана, является данная формула теоремой или нет, мы должны проверить для бесконечного множества формул, являются ли они квазитавтологиями, а это невозможно сделать за конечное число шагов. Разумеется, теорема полноты также не дает решения проблемы разрешимости, так как мы не можем установить с ее помощью, верна ли данная формула в T .

Можно сформулировать еще более общую проблему, чем проблема разрешимости для формальных систем. Предположим, что A — подмножество множества E . *Разрешающим методом* для A в E называется такой метод, с помощью которого для каждого данного элемента a из E мы за конечное число шагов можем решить, принадлежит элемент a множеству A или нет. *Проблема разрешимости* для A в E состоит в следующем: найти разрешающий метод для A в E или доказать, что такого метода не существует.

Разрешающий метод для формальной системы F является частным случаем, в котором E — множество формул

из F , а A — множество теорем из F . В математике возникло много аналогичных проблем. Например, еще не решена десятая проблема Гильберта *): найти метод, с помощью которого можно узнавать, разрешимо ли данное диофантово уравнение. Здесь E — множество диофантовых уравнений, а A — множество тех диофантовых уравнений, для которых существует решение. Еще один пример рассматривается в приложении I.

Чтобы наше определение разрешающего метода для A в E имело смысл, каждый элемент из E должен быть таков, что он может быть задан нам за один шаг. Это означает, что элементами множества E должны быть конкретные объекты. В приведенных выше примерах элементами множества E были выражения некоторого языка; такое выражение может быть нам задано, если оно написано перед нами. Если E — множество натуральных чисел, то мы можем, как и в § 4.3, заменить натуральное число n символом, состоящим из n черточек, а затем действовать в том же духе. Не было бы никакой разницы, если бы натуральное число n было задано десятичной записью, так как у нас есть метод перехода к выражению, состоящему из n черточек.

Мы можем сформулировать аналогичную проблему для отображения F из множества A в множество B . *Разрешающим методом* для F называется метод, с помощью которого по заданному элементу a из A мы можем за конечное число шагов получить $F(a)$. Здесь как элементы множества A , так и элементы множества B должны быть конкретными объектами. *Проблема разрешимости* для F : найти разрешающий метод для F или доказать, что такого метода не существует.

Проблема разрешимости для функций является обобщением проблемы разрешимости для множеств. Действительно, предположим, что A — подмножество множества E . Определим отображение F из множества E в множество натуральных чисел, полагая $F(a) = 0$, если a принадлежит A , и $F(a) = 1$, если a не принадлежит A . В таком случае разрешающий метод для F давал бы разрешающий метод

*) Часто говорят также *проблема разрешения*. — Прим. ред.

*) Эта проблема решена отрицательно Ю. В. Матиясевичем в 1970 г. — Прим. перев.

для A в E и наоборот, так что проблема разрешимости для F эквивалентна проблеме разрешимости для A в E .

До сих пор наши определения были очень неточны в одном отношении: мы не указывали точно, что такое *метод*. Делая шаг к объяснению этого, мы отмечаем, что метод должен быть *механическим*. Возможно, лучший способ разъяснить последнее замечание — это привести несколько примеров методов, которые при этом исключаются. Во-первых, исключаются методы, содержащие вероятностные процедуры; бросая монетку, мы не можем решить, принадлежит элемент a множеству A или нет. Во-вторых, исключаются методы, использующие магию; мы не можем установить, принадлежит a множеству A или нет, вопрошая гадалку. В-третьих, исключаются методы, требующие интуиции; мы не можем пользоваться методом, который требуется нам для решения проблемы, если этот метод не содержит указаний для решения этой проблемы. Очевидно, эти исключения неизбежны, если мы хотим уметь давать отрицательные решения проблемы разрешимости. Например, мы не можем привести математическое доказательство того, что гадалка не в состоянии указать, принадлежит элемент a множеству A или нет.

В качестве более позитивного указания, механический метод — это метод, который можно реализовать при помощи соответственно сконструированной машины. Разумеется, мы подразумеваем идеальную машину, не ограниченную, подобно реальным машинам, проблемами размера, механической прочности и т. д. Машина для вычисления F будет иметь входное устройство, в которое мы можем вводить аргумент a ; затем она вычислит $F(a)$. Разумеется, сама машина не должна зависеть от a . Это подразумевается в понятии метода; если мы по-разному вычисляем $F(a)$ для разных a , то мы будем иметь всё, что угодно, только не метод.

До сих пор мы еще не дали точного определения *метода*. Действительно, кажется совершенно безнадежным описать, скажем, всевозможные механические методы отображений натуральных чисел в натуральные числа. Однако мы утверждаем, что это не является необходимым для решения проблем разрешимости.

Сначала предположим, что мы хотим дать положительное решение проблемы разрешимости. Тогда мы просто

укажем разрешающий метод и проверим, что он механический и что он всегда приводит к правильным ответам.

Множество или отображение *вычислимо*, если оно имеет разрешающий метод. Таким образом, отрицательное решение проблемы разрешимости заключается в доказательстве того, что какое-то множество или отображение невычислимо. Несомненно, для этого достаточно дать точное определение *вычислимости*. Может показаться, что от этого мало пользы, так как неочевидно, что мы можем определить *вычислимость* без того, чтобы вначале определить *метод*. Однако мы увидим, что это можно сделать по крайней мере в некоторых случаях.

В оставшейся части этой главы мы будем придерживаться следующей процедуры. Мы введем класс функций из натуральных чисел в натуральные числа. После некоторого изучения этого класса мы приведем аргументы в пользу того, что этот класс в точности совпадает с классом вычислимых функций из натуральных чисел в натуральные числа. Затем мы воспользуемся этим для получения точной формулировки проблемы разрешимости для теорий. Наконец, мы укажем методы получения решений проблем разрешимости для теорий.

6.2. Рекурсивные функции

Мы примем некоторые соглашения, которые значительно сократят изложение наших результатов. В этой главе, если не оговорено противное, *число* означает *натуральное число*, *множество* означает *множество натуральных чисел*, *функция* означает *функция из множества натуральных чисел в множество натуральных чисел*, *предикат* означает *предикат на множестве натуральных чисел*.

Мы будем применять строчные латинские буквы для обозначения натуральных чисел. Для обозначения функций и предикатов мы будем использовать прописные латинские буквы, обычно F , G и H для функций и P , Q и R для предикатов. Символы из N будем употреблять в наших рассуждениях неформально в их обычном значении. Таким образом, запись

$$\forall x P(a, x) \vee F(a, k) = 2$$

означает *или* $P(a, x)$ для всех чисел x , *или* $F(a, k) = 2$.

Понятия о свободном и связанном вхождении переменной будут употребляться в том же смысле, что и в § 2.3; вхождение x свободно, если значение выражения зависит от значения x .

Строчные готические буквы мы будем употреблять для обозначения конечных последовательностей различных латинских букв. Так, мы можем писать $F(a)$ вместо $F(a_1, \dots, a_n)$. Если две различные готические буквы, скажем a и b , встречаются в одном и том же контексте, то подразумевается, что буквы в последовательности, обозначенной через a , полностью отличны от букв в последовательности, обозначенной через b . Если некоторая готическая буква встречается как аргумент функции или предиката, то предполагается, что обозначенная этой буквой последовательность имеет соответствующее число букв. Так, если F — n -арная функция и мы пишем $F(a)$, то мы подразумеваем, что a — последовательность, состоящая из n букв. Если a означает $a_1, \dots, a_n$, то мы обозначаем $\exists a_1 \dots \exists a_n$ через $\exists a$ и $\forall a_1 \dots \forall a_n$ через $\forall a$.

Пусть P — n -арный предикат, определим n -арную функцию K_P следующим образом:

$$K_P(a) = \begin{cases} 0, & \text{если } P(a), \\ 1, & \text{если } \neg P(a). \end{cases}$$

Функцию K_P мы называем *представляющей функций* предиката P . Как мы отметили в предыдущем параграфе, предикат вычислим тогда и только тогда, когда его представляющая функция вычислима.

Приведем теперь несколько примеров вычислимых функций. Пусть $1 \leq i \leq n$, определим функцию I_i^n следующим образом:

$$I_i^n(a_1, \dots, a_n) = a_i.$$

Ясно, что I_i^n вычислима. Бинарные функции $+$ и $\cdot$ вычислимы; разрешающие методы для этих функций изучаются в элементарной школьной арифметике. Бинарный предикат $<$ вычислим, так как вычислима его представляющая функция $K_<$.

Теперь укажем два способа получения вычислимых функций из других вычислимых функций. Первый: предположим, что мы определили функцию F следующим

образом:

$$F(a) = G(H_1(a), \dots, H_k(a)),$$

где $G, H_1, \dots, H_k$ — вычислимые функции. Тогда F вычислима. Действительно, $F(a)$ может быть вычислена, если сначала вычислить значения $H_1(a) = b_1, \dots, H_k(a) = b_k$, а затем вычислить $G(b_1, \dots, b_k)$.

Чтобы изложить второй метод, нам надо ввести некоторые обозначения. Если $\dots x \dots$ — утверждение, истинное для некоторого x , то $\mu x(\dots x \dots)$ означает наименьшее x , для которого $\dots x \dots$ истинно. Например, $\mu x(x=a) = a$. Как видно из этого примера, значение $\mu x(\dots x \dots)$ не зависит от значений x ; это означает, что вхождение x в $\mu x(\dots x \dots)$ связано. Выражение μx мы называем *μ -оператором*.

Теперь предположим, что мы определили F следующим образом:

$$F(a) = \mu x(G(a, x) = 0),$$

где G — такая вычислимая функция, что для каждого a существует такое x , что $G(a, x) = 0$. (Это последнее условие необходимо для того, чтобы гарантировать, что $F(a)$ определена для всех a .) Тогда F вычислима. Действительно, мы можем вычислить $F(a)$, последовательно вычисляя $G(a, 0), G(a, 1), \dots$ до тех пор, пока мы не получим нулевое значение.

Теперь мы определим рекурсивные функции с помощью обобщенного индуктивного определения, состоящего из трех правил R1 — R3.

R1. $I_i^n, +, \cdot$ и $K_<$ рекурсивны.

R2. Если $G, H_1, \dots, H_k$ рекурсивны, а F определена следующим образом:

$$F(a) = G(H_1(a), \dots, H_k(a)),$$

то F рекурсивна.

R3. Если G рекурсивна и $\forall a \exists x (G(a, x) = 0)$, а F определена следующим образом:

$$F(a) = \mu x(G(a, x) = 0),$$

то F рекурсивна.

Чтобы доказать, что каждая рекурсивная функция имеет некоторое свойство P , достаточно доказать, что R1 — R3 остаются справедливыми, если слова *рекурсивные*

функции заменить на функции, имеющие свойство P . Такое доказательство называется *доказательством индукцией по рекурсивным функциям*. Используя предшествующие рассуждения, мы можем доказать индукцией по рекурсивным функциям, что каждая рекурсивная функция вычислима. Обратное не очевидно; мы вернемся к этому в § 6.5.

Предикат называется *рекурсивным*, если его представляющая функция рекурсивна. Вследствие сказанного выше каждый рекурсивный предикат вычислим. Рассмотрение обратного утверждения мы снова отложим до § 6.5.

6.3. Явные определения

Пополним список правил R1—R3 новыми правилами образования рекурсивных функций и предикатов.

R4. Если $Q, H_1, \dots, H_k$ рекурсивны, а P определен следующим образом:

$$P(a) \leftrightarrow Q(H_1(a), \dots, H_k(a)),$$

то P рекурсивен.

Доказательство. Мы имеем

$$K_P(a) = K_Q(H_1(a), \dots, H_k(a)),$$

следовательно, P рекурсивен по R2 и по определению рекурсивного предиката.

R5. Если P рекурсивен и $\forall a \exists x P(a, x)$, а F определена следующим образом:

$$F(a) = \mu x P(a, x),$$

то F рекурсивна.

Доказательство. Так как $F(a) = \mu x (K_P(a, x) = 0)$, то F рекурсивна по R3.

Мы уже встречали определения вида $F(a) = \dots$ или $P(a) \leftrightarrow \dots$, где $\dots$ и $\dots$ содержат только ранее определенные символы. Такое определение называется *явным определением*. Используя R1—R5, мы можем доказать рекурсивность функций и предикатов, заданных какими-то явными определениями. Проиллюстрируем это.

Предположим, что F определена следующим образом:

$$F(a, b, c) = G(H(b, c), K(G(b, c, c), a), c),$$

где G, H и K — ранее определенные рекурсивные функции.

Мы будем последовательно проверять, являются ли все большие и большие части выражения справа рекурсивными функциями от a, b, c . С этой целью мы определяем

$$F_1(a, b, c) = a,$$

$$F_2(a, b, c) = b,$$

$$F_3(a, b, c) = c,$$

$$F_4(a, b, c) = H(b, c),$$

$$F_5(a, b, c) = G(b, c, c),$$

$$F_6(a, b, c) = K(G(b, c, c), a).$$

Функция F_1 есть I_1^3 и, следовательно, рекурсивна по R1. Аналогично, функции F_2 и F_3 рекурсивны. Далее,

$$F_4(a, b, c) = H(F_2(a, b, c), F_3(a, b, c)),$$

так что F_4 рекурсивна по R2. Аналогично, F_5 рекурсивна. Так как

$$F_6(a, b, c) = K(F_5(a, b, c), F_1(a, b, c)),$$

то F_6 рекурсивна по R2. Наконец,

$$F(a, b, c) = G(F_4(a, b, c), F_6(a, b, c), F_3(a, b, c));$$

следовательно, F рекурсивна по R2.

Аналогичная техника применяется к предикатам. Если в правой части встречаются связанные вхождения переменной, то некоторые из используемых в доказательстве функций и предикатов могут иметь эту переменную в качестве аргумента, а некоторые нет. Так предположим, что P определен следующим образом:

$$P(a, b) \leftrightarrow Q(b, \mu x R(x, F(b, a))),$$

где Q, R и F рекурсивны и таковы, что $\mu x R(x, F(b, a))$ определено для всех a и b . Затем определим

$$F_1(a, b, x) = F(b, a) = F(I_2^3(a, b, x), I_1^3(a, b, x)),$$

$$P_1(a, b, x) \leftrightarrow R(x, F(b, a)) \leftrightarrow R(I_2^3(a, b, x), F_1(a, b, x)),$$

$$F_2(a, b) = \mu x R(x, F(b, a)) = \mu x P_1(a, b, x),$$

$$P(a, b) \leftrightarrow Q(I_2^2(a, b), F_2(a, b)).$$

Используя R1—R5, убеждаемся, что все эти функции и предикаты рекурсивны.

Наши наблюдения мы можем подытожить следующим образом: функция рекурсивна или предикат рекурсивен,

если она (он) имеет явное определение, использующее только переменные, символы рекурсивных функций и рекурсивных предикатов и μ -операторы. (Подразумевается, что эти μ -операторы применяются только тогда, когда они определены для всех значений переменных.) Остальные результаты этого параграфа дадут возможность расширить класс символов, которые могут быть использованы в таких определениях.

R6. Каждая константная функция рекурсивна.

Доказательство. Пусть F_k — n -арная функция с постоянным значением k ; докажем индукцией по k , что F_k рекурсивна. Для $k=0$ мы имеем явное определение

$$F_0(a) = \mu x (I_n^{n+1}(a, x) = 0);$$

в то же время для $k=r+1$ мы имеем явное определение

$$F_k(a) = \mu x (F_r(a) < x).$$

Заметим, что последнее определение законно, так как предикат $<$ рекурсивен по R1.

Вследствие R6 мы можем использовать константные функции в явных определениях рекурсивных функций и предикатов.

Обозначим через $\neg P$ предикат, определенный следующим образом: $(\neg P)(a) \leftrightarrow \neg P(a)$. Определим $P \vee Q$ следующим образом:

$$(P \vee Q)(a) \leftrightarrow P(a) \vee Q(a),$$

аналогично определим $P \rightarrow Q$, $P \& Q$ и $P \leftrightarrow Q$.

R7. Если P рекурсивен, то $\neg P$ рекурсивен. Если P и Q рекурсивны, то $P \vee Q$, $P \rightarrow Q$, $P \& Q$ и $P \leftrightarrow Q$ рекурсивны.

Доказательство. Мы имеем явные определения

$$K_{\neg P}(a) = K_{<}(0, K_P(a)), \quad K_{P \vee Q}(a) = K_P(a) \cdot K_Q(a).$$

Отсюда и из определения рекурсивного предиката мы видим, что предикаты $\neg P$ и $P \vee Q$ рекурсивны. В оставшихся случаях мы пользуемся тем, что $P \rightarrow Q$ есть $\neg P \vee Q$, $P \& Q$ есть $\neg(P \rightarrow \neg Q)$, а $P \leftrightarrow Q$ есть $(P \rightarrow Q) \& (Q \rightarrow P)$.

Вследствие R7 мы можем употреблять $\neg$, $\vee$, $\&$, $\rightarrow$ и $\leftrightarrow$ в явных определениях рекурсивных функций и предикатов.

R8. Предикаты $<$, $\leq$, $>$, $\geq$ и $=$ рекурсивны.

Доказательство. По R1 предикат $<$ рекурсивен. Остальные предикаты имеют следующие явные определения:

$$\begin{aligned} a \leq b &\leftrightarrow \neg(b < a), \\ a > b &\leftrightarrow b < a, \\ a \geq b &\leftrightarrow b \leq a, \\ a = b &\leftrightarrow a \leq b \& b \leq a. \end{aligned}$$

Теперь мы введем модифицированный тип μ -оператора, который будет свободен от недостатка иногда быть неопределенным. Предположим, что $_x_$ — формула, а $\dots$ — выражение, не содержащее x и представляющее некоторое число. Затем определим

$$\mu x_{x < \dots} (_x_) = \mu x (_x_ \vee x = \dots).$$

Ясно, что правая часть всегда определена. Значением $\mu x_{x < \dots} (_x_)$ является наименьшее x , меньшее $\dots$ и такое, что $_x_$ истинна, если только такое x существует, если же такого x не существует, то $\mu x_{x < \dots} (_x_) = \dots$. Заметим, что вхождения x в $\mu x_{x < \dots} (_x_)$ связанные. Мы называем $\mu x_{x < \dots}$ *ограниченным μ -оператором*, в отличие от *неограниченного μ -оператора* μx . (Однако μ -оператором будет по-прежнему называться *неограниченный μ -оператор*.)

Из определения ограниченного μ -оператора и предшествующих результатов следует

R9. Если P рекурсивен, а F определена следующим образом:

$$F(a, a) = \mu x_{x < a} P(a, x),$$

то F рекурсивна.

Вследствие этого мы можем употреблять ограниченный μ -оператор в явных определениях рекурсивных функций и предикатов.

Позднее мы увидим, что, используя кванторы, мы можем явно определять нерекурсивные предикаты. Поэтому мы введем модифицированные кванторы, которые могут употребляться в явных определениях рекурсивных функций и предикатов.

Пусть $\text{---}x\text{---}$ и $\dots$ имеют прежнее значение. Мы определяем

$$\begin{aligned} \text{и } \exists x_{x < \dots} (\text{---}x\text{---}) &\leftrightarrow \mu x_{x < \dots} (\text{---}x\text{---}) < \dots \\ \text{и } \forall x_{x < \dots} (\text{---}x\text{---}) &\leftrightarrow \neg \exists x_{x < \dots} \neg (\text{---}x\text{---}). \end{aligned}$$

В таком случае $\exists x_{x < \dots} (\text{---}x\text{---})$ истинна тогда и только тогда, когда $\text{---}x\text{---}$ истинна для некоторого x , меньшего $\dots$, и $\forall x_{x < \dots} (\text{---}x\text{---})$ истинна тогда и только тогда, когда $\text{---}x\text{---}$ истинна для каждого x , меньшего $\dots$. Таким образом, мы можем представить себе $\exists x_{x < \dots}$ как квантор существования по переменной, областью изменения которой являются все числа, меньшие $\dots$, аналогично можно объяснить $\forall x_{x < \dots}$. Мы называем $\exists x_{x < \dots}$ и $\forall x_{x < \dots}$ *ограниченными кванторами*, первый есть *ограниченный квантор существования*, а второй — *ограниченный квантор всеобщности*. Напротив, $\exists x$ и $\forall x$ называются *неограниченными кванторами*. (Однако квантор по-прежнему означает *неограниченный квантор*.)

Из определений ограниченных кванторов и предшествующих результатов следует

R10. Если R рекурсивен, а P и Q определены следующим образом:

$$P(a, a) \leftrightarrow \exists x_{x < a} R(a, x),$$

$$Q(a, a) \leftrightarrow \forall x_{x < a} R(a, x),$$

то P и Q рекурсивны.

Вследствие этого мы можем употреблять ограниченные кванторы в явных определениях рекурсивных функций и предикатов.

Иногда мы будем использовать $x \leq \dots$ в качестве нижнего индекса при μx , $\exists x$ или $\forall x$, считая это сокращением для $x < \dots + 1$. Вследствие сказанного выше мы можем употреблять эту запись в явных определениях.

Обычная функция вычитания не является функцией в нашем понимании, так как ее значениями не всегда являются натуральные числа. Поэтому мы определяем модифицированную функцию вычитания $\dot{-}$:

$$a \dot{-} b = a - b, \text{ если } a \geq b,$$

в противном случае $a \dot{-} b = 0$.

R11. Функция $\dot{-}$ рекурсивна.

Доказательство. Мы имеем явное определение

$$a \dot{-} b = \mu x (b + x = a \vee a < b).$$

Некоторым обобщением явного определения является *определение разбором случаев*. Здесь значения функции или предиката в различных случаях задаются по-разному. Примером является приведенное выше определение функции $\dot{-}$.

R12. Пусть $G_1, \dots, G_k$ — рекурсивные функции, а $R_1, \dots, R_k$ — такие рекурсивные предикаты, что для каждого a в точности одно из $R_1(a), \dots, R_k(a)$ истинно. Если F определена следующим образом:

$$F(a) = \begin{cases} G_1(a), & \text{если } R_1(a), \\ \dots & \dots \\ G_k(a), & \text{если } R_k(a), \end{cases}$$

то F рекурсивна.

Доказательство. Мы имеем явное определение

$$F(a) = G_1(a) \cdot K_{\neg R_1}(a) + \dots + G_k(a) \cdot K_{\neg R_k}(a).$$

R13. Пусть $Q_1, \dots, Q_k$ — рекурсивные предикаты, и пусть $R_1, \dots, R_k$ — такие рекурсивные предикаты, что для каждого a в точности одно из $R_1(a), \dots, R_k(a)$ истинно. Если P определен следующим образом:

$$P(a) \leftrightarrow \begin{cases} Q_1(a), & \text{если } R_1(a), \\ \dots & \dots \\ Q_k(a), & \text{если } R_k(a), \end{cases}$$

то P рекурсивен.

Доказательство. Мы можем определить K_P следующим образом:

$$K_P(a) = \begin{cases} K_{Q_1}(a), & \text{если } R_1(a), \\ \dots & \dots \\ K_{Q_k}(a), & \text{если } R_k(a). \end{cases}$$

Следовательно, P рекурсивен по R12.

Обычно $G_1, \dots, G_k, R_1, \dots, R_k$ из R12 и $Q_1, \dots, Q_k, R_1, \dots, R_k$ из R13 заменяются явными определениями этих функций и предикатов. Так как R_k есть $\neg(R_1 \vee \dots \vee R_{k-1})$, то мы иногда вместо R_k пишем просто

в остальных случаях. Так, типичным определением, использующим R12, является

$$F(a, b) = \begin{cases} a, & \text{если } a < b, \\ b + 2, & \text{если } b \leq a \text{ и } a = 4, \\ 2 & \text{в остальных случаях.} \end{cases}$$

Разумеется, мы можем применять полученные результаты к множествам (т. е. к унарным предикатам). Так, согласно R7 объединение и пересечение двух рекурсивных множеств рекурсивно и дополнение рекурсивного множества рекурсивно. Кроме того, каждое конечное множество A рекурсивно. Действительно, если A пусто, то оно имеет явное определение

$$A(a) \leftrightarrow a < a,$$

если же A содержит элементы $k_1, \dots, k_n$, то оно имеет явное определение

$$A(a) \leftrightarrow a = k_1 \vee \dots \vee a = k_n.$$

Здесь мы сделаем предупреждение относительно употребления многоточий в явных определениях. В приведенном выше примере выражение, изображаемое многоточием, зависело от A ; если бы мы знали, что за множество есть A , то мы могли бы полностью его выписать. Однако мы не должны употреблять многоточия, если изображаемые ими выражения зависят от значения какого-нибудь аргумента. Так,

$$P(a, b) \leftrightarrow a = F(0) \vee a = F(1) \vee \dots \vee a = F(b)$$

не является правильным явным определением, так как изображаемое многоточием выражение зависит от значения b .

6.4. Номера последовательностей

Следующая наша цель — так сопоставить число каждой конечной последовательности чисел, чтобы соответствующие функции и предикаты были рекурсивны. Это будет связано со следующим результатом.

Лемма (Гёдель). Существует такая бинарная рекурсивная функция β , что

$$\beta(a, i) \leq a \div 1$$

для любых a и i , и такая, что для любых чисел $a_0, a_1, \dots, a_{n-1}$ существует такое число a , что $\beta(a, i) = a_i$ для любого $i < n$.

Для доказательства леммы нам понадобятся несколько простых фактов из теории чисел. Так как позже нам надо будет убедиться в том, что эти факты доказуемы в некоторой теории, то приведем подробные доказательства.

Будем писать $\text{Div}(a, b)$, если a делится на b , т. е. если $\exists x (a = b \cdot x)$. Если a и b отличны от 0 и $\forall x (\text{Div}(ax, b) \rightarrow \text{Div}(x, b))$, то мы говорим, что a и b взаимно просты, и пишем $\text{RP}(a, b)$. Тогда

$$\text{RP}(a, b) \rightarrow \text{RP}(b, a). \quad (1)$$

Действительно, допустим, что $\text{RP}(a, b)$ и что $\text{Div}(bx, a)$, тогда $bx = ya$ для некоторого y . Отсюда $\text{Div}(ay, b)$, так что $\text{Div}(y, b)$ и $y = bz$ для некоторого z . Вследствие этого $bx = abz$ и потому $x = az$; таким образом, $\text{Div}(x, a)$.

Предположим, что $a_1, \dots, a_n, b_1, \dots, b_m$ отличны от 0 и 1 и что $\text{RP}(a_i, b_j)$ для всех i и j . Тогда существует число c , которое делится на каждое a_i и не делится ни на какое b_j . Мы докажем это индукцией по n . Если $n = 0$, то положим $c = 1$. Если же $n \neq 0$, то существует такое c' , которое делится на $a_1, \dots, a_{n-1}$ и не делится на $b_1, \dots, b_m$; тогда положим $c = a_n c'$.

Далее докажем, что

$$k \neq 0 \text{ и } z \neq 0 \text{ и } \text{Div}(z, k) \rightarrow \text{RP}(1 + (j + k)z, 1 + jz). \quad (2)$$

Прежде всего мы имеем

$$\text{Div}(x + xjz, z) \rightarrow \text{Div}(x, z) \text{ для всех } x,$$

так что $\text{RP}(1 + jz, z)$. Из (1) получаем $\text{RP}(z, 1 + jz)$. Теперь предположим, что

$$\text{Div}(x + x(j + k)z, 1 + jz).$$

Тогда ясно, что $\text{Div}(xkz, 1 + jz)$. Вследствие $\text{RP}(z, 1 + jz)$ мы имеем

$$\text{Div}(xk, 1 + jz).$$

Так как $\text{Div}(z, k)$, то отсюда следует, что $\text{Div}(xz, 1 + jz)$. Вновь, используя $\text{RP}(z, 1 + jz)$, получаем $\text{Div}(x, 1 + jz)$. Отсюда следует (2).

Введем функцию OP :

$$\text{OP}(a, b) = (a + b) \cdot (a + b) + a + 1. \quad (3)$$

Тогда

$$\text{OP}(a, b) = \text{OP}(a', b') \rightarrow a = a' \& b = b'. \quad (4)$$

Действительно, предположим, что левая часть верна. Если $a + b < a' + b'$, то

$$\text{OP}(a, b) \leq (a + b + 1)^2 \leq (a' + b')^2 < \text{OP}(a', b'),$$

что невозможно. Аналогично, невозможно $a' + b' < a + b$, так что $a + b = a' + b'$. Отсюда и из $\text{OP}(a, b) = \text{OP}(a', b')$ получаем $a = a'$, а из этого и из

$$a + b = a' + b'$$

получаем $b = b'$.

Теперь определим β следующим образом:

$$\beta(a, i) = \mu x_{x < a \div 1} \exists y_{y < a} \exists z_{z < a} (a = \text{OP}(y, z) \& \& \text{Div}(y, 1 + (\text{OP}(x, i) + 1) \cdot z)). \quad (5)$$

Из этого явного определения видно, что если мы докажем рекурсивность Div и OP , то β рекурсивна. Однако Div имеет явное определение

$$\text{Div}(a, b) \leftrightarrow \exists x_{x \leq a} (a = x \cdot b),$$

а OP имеет явное определение (3). Ясно также, что $\beta(a, i) \leq a \div 1$.

Пусть теперь даны $a_0, a_1, \dots, a_{n-1}$; найдем то a , о котором говорится в лемме. Пусть c — наибольшее из $\text{OP}(a_i, i) + 1$, и пусть z — не равное нулю число, делящееся на все числа, меньшие c . Если $j < l < c$, то из (2) при $k = l - j$ следует $\text{RP}(1 + jz, 1 + lz)$. Из полученного выше результата следует, что существует такое число y , что при $j < c$ число y делится на $1 + jz$ тогда и только тогда, когда j есть одно из $\text{OP}(a_i, i) + 1$. Мы полагаем $a = \text{OP}(y, z)$.

Из определения OP мы имеем $a_i < y < a$ и $z < a$. Вследствие (4) y и z — единственные числа, удовлетворяющие равенству $a = \text{OP}(y, z)$. Следовательно, чтобы доказать, что $\beta(a, i) = a_i$, достаточно показать, что a_i есть такое наименьшее число x , что

$$\text{Div}(y, 1 + (\text{OP}(x, i) + 1) \cdot z).$$

Для этого достаточно доказать, что если $x < a_i$, то $\text{OP}(x, i) < c$ и $\text{OP}(x, i)$ отлично от любого $\text{OP}(a_j, j)$. Однако $\text{OP}(x, i) \leq \text{OP}(a_i, i) < c$ и $\text{OP}(x, i)$ отлично от любого $\text{OP}(a_j, j)$ вследствие (4).

Далее мы будем предполагать, что β — функция, определенная в (5). Однако все свойства функции, которыми мы воспользуемся, указаны в лемме. Отметим, что из $\beta(a, i) \leq a \div 1$ мы получаем

$$\beta(0, i) = 0 \quad (6)$$

и

$$a \neq 0 \rightarrow \beta(a, i) < a. \quad (7)$$

Теперь мы сопоставим каждой n -ке $(a_1, \dots, a_n)$ такое наименьшее число a , что $\beta(a, 0) = n$ и $\beta(a, i) = a_i$ для $i = 1, \dots, n$. Согласно лемме такое число существует. Это число мы назовем *номером последовательности* $(a_1, \dots, a_n)$ и обозначим его через $\langle a_1, \dots, a_n \rangle$. Мы допускаем также случай $n = 0$; в соответствии с (6) мы имеем $\langle \rangle = 0$.

Для каждого фиксированного n $\langle a_1, \dots, a_n \rangle$ является рекурсивной функцией от $a_1, \dots, a_n$. Действительно, мы имеем явное определение

$$\begin{aligned} \langle a_1, \dots, a_n \rangle &= \mu x (\beta(x, 0) = n \& \beta(x, 1) = \\ &= a_1 \& \dots \& \beta(x, n) = a_n). \end{aligned}$$

Кроме того, по $\langle a_1, \dots, a_n \rangle$ можно найти $n, a_1, \dots, a_n$ с помощью рекурсивных функций. Более конкретно, определим явно две рекурсивные функции

$$\begin{aligned} \text{lh}(a) &= \beta(a, 0), \\ (a)_i &= \beta(a, i + 1). \end{aligned}$$

Тогда, если a есть $\langle a_0, \dots, a_{n-1} \rangle$, то мы имеем $n = \text{lh}(a)$ и $(a)_i = a_i$ при $i < n$. Вместо $((a)_i)_j$ будем сокращенно писать $(a)_{i,j}$. Из (7) получаем

$$a \neq \langle \rangle \rightarrow \text{lh}(a) < a \& (a)_i < a. \quad (8)$$

Введем некоторые другие рекурсивные функции и предикаты, связанные с номерами последовательностей. Множество номеров последовательностей обозначается через Seq . Оно рекурсивно, так как имеет явное определение

$$\text{Seq}(a) \leftrightarrow \forall x_{x < a} (\text{lh}(x) \neq \text{lh}(a) \vee \exists i_{i < \text{lh}(a)} ((x)_i \neq (a)_i)).$$

Мы определим In так, чтобы

$$\text{In}(\langle a_1, \dots, a_n \rangle, i) = \langle a_1, \dots, a_j \rangle$$

при $i \leq n$:

$$\text{In}(a, i) = \mu x (\text{lh}(x) = i \& \forall j_{j < i} ((x)_j = (a)_j)).$$

Наконец, мы так определим $*$, чтобы

$$\langle a_1, \dots, a_n \rangle * \langle b_1, \dots, b_m \rangle = \langle a_1, \dots, a_n, b_1, \dots, b_m \rangle.$$

Явное определение функции $*$:

$$\begin{aligned} a * b &= \mu x (\text{lh}(x) = \text{lh}(a) + \text{lh}(b) \\ &\quad \& \forall i < \text{lh}(a) ((x)_i = (a)_i) \\ &\quad \& \forall i < \text{lh}(b) ((x)_{\text{lh}(a) + i} = (b)_i)). \end{aligned}$$

Одним из применений номеров последовательностей является замена n -арных функций и предикатов унарными функциями и предикатами. Если F — некоторая n -арная функция, то мы определим унарную функцию $\langle F \rangle$, называемую *сверткой* функции F , следующим образом:

$$\langle F \rangle(a) = F((a)_0, \dots, (a)_{n-1}). \quad (9)$$

По $\langle F \rangle$ мы можем восстановить F :

$$F(a_1, \dots, a_n) = \langle F \rangle(\langle a_1, \dots, a_n \rangle). \quad (10)$$

Пусть P — n -арный предикат; определим унарный предикат $\langle P \rangle$, называемый *сверткой* предиката P , следующим образом:

$$\langle P \rangle(a) \leftrightarrow P((a)_0, \dots, (a)_{n-1}). \quad (11)$$

По $\langle P \rangle$ мы можем восстановить P :

$$P(a_1, \dots, a_n) \leftrightarrow \langle P \rangle(\langle a_1, \dots, a_n \rangle). \quad (12)$$

(9)–(12) мы называем *формулами свертывания*; из них следует, что F рекурсивна тогда и только тогда, когда $\langle F \rangle$ рекурсивна, и что P рекурсивен тогда и только тогда, когда $\langle P \rangle$ рекурсивен. Заметим также, что $\langle K_P \rangle = K_{\langle P \rangle}$.

Теперь мы увидим, как номера последовательностей могут применяться для индуктивного определения рекурсивных функций и предикатов. Пусть F — n -арная функция и $n \neq 0$, определим новую n -арную функцию $\bar{F}$ следующим образом:

$$\bar{F}(a, a) = \langle F(0, a), F(1, a), \dots, F(a-1, a) \rangle. \quad (13)$$

Грубо говоря, $\bar{F}(a, a)$ содержит всю информацию о значениях $F(i, a)$ при $i < a$.

Мы покажем, что F рекурсивна тогда и только тогда, когда $\bar{F}$ рекурсивна. Предположим, что F рекурсивна. Мы не можем использовать (13) в качестве явного опре-

деления, так как изображаемое многоточием выражение зависит от a . Однако мы имеем такое явное определение:

$$\bar{F}(a, a) = \mu x (\text{lh}(x) = a \& \forall i < a ((x)_i = F(i, a))). \quad (14)$$

Если $\bar{F}$ рекурсивна, то для F мы имеем явное определение

$$F(a, a) = (\bar{F}(a+1, a))_a. \quad (15)$$

Предположим теперь, что G — $(n+1)$ -арная функция. Равенство

$$F(a, a) = G(\bar{F}(a, a), a, a)$$

дает значение $F(a, a)$, когда известны значения $F(i, a)$ для $i < a$. Поэтому это правильное индуктивное определение функции F .

R14. Если G рекурсивна, а F определена индуктивно следующим образом:

$$F(a, a) = G(\bar{F}(a, a), a, a),$$

то F рекурсивна.

Доказательство. Определим H следующим образом:

$$\begin{aligned} H(a, a) &= \mu x (\text{Seq}(x) \& \text{lh}(x) = \\ &= a \& \forall i < a ((x)_i = G(\text{In}(x, i), i, a))). \end{aligned} \quad (16)$$

Тогда ясно, что H совпадает с $\bar{F}$, так что мы можем определить F следующим образом:

$$F(a, a) = G(H(a, a), a, a). \quad (17)$$

Из явных определений (16) и (17) мы видим, что F рекурсивна.

На практике при употреблении R14 функция G имеет явное определение или определение разбором случаев. Поэтому равенство, определяющее F , имеет вид явного определения или определения разбором случаев, за исключением того, что $\bar{F}(a, a)$ может появляться в правой части. Так, мы можем определить рекурсивную функцию F следующим образом:

$$F(a, b) = \bar{F}(a, b) + K(b) + a,$$

где K — некоторая ранее определенная рекурсивная функция. При определении разбором случаев мы даже можем допустить появление в правой части некоторых выражений вида $F(\dots, a)$. Например, предположим, что G и H

рекурсивны, и определим F следующим образом:

$$F(a, b) = \begin{cases} F(G(a), b), & \text{если } G(a) < a, \\ H(a, b) & \text{в остальных случаях.} \end{cases}$$

Чтобы представить это в форме R14, заметим, что из $G(a) < a$ следует

$$F(G(a), b) = (\bar{F}(a, b))_{G(a)},$$

так что мы можем заменить в первой строке $F(G(a), b)$ на $(\bar{F}(a, b))_{G(a)}$. Общим условием является следующее: в случае употребления $F(\dots, a)$ мы должны суметь доказать, что $\dots < a$. Часто встречается следующий тип индуктивного определения:

$$F(0, a) = G(a), F(a+1, a) = H(F(a, a), a, a),$$

где G и H определены ранее. Чтобы убедиться, что оно подпадает под правило R14, мы перепишем его в виде

$$F(a, a) = \begin{cases} G(a), & \text{если } a=0, \\ H(F(a \div 1, a), a \div 1, a) & \text{в остальных случаях.} \end{cases}$$

При явном определении предиката $P(a, a)$ мы можем использовать справа $\bar{K}_P(a, a)$. Действительно, если определение имеет вид $P(a, a) \leftrightarrow \dots$, то мы можем определить K_P индуктивно следующим образом:

$$K_P(a, a) = \begin{cases} 0, & \text{если } \dots, \\ 1 & \text{в остальных случаях.} \end{cases}$$

Подобное же замечание справедливо в отношении определения разбором случаев. В таком определении мы также можем употреблять справа $P(\dots, a)$, если мы можем показать, что при этом $\dots < a$. Действительно, мы можем заменить $P(\dots, a)$ на $K_P(\dots, a) = 0$, а затем поступать так, как объяснено выше.

6.5. Тезис Чёрча

Чтобы использовать рекурсивность при исследовании проблем разрешимости, мы должны быть убеждены в истинности следующего утверждения: каждая вычислимая функция рекурсивна и каждый вычислимый предикат рекурсивен. Это утверждение известно как *тезис Чёрча*.

В проведении доказательства тезиса Чёрча имеется очевидная трудность: у нас нет точного определения *вычислимости*. Это не обязательно является непреодолимой трудностью: в § 6.2 мы доказали, что каждая рекурсивная функция вычислима и каждый рекурсивный предикат вычислим, не пользуясь подобным определением. Если мы проанализируем это доказательство, то увидим, что мы использовали только такие свойства вычислимых функций и предикатов, которые были очевидны даже при нашем туманном описании вычислимости. Возникает вопрос, сможем ли мы таким же способом доказать тезис Чёрча?

Очевидно, что мы сможем доказать тезис Чёрча для предикатов, если предположим истинность тезиса Чёрча для функций, так как предикат вычислим или рекурсивен тогда и только тогда, когда его представляющая функция вычислима или рекурсивна. К несчастью, еще никому не удалось доказать тезис Чёрча для функций или хотя бы выделить те свойства вычислимых функций, которые были бы необходимы для такого доказательства. Но и не имея такого доказательства, мы все же надеемся найти аргументы в пользу того, что тезис Чёрча справедлив. Известно много подобных аргументов, так много, что почти все логики считают тезис Чёрча верным. Изложим вкратце эти аргументы.

Прежде всего показана рекурсивность огромного количества вычислимых функций. Некоторые из них рассматривались в предшествующих параграфах. Функции, встречающиеся в элементарной теории чисел, обычно определены по индукции и могут рассматриваться в духе последнего параграфа. Например, a^b можно определить индуктивно следующим образом: $a^0 = 1$, $a^{b+1} = a^b \cdot a$. Уже обсуждавшимися методами можно показать рекурсивность некоторых вычислимых функций, встречающихся в анализе (см. задачу 3). Еще один класс вычислимых функций, рекурсивность которых может быть доказана, будет рассмотрен в следующем параграфе. В дополнение к этим положительным аргументам имеется сильный отрицательный: еще никто не сумел построить вычислимую функцию, рекурсивность которой нельзя было бы доказать, или хотя бы указать правдоподобный метод построения такой функции.

Следующим аргументом в том же направлении служит то, что, как было показано, многие общие методы получения вычислимых функций из вычислимых функций при применении к рекурсивным функциям дают рекурсивные функции. Некоторые такие методы мы уже рассматривали, а другие рассмотрим позднее. И снова имеется дополнительный аргумент: еще никто не указал метода, для которого было бы видно, что, будучи применен к вычислимым функциям, он дает вычислимые функции, и для которого не было бы показано, что, будучи применен к рекурсивным функциям, он дает рекурсивные функции.

Мы получим еще больше аргументов, если попытаемся непосредственно определить понятие *вычислимый*. Для простоты рассмотрим унарную вычислимую функцию F . Разумно предположить, что вычисление заключается в выписывании выражений на листе бумаги (или что оно может быть к этому сведено). Как станет ясно из следующего параграфа, не теряя общности, можно предположить, что выписываемые выражения являются числами (точнее, выражениями, обозначающими числа). Поэтому мы пишем $a_0, a_1, \dots, a_n$, где a_0 есть a и a_n есть $F(a)$. Теперь разрешающий метод указывает нам, как получить a_i из $a_0, \dots, a_{i-1}$ или, что эквивалентно, из $\langle a_0, \dots, a_{i-1} \rangle$. Следовательно, существует некоторая вычислимая функция G такая, что $G(\langle a_0, \dots, a_{i-1} \rangle) = a_i$. Разрешающий метод также указывает нам, когда вычисление закончено, поэтому существует некоторый вычислимый предикат P такой, что $P(\langle a_0, \dots, a_i \rangle)$ ложен при $i < n$ и истинен при $i = n$.

Наша попытка определить понятие вычислимости закончилась порочным кругом, так как G и P должны предполагаться вычислимыми. Тем не менее G должна быть очень простой вычислимой функцией, потому что она описывает единственный шаг в вычислении; то же самое относится и к P . Поэтому, основываясь на прочих доводах в пользу тезиса Чёрча, мы можем ожидать, что G и P рекурсивны. Предполагая это, мы можем доказать, что F рекурсивна. Действительно, если мы определим

$$H(i, a) = \begin{cases} a, & \text{если } i = 0, \\ G(H(i, a)) & \text{в остальных случаях,} \end{cases}$$

$$K(a) = \mu x P(H(x+1, a)),$$

то

$$F(a) = H(K(a), a).$$

Дальнейшие аргументы (в пользу тезиса Чёрча) даются нам различными точными определениями, которые предлагались для вычислимых функций. Для каждого из этих определений очевидно, что подпадающие под них функции вычислимы, и обратное кажется очень правдоподобным. (В некоторых случаях можно привести весьма убедительные аргументы в пользу этого обратного.) Имеется много типов таких определений. В некоторых утверждается, что функция может быть вычислена на машине определенного типа. В других говорится, что функция может быть вычислена в формальной системе подходящего вида. Третьи похожи на определение из предыдущего абзаца, но с точно определенными возможностями для G и P . Четвертые аналогичны определению, которое мы давали. Имеются также и другие типы определений, и для каждого типа имеются несколько отличающихся друг от друга определений.

Из этих определений аргументы в пользу тезиса Чёрча получаются двумя путями. Во-первых, можно показать, что все функции, подпадающие под эти определения, рекурсивны. Поэтому любой аргумент в пользу того, что все вычислимые функции подпадают под одно из этих определений, становится и доводом в пользу тезиса Чёрча. Во-вторых, класс функций, задаваемый каждым из этих определений, в точности совпадает с классом рекурсивных функций. Это несомненно наводит на мысль, что этот класс функций является весьма естественным классом; последнее очень трудно объяснить, если этот класс не совпадает в точности с классом вычислимых функций.

Впредь мы будем принимать тезис Чёрча. Он никогда не будет использоваться в наших теоремах и доказательствах, потому что они не будут опираться на вычислимость. Его значение будет заключаться в том, чтобы показывать, что наши теоремы являются решениями поставленных нами проблем. Так, если мы докажем, что множество A не рекурсивно, то нам понадобится тезис Чёрча для того, чтобы убедиться, что мы дали отрицательное решение проблемы разрешимости для A .

Существует и другой способ применения тезиса Чёрча. Мы можем определить функцию, а затем утверждать, что

так как очевидно, что эта функция вычислима, то она рекурсивна вследствие тезиса Чёрча. Такое использование тезиса Чёрча хотя и является очень удобным при определенных условиях, не является на самом деле необходимым. Читатель, не желающий принимать тезис Чёрча, может доказать, что рассматриваемая функция рекурсивна, используя методы этой и следующей глав.

Мы можем воспользоваться тезисом Чёрча для установления другой связи между вычислимостью и рекурсивностью. Мы говорим, что предикат P *позитивно вычислим*, если существует метод, который, будучи применен к a , приведет к заключению, что $P(a)$ истинно, если такое заключение верно, и не даст результата, если $P(a)$ ложно. Мы утверждаем, что предикат P *позитивно вычислим* тогда и только тогда, когда существует такой вычислимый предикат Q , что для всех a

$$P(a) \leftrightarrow \exists x Q(a, x).$$

Действительно, если такой предикат Q существует, то мы можем вычислить P в указанном ранее смысле, последовательно вычисляя $Q(a, 0)$, $Q(a, 1)$, ... до тех пор, пока не приходим к такому i , что $Q(a, i)$ истинно, и тем самым к заключению, что $P(a)$ истинно. Обратно, предположим, что P *позитивно вычислим*, и пусть $Q(a, x)$ означает, что x шагов в вычислении $P(a)$ приводят к заключению, что $P(a)$ истинно. Тогда Q вычислим и

$$P(a) \leftrightarrow \exists x Q(a, x)$$

для всех a .

Предикат P называется *рекурсивно перечислимым*, если существует такой рекурсивный предикат Q , что $P(a) \leftrightarrow \exists x Q(a, x)$ для всех a . Из сказанного выше и вычислимости рекурсивных предикатов мы видим, что каждый рекурсивно перечислимый предикат *позитивно вычислим*. Если к тому же мы принимаем тезис Чёрча, то мы можем заключить, что предикат *позитивно вычислим* тогда и только тогда, когда он *рекурсивно перечислим*.

Каждый рекурсивный предикат P рекурсивно перечислим; действительно, $P(a) \leftrightarrow \exists x Q(a, x)$, где Q — рекурсивный предикат, определенный следующим образом: $Q(a, x) \leftrightarrow P(a)$. Как мы увидим позже, обратное неверно.

6.6. Номера выражений

Прежде чем рассмотреть проблему разрешимости для какой-то формальной системы, мы должны точно знать, какие символы имеются в этой формальной системе. В случае теории это означает, что мы должны знать нелогические символы, так как остальные символы фиксированы. В простейшем случае число нелогических символов конечно; тогда мы можем просто дать список этих символов. Поэтому в оставшейся части этой главы мы будем предполагать, что *все языки и теории первого порядка имеют только конечное число нелогических символов*. Читатель увидит, что большинство результатов на самом деле применимо и при некоторых более общих условиях.

Теперь покажем, как проблема разрешимости для теорий связана с рекурсивными функциями. Пусть L — некоторый язык первого порядка (удовлетворяющий приведенному выше условию). Каждому символу языка L мы сопоставим некоторое число. Число, сопоставленное символу u , называется *номером символа u* и обозначается через $SN(u)$. Если $z_0, z_1, \dots$ — переменные, расположенные в алфавитном порядке, то мы полагаем $SN(z_i)$ равным $2i$. Остальным символам (число которых конечно) мы сопоставляем произвольные номера символов, удовлетворяющие лишь следующему условию: различным символам должны быть сопоставлены различные номера символов. Впредь мы будем предполагать, что сопоставление номеров символов для каждого рассматриваемого языка первого порядка фиксировано.

Теперь мы сопоставим число каждому указателю языка L . Число, сопоставленное указателю u , называется *номером выражения u* *) и обозначается через $\lceil u \rceil$. Оно определяется индукцией по длине u . По теореме построения u есть $v v_1 \dots v_n$, где v — некоторый символ индекса n , а $v_1, \dots, v_n$ — указатели. Затем мы полагаем

$$\lceil u \rceil = \langle SN(v), \lceil v_1 \rceil, \dots, \lceil v_n \rceil \rangle.$$

Ясно, что различные указатели имеют различные номера. Так как функции $\langle a_1, \dots, a_n \rangle$ вычислимы, то мы можем

*) Часто, если это не вызывает недоразумений, вместо *номер символа* или *номер выражения* мы будем говорить просто *номер*. — Прим. перев.

фактически вычислить $\lceil u \rceil$, если u задано (при условии, что мы имеем список нелогических символов и их номеров). Обратно, если нам дано число a , то мы можем установить, является ли это число номером какого-либо выражения, и если это так, то мы можем найти указатель с этим номером. Как это сделать, мы покажем индукцией по a . Вначале мы установим, является ли a номером последовательности, отличным от $\langle \rangle$; мы можем это сделать, потому что множество Seq вычислимо. Если это не так, то a не является номером никакого выражения. Если же это так, то мы найдем такие числа $a_0, a_1, \dots, a_n$, что $a = \langle a_0, a_1, \dots, a_n \rangle$; это мы можем сделать, так как функции lh и $(x)_i$ вычислимы. Теперь посмотрим, является ли a_0 номером символа v индекса n . Если не является, то a не является номером никакого выражения. Если же это имеет место, то мы посмотрим, является ли a_i номером указателя v_i ($i = 1, 2, \dots, n$). Это мы можем сделать по индуктивному предположению, потому что $a_i < a$ согласно (8) из § 6.4. Предполагая, что все это выполнено, остается лишь взглянуть на выражение $vv_1 \dots v_n$, чтобы увидеть, является ли оно указателем.

Теперь предположим, что T — некоторая теория языка L , и пусть Thm_T — множество номеров теорем теории T . Мы покажем, что T имеет разрешающий метод тогда и только тогда, когда множество Thm_T вычислимо.

Предположим, что мы имеем разрешающий метод для T . Для каждого данного числа a мы можем следующим образом установить, принадлежит ли a множеству Thm_T . Вначале выясним, является ли a номером некоторого выражения. Если не является, то a не принадлежит множеству Thm_T . Если является, то мы найдем такой указатель u , что $a = \lceil u \rceil$. Тогда a принадлежит множеству Thm_T в том и только в том случае, когда u является некоторой формулой и u является теоремой теории T . Теперь предположим, что множество Thm_T вычислимо. По данной формуле A теории T мы установим, является формула A теоремой теории T или нет, вычислив $\lceil A \rceil$ и установив, принадлежит ли это число множеству Thm_T .

Мы говорим, что теория T разрешима, если множество Thm_T рекурсивно, в противном случае мы говорим, что теория T неразрешима. Соединяя предшествующие рассуждения с тезисом Чёрча, мы видим, что T имеет

разрешающий метод тогда и только тогда, когда T разрешима. (Можно показать, что разрешимость T не зависит от конкретного сопоставления номеров символам; см. задачу 6.)

Выше мы показали, что множество всех номеров выражений вычислимо. То же самое можно показать для других важных множеств номеров выражений. Согласно тезису Чёрча отсюда следует, что эти множества рекурсивны. Мы проверим это для некоторых из указанных множеств. Помимо того, что это даст дополнительные аргументы в пользу тезиса Чёрча, эти результаты позднее нам понадобятся.

Продолжим определение некоторых функций и предикатов. Сначала мы для каждой функции и каждого предиката дадим формальное определение (явное, разбором случаев или по индукции), которое покажет, что эта функция рекурсивна или этот предикат рекурсивен. Это определение мы сопровождаем объяснением того, что означает данная функция или данный предикат. Иногда это объяснение неполно, и касается лишь тех случаев, которые представляют интерес. Символы всех этих функций и предикатов должны бы быть снабжены нижним индексом T , чтобы показать, что они относятся к теории T , однако мы его опускаем здесь и в других случаях, когда рассматривается только одна теория.

(A) $\text{Vble}(a) \leftrightarrow a = \langle (a)_0 \rangle \& \exists y_{y \leq a} ((a)_0 = 2 \cdot y)$.

$\text{Vble}(a)$ означает, что $a = \lceil x \rceil$ для некоторой переменной x . (Ограничение $y \leq a$ следует из (8) из § 6.4; отсюда же следуют некоторые ограничения в дальнейших определениях.)

Определения (Б) и (В) мы дадим для специального случая теории N , однако ясно, что этот метод является вполне общим.

(Б) $\text{Term}(a) \leftrightarrow \begin{cases} 0 = 0, & \text{если } a = \langle \text{SN}(0) \rangle, \\ \text{Term}((a)_1), & \text{если } a = \langle \text{SN}(S), (a)_1 \rangle, \\ \text{Term}((a)_1) \& \text{Term}((a)_2), & \text{если } a = \langle \text{SN}(+), (a)_1, (a)_2 \rangle \vee \\ & \vee a = \langle \text{SN}(\cdot), (a)_1, (a)_2 \rangle, \\ \text{Vble}(a) & \text{в остальных случаях.} \end{cases}$

$\text{Term}(a)$ означает, что $a = \lceil a \rceil$ для некоторого термина a . Это определение является индуктивным определением, имеющим вид, описанный в § 6.4.

(B) $A\text{For}(a) \leftrightarrow a = \langle (a)_0, (a)_1, (a)_2 \rangle \& ((a)_0 = \text{SN}(=) \vee \vee (a)_0 = \text{SN}(<)) \& \text{Term}((a)_1) \& \text{Term}((a)_2)$.

$A\text{For}(a)$ означает, что $a = \ulcorner A \urcorner$ для некоторой атомной формулы A .

(Г) $\text{For}(a) \leftrightarrow \begin{cases} \text{For}((a)_1), & \text{если } a = \langle \text{SN}(\neg), (a)_1 \rangle, \\ \text{For}((a)_1) \& \text{For}((a)_2), & \text{если } a = \langle \text{SN}(\vee), (a)_1, (a)_2 \rangle, \\ \text{Var}((a)_1) \& \text{For}((a)_2), & \text{если } a = \langle \text{SN}(\exists), (a)_1, (a)_2 \rangle, \\ A\text{For}(a) & \text{в остальных случаях.} \end{cases}$

$\text{For}(a)$ означает, что $a = \ulcorner A \urcorner$ для некоторой формулы A .

Следующие три определения мы дадим для теории, в которой имеются только унарные и бинарные функциональные и предикатные символы, однако метод опять является вполне общим.

(Д) $\text{Sub}(a, b, c) = \begin{cases} c, & \text{если } \text{Vble}(a) \& a = b, \\ \langle (a)_0, \text{Sub}((a)_1, b, c) \rangle, & \text{если } a = \langle (a)_0, (a)_1 \rangle, \\ \langle (a)_0, \text{Sub}((a)_1, b, c), \text{Sub}((a)_2, b, c) \rangle, & \text{если } a = \langle (a)_0, (a)_1, (a)_2 \rangle \& (a)_0 \neq \text{SN}(\exists), \\ \langle (a)_0, (a)_1, \text{Sub}((a)_2, b, c) \rangle, & \text{если } a = \langle \text{SN}(\exists), (a)_1, (a)_2 \rangle \& (a)_1 \neq b, \\ a & \text{в остальных случаях.} \end{cases}$

$\text{Sub}(\ulcorner a \urcorner, \ulcorner x \urcorner, \ulcorner b \urcorner) = \ulcorner a_x[b] \urcorner$;

$\text{Sub}(\ulcorner A \urcorner, \ulcorner x \urcorner, \ulcorner a \urcorner) = \ulcorner A_x[a] \urcorner$.

(Е) $\text{Fr}(a, b) \leftrightarrow \begin{cases} a = b, & \text{если } \text{Vble}(a), \\ \text{Fr}((a)_1, b), & \text{если } a = \langle (a)_0, (a)_1 \rangle, \\ \text{Fr}((a)_1, b) \vee \text{Fr}((a)_2, b), & \text{если } a = \langle (a)_0, (a)_1, (a)_2 \rangle \& (a)_0 \neq \text{SN}(\exists), \\ \text{Fr}((a)_2, b) \& (a)_1 \neq b & \text{в остальных случаях.} \end{cases}$

$\text{Fr}(\ulcorner A \urcorner, \ulcorner x \urcorner)$ означает, что переменная x свободна в A .

(Ж) $\text{Subtl}(a, b, c) \leftrightarrow \begin{cases} \text{Subtl}((a)_1, b, c), & \text{если } a = \langle (a)_0, (a)_1 \rangle, \\ \text{Subtl}((a)_1, b, c) \& \text{Subtl}((a)_2, b, c), & \text{если } a = \langle (a)_0, (a)_1, (a)_2 \rangle \& (a)_0 \neq \text{SN}(\exists), \\ \text{Subtl}((a)_2, b, c) \& (\neg \text{Fr}((a)_2, b) \vee \vee \neg \text{Fr}(c, (a)_1)), & \text{если } a = \langle \text{SN}(\exists), (a)_1, (a)_2 \rangle \& (a)_1 \neq b, \\ 0 = 0 & \text{в остальных случаях.} \end{cases}$

$\text{Subtl}(\ulcorner A \urcorner, \ulcorner x \urcorner, \ulcorner a \urcorner)$ означает, что a допустим для подстановки вместо x в A .

(З) $\text{PAx}(a) \leftrightarrow \exists x_{x < a} (\text{For}(x) \& a = \langle \text{SN}(\vee), \langle \text{SN}(\neg), x \rangle, x \rangle)$.

$\text{PAx}(a)$ означает, что a является номером пропозициональной аксиомы. Следующие три определения соответствуют аналогичным образом аксиомам подстановки, аксиомам тождества и аксиомам равенства.

(И) $\text{SAx}(a) \leftrightarrow \exists x_{x < a} \exists y_{y < a} \exists z_{z < a} (\text{Vble}(x) \& \& \text{For}(y) \& \text{Term}(z) \& \text{Subtl}(y, x, z) \& a = \langle \text{SN}(\vee), \langle \text{SN}(\neg), \text{Sub}(y, x, z) \rangle, \langle \text{SN}(\exists), x, y \rangle \rangle)$.

(К) $\text{IAx}(a) \leftrightarrow \exists x_{x < a} (\text{Vble}(x) \& a = \langle \text{SN}(=), x, x \rangle)$.

(Л) $\text{EAx}(a) \leftrightarrow \dots$

Мы предоставляем читателю заполнить правую часть в (Л) для теории N и убедиться, что метод является общим.

(М) $\text{ER}(a, b) \leftrightarrow b = \langle \text{SN}(\vee), (b)_1, a \rangle$.

$\text{ER}(\ulcorner A \urcorner, \ulcorner B \urcorner)$ означает, что B выводима из A по правилу расширения. Следующие четыре определения подобным же образом соответствуют правилу сокращения, правилу ассоциативности, правилу сечения и правилу $\exists$ -введения.

(Н) $\text{CR}(a, b) \leftrightarrow a = \langle \text{SN}(\vee), b, b \rangle$.

(О) $\text{AR}(a, b) \leftrightarrow (a)_0 = \text{SN}(\vee) \& (a)_{2,0} = \text{SN}(\vee) \& \& b = \langle \text{SN}(\vee), \langle \text{SN}(\vee), (a)_1, (a)_{2,1} \rangle, (a)_{2,2} \rangle$.

(П) $\text{TR}(a, b, c) \leftrightarrow (a)_0 = \text{SN}(\vee) \& (b)_0 = \text{SN}(\vee) \& (b)_1 = \langle \text{SN}(\neg), (a)_1 \rangle \& c = \langle \text{SN}(\vee), (a)_2, (b)_2 \rangle$.

(Р) $\text{IR}(a, b) \leftrightarrow (a)_0 = \text{SN}(\vee) \& (a)_{1,0} = \text{SN}(\neg) \& \& b = \langle \text{SN}(\vee), \langle \text{SN}(\neg), \langle \text{SN}(\exists), (b)_{1,1,1}, (a)_1 \rangle \rangle, (a)_2 \rangle$.

Множество номеров нелогических аксиом теории T обозначается через NLAx_T . Так как это совершенно произвольное подмножество множества For_T , то оно не обязано быть рекурсивным. Если же оно рекурсивно, то мы говорим, что теория T *рекурсивно аксиоматизированная*. Остальные определяемые нами функции и предикаты будут рекурсивны только при предположении, что T рекурсивно аксиоматизированная.

Каждая конечно аксиоматизируемая теория является рекурсивно аксиоматизированной; в частности, рекурсивно аксиоматизированной является теория N . Можно доказать, что теории ACF и RCF также рекурсивно аксиоматизированные, приводя в каждом случае (аналогично вышеприведенным определениям) определение множества $NLAx$.

$$(C) Ax(a) \leftrightarrow PAx(a) \vee SAx(a) \vee IAx(a) \vee EAx(a) \vee \vee NLAx(a).$$

Ax является множеством номеров аксиом.

Теперь мы сопоставим некоторое число каждой конечной последовательности выражений, сопоставляя последовательности $u_1, \dots, u_n$ число $\langle \ulcorner u_1 \urcorner, \dots, \ulcorner u_n \urcorner \rangle$.

$$(T) Prf(a) \leftrightarrow Seq(a) \& lh(a) \neq 0 \& \forall i_{i < lh(a)} ((Ax((a)_i) \vee \vee \exists j_{j < i} \exists k_{k < i} (ER((a)_j, (a)_i) \vee \vee CR((a)_j, (a)_i) \vee AR((a)_j, (a)_i) \vee \vee Tr((a)_j, (a)_i) \vee IR((a)_j, (a)_i))) \& For((a)_i)).$$

Prf является множеством номеров доказательств.

$$(Y) Pr(a, b) \leftrightarrow Prf(b) \& a = (b)_{lh(b)-1}.$$

$Pr(\ulcorner A \urcorner, b)$ означает, что b является номером доказательства формулы A .

Теперь мы можем определить Thm следующим образом:

$$Thm(a) \leftrightarrow \exists x Pr(a, x).$$

Так как здесь имеется неограниченный квантор, то мы не можем утверждать, что множество Thm рекурсивно. Однако мы можем утверждать следующее.

Теорема. Если T — рекурсивно аксиоматизированная теория, то множество Thm_T рекурсивно перечислимо.

В заключение мы приведем еще одно определение, относящееся к теории N , которое будет полезно позднее.

$$(Ф) Num(0) = \langle SN(0) \rangle, \\ Num(a+1) = \langle SN(S), Num(a) \rangle.$$

$Num(a)$ является номером выражения, состоящего из a символов S , после которых следует 0, т. е. выражения теории N , обозначающего a .

6.7. Представимость

Теперь мы покажем, что каждая рекурсивная функция и каждый рекурсивный предикат могут в известном смысле быть вычислены в теории N . (Фактически нелогически аксиомы теории N выбраны именно для этой цели.) В это параграфе $\vdash$ означает $\vdash_N$.

Термы $0, S0, SS0, \dots$ называются *цифрами*. Мы употребляем k_n как имя цифры, которая имеет n вхождений символа S . Таким образом, цифрами являются $k_0, k_1, k_2, \dots$

Пусть F — n -арная функция, A — формула теории N , $x_1, \dots, x_n, y$ — различные переменные. Мы говорим, что A от $x_1, \dots, x_n, y$ представляет F , если для любых $a_1, \dots, a_n$

$$\vdash A_{x_1, \dots, x_n}[k_{a_1}, \dots, k_{a_n}] \leftrightarrow y = k_b,$$

где $b = F(a_1, \dots, a_n)$. Мы говорим, что функция F *представима*, если для некоторых $A, x_1, \dots, x_n, y$ формула A от $x_1, \dots, x_n, y$ представляет F .

Пусть P — n -арный предикат, A — формула теории N , $x_1, \dots, x_n$ — различные переменные. Мы говорим, что A от $x_1, \dots, x_n$ представляет P , если для любых $a_1, \dots, a_n$

$$P(a_1, \dots, a_n) \rightarrow \vdash A_{x_1, \dots, x_n}[k_{a_1}, \dots, k_{a_n}]$$

и

$$\neg P(a_1, \dots, a_n) \rightarrow \vdash \neg A_{x_1, \dots, x_n}[k_{a_1}, \dots, k_{a_n}].$$

Мы говорим, что предикат P *представим*, если для некоторых $A, x_1, \dots, x_n$ формула A от $x_1, \dots, x_n$ представляет P .

Если F представима, а $x_1, \dots, x_n, y$ — различные переменные, то существует такая формула A , что A от $x_1, \dots, x_n, y$ представляет F . Действительно, предположим, что A' от $x'_1, \dots, x'_n, y'$ представляет F . Ввиду теоремы о варианте мы можем предположить, что $x_1, \dots, x_n, y$ не связаны в A' . Тогда мы можем взять в качестве A формулу

$$A'_{x'_1, \dots, x'_n, y'}[x_1, \dots, x_n, y].$$

Аналогичное замечание можно сделать и о представимых предикатах.

Пусть F — n -арная функция, a — терм теории N , $x_1, \dots, x_n$ — различные переменные. Мы говорим, что a от $x_1, \dots, x_n$ представляет F , если для любых $a_1, \dots, a_n$

$$\vdash a_{x_1, \dots, x_n}[k_{a_1}, \dots, k_{a_n}] = k_b,$$

где $b = F(a_1, \dots, a_n)$. Если это имеет место и y — новая переменная, то из теоремы равенства следует, что формула $y = a$ от $x_1, \dots, x_n, y$ представляет F .

Теперь рассмотрим несколько примеров. Сначала мы покажем, что $x=y$ от x, y представляет $=$. Для этого нам надо доказать, что

$$\vdash k_m = k_n, \text{ если } m=n, \quad (1)$$

$$\vdash k_m \neq k_n, \text{ если } m \neq n. \quad (2)$$

Действительно, (1) следует из аксиом тождества. Ввиду теоремы симметрии достаточно доказать (2) при $m > n$. Мы сделаем это индукцией по n . Если $n=0$, то (2) следует из N1. Если $n > 0$, то $\vdash k_m = k_n \rightarrow k_{m-1} = k_{n-1}$ по N2 и $\vdash k_{m-1} \neq k_{n-1}$ по индуктивному предположению, следовательно, $\vdash k_m \neq k_n$ по теореме тавтологии.

Покажем теперь, что $x+y$ от x, y представляет $+$. Нам надо показать, что

$$\vdash k_m + k_n = k_{m+n}. \quad (3)$$

Докажем это индукцией по n . Если $n=0$, то (3) следует из N3. Предположим, что (3) выполняется для некоторого n . Тогда по теореме равенства

$$\vdash S(k_m + k_n) = k_{m+n+1}.$$

Отсюда, из теоремы равенства и из N4

$$\vdash k_m + k_{n+1} = k_{m+n+1},$$

а это есть утверждение (3), в котором n заменено на $n+1$.

Аналогичные рассуждения, использующие N5, N6 и (3), показывают, что

$$\vdash k_m \cdot k_n = k_{mn}. \quad (4)$$

Поэтому $x \cdot y$ от x, y представляет $\cdot$.

Теперь мы покажем, что $x < y$ от x, y представляет $<$. Нам надо доказать, что

$$\vdash k_m < k_n, \text{ если } m < n, \quad (5)$$

$$\vdash \neg(k_m < k_n), \text{ если } m \geq n. \quad (6)$$

Докажем это индукцией по n . Если $n=0$, то (5) невозможно и (6) следует из N7. Предположим теперь, что для некоторого n (5) и (6) выполняются. Вследствие N8

$$\vdash k_m < k_{n+1} \leftrightarrow (k_m < k_n \vee k_m = k_n). \quad (7)$$

Предположим, что $m < n+1$. Если $m < n$, то $\vdash k_m < k_n$ по индуктивному предположению, если же $m=n$, то

$\vdash k_m = k_n$ вследствие (1). В обоих случаях $\vdash k_m < k_{n+1}$ вследствие (7) и теоремы тавтологии. Предположим теперь, что $m \geq n+1$. Тогда $\vdash \neg(k_m < k_n)$ по индуктивному предположению и $\vdash \neg(k_m = k_n)$ вследствие (2). Отсюда $\vdash \neg(k_m < k_{n+1})$ вследствие (7) и теоремы тавтологии.

Лемма 1. Любой предикат P представим тогда и только тогда, когда K_P представима.

Доказательство. Предположим, что A от $x_1, \dots, x_n$ представляет P . Пусть B есть

$$(A \& y = k_0) \vee (\neg A \& y = k_1).$$

Мы утверждаем, что B от $x_1, \dots, x_n, y$ представляет K_P . Предположим, что

$$K_P(a_1, \dots, a_n) = 0.$$

Тогда $P(a_1, \dots, a_n)$; следовательно, $\vdash A[k_{a_1}, \dots, k_{a_n}]$. Отсюда и по теореме тавтологии получаем

$$\vdash B[k_{a_1}, \dots, k_{a_n}] \leftrightarrow y = k_0.$$

Аналогичное доказательство справедливо и при $K_P(a_1, \dots, a_n) = 1$.

Предположим теперь, что A от $x_1, \dots, x_n, y$ представляет K_P . Покажем, что $A_y[0]$ от $x_1, \dots, x_n$ представляет P . Если $P(a_1, \dots, a_n)$, то $K_P(a_1, \dots, a_n) = 0$ и потому

$$\vdash A[k_{a_1}, \dots, k_{a_n}] \leftrightarrow y = k_0.$$

Подставляя k_0 вместо y и применяя (1) и теорему тавтологии, получаем

$$\vdash A[k_{a_1}, \dots, k_{a_n}, k_0].$$

Если $\neg P(a_1, \dots, a_n)$, то мы рассуждаем аналогично, пользуясь (2) вместо (1).

Теорема о представимости. Каждая рекурсивная функция и каждый рекурсивный предикат представимы.

Доказательство. Вследствие леммы 1 достаточно доказать это для функций. Мы сделаем это индукцией по рекурсивным функциям, т. е. покажем, что представимые функции удовлетворяют правилам R1—R3.

Ясно, что x_i от $x_1, \dots, x_n$ представляет I_i^n . Мы видели, что $+$, $\cdot$ и $<$ представимы, поэтому $K_<$ предста-

вима в силу леммы 1. Это обеспечивает выполнение правила R1.

Теперь предположим, что F определена следующим образом:

$$F(a_1, \dots, a_n) = G(H_1(a_1, \dots, a_n), \dots, H_k(a_1, \dots, a_n)),$$

где $G, H_1, \dots, H_k$ представимы. Пусть $x_1, \dots, x_n, y_1, \dots, y_k, z$ — различные переменные. Выберем такие A_i , что A_i от $x_1, \dots, x_n, y_i$ представляет H_i , и выберем B так, что B от $y_1, \dots, y_k, z$ представляет G . Пусть C есть

$$\exists y_1 \dots \exists y_k (A_1 \& \dots \& A_k \& B).$$

Мы покажем, что C от $x_1, \dots, x_n, z$ представляет F . Пусть $F(a_1, \dots, a_n) = c$. Тогда $H_i(a_1, \dots, a_n) = b_i$ и $G(b_1, \dots, b_k) = c$. Пусть A'_i и C' получены из A_i и C подстановкой $k_{a_1}, \dots, k_{a_n}$ вместо $x_1, \dots, x_n$. Ввиду выбора A_i имеем

$$\vdash A'_i \leftrightarrow y_i = k_{b_i}.$$

Вследствие теоремы эквивалентности

$$\vdash C' \leftrightarrow \exists y_1 \dots \exists y_k (y_1 = k_{b_1} \& \dots \& y_k = k_{b_k} \& B).$$

Повторно применяя теорему эквивалентности и следствие 3 теоремы равенства, мы получаем, что

$$\vdash C' \leftrightarrow B_{y_1, \dots, y_k} [k_{b_1}, \dots, k_{b_k}].$$

По выбору B и по теореме тавтологии

$$\vdash C' \leftrightarrow z = k_c.$$

Прежде чем перейти к R3, нам надо доказать еще две леммы.

Лемма 2. $\vdash A_x[k_0] \rightarrow \dots \rightarrow A_x[k_{n-1}] \rightarrow x < k_n \rightarrow A$.

Доказательство. Мы пользуемся индукцией по n . При $n=0$ утверждение, которое надо доказать, превращается в $x < 0 \rightarrow A$, а это следует из N7. Теперь предположим, что лемма верна при некотором n . Вследствие N8

$$\vdash x < k_{n+1} \leftrightarrow x < k_n \vee x = k_n. \quad (8)$$

По теореме эквивалентности

$$\vdash x = k_n \rightarrow (A \leftrightarrow A_x[k_n]). \quad (9)$$

Из (8), (9) и индуктивного предположения по теореме тавтологии получаем

$$\vdash A_x[k_0] \rightarrow \dots \rightarrow A_x[k_{n-1}] \rightarrow A_x[k_n] \rightarrow x < k_{n+1} \rightarrow A,$$

а это является утверждением леммы, в котором n заменено на $n+1$.

Лемма 3. Если $\vdash \neg A_x[k_i]$ для каждого $i < n$ и $\vdash \neg A_x[k_n]$, то

$$\vdash A \& \forall y (y < x \rightarrow \neg A_x[y]) \leftrightarrow x = k_n.$$

Доказательство. Пусть B — левая часть доказываемой эквивалентности. По теореме равенства

$$\vdash x = k_n \rightarrow (B \leftrightarrow A_x[k_n] \& \forall y (y < k_n \rightarrow \neg A_x[y])). \quad (10)$$

По лемме 2, правилу отделения и правилу обобщения получаем

$$\vdash \forall y (y < k_n \rightarrow \neg A_x[y]). \quad (11)$$

Из (10), (11) и $\vdash A_x[k_n]$ по теореме тавтологии получаем

$$\vdash x = k_n \rightarrow B. \quad (12)$$

По теореме подстановки

$$\vdash \forall y (y < x \rightarrow \neg A_x[y]) \rightarrow (k_n < x \rightarrow \neg A_x[k_n]).$$

Отсюда и из $\vdash A_x[k_n]$

$$\vdash B \rightarrow \neg (k_n < x). \quad (13)$$

По лемме 2 и правилу отделения $\vdash x < k_n \rightarrow \neg A$, поэтому

$$\vdash B \rightarrow \neg (x < k_n). \quad (14)$$

Вследствие N9

$$\vdash x < k_n \vee x = k_n \vee k_n < x. \quad (15)$$

Из (12), (13), (14) и (15) мы по теореме тавтологии получаем, что $\vdash B \leftrightarrow x = k_n$.

Теперь мы покажем, что представимые функции удовлетворяют правилу R3. Предположим, что F определена следующим образом:

$$F(a_1, \dots, a_n) = \mu x (G(a_1, \dots, a_n, x) = 0),$$

где G представима. Пусть A от $x_1, \dots, x_n, y, z$ представляет G . Пусть w — новая переменная, и пусть B есть

$$A_z[0] \& \forall w (w < y \rightarrow \neg A_{y,z}[w, 0]).$$

Покажем, что B от $x_1, \dots, x_n, y$ представляет F .

Пусть $F(a_1, \dots, a_n) = b$; положим $c_i = G(a_1, \dots, a_n, i)$. Пусть формулы A' и B' получены из формул A и B подстановкой $k_{a_1}, \dots, k_{a_n}$ вместо $x_1, \dots, x_n$. Тогда по выбору A

$$\vdash A'_y[k_i] \leftrightarrow z = k_{c_i}.$$

Отсюда

$$\vdash A'_{y,z}[k_i, 0] \leftrightarrow k_0 = k_{c_i}. \quad (16)$$

Если $i < b$, то $c_i \neq 0$, так что из (16) и (2) получаем

$$\vdash \neg A'_{y,z}[k_i, 0] \text{ для } i < b. \quad (17)$$

Так как $c_b = 0$, то из (16) и (1) мы имеем

$$\vdash A'_{y,z}[k_b, 0].$$

Отсюда, из (17) и по лемме 3 получаем $\vdash B' \leftrightarrow y = k_b$.

6.8. Теорема Чёрча и теорема о неполноте

Теперь мы в состоянии применить наши результаты для решения проблемы разрешимости для теорий.

Пусть P — некоторый бинарный предикат. Определим для каждого числа b унарный предикат $P_{(b)}$ следующим образом:

$$P_{(b)}(a) \leftrightarrow P(a, b).$$

Следующая простая лемма играет фундаментальную роль.

Диагональная лемма (Кантор). Пусть P — бинарный предикат, а Q — унарный предикат, определенный следующим образом: $Q(a) \leftrightarrow \neg P(a, a)$. Тогда Q отличен от всех $P_{(b)}$.

Доказательство. Если Q совпадает с $P_{(b)}$, то

$$P(b, b) \leftrightarrow P_{(b)}(b) \leftrightarrow Q(b) \leftrightarrow \neg P(b, b);$$

получаем противоречие.

Пусть z — некоторая фиксированная переменная (например, первая из переменных, расположенных в алфавитном порядке). Пусть T является расширением теории N .

Для каждой формулы A теории T через $E(A)$ обозначается множество таких n , что $\vdash_T A_z[k_n]$. Если T противоречива, то каждое множество $E(A)$ совпадает с множеством всех чисел. Покажем, что если T непротиворечива, то каждое рекурсивное множество совпадает с некоторым множеством $E(A)$. Пусть A — рекурсивное множество, выберем в соответствии с теоремой о представимости такую формулу A , что A от z представляет A . Тогда если n принадлежит A , то $\vdash_N A_z[k_n]$, поэтому $\vdash_T A_z[k_n]$, следовательно, n принадлежит $E(A)$. Если n не принадлежит A , то $\vdash_N \neg A_z[k_n]$, поэтому $\vdash_T \neg A_z[k_n]$. Ввиду непротиворечивости T n не принадлежит $E(A)$.

Теперь определим

$$P(a, b) \leftrightarrow \text{Thm}_T(\text{Sub}(b, \ulcorner z \urcorner, \text{Num}(a))).$$

Тогда если $b = \ulcorner A \urcorner$, то $P_{(b)}$ совпадает с $E(A)$. Если мы определим Q следующим образом: $Q(a) \leftrightarrow \neg P(a, a)$, то по диагональной лемме это Q отлично от всех $E(A)$ и поэтому не рекурсивно. Далее, Q имеет явное определение

$$Q(a) \leftrightarrow \neg \text{Thm}_T(\text{Sub}(a, \ulcorner z \urcorner, \text{Num}(a))),$$

и функции Sub и Num рекурсивны. Вследствие этого Thm_T не рекурсивно. Таким образом, мы доказали следующую теорему.

Теорема Чёрча*). Если T — непротиворечивое расширение теории N , то теория T неразрешима.

В частности, неразрешима теория N . (Ввиду теоремы из § 6.6 это доказывает, что Thm_N является рекурсивно перечислимым не рекурсивным множеством.) В следующем параграфе мы увидим, что теорема Чёрча может быть использована для доказательства неразрешимости многих других теорий. А сейчас мы применим теорему Чёрча для получения очень важного утверждения о полноте.

Теорема об отрицании. Предикат P рекурсивен тогда и только тогда, когда как P , так и $\neg P$ рекурсивно перечислимы.

*) Чёрчу принадлежит более слабый результат. Конечно аксиоматизируемые подтеории арифметики, имеющие свойство, указанное в теореме, найдены А. Тарским и А. Мостовским, теория, близкая N , найдена Р. Робинсоном. — Прим. ред.

Доказательство. Если P рекурсивен, то $\neg P$ также рекурсивен, поэтому и P и $\neg P$ рекурсивно перечислимы. Теперь предположим, что P и $\neg P$ рекурсивно перечислимы, и пусть

$P(a) \leftrightarrow \exists x Q(a, x)$ и $\neg P(a) \leftrightarrow \exists x R(a, x)$, где Q и R рекурсивны. Для любого a либо $Q(a, x)$, либо $R(a, x)$, поэтому существует такое x , что либо $Q(a, x)$, либо $R(a, x)$. Следовательно, мы можем определить рекурсивную функцию F следующим образом:

$$F(a) = \mu x (Q(a, x) \vee R(a, x)).$$

Мы утверждаем, что

$$P(a) \leftrightarrow Q(a, F(a)). \quad (1)$$

Действительно, если $Q(a, F(a))$, то $\exists x Q(a, x)$, и поэтому $P(a)$. Если же $\neg Q(a, F(a))$, то $R(a, F(a))$, поэтому $\exists x R(a, x)$ и потому $\neg P(a)$. Из явного определения (1) мы видим, что P рекурсивен.

Лемма. Если T — рекурсивно аксиоматизированная и полная теория, то T разрешима.

Доказательство. Определим рекурсивные функции F и K следующим образом:

$$\begin{aligned} F(0, a) &= a, \\ F(n+1, a) &= \langle \text{SN}(\neg), \langle \text{SN}(\exists), \langle 2n \rangle, \langle \text{SN}(\neg), F(n, a) \rangle \rangle \rangle, \\ K(a) &= F(a+1, a). \end{aligned}$$

Если $a = \ulcorner A \urcorner$, то $K(a) = \ulcorner \forall z_0 \forall z_1 \dots \forall z_a A \urcorner$, где $z_0, z_1, \dots$ — переменные, расположенные в алфавитном порядке. Если z_i входит в A , то $i < \ulcorner z_i \urcorner < \ulcorner A \urcorner = a$, следовательно, $\forall z_0 \forall z_1 \dots \forall z_a A$ замкнута; по правилу обобщения она является теоремой тогда и только тогда, когда A является теоремой. Тогда ввиду полноты T формула A не является теоремой тогда и только тогда, когда формула

$$\neg \forall z_0 \forall z_1 \dots \forall z_a A$$

является теоремой. Таким образом, мы имеем

$$\begin{aligned} \neg \text{Thm}(a) &\leftrightarrow \neg \text{For}(a) \vee \text{Thm}(\langle \text{SN}(\neg), K(a) \rangle) \\ &\leftrightarrow \exists y (\neg \text{For}(a) \vee \text{Pr}(\langle \text{SN}(\neg), K(a) \rangle, y)). \end{aligned}$$

Вследствие этого $\neg \text{Thm}$ рекурсивно перечислимо. Так

как Thm рекурсивно перечислимо, то по теореме об отрицании Thm рекурсивно. Таким образом, T разрешима.

Эта лемма указывает третье применение полных теорий, упоминавшихся в § 5.5. Вместе с предыдущими результатами их можно использовать для того, чтобы показать, что RCF и все $\text{ACF}(n)$ разрешимы.

Из леммы и теоремы Чёрча мы получаем следующий результат.

Теорема о неполноте (Гёдель — Россер). Если T является рекурсивно аксиоматизированным расширением теории N , то теория T неполна.

Теорема о неполноте имеет важные следствия, касающиеся аксиоматического метода. Идея аксиоматического метода состоит в том, что, имея различные понятия, мы вводим язык для выражения утверждений об этих понятиях, а затем вводим аксиоматическую систему для доказательства утверждений об этих понятиях. Аксиоматическая система должна быть такой, чтобы все теоремы аксиоматической системы были истинными, и мы надеемся, что она будет такова, что все истинные предложения этого языка будут теоремами. Во всяком случае, нам, конечно, нужно, чтобы аксиомы и правила аксиоматической системы были такими, чтобы мы могли решить, что является и что не является доказательством. (В противном случае мы могли бы достигнуть нашей цели, просто выбрав в качестве аксиом все истинные предложения.)

Теперь предположим, что эти понятия берутся из $\mathcal{N}$ и что избранный язык есть $L(N)$. Предположим далее, что мы хотим, чтобы наша аксиоматическая система была формализуема как теория. Требование, чтобы мы могли опознавать доказательство, означает, в частности, что когда мы видим какую-либо нелогическую аксиому, мы должны уметь ее опознать. Ввиду тезиса Чёрча это означает, что наша теория T должна быть рекурсивно аксиоматизированной. Если доказуемыми в T являются истинные предложения из $\mathcal{N}$ и только они, то T должна быть эквивалентна $\text{Th}(\mathcal{N})$ и, следовательно, должна быть полным расширением теории N . Однако это невозможно по теореме о неполноте.

Рассуждая менее формально, мы можем увидеть, что ограничение на теории или на язык $L(N)$ несущественно для доказательства. Предположим, что мы имеем аксиома-

тическую систему, в которой каждая замкнутая формула A теории N выражена формулой A^* , и предположим, что мы можем фактически построить A^* , если дана формула A . Предположим также, что A^* доказуема в нашей аксиоматической системе тогда и только тогда, когда A истинна в $\mathcal{N}$. Наконец, предположим, что наша аксиоматическая теория удовлетворяет требованию, что мы можем опознавать доказательство. Тогда мы в состоянии решить, истинна A или ложна. Единственно, что мы должны делать, — это просматривать все последовательности формул из нашей аксиоматической системы до тех пор, пока мы не придем к такой последовательности, которая является либо доказательством A^* , либо доказательством $(\neg A)^*$. Если она является доказательством A^* , то A истинна; если она является доказательством $(\neg A)^*$, то A ложна. Таким образом мы получили разрешающий метод для $\text{Th}(\mathcal{N})$, что невозможно по теореме Чёрча. Поэтому мы приходим к такому заключению: не существует корректной аксиоматической системы, в которой мы могли бы доказать все истинные факты о натуральных числах, выражимые в $L(N)$; этих фактов много меньше, чем всех математических истин.

Это важное ограничение должно быть правильно понято. Здесь не утверждается, что существует некоторая математическая истина, которую нельзя доказать ни в какой корректной аксиоматической системе. Ясно, что это не так, потому что мы можем получить новую корректную систему, присоединяя эту истину в качестве аксиомы. Проблема заключается в следующем: может ли каждая математическая истина (или хотя бы каждая математическая истина, выражимая в $L(N)$) быть доказана из аксиом, истинность которых очевидна. Однако мы не можем надеяться достигнуть большого прогресса в решении этой проблемы до тех пор, пока мы не представим себе более четко, что же означает на самом деле «быть очевидно истинным».

Теорема о неполноте показывает нам, что если T является непротиворечивым рекурсивно аксиоматизированным расширением теории N , то некоторая замкнутая формула A теории T неразрешима в T . Отсюда следует, что если мы внимательно проанализируем детали доказательства, то обнаружим, что если T задана, то мы можем фактически построить формулу A .

6.9. Неразрешимость

Теперь мы изложим несколько новых методов доказательств неразрешимости теорий. Эти методы могут сочетаться с леммой из § 6.8 для доказательства неполноты теорий.

В этом параграфе мы возвратимся к первоначальному интуитивному описанию проблемы разрешимости для теорий. Чтобы превратить наши доказательства в формальные доказательства, надо просто проверить, что используемые функции и предикаты рекурсивны.

Наш план заключается в следующем: скомбинировать теорему Чёрча с основным методом, чтобы показать, что неразрешимость одной теории влечет за собой неразрешимость другой. Основным методом заключается в следующем. Предположим, что каждой формуле A теории T соответствует такая формула A^* теории T' , что $\vdash_T A$ тогда и только тогда, когда $\vdash_{T'} A^*$. Предположим также, что мы имеем какой-то метод построения формулы A^* по данной формуле A . Ясно, что тогда разрешающий метод для T' приводит к разрешающему методу для T , поэтому если T неразрешима, то T' также неразрешима.

Конечным расширением теории T называется такое простое расширение T' теории T , что в T' существует только конечное число нелогических аксиом, не являющихся теоремами теории T . Интерпретация I теории T в теории T' называется *точной*, если для каждой формулы A теории T из $\vdash_T A^{(1)}$ следует $\vdash_{T'} A$.

Теорема 1. *Если T' — консервативное расширение теории T и T неразрешима, то T' неразрешима. Если T — конечное расширение теории T' и T неразрешима, то T' неразрешима. Если T — расширение теории T' с помощью определений и T неразрешима, то T' неразрешима. Если I — точная интерпретация теории T в теории T' и T неразрешима, то T' неразрешима.*

Доказательство. В каждом случае мы определим формулу A^* для использования основного метода. Если T' — консервативное расширение теории T , то A^* есть A . Если T — конечное расширение теории T' , то A^* есть $B_1 \rightarrow \dots \rightarrow B_n \rightarrow A$, где $B_1, \dots, B_n$ — замыкания тех нелогических аксиом из T , которые не являются теоремами теории T' ; тогда по теореме редукции имеем $\vdash_T A$ тогда

и только тогда, когда $\vdash_{T'} A^*$. Если T — расширение теории T' с помощью определений, то A^* — перевод A в T' . Если I — точная интерпретация для теории T в теории T' , то A^* есть $A^{(I)}$.

В качестве примера рассмотрим теорию T языка N , не имеющую нелогических аксиом. Тогда N является конечным расширением теории T , и вследствие теоремы 1 и теоремы Чёрча T неразрешима.

Структура $\mathcal{A}$ называется *строго неразрешимой*, если неразрешимой является каждая теория, для которой $\mathcal{A}$ является моделью.

Теорема 2. Структура $\mathcal{N}$ строго неразрешима.

Доказательство. Пусть $\mathcal{N}$ — модель теории T . Тогда $\mathcal{N}$ является моделью теории $T \cup N$ и потому теория $T \cup N$ непротиворечива. Вследствие теоремы Чёрча $T \cup N$ неразрешима. Так как $T \cup N$ — конечное расширение теории T , то T неразрешима вследствие теоремы 1.

Если T — обогащение теории $\text{Th}(\mathcal{A})$ с помощью определений, то существует единственное обогащение структуры $\mathcal{A}$, являющееся моделью теории T . Такое обогащение структуры $\mathcal{A}$ называется *обогащением структуры $\mathcal{A}$ с помощью определений*.

Лемма. Если $\mathcal{B}$ является обогащением структуры $\mathcal{A}$ с помощью определений и $\mathcal{B}$ строго неразрешима, то $\mathcal{A}$ также строго неразрешима.

Доказательство. Пусть $\mathcal{A}$ является моделью теории T ; нам надо показать, что T неразрешима. Мы знаем, что $\mathcal{B}$ является моделью расширения U теории $\text{Th}(\mathcal{A})$ с помощью определений. Образует T_1 из T , присоединяя в качестве новых нелогических аксиом условия существования и единственности, необходимые для определяющих аксиом теории U . Тогда $\mathcal{A}$ будет моделью теории T_1 . Кроме того, T_1 является конечным расширением теории T (так как мы допускаем только конечное число нелогических символов), поэтому вследствие теоремы 1 достаточно доказать, что T' неразрешима.

Пусть U_1 — расширение теории T_1 с помощью определений, полученное присоединением новых нелогических символов из U вместе с их определяющими аксиомами. Так как $\mathcal{A}$ является моделью теории T_1 , то $\text{Th}(\mathcal{A})$ является расширением теории T_1 , и поэтому U является расширением теории U_1 . Вследствие этого $\mathcal{B}$ является

моделью теории U_1 , и потому теория U_1 неразрешима. По теореме 1 теория T_1 неразрешима.

Интерпретация I языка L в языке L' называется *простой*, если u_I совпадает с u для каждого нелогического символа u языка L . Предположим, что I является простой интерпретацией языка L в теории T' , где $L(T') = L'$, и что $\mathcal{A}$ является моделью теории T' . Из истинности в $\mathcal{A}$ утверждений (1) и (2) из § 4.7 мы видим, что $(U_1)_{\mathcal{A}}$ является универсумом некоторой подструктуры $\mathcal{B}$ структуры $\mathcal{A}$. Структура $\mathcal{B}|L$ обозначается через $\mathcal{A}_I$.

Так как каждый индивид из $\mathcal{A}_I$ имеет одинаковое имя как в $L(\mathcal{A}_I)$, так и в $L'(\mathcal{A})$, то мы можем расширить I до простой интерпретации языка $L(\mathcal{A}_I)$ в языке $L'(\mathcal{A}_I)$. Тогда $\mathcal{A}_I(A) = \mathcal{A}(A_I)$ для каждой замкнутой формулы A языка $L(\mathcal{A}_I)$. Доказательство ведется индукцией по длине формулы A . Если формула A атомная, то A_I есть A и $\mathcal{A}_I(A) = \mathcal{B}(A) = \mathcal{A}(A)$. Если A является отрицанием или дизъюнкцией, то результат следует непосредственно из индуктивного предположения. Предположим теперь, что A есть $\exists x B$. Используя индуктивное предположение и вспоминая, что

$$|\mathcal{A}_I| = (U_1)_{\mathcal{A}},$$

получаем

$$\begin{aligned} \mathcal{A}_I(A) = U &\leftrightarrow \mathcal{A}_I(B_x[i]) = \text{И для некоторого } i \text{ из } L(\mathcal{A}_I) \\ &\leftrightarrow \mathcal{A}((B_I)_x[i]) = \text{И для некоторого } i \text{ из } L(\mathcal{A}_I) \\ &\leftrightarrow \mathcal{A}(U_i \& (B_I)_x[i]) = \text{И для некоторого } i \text{ из } L(\mathcal{A}) \\ &\leftrightarrow \mathcal{A}(\exists x (U_1 x \& B_I)) = \text{И} \\ &\leftrightarrow \mathcal{A}(A_I) = \text{И}. \end{aligned}$$

Пусть теперь A — предложение языка L , а B — замыкание A . Тогда B_I является замыканием $A^{(I)}$. Отсюда и вследствие равенства $\mathcal{A}_I(B) = \mathcal{A}(B_I)$ мы получаем, что A истинна в $\mathcal{A}_I$ тогда и только тогда, когда $A^{(I)}$ истинна в $\mathcal{A}$.

Мы говорим, что предикат на $|\mathcal{A}|$ или функция из $|\mathcal{A}|$ в $|\mathcal{A}|$ *определим* (a) в $\mathcal{A}$, если он (она) входит в некоторое обогащение структуры $\mathcal{A}$ с помощью определений. Вследствие этого предикат p на $|\mathcal{A}|$ определим в $\mathcal{A}$ тогда и только тогда, когда существует такая формула D , что

$$pa_1 \dots a_n \leftrightarrow \mathcal{A}(D[i_1, \dots, i_n]) = \text{И},$$

где $i_1, \dots, i_n$ — имена индивидов $a_1, \dots, a_n$; и функция f из $|\mathcal{A}|$ в $|\mathcal{A}|$ определима в $\mathcal{A}$ тогда и только тогда, когда существует такая формула D , что

$$fa_1 \dots a_n = b \leftrightarrow \mathcal{A}(D[i_1, \dots, i_n, j]) = \mathbf{И},$$

где $i_1, \dots, i_n, j$ — имена индивидов $a_1, \dots, a_n, b$. (Легко заметить, что последнее условие гарантирует, что нужные условия существования и единственности истинны в $\mathcal{A}$ и потому являются теоремами теории $\text{Th}(\mathcal{A})$.)

Структура $\mathcal{A}$ определима в структуре $\mathcal{B}$, если множество $|\mathcal{A}|$ является подмножеством множества $|\mathcal{B}|$, определенным в $\mathcal{B}$, и каждая функция и каждый предикат из $\mathcal{A}$ являются ограничением на $|\mathcal{A}|$ соответствующих функций или предикатов, определенных в $\mathcal{B}$.

Предположим, что структура $\mathcal{A}$ определима в структуре $\mathcal{B}$. Тогда мы можем найти такое обогащение $\mathcal{C}$ структуры $\mathcal{B}$ с помощью определений, что $|\mathcal{A}|$ является предикатом $p_{\mathcal{C}}$ структуры $\mathcal{C}$, и такое, что каждая функция и каждый предикат из $\mathcal{A}$ являются ограничением на $|\mathcal{A}|$ каких-то функций или предикатов из $\mathcal{C}$. Мы можем предполагать, что обозначения выбраны так, что $u_{\mathcal{A}}$ является ограничением $u_{\mathcal{C}}$ для каждого нелогического символа u языка структуры $\mathcal{A}$. Пусть теперь I является простой интерпретацией языка структуры $\mathcal{A}$ в языке структуры $\mathcal{C}$, в которой $U_I = p$. Тогда I является интерпретацией языка структуры $\mathcal{A}$ в теории $\text{Th}(\mathcal{C})$ и $\mathcal{C}_I = \mathcal{A}$.

Теорема 3 (Тарский). Если структура $\mathcal{A}$ определима в структуре $\mathcal{B}$ и $\mathcal{A}$ строго неразрешима, то $\mathcal{B}$ строго неразрешима.

Доказательство. Пусть $\mathcal{C}$ и I определены, как ранее. Вследствие леммы достаточно показать, что $\mathcal{C}$ строго неразрешима.

Пусть структура $\mathcal{C}$ является моделью теории T ; нам надо доказать, что T неразрешима. Образует T_1 из T , присоединив к T аксиому $\exists x U_I x$ и для каждого функционального символа f языка L (языка структуры $\mathcal{A}$) аксиому

$$U_I x_1 \rightarrow \dots \rightarrow U_I x_n \rightarrow U_I f x_1 \dots x_n,$$

где $x_1, \dots, x_n$ различны. Тогда теория T_1 является конечным расширением теории T , так что в силу теоремы 1 достаточно доказать, что T_1 неразрешима. Так

как I является интерпретацией в теории $\text{Th}(\mathcal{C})$, то присоединенные аксиомы истинны в $\mathcal{C}$ и потому $\mathcal{C}$ является моделью теории T_1 .

Пусть U — теория языка L , нелогическими аксиомами которой являются такие формулы A , что $\vdash_{T_1} A^{(I)}$. Для каждой такой A формула $A^{(I)}$ истинна в $\mathcal{C}$, поэтому A истинна в $\mathcal{C}_I = \mathcal{A}$. Таким образом, $\mathcal{A}$ является моделью теории U , и потому U неразрешима. Очевидно, I является точной интерпретацией теории U в теории T_1 , так что T_1 неразрешима по теореме 1.

Укажем теперь некоторые применения этих результатов. Пусть $\mathcal{A}$ — кольцо целых чисел, рассматриваемое как структура языка FL. Мы утверждаем, что структура $\mathcal{N}$ определима в структуре $\mathcal{A}$. Труднее всего показать, что множество $|\mathcal{N}|$ определимо в структуре $\mathcal{A}$. Для этого воспользуемся теоремой Лагранжа: каждое натуральное число представимо в виде суммы четырех квадратов натуральных чисел. Таким образом, если A есть

$$\exists y \exists z \exists y' \exists z' (x = y \cdot y + z \cdot z + y' \cdot y' + z' \cdot z')$$

и i — имя индивида a из $\mathcal{A}$, то $\mathcal{A}(A_x[i]) = \mathbf{И}$ тогда и только тогда, когда a является натуральным числом. Замечая, что $S(a) = a + 1$ и что $a < b$ тогда и только тогда, когда $a + c + 1 = b$ для некоторого натурального числа c , мы легко покажем, что $0, S, +, \cdot$ и $<$ являются ограничениями функций и предикатов, определенных в структуре $\mathcal{A}$.

Вследствие теорем 2 и 3 структура $\mathcal{A}$ строго неразрешима, поэтому любая теория языка FL, имеющая моделью $\mathcal{A}$, неразрешима. Среди этих теорий находятся элементарные теории колец, коммутативных колец и областей целостности.

Пусть теперь $\mathcal{A}$ определена, как прежде, а $\mathcal{B}$ — поле рациональных чисел. Тогда структура $\mathcal{A}$ определима в структуре $\mathcal{B}$. Единственной трудностью является следующая: показать, что $|\mathcal{A}|$ определима в $\mathcal{B}$. Это сделала Джулия Робинсон, используя теорию квадратичных форм. (Мы не будем здесь излагать это решение.) Вследствие теоремы 3 структура $\mathcal{B}$ строго неразрешима. Отсюда мы можем вывести неразрешимость FL, FL(0) и других теорий.

Задачи

Предполагается, что все теории имеют лишь конечное число нелогических символов.

1. *Примитивно рекурсивные функции* определяются с помощью следующего обобщенного индуктивного определения.

PR1. Константные функции, функция следования $S(x) = x + 1$ и функции I_i^n примитивно рекурсивны.

PR2. Если $G, H_1, \dots, H_k$ примитивно рекурсивны, а F определена следующим образом:

$$F(a) = G(H_1(a), \dots, H_k(a)),$$

то F примитивно рекурсивна.

PR3. Если G и H примитивно рекурсивны, а F определена следующим образом:

$$\begin{aligned} F(0, a) &= G(a), \\ F(a+1, a) &= H(F(a, a), a, a), \end{aligned}$$

то F примитивно рекурсивна.

Предикат *примитивно рекурсивен*, если его представляющая функция примитивно рекурсивна.

(а) Показать, что R1, R2, R4 и R6 — R13 верны, если *рекурсивный* заменить на *примитивно рекурсивный*. [Последними доказывать R9 и R10.]

(б) Показать, что β примитивно рекурсивна.

(в) Показать, что существует такая примитивно рекурсивная функция F , что если

$$n < a, \quad a_0 < a, \dots, a_{n-1} < a,$$

то существует такое $x < F(a)$, что $\beta(x, i) = a_i$ при $i < n$.

(г) Показать, что $\langle a_1, \dots, a_n \rangle$, $lh(a)_i$, Seq, In и * примитивно рекурсивны. [Воспользоваться (в) и R9.] Показать, что R14 справедливо, если *рекурсивна* заменить на *примитивно рекурсивна*.

(д) Показать, что если множество $NLAx_T$ примитивно рекурсивно, то функции и предикаты, определенные в § 6.6, примитивно рекурсивны.

2. Пусть H и K — рекурсивные функции, и пусть F и G определены индуктивно следующим образом:

$$\begin{aligned} F(a, a) &= H(F(a, a), \bar{G}(a, a), a, a), \\ G(a, a) &= K(F(a+1, a), \bar{G}(a, a), a, a). \end{aligned}$$

Показать, что F и G рекурсивны. [Пусть $L(a, a) = \langle F(a, a), G(a, a) \rangle$; пользуясь R14, показать, что L рекурсивна.]

3. Действительное число a *рекурсивно*, если существуют такие рекурсивные функции F и G , что при $n \neq 0$ мы имеем $G(n) \neq 0$ и $||a| - F(n)/G(n)| < 1/n$.

(а) Показать, что каждое рациональное число рекурсивно.

(б) Показать, что e и π рекурсивны. [Воспользоваться подходящими разложениями в ряд e и π вместе с оценками скорости сходимости этих рядов.]

(в) Показать, что если a и b рекурсивны, то $a+b$, $a-b$ и $a \cdot b$ рекурсивны. Если к тому же $b \neq 0$, то показать, что a/b рекурсивно. [Следовать доказательствам непрерывности этих функций.]

(г) Пусть $P_a(m, n)$ означает, что $n \neq 0$ и $m/n < |a|$. Показать, что a рекурсивно тогда и только тогда, когда P_a рекурсивен. [Предположим, что a рекурсивно и иррационально. Тогда $m/n < |a|$ тогда и только тогда, когда

$$m/n < F(k)/G(k) - 1/k \text{ для некоторого } k,$$

и $m/n > |a|$ тогда и только тогда, когда

$$m/n > F(k)/G(k) + 1/k \text{ для некоторого } k,$$

где F и G определены выше.]

(д) Показать, что действительное число a рекурсивно тогда и только тогда, когда существует такая рекурсивная функция F , что $F(n) \leq 9$ при $n \neq 0$ и $|a| = \sum F(n) \cdot 10^{-n}$. [Если a рекурсивно и иррационально, то F определена неравенствами $|a| - 10^{-k} < \sum_{n=0}^k F(n) \cdot 10^{-n} < |a|$.]

4. Унарная функция F *перечисляет* множество A , если элементами множества A являются в точности элементы последовательности $F(0), F(1), \dots$

(а) Показать, что непустое множество A рекурсивно перечислимо тогда и только тогда, когда оно перечисляется рекурсивной функцией.

(б) Показать, что каждое бесконечное рекурсивно перечислимое множество перечисляется инъективной рекурсивной функцией.

(в) Показать, что бесконечное множество A рекурсивно тогда и только тогда, когда оно перечисляется такой рекурсивной функцией F , что $F(n) < F(n+1)$ для всех n .

(г) Показать, что каждое бесконечное рекурсивно перечислимое множество имеет бесконечное рекурсивное подмножество. [Воспользоваться (б) и (в).]

5. Теория называется *рекурсивно аксиоматизируемой*, если она эквивалентна рекурсивно аксиоматизированной теории.

(а) Показать, что T рекурсивно аксиоматизируема тогда и только тогда, когда Thm_T рекурсивно перечислимо. [Пусть Thm_T рекурсивно перечислимо, выбрать F такую же, как и в 4 (а). Предположить, что нелогическими аксиомами из T' являются A_0 & $A_1 \dots$ & A_n , причем $\ulcorner A_i \urcorner = F(i)$, и применить 4 (в).]

(б) Привести пример рекурсивно аксиоматизируемой теории, не являющейся рекурсивно аксиоматизированной.

6. Пусть символам теории T сопоставлены номера двумя различными способами, и пусть $\ulcorner u \urcorner$ и $\ulcorner u' \urcorner$ являются соответствующими номерами выражений u . Показать, что существует такая рекурсивная функция F , что $F(\ulcorner u \urcorner) = \ulcorner u' \urcorner$ для любого указателя u . Доказать, что теория T является разрешимой (рекурсивно аксиоматизированной) при одном способе сопоставления номеров символам тогда и только тогда, когда она является разрешимой (рекурсивно аксиоматизированной) при другом способе сопоставления.

7. Теория называется *численной*, если она содержит символы 0 и S. Представимость в такой теории мы определяем так же, как и в N.

(а) Показать, что если T — рекурсивно аксиоматизированная численная теория и если $\vdash_T k_m = k_n$ влечет $m = n$ для любых m и n , то каждая представимая в T функция рекурсивна и каждый представимый в T предикат рекурсивен. Доказать, что функция рекурсивна (предикат рекурсивен) тогда и только тогда, когда она (он) представима (представим) в некоторой конечно аксиоматизированной численной теории такой, что $\vdash_T k_m = k_n$ влечет $m = n$ для любых m и n .

(б) Показать, что если теория T является расширением теории N , то функции, представимые в T , удовлетворяют R1—R3. Затем показать, что если T непротиворечива, то $\text{Th}_m T$ не представима в T . [Воспользоваться доказательством теоремы Чёрча.]

(в) Формула A численной теории T называется *определением истинности*, если $\vdash_T B \leftrightarrow A_x[k_{\neg B}]$ для каждой замкнутой формулы B теории T . Показать, что если теория T является непротиворечивым расширением теории N , то не существует определения истинности в T . [Применить (б) и теорему Линденбаума.]

8. Пусть T — численная теория. Формула A от различных переменных $x_1, \dots, x_n$ слабо представляет P , если для любых $a_1, \dots, a_n$

$$\vdash_T A_{x_1, \dots, x_n}[k_{a_1}, \dots, k_{a_n}] \Leftrightarrow P(a_1, \dots, a_n).$$

Предикат P является *слабо представимым* в теории P , если он слабо представим в T некоторой формулой от некоторой последовательности переменных.

(а) Показать, что если теория T непротиворечива, то каждый представимый в теории T предикат является слабо представимым в теории T .

(б) Пусть P и Q — n -арные рекурсивно перечислимые предикаты. Показать, что существуют формула A из N и различные переменные $x_1, \dots, x_n$ такие, что]

$$P(a_1, \dots, a_n) \& \neg Q(a_1, \dots, a_n) \Rightarrow \vdash_N A[k_{a_1}, \dots, k_{a_n}],$$

$$Q(a_1, \dots, a_n) \& \neg P(a_1, \dots, a_n) \Rightarrow \vdash_N \neg A[k_{a_1}, \dots, k_{a_n}].$$

[Взять в качестве A формулу $\exists x (B \& \forall y (y < x \rightarrow \neg C))$, где B представляет такой предикат P_1 , что $P(a) \leftrightarrow \exists x P_1(a, x)$, а C представляет такой предикат Q_1 , что $Q(a) \leftrightarrow \exists x Q_1(a, x)$.]

(в) Показать, что если T — непротиворечивое рекурсивно аксиоматизированное расширение теории N , то каждый рекурсивно перечислимый предикат P слабо представим в теории T . [Выбрать такой рекурсивно перечислимый предикат Q , что для всех A

$$Q(a_1, \dots, a_n, \ulcorner A \urcorner) \Leftrightarrow \vdash_T A_{x_1, \dots, x_n, y}[k_{a_1}, \dots, k_{a_n}, k_{\ulcorner A \urcorner}].$$

Выбрать A такую же, как и в (б), и взять в качестве B формулу $A_y[k_{\ulcorner A \urcorner}]$.

(г) Показать, что если теория T рекурсивно аксиоматизированная, то каждый слабо представимый в теории T предикат рекурсивно перечислим. Затем показать, что предикат рекурсивно перечислим

тогда и только тогда, когда он слабо представим в некоторой конечно аксиоматизированной численной теории. [Использовать (в).]

9. Пусть C_n — формула, утверждающая, что существует ровно n индивидов.

(а) Пусть теория T конечно аксиоматизируема. Показать, что существует разрешающий метод для формул вида $C_n \rightarrow A$. [Использовать 13 (б) из главы 4.]

(б) Показать, что если теория T конечно аксиоматизируемая и m -категоричная для некоторого бесконечного кардинала m , то T разрешима. [Пусть теория T' получена из T присоединением в качестве аксиом всех $\neg C_n$. Используя теорему Лося—Вота и лемму из § 6.8, показать, что T' разрешима. Показать, что по данной замкнутой теореме A из T'_1 мы можем найти такое n , что $\vdash_T \neg C_1 \rightarrow \dots \rightarrow \neg C_n \rightarrow A$. Затем использовать (а).]

(в) Показать, что (б) будет ложно, если конечно аксиоматизируемая заменить на рекурсивно аксиоматизированная. [Пусть A — нерекурсивно рекурсивно перечислимое множество. Выбрать в качестве T теорию, в которых нет нелогических символов и нелогическими аксиомами которой являются $\neg C_n$ для n из A , и воспользоваться 5 (а).]

10. Структура $\mathcal{A}$ называется *неразрешимой*, если теория $\text{Th}(\mathcal{A})$ неразрешима.

(а) Показать, что если $\mathcal{A}$ неразрешима, то любое обогащение структуры $\mathcal{A}$ неразрешимо.

(б) Показать, что если структура $\mathcal{B}$ является обогащением структуры $\mathcal{A}$ с помощью определений и $\mathcal{B}$ неразрешима, то $\mathcal{A}$ неразрешима. [Показать, что расширение с помощью определений полной теории является полным. Пользуясь леммой 1 из § 5.5, показать, что теория $\text{Th}(\mathcal{B})$ эквивалентна расширению теории $\text{Th}(\mathcal{A})$ с помощью определений.]

(в) Показать, что если структура $\mathcal{A}$ определима в структуре $\mathcal{B}$ и $\mathcal{A}$ неразрешима, то $\mathcal{B}$ неразрешима. [Показать, что теория $\text{Th}(\mathcal{A})$ имеет точную интерпретацию в теории $\text{Th}(\mathcal{B})$.]

11. Непротиворечивая теория T называется *существенно неразрешимой* (строго неразрешимой), если каждая модель теории T неразрешима (строго неразрешима).

(а) Показать, что если теория T непротиворечива и разрешима, то T имеет полное разрешимое простое расширение. [Воспользоваться доказательством теоремы Линденбаума, описанным в задаче 1 из главы 4.]

(б) Показать, что непротиворечивая теория T существенно неразрешима тогда и только тогда, когда каждое непротиворечивое простое расширение теории T неразрешимо. [Использовать (а) и лемму 1 из § 5.5.]

(в) Теория T' *совместима* с теорией T , если $L(T') = L(T)$ и теория $T \cup T'$ непротиворечива. Показать, что непротиворечивая теория T строго неразрешима тогда и только тогда, когда каждая совместимая с T теория неразрешима.

(г) Показать, что если теория T конечно аксиоматизируема и существенно неразрешима, то T строго неразрешима. [Воспользоваться доказательством теоремы 2 из § 6.9.] Затем показать, что N строго неразрешима. [Использовать (б).]

(д) Показать, что если теория T существенно неразрешима (строго неразрешима), то каждое непротиворечивое расширение теории T существенно неразрешимо (строго неразрешимо). [Показать, что любое обобщение строго неразрешимой структуры строго неразрешимо, а затем воспользоваться этим и 10 (а).]

(е) Показать, что если теория T' является расширением теории T с помощью определений и T' существенно неразрешима (строго неразрешима), то T существенно неразрешима (строго неразрешима). [Использовать 10 (б) и лемму из § 6.9.]

(ж) Показать, что если теория T интерпретируема в непротиворечивой теории T' и T существенно неразрешима (строго неразрешима), то T' существенно неразрешима (строго неразрешима). [Вследствие (е) мы можем предположить, что существует интерпретация теории T в T' . Показать, что если $\mathcal{B}$ является моделью теории T' , то некоторая модель теории T определима в структуре $\mathcal{B}$. Затем воспользоваться 10 (в) и теоремой 3 из § 6.9.]

12. Непустое множество Γ замкнутых формул теории T называется базой теории T , если для каждой двух моделей $\mathcal{A}$ и $\mathcal{B}$ теории T выполняется условие: если $\mathcal{A}(\Gamma) = \mathcal{B}(\Gamma)$ для всех Γ из Γ , то $\mathcal{A}$ и $\mathcal{B}$ элементарно эквивалентны. Через $\mathcal{D}(\Gamma)$ мы обозначим множество дизъюнкций формул, являющихся либо формулами из Γ , либо отрицаниями формул из Γ , а через $\mathcal{B}(\Gamma)$ — множество конъюнкций формул из $\mathcal{D}(\Gamma)$.

(а) Показать, что если Γ является базой теории T , то каждая замкнутая формула теории T эквивалентна в T формуле из $\mathcal{B}(\Gamma)$. [Воспользоваться доказательством леммы 4 из § 5.5.]

(б) Предположим, что теория T рекурсивно аксиоматизированная, Γ является базой теории T , и мы имеем метод решения вопроса о том, принадлежит ли данная формула множеству Γ . Показать, что для данной замкнутой формулы A теории T мы можем найти формулу из $\mathcal{B}(\Gamma)$, эквивалентную A в T .

(в) Пусть теория T рекурсивно аксиоматизированная и Γ — база теории T . Предположим, что мы имеем метод для решения вопроса о том, принадлежит ли данная формула множеству Γ или нет, и метод для решения вопроса о том, является ли данное предложение из $\mathcal{D}(\Gamma)$ теоремой теории T . Показать, что теория T разрешима. [Использовать (б).]

(г) Показать, что теория EQ разрешима. [Использовать (в) и задачу 21 из главы 5.]

(д) Показать, что если теория T конечно аксиоматизируемая и все нелогические символы теории T являются унарными предикатными символами, то T разрешима. [Показать, что мы можем предполагать, что T не имеет нелогических аксиом, и использовать (в) и задачу 22 из главы 5.]

13. Множество R отделяет множество P от множества Q , если P является подмножеством множества R , и Q и R не пересекаются. Непересекающиеся множества P и Q называются рекурсивно неотделимыми, если не существует рекурсивного множества, отделяющего P от Q . Теория T рекурсивно неотделима, если множество Thm_T является рекурсивно неотделимым от множества номеров отрицаний теорем теории T .

(а) Пусть P и Q — непересекающиеся множества, и пусть T — такая численная теория, что для каждого рекурсивного множества A существует формула A теории T такая, что для любого n справедливо $P(\ulcorner A[k_n] \urcorner)$, если n принадлежит A , и $Q(\ulcorner A[k_n] \urcorner)$, если n не принадлежит A . Показать, что P и Q рекурсивно неотделимы. [Пусть R отделяет P от Q , обозначить через $E'(A)$ множество таких n , что $R(\ulcorner A[k_n] \urcorner)$, и вести доказательство аналогично доказательству теоремы Чёрча.]

(б) Показать, что если каждое рекурсивное множество слабо представимо в теории T , то T неразрешима. [Использовать (а).]

(в) Показать, что если теория T непротиворечива и каждое рекурсивное множество представимо в T , то T рекурсивно неотделима. [Использовать (а).] Затем показать, что существуют рекурсивно неотделимые рекурсивно перечислимые множества.

(г) Показать, что если теория T рекурсивно неотделима, то T существенно неразрешима. [Использовать 11 (б).]

14. Теория T называется наследственно неразрешимой, если каждая теория, для которой T является простым расширением, неразрешима.

(а) Показать, что $\mathcal{A}$ строго неразрешима тогда и только тогда, когда $\text{Th}(\mathcal{A})$ наследственно неразрешима.

(б) Показать, что если теория T имеет строго неразрешимую модель, то T наследственно неразрешима. Затем показать, что строго неразрешимая теория наследственно неразрешима.

(в) Показать, что элементарная теория колец является наследственно неразрешимой, однако не является существенно неразрешимой. [Использовать (б) и 11 (б).]

(г) Пусть A и B — рекурсивно неотделимые рекурсивно перечислимые множества [см. 13 (в)]. Пусть $A_{n,k}$ определена так же, как в задаче 21 (а) из главы 5. Пусть теория T получена из теории EQ присоединением в качестве аксиомы $A_{1,k}$ для каждого k из A и присоединением в качестве аксиомы $\neg A_{1,k}$ для каждого k из B . Показать, что теория T рекурсивно аксиоматизируема и существенно неразрешима. [Использовать 5 (а) и 13 (г).] Показать, что каждая конечная часть теории T разрешима, а затем показать, что T не является наследственно неразрешимой. [Использовать 12 (г) и теорему 1 из § 6.9.]

15. (а) Показать, что если теория T рекурсивно аксиоматизируема и имеет только конечное число неэквивалентных полных простых расширений, то T разрешима. [Показать, что если A — замкнутая формула и если теории $T(A)$ и $T(\neg A)$ разрешимы, то T разрешима. Затем воспользоваться индукцией по числу неэквивалентных полных простых расширений.]

(б) Показать, что существует рекурсивно аксиоматизируемая неразрешимая теория, имеющая только счетное число неэквивалентных полных простых расширений, каждое из которых разрешимо. [Использовать пример из 9 (в).]

16. (а) Показать, что существует строго неразрешимая структура для языка, который имеет единственный нелогический символ — 4-арный предикатный символ R . [Пусть $|\mathcal{A}|$ является множеством натуральных чисел, и пусть $R_{\mathcal{A}}$ — множество всех четверок вида $(1, m, n, m+n)$ и $(0, m, n, m \cdot n)$. Замечая, что $R(m, m, m, m)$ тогда и только

тогда, когда $m=0$, показать, что структура $\mathcal{N}$ определима в структуре $\mathcal{A}$.]

(б) Обогащение $\mathcal{B}$ структуры $\mathcal{A}$ называется *несущественным*, если символами языка структуры $\mathcal{B}$, не являющимися символами языка структуры $\mathcal{A}$, являются лишь константы. Показать, что если структура $\mathcal{B}$ является несущественным обогащением структуры $\mathcal{A}$ и $\mathcal{B}$ строго неразрешима, то $\mathcal{A}$ строго неразрешима. [Пусть $\mathcal{A}$ — модель теории T . Получить T' из T , присоединяя новые константы из $\mathcal{B}$, и применить теорему о константах.]

(в) Показать, что существует строго неразрешимая структура для языка, единственным нелогическим символом которого является бинарный предикатный символ P . [Пусть структура $\mathcal{A}$ такая же, как в (а). Пусть $|\mathcal{B}|$ состоит из элементов $|\mathcal{A}|$, упорядоченных пар элементов $|\mathcal{A}|$ и некоторого нового элемента u . Пусть $P_{\mathcal{B}}$ состоит из следующих упорядоченных пар элементов $|\mathcal{B}|$ (где a, b, c и d означают элементы из $|\mathcal{A}|$): все $((a, b), (c, d))$ такие, что $R_{\mathcal{A}}(a, b, c, d)$; все $(a, (a, b))$; все $((a, b), b)$; все (u, a) и все $((a, b), u)$. Показать, что структура $\mathcal{A}$ определима в несущественном обогащении структуры $\mathcal{B}$, и воспользоваться (б).]

17. (а) Пусть T — теория, единственным нелогическим символом которой является бинарный предикатный символ P , а нелогическими аксиомами — $\neg P(x, x)$ и $P(x, y) \rightarrow P(y, x)$. Показать, что T имеет строго неразрешимую модель. [Пусть структура $\mathcal{A}$ удовлетворяет условиям задачи 16 (в). Пусть для каждого элемента a из $|\mathcal{A}|$ множество $|\mathcal{B}|$ содержит три элемента a_1, a_2, a_3 , и пусть $|\mathcal{B}|$ содержит еще два элемента u и v . Пусть $P_{\mathcal{B}}$ состоит из всех пар $(a_1, a_2), (a_2, a_3), (u, a_1), (v, a_2)$; всех пар (a_1, b_3) таких, что (a, b) принадлежит $P_{\mathcal{A}}$, и пар, им обратных. Показать, что структура $\mathcal{A}$ определима в несущественном обогащении структуры $\mathcal{B}$.]

(б) Пусть РО — теория, единственным нелогическим символом которой является $<$ и аксиомами которой является $\neg(x < x)$ и $x < y \rightarrow y < z \rightarrow x < z$. Тогда моделями для РО являются частично упорядоченные множества. Пусть теория ЛТ — расширение теории РО, полученное присоединением аксиом, утверждающих, что каждые два элемента имеют наименьшую верхнюю грань и наибольшую нижнюю грань. Показать, что ЛТ имеет строго неразрешимую модель. [Пусть $\mathcal{A}$ удовлетворяет условиям задачи (а). Пусть E состоит из элементов из $|\mathcal{A}|$ и упорядоченных пар из $P_{\mathcal{A}}$. Пусть $|\mathcal{B}|$ является классом всех таких подмножеств F множества E , что если (a, b) принадлежит F , то a и b принадлежат F . Показать, что объединение и пересечение любых двух членов из $|\mathcal{B}|$ принадлежит $|\mathcal{B}|$. Далее, пусть $F <_{\mathcal{B}} F'$, если F — собственное подмножество множества F' . Показать, что некоторая структура, изоморфная структуре $\mathcal{A}$, определима в структуре $\mathcal{B}$.]

(в) Показать, что существует строго неразрешимая структура для языка, нелогическими символами которого являются лишь два унарных функциональных символа. [Пусть $\mathcal{A}$ удовлетворяет условиям задачи (а). Пусть $|\mathcal{B}|$ состоит из индивидов из $\mathcal{A}$ и пар из $P_{\mathcal{A}}$. Пусть

$$f_{\mathcal{B}}((a, b)) = a, g_{\mathcal{B}}((a, b)) = b, f_{\mathcal{B}}(a) = g_{\mathcal{B}}(a) = a$$

для a, b из $|\mathcal{A}|$. Показать, что структура $\mathcal{A}$ определима в структуре $\mathcal{B}$.]

18. Пусть $\mathcal{A}$ — множество биективных отображений множества целых чисел в себя. Мы рассматриваем $\mathcal{A}$ как группу и, следовательно, как модель теории G с композицией функций в качестве групповой операции. Пусть S — элемент из $\mathcal{A}$, определенный следующим образом: $S(i) = i + 1$.

(а) Показать, что отображение, сопоставляющее числу i отображение S^i , является биективным отображением множества целых чисел в множество индивидов структуры $\mathcal{A}$, перестановочных с S . [Если отображение F перестановочно с S , то $F(S^i(0)) = S^i(F(0))$.]

(б) Показать, что для любых чисел i и j число j делится на i тогда и только тогда, когда S^j перестановочно с каждым индивидом структуры $\mathcal{A}$, с которым перестановочно S^i . [Пусть $i \neq 0$ и условие выполняется; применить его к F , определенному следующим образом: $F(k) = k + i$, если k делится на i , $F(k) = k$ в противном случае.]

(в) Пусть структура $\mathcal{B}$ определена следующим образом: $|\mathcal{B}|$ — множество целых чисел, $1_{\mathcal{B}}$ — целое число 1, $+$ — функция сложения, а $D_{\mathcal{B}}$ — предикат делимости (это означает, что $D_{\mathcal{B}}(i, j)$ тогда и только тогда, когда i делится на j). Показать, что структура $\mathcal{B}$ строго неразрешима. [Показать, что кольцо целых чисел определимо в структуре $\mathcal{B}$. Для этого заметить, что i^2 является единственным целым числом j таким, что $j + i$ является наименьшим общим кратным чисел i и $i + 1$, а $j - i$ является наименьшим общим кратным чисел i и $i - 1$; затем определить $i \cdot j$ с помощью равенства $(i + j)^2 = i^2 + i \cdot j + i \cdot j + j^2$.]

(г) Показать, что структура $\mathcal{A}$ строго неразрешима. [Пользуясь (а) и (б), определить в несущественном обогащении структуры $\mathcal{A}$ модель, изоморфную структуре $\mathcal{B}$.]

19. Пусть J_0 — теория, полученная из теории N заменой аксиом $N2$ и $N8$ следующими тремя аксиомами: $S0 \neq 0$,

$$Sx \neq x \rightarrow Sy \neq y \rightarrow Sx = Sy \rightarrow x = y,$$

$$Sx \neq x \rightarrow (y < Sx \leftrightarrow y < x \vee y = x).$$

Пусть теория J получена из теории J_0 присоединением в качестве новых аксиом всех предложений $k_{n+1} \neq k_n$.

(а) Показать, что если $m \neq n$, то

$$\vdash_{J_0} k_{m+1} \neq k_m \rightarrow k_{n+1} \neq k_n \rightarrow k_m \neq k_n.$$

(б) Показать, что если функция F рекурсивна, то существуют формула A и различные переменные $x_1, \dots, x_n, y$ такие, что если $F(a_1, \dots, a_n) = b$, то

$$\vdash_{J_0} A[k_{a_1}, \dots, k_{a_n}, k_b],$$

$$\vdash_J A[k_{a_1}, \dots, k_{a_n}] \leftrightarrow y = k_b.$$

[Следовать доказательству теоремы о представимости. Если F есть $K_{<}$, то взять в качестве A

$$Sx_1 \neq x_1 \rightarrow Sx_2 \neq x_2 \rightarrow (x_1 < x_2 \& y = k_0) \vee (\neg(x_1 < x_2) \& y = k_1).$$

При рассмотрении R3 учесть, что G можно выбрать так, что $G(a, b) \leq 1$, так как мы можем заменить $G(a, b)$ на $K_{<}(G(a, b), 1)$.]

(в) Показать, что если предикат P рекурсивный, то существуют формула A и различные переменные $x_1, \dots, x_n$ такие, что

$$P(a_1, \dots, a_n) \rightarrow \vdash_{J_0} A[k_{a_1}, \dots, k_{a_n}],$$

$$\neg P(a_1, \dots, a_n) \rightarrow \vdash_J \neg A[k_{a_1}, \dots, k_{a_n}].$$

[Использовать (б).]

(г) Показать, что теория J строго неразрешима. [Пусть теория T совместима с теорией J . Пусть P и A те же, что и в (в), и пусть B является конъюнкцией замыканий нелогических аксиом теории J_0 . Показать, что $B \rightarrow A$ слабо представляет P в теории T и воспользоваться 13 (б) и 11 (в).]

(д) Показать, что каждая конечно аксиоматизируемая часть теории J имеет конечную модель. [Для каждого натурального числа n рассмотреть структуру $\mathcal{A}$ с индивидами $0, 1, \dots, n$, в которой

$$S_{\mathcal{A}}(a) = \min(a+1, n), \quad a +_{\mathcal{A}} b = \min(a+b, n),$$

$$a \cdot_{\mathcal{A}} b = \min(a \cdot b, n), \quad a <_{\mathcal{A}} b \leftrightarrow a < b.]$$

(е) Пусть T — теория языка $L(N)$, нелогическими аксиомами которой являются все предложения, истинные в каждой конечной структуре для этого языка. Показать, что теория T неразрешима. [Использовать (г), (д), 11 (в) и теорему компактности.]

ТЕОРИЯ РЕКУРСИИ

7.1. Частичные функции

Образование F множества A в множество B полностью определяются любым разрешающим методом для F : значением $F(a)$ должен быть элемент из B , полученный при применении метода к a . Однако произвольный метод получения элементов множества B из элементов множества A может не быть разрешающим методом для отображения из A в B , так как этот метод может не давать ответа для некоторых a из A . Например, метод может требовать решения некоторого множества уравнений, а уравнения могут не иметь решения для некоторого a . К тому же может существовать такое a , для которого вычисление прямым способом никогда не окончится. Это произойдет, например, если мы попытаемся найти $\mu x R(a, x)$ обычным методом, а a таково, что $\forall x \neg R(a, x)$.

Все это приводит к новому определению. *Частичным отображением* F из A в B называется отображение некоторого подмножества множества A , называемого *областью определения* отображения F , в B . Таким образом, отображение A в B — это частичное отображение A в B , областью определения которого является A . Если мы хотим противопоставить отображения частичным отображениям, то мы говорим *всюду определенное отображение* вместо *отображение*.

Разрешающим методом для частичного отображения F из A в B называется метод, который, будучи применен к произвольному элементу a из A , даст значение $F(a)$, если a принадлежит области определения отображения F , и не даст результата, если a не принадлежит области определения отображения F . Мы говорим, что F *вычислимо*, если оно имеет разрешающий метод. Эти определения согласуются с данными ранее, если отображение F всюду определенное.

Может показаться неестественным требование, чтобы метод, будучи применен к элементу из A , не принадлежащему области определения отображения F , не давал результата. Однако это гарантирует, что разрешающий метод для частичного отображения F полностью определяет F . Действительно, область определения отображения F — это множество таких a , что метод, будучи применен к a , дает результат, и $F(a)$ для такого a является значением, полученным при применении метода к a . Отсюда видно, что каждый метод получения элемента из множества B по заданному элементу из множества A является разрешающим методом для некоторого однозначно определенного частичного отображения из A в B . Если какой-то метод дает результат $F(a)$ для каждого a из области определения отображения F , то соответствующее этому методу частичное отображение является продолжением F , так что на самом деле мы при нашем ограничении ничего не теряем.

Частичное подмножество A множества E состоит из некоторого подмножества множества E , называемого *областью определения* множества A , и указания для каждого элемента из области определения, находится ли этот элемент *в* A или *вне* A . Таким образом, частичное подмножество множества E может быть задано указанием области определения и подмножества области определения, состоящего из тех элементов, которые принадлежат частичному подмножеству. Любое подмножество множества E — это просто частичное подмножество множества E , областью определения которого является E . Мы говорим *всюду определенное подмножество* вместо *подмножество*, если мы хотим подчеркнуть различие с частичными подмножествами.

Разрешающим методом для частичного подмножества A множества E называется метод, который, будучи применен к любому элементу области определения множества A , покажет нам, лежит ли этот элемент в A или вне A , и который, будучи применен к любому элементу из E , не принадлежащему области определения множества A , не дает результата. Частичное подмножество *вычислимо*, если оно имеет разрешающий метод.

Эти понятия обобщаются на функции и предикаты. Так, *n -арной частичной функцией* из A в B называется

частичное отображение множества n -ок элементов, принадлежащих A , в B , а *n -арным частичным предикатом* на A называется частичное подмножество множества n -ок элементов из A . И снова мы говорим *всюду определенная функция* и *всюду определенный предикат* вместо *функция* и *предикат*.

В этой главе мы будем придерживаться соглашений, сформулированных в начале § 6.2 и дополненных следующими: *частичная функция* означает *частичная функция из множества натуральных чисел в множество натуральных чисел*, а *частичный предикат* означает *частичный предикат на множестве натуральных чисел*.

Буквы, использовавшиеся ранее для обозначения функций и предикатов, будут теперь использоваться для обозначения частичных функций и частичных предикатов. Вследствие этого некоторые выражения теперь не имеют значения или, как мы будем говорить, *не определены* при некоторых значениях переменных. Так, $F(a)$ не определено, если a не принадлежит области определения функции F . Также и $P(a)$ не определен, если a не принадлежит области определения предиката P . (Если a принадлежит области определения предиката P , то $P(a)$ истинен, если a принадлежит P , и ложен, если a не принадлежит P .)

Мы условимся, что сложное выражение определено только тогда, когда определены все его части. Так, $F(G(a))$ определено тогда и только тогда, когда a принадлежит области определения функции G и $G(a)$ принадлежит области определения функции F . Аналогично, $P(a) \vee \vee Q(a)$ определен тогда и только тогда, когда a принадлежит как области определения предиката P , так и области определения предиката Q .

Если мы попытаемся явно задать частичную функцию F равенством $F(a) = G(H(a))$, где функции G и H частичные, то мы столкнемся с трудностями. Если $G(H(a))$ не определено, то $F(a) = G(H(a))$ не определено и потому не может ничего сообщить нам об $F(a)$. Мы обойдем это затруднение, введя новый символ. Если $_$ и $\dots$ — выражения (обозначающие числа), которые могут быть не определены, то $_ \simeq \dots$ означает, что или как $_$, так и $\dots$ определены и имеют одинаковые значения, или $_$ и $\dots$ оба не определены. (Это является исключением из уста-

новленного ранее правила; $— \simeq \dots$ всегда определено, даже если одно из $—$ или $\dots$ не определено.) Теперь мы можем явно определить частичную функцию F следующим образом: $F(a) \simeq G(H(a))$. Это означает, что область определения функции F состоит из таких a , что $G(H(a))$ определено, и что для этих a справедливо $F(a) = G(H(a))$.

Мы введем еще один символ, употребляемый в явных определениях частичных предикатов. Если $—$ и $\dots$ — предложения, которые могут быть не определены, то $— \Leftrightarrow \dots$ означает, что или как $—$, так и $\dots$ определены и истинны, или оба определены и ложны, или оба не определены. Таким образом, мы можем явно определить частичный предикат P следующим образом:

$$P(a) \Leftrightarrow Q(F(a))$$

(где Q и F частичные).

Обычно мы будем избегать пользоваться связанными переменными в выражениях, которые могут быть не определены. Тем не менее мы хотим придать смысл выражению $\mu x(\dots x \dots)$, где $\dots x \dots$ — предложение, не определенное при некоторых значениях x . Мы хотим сделать это таким способом, чтобы если R вычислим и F определена следующим образом:

$$F(a) \simeq \mu x R(a, x),$$

то F была вычислима. Предположим, что мы вычисляем $F(a)$ таким же способом, как если бы R был всюду определен, т. е. мы вычисляем $R(a, 0)$, $R(a, 1)$, $\dots$, пока мы не найдем такое a , что $R(a, a)$ истинно, а затем делаем вывод, что $F(a) = a$. Тогда мы получим a как значение для $F(a)$ в том и только в том случае, если a есть такое наименьшее x , что $R(a, x)$, и $R(a, x)$ определен для всех x , меньших этого a . Поэтому мы определяем $\mu x(\dots x \dots)$ как наименьшее число a такое, что $\dots a \dots$ определено и истинно, при условии, что $\dots x \dots$ определено для всех x , меньших этого a . Если это последнее условие не выполнено или если не существует такого a , что $\dots a \dots$ определено и истинно, то $\mu x(\dots x \dots)$ не определено. Заметим, что это согласовывается с нашим прежним определением, когда $\dots x \dots$ определено для всех x .

Представляющей частичной функцией K_P частичного предиката P называется частичная функция, область

определения которой совпадает с областью определения предиката P и которая следующим образом определена для аргумента a в этой области определения: $K_P(a) = 0$, если $P(a)$, и $K_P(a) = 1$, если $\neg P(a)$. Очевидно, P вычислим тогда и только тогда, когда K_P вычислима.

Если F — n -арная частичная функция, то графиком F , обозначаемым через $\mathcal{G}_F$, называется $(n+1)$ -арный всюду определенный предикат, определенный следующим образом:

$$\mathcal{G}_F(a, a) \leftrightarrow F(a) \simeq a.$$

Вследствие этого мы имеем

$$F(a) \simeq \mu x \mathcal{G}_F(a, x),$$

так что F может быть восстановлена по $\mathcal{G}_F$.

Покажем, что F вычислима тогда и только тогда, когда $\mathcal{G}_F$ позитивно вычислим. Предположим, что F вычислима. Мы вычисляем $\mathcal{G}_F(a, a)$ следующим образом: по данным a и a вычисляем $F(a)$; если мы получаем некоторое значение и это значение есть a , то мы делаем заключение, что $\mathcal{G}_F(a, a)$ истинно. Ясно, что это дает правильный ответ, если $\mathcal{G}_F(a, a)$, и не дает ответа, если $\neg \mathcal{G}_F(a, a)$, поэтому $\mathcal{G}_F$ позитивно вычислим.

Чтобы доказать обратное утверждение, заметим вначале, что

$$\forall y (\mathcal{G}_F(a, y) \leftrightarrow \exists x R(a, y, x)) \rightarrow F(a) \simeq (\mu z R(a, (z)_0, (z)_1))_0. \quad (1)$$

Действительно, если $F(a)$ определена, то пусть $y = F(a)$, и выберем такое x , что $R(a, y, x)$. Полагая $z = \langle y, x \rangle$, получаем $R(a, (z)_0, (z)_1)$, поэтому

$$(\mu z R(a, (z)_0, (z)_1))_0$$

определено. Предположим теперь, что

$$(\mu z R(a, (z)_0, (z)_1))_0$$

определено, и пусть

$$u = \mu z R(a, (z)_0, (z)_1).$$

Тогда $R(a, (u)_0, (u)_1)$, отсюда $\exists x R(a, (u)_0, x)$, так что $\mathcal{G}_F(a, (u)_0)$, и потому $F(a) = (u)_0$. Это доказывает (1).

Теперь предположим, что $\mathcal{G}_F$ позитивно вычислим. Тогда существует такой вычислимый предикат R , что

$$\mathcal{G}_F(a, y) \leftrightarrow \exists x R(a, y, x)$$

для любых a и y . Поэтому вследствие (1)

$$F(a) \simeq (\mu z R(a, (z)_0, (z)_1))_0.$$

Ввиду вычислимости $(a)_i$ отсюда следует, что F также вычислима.

Частичная функция F рекурсивна, если ее график рекурсивно перечислим. Частичный предикат P рекурсивен, если рекурсивна его представляющая частичная функция. Ввиду сказанного выше, а также вследствие тезиса Чёрча частичная функция рекурсивна тогда и только тогда, когда она вычислима, частичный предикат рекурсивен тогда и только тогда, когда он вычислим.

Так как каждая всюду определенная функция является частичной функцией, то мы теперь имеем два определения *рекурсивности* для всюду определенных функций. Чтобы установить, что они совпадают, мы должны доказать следующее: всюду определенная функция рекурсивна (в старом смысле) тогда и только тогда, когда ее график рекурсивно перечислим. Действительно, если F всюду определена, то $\mathcal{G}_F$ имеет явное определение

$$\mathcal{G}_F(a, a) \leftrightarrow F(a) = a.$$

Поэтому если F рекурсивна, то $\mathcal{G}_F$ рекурсивен и, следовательно, рекурсивно перечислим. Предположим теперь, что $\mathcal{G}_F$ рекурсивно перечислим, например,

$$\mathcal{G}_F(a, y) \leftrightarrow \exists x R(a, y, x)$$

для всех a и y . Тогда по (1)

$$F(a) = (\mu z R(a, (z)_0, (z)_1))_0,$$

и поэтому F рекурсивна. Отсюда сразу же следует, что два определения понятия *рекурсивный* для всюду определенного предиката совпадают.

Прежде чем рассматривать свойства рекурсивных частичных функций и предикатов, мы введем еще одно обобщение понятия рекурсивности.

7.2. Функционалы и отношения

Мы рассматривали проблему разрешимости для отображения A в B только в случае, когда элементами множеств A и B были конкретные объекты. Теперь мы обсудим случай, когда элементы множеств A и B являются

простейшим типом абстрактных объектов, а именно, функциями.

Можно считать, что каждая n -арная функция F состоит из бесконечного числа частей, каждая из которых есть значение функции F для одной n -ки чисел. Каждую часть можно заменить конкретным объектом, например равенством, дающим значение функции F для этой n -ки. Однако мы не можем заменить F единственным конкретным объектом.

Предположим, что Φ — отображение множества A конкретных объектов в множество B n -арных функций. Ясно, что мы не можем найти по данному элементу a из A бесконечно много частей $\Phi(a)$ при финитном вычислении. Самое большее, чего мы можем достигнуть, — это получить в качестве результата вычисления разрешающий метод для $\Phi(a)$. Поэтому мы определим разрешающий метод для Φ как метод, с помощью которого по данному элементу a из A мы за конечное число шагов можем найти разрешающий метод для $\Phi(a)$. (Разумеется, такой метод может существовать только тогда, когда все значения Φ — вычисляемые функции.)

Предположим, что у нас есть разрешающий метод для Φ . Для данного элемента a из A и данной n -ки чисел $x_1, \dots, x_n$ мы можем вычислить значение $\Phi(a)$ от $x_1, \dots, x_n$. Если мы обозначим это значение через $\Phi'(a, x_1, \dots, x_n)$, то это значит, что мы имеем разрешающий метод для Φ' . Итак, ясно, что вместе с разрешающим методом для Φ нам дается разрешающий метод для Φ' .

Мы можем воспользоваться этим, чтобы определить *разрешающий метод* для отображения Φ произвольного множества A в некоторое множество B n -арных функций. Определим Φ' , как ранее, и определим разрешающий метод для Φ как разрешающий метод для Φ' . Таким образом, мы всегда можем переходить к случаю отображений в множество натуральных чисел.

Рассмотрим теперь отображение Φ множества A n -арных функций в множество натуральных чисел. Чтобы представить себе, как информация об F используется в вычислении $\Phi(F)$, мы рассмотрим характерный пример. Пусть $n = 1$, и пусть

$$\Phi(F) = 2F(F(0) + 2).$$

Чтобы найти $\Phi(F)$, мы сначала должны узнать значение $F(0)$. Предположим, что оно равно 3. Прибавим к нему 2, получим 5. Чтобы продолжить вычисления, мы должны знать значение $F(5)$. Предположим, что оно равно 4. Тогда, умножив его на 2, получим 8. Делаем вывод, что $\Phi(F) = 8$. Заметим, что для вычисления безразлично, как мы получили $F(0)$ и $F(5)$; если только $F(0) = 3$ и $F(5) = 4$, то мы получаем $\Phi(F) = 8$.

Таким образом, мы видим, что функция F используется в вычислении $\Phi(F)$ путем использования значений функции F для некоторых n -ок $(a_1, \dots, a_n)$. В некоторых случаях $a_1, \dots, a_n$ даются в указаниях к вычислению $\Phi(F)$, в других случаях $a_1, \dots, a_n$ вычисляются в процессе вычисления, возможно, используя другие значения функции F . В нашем примере значение аргумента 0 было дано как указание к вычислению, тогда как значение аргумента 5 было вычислено с использованием значения $F(0) = 3$.

Как мы упоминали, для описания разрешающего метода несущественно, как получены значения F . Чтобы как-то пояснить это, предположим, что с начала вычисления $\Phi(F)$ у нас имеется некий объект, который, если его снабдить какой-то n -кой чисел, выдаст значение функции F на этой n -ке. Этот объект не может быть машиной, так как F может быть невычислимой. Следуя Тьюрингу, мы называем такой объект *оракулом* для F (потому что он дает правильный ответ, обходясь без какого-либо явного способа сделать это). Таким образом, мы можем сказать, что разрешающий метод для Φ — это такой метод, с помощью которого, имея оракул для F , мы можем за конечное число шагов вычислять $\Phi(F)$.

Оракул для F может быть заменен оракулом для $\langle F \rangle$ и наоборот, так как мы можем найти $F(a)$, вычисляя $\langle a \rangle$ и спрашивая оракул для $\langle F \rangle$ об $\langle F \rangle(\langle a \rangle)$, и мы можем найти $\langle F \rangle(a)$, вычисляя $(a)_0, \dots, (a)_{n-1}$ и спрашивая оракул для F об $F((a)_0, \dots, (a)_{n-1})$. Вследствие этого без потери общности мы можем ограничиться рассмотрением только множеств A унарных функций.

Таким образом, мы приходим к следующим определениям. Пусть $N_{m,n}$ — множество $(m+n)$ -ок $(\alpha_1, \dots, \alpha_m, a_1, \dots, a_n)$, где $\alpha_1, \dots, \alpha_m$ — унарные всюду определенные функции, а $a_1, \dots, a_n$ — числа. (m, n) -арным *частичным*

(всюду определенным) функционалом является частичное (всюду определенное) отображение $N_{m,n}$ в множество чисел. Всяду определенный функционал называется просто *функционалом*. Очевидно, $(0, n)$ -арные частичные (всюду определенные) функционалы — это просто n -арные частичные (всюду определенные) функции.

(m, n) -арным *частичным* (всюду определенным) *отношением* называется частичное (всюду определенное) подмножество множества $N_{m,n}$. Всяду определенное отношение называется просто *отношением*. $(0, n)$ -арные частичные (всюду определенные) отношения — это просто n -арные частичные (всюду определенные) предикаты.

Буквы, употреблявшиеся ранее для обозначения частичных функций и частичных предикатов, будут теперь употребляться для обозначения соответственно частичных функционалов и частичных отношений. Строчные греческие буквы мы применяем для обозначения всюду определенных унарных функций. Эти буквы будут называться *функциональными переменными*, если они употребляются в качестве переменных; употребляемые в качестве переменных строчные латинские буквы будут называться *числовыми переменными*. Мы будем пользоваться прописными готическими буквами для обозначения таких конечных последовательностей различных греческих и латинских букв, в которых греческие буквы (если они есть) предшествуют всем латинским буквам (если они есть). Если две различные готические буквы встречаются в одном контексте, то предполагается, что обозначенные ими последовательности не имеют общих букв. Как и при употреблении строчных готических букв, мы предполагаем, что число букв в последовательности выбрано в соответствии с контекстом. Так, если функционал F является (m, n) -арным и мы пишем $F(\mathfrak{A})$, то мы предполагаем, что $\mathfrak{A}$ состоит из m греческих букв и n латинских букв.

Мы ограничили аргументы (m, n) -ками, в которых m функций предшествуют n числам. Очевидно, что на самом деле при таком ограничении общность не теряется. Для удобства обозначений мы можем иногда писать некоторые из функциональных символов после некоторых числовых символов. Если это имеет место, то подразумевается, что символы функций должны быть поставлены перед символами чисел без какого-либо другого изменения порядка

символов. Например, если мы пишем $F(\mathbb{N}, \mathbb{N})$, то подразумевается, что функциональные переменные из $\mathbb{N}$ должны быть передвинуты вперед числовых переменных из $\mathbb{N}$.

Представляющим частичным функционалом K_P частичного отношения P называется частичный функционал, область определения которого та же, что и у P , и который следующим образом определен для аргументов $\mathbb{N}$ в этой области определения: $K_P(\mathbb{N}) = 0$, если $P(\mathbb{N})$, и $K_P(\mathbb{N}) = 1$, если $\neg P(\mathbb{N})$.

Мы говорим, что нам дана (m, n) -ка $\mathbb{N}$, если нам даны n чисел из $\mathbb{N}$ и оракулы для m функций из $\mathbb{N}$. Это дает нам право использовать определения из предыдущего параграфа для определения разрешающего метода и вычислимости для частичных функционалов и частичных отношений. Ясно, что частичное отношение вычислимо тогда и только тогда, когда его представляющий частичный функционал вычислим.

Всюду определенное отношение P позитивно вычислимо, если существует такой метод, который при применении к $\mathbb{N}$ установит, что $P(\mathbb{N})$ истинно, если это действительно так, и не даст никакого результата, если $P(\mathbb{N})$ ложно. Мы покажем, что это понятие можно свести к понятию вычислимого всюду определенного предиката. Сначала введем следующее обозначение: если $\mathbb{N}$ есть $\alpha_1, \dots, \alpha_m, a_1, \dots, a_n$, то $\bar{\mathbb{N}}(x)$ есть $\bar{\alpha}_1(x), \dots, \bar{\alpha}_m(x), a_1, \dots, a_n$. Тогда мы утверждаем, что (m, n) -арное всюду определенное отношение P позитивно вычислимо тогда и только тогда, когда существует такой вычислимый $(m+n+1)$ -арный всюду определенный предикат Q , что

$$P(\mathbb{N}) \leftrightarrow \exists x Q(\bar{\mathbb{N}}(x), x)$$

для всех $\mathbb{N}$.

Для простоты предположим, что $\mathbb{N}$ есть α, a . Пусть отношение P позитивно вычислимо. Определим разрешающий метод для 3-арного всюду определенного предиката Q . Чтобы вычислить $Q(b, a, x)$, сделаем x шагов в вычислении $P(\alpha, a)$. Однако мы не будем пользоваться оракулом для α . Вместо этого, когда нам нужно значение $\alpha(i)$, мы пользуемся значением $(b)_i$, если $i < x$, и прекращаем вычисление, если $i \geq x$. Если это вычисление дает ответ,

*) Определение $\bar{\alpha}(x)$ см. в (13) из § 6.4. — Прим. ред.

что $P(\alpha, a)$ истинно, то $Q(b, a, x)$ истинно; в противном случае $Q(b, a, x)$ ложно. Теперь вычисление $Q(\bar{\alpha}(x), a, x)$ есть просто часть правильного вычисления $P(\alpha, a)$, так что если $\exists x Q(\bar{\alpha}(x), a, x)$, то $P(\alpha, a)$. Наоборот, предположим, что $P(\alpha, a)$. Выберем x настолько большим, чтобы для вычисления $P(\alpha, a)$ требовалось менее x шагов и чтобы все аргументы, для которых в вычислении требуются значения α , были меньше x . Тогда $Q(\bar{\alpha}(x), a, x)$.

Теперь предположим, что существует такой вычислимый предикат Q , что $P(\alpha, a) \leftrightarrow \exists x Q(\bar{\alpha}(x), a, x)$ для всех α и a . На x -м шаге в вычислении $P(\alpha, a)$ мы пользуемся оракулом для α , чтобы вычислить $\bar{\alpha}(x)$, а затем вычисляем $Q(\bar{\alpha}(x), a, x)$. Если $Q(\bar{\alpha}(x), a, x)$ истинно, то мы решаем, что $P(\alpha, a)$ истинно; в противном случае мы переходим к следующему шагу. Ясно, что это дает правильный ответ, если $P(\alpha, a)$, и не дает ответа, если $\neg P(\alpha, a)$.

(m, n) -арное всюду определенное отношение P рекурсивно перечислимо, если существует такой рекурсивный $(m+n+1)$ -арный всюду определенный предикат Q , что

$$P(\mathbb{N}) \leftrightarrow \exists x Q(\bar{\mathbb{N}}(x), x)$$

для всех $\mathbb{N}$. Вследствие сказанного выше, а также вследствие тезиса Чёрча отношение рекурсивно перечислимо тогда и только тогда, когда оно позитивно вычислимо. Заметим, что наше определение согласуется с данным ранее определением рекурсивной перечислимости для предикатов.

Пусть F — (m, n) -арная частичная функция; определим $(m, n+1)$ -арное всюду определенное отношение $\mathcal{G}_F$, называемое графиком F , следующим образом:

$$\mathcal{G}_F(\mathbb{N}, a) \leftrightarrow F(\mathbb{N}) \simeq a.$$

Мы можем распространить (1) из § 7.1 на этот случай:

$$\forall y (\mathcal{G}_F(\mathbb{N}, y) \leftrightarrow \exists x R(\mathbb{N}, y, x)) \rightarrow F(\mathbb{N}) \simeq (\mu z R(\mathbb{N}, (z)_0, (z)_1))_0. \quad (1)$$

Как в случае частичных функций, мы можем доказать, что частичный функционал вычислим тогда и только тогда, когда его график позитивно вычислим.

Частичный функционал рекурсивен, если его график рекурсивно перечислим. Частичное отношение рекурсивно,

если его представляющий частичный функционал рекурсивен. Вследствие сказанного выше, а также вследствие тезиса Чёрча частичный функционал рекурсивен тогда и только тогда, когда он вычислим, частичное отношение рекурсивно тогда и только тогда, когда оно вычислимо.

7.3. Свойства рекурсивных функционалов

Мы начинаем с рассмотрения некоторых правил образования рекурсивно перечислимых отношений.

RE1. Если Q рекурсивно перечислимо, а P определено следующим образом:

$$P(\alpha_1, \dots, \alpha_m, a) \leftrightarrow Q(\alpha_{i_1}, \dots, \alpha_{i_r}, F_1(a), \dots, F_k(a)),$$

где числа $i_1, \dots, i_r$ находятся среди $1, \dots, m$, а $F_1, \dots, F_k$ — всюду определенные рекурсивные функции, то P рекурсивно перечислимо.

Доказательство. Для некоторого рекурсивного предиката R

$$Q(\mathfrak{A}) \leftrightarrow \exists x R(\bar{\mathfrak{A}}(x), x).$$

Отсюда

$$\begin{aligned} P(\alpha_1, \dots, \alpha_m, a) &\leftrightarrow \exists x R(\bar{\alpha}_{i_1}(x), \dots, \bar{\alpha}_{i_r}(x), F_1(a), \dots, F_k(a), x) \\ &\leftrightarrow \exists x R'(\bar{\alpha}_1(x), \dots, \bar{\alpha}_m(x), a, x), \end{aligned}$$

где R' — рекурсивный предикат, определенный следующим образом:

$$R'(b_1, \dots, b_m, a, x) \leftrightarrow R(b_{i_1}, \dots, b_{i_r}, F_1(a), \dots, F_k(a), x).$$

Таким образом, P рекурсивно перечислимо.

Предположим, что отношение P имеет явное определение, использующее только переменные и символы рекурсивно перечислимых отношений и рекурсивных функций. Предположим также, что функциональные переменные встречаются только как аргументы рекурсивно перечислимых отношений, а символы рекурсивных функций не встречаются в качестве аргументов этих отношений. Тогда P рекурсивно перечислимо. Действительно, определение должно иметь вид

$$P(\alpha_1, \dots, \alpha_m, a) \leftrightarrow Q(\alpha_{i_1}, \dots, \alpha_{i_r}, A_1, \dots, A_k),$$

где A_i состоит из числовых переменных и символов рекурсивных функций. Тогда мы определяем $F_i(a) = A_i$ и применяем RE1.

В частности, каждое рекурсивное отношение P рекурсивно перечислимо, так как $P(\mathfrak{A}) \leftrightarrow \mathfrak{G}_{K_P}(\mathfrak{A}, 0)$, а $\mathfrak{G}_{K_P}$ рекурсивно перечислимо.

Если $\mathfrak{A}$ есть $\alpha_1, \dots, \alpha_m, a_1, \dots, a_n$, то мы пишем $\text{In}(\bar{\mathfrak{A}}(x), y)$ вместо *)

$$\text{In}(\bar{\alpha}_1(x), y), \dots, \text{In}(\bar{\alpha}_m(x), y), a_1, \dots, a_n.$$

Тогда, если $y \leq x$, то $\text{In}(\bar{\mathfrak{A}}(x), y)$ есть в точности $\bar{\mathfrak{A}}(y)$.

RE2. Если Q рекурсивно перечислимо и P определено следующим образом:

$$P(\mathfrak{A}) \leftrightarrow \exists x Q(\mathfrak{A}, x),$$

то P рекурсивно перечислимо.

Доказательство. Мы имеем

$$Q(\mathfrak{A}, x) \leftrightarrow \exists y R(\bar{\mathfrak{A}}(y), x, y),$$

где R рекурсивно. Тогда

$$P(\mathfrak{A}) \leftrightarrow \exists x \exists y R(\bar{\mathfrak{A}}(y), x, y). \quad (1)$$

Теперь, если z пробегает все числа, то $((z)_0, (z)_1)$ пробегает все пары чисел (x, y) . Следовательно, мы можем переписать (1) следующим образом:

$$P(\mathfrak{A}) \leftrightarrow \exists z R(\bar{\mathfrak{A}}((z)_1), (z)_0, (z)_1). \quad (2)$$

Так как согласно (8) из § 6.4 $(z)_1 \leq z$, то

$$\bar{\mathfrak{A}}((z)_1) = \text{In}(\bar{\mathfrak{A}}(z), (z)_1).$$

Отсюда

$$\begin{aligned} P(\mathfrak{A}) &\leftrightarrow \exists z R(\text{In}(\bar{\mathfrak{A}}(z), (z)_1), (z)_0, (z)_1) \\ &\leftrightarrow \exists z R'(\bar{\mathfrak{A}}(z), z), \end{aligned}$$

где R' — рекурсивный предикат, определенный следующим образом: $R'(a, z) \leftrightarrow R(\text{In}(a, (z)_1), (z)_0, (z)_1)$. Таким образом, P рекурсивно перечислимо.

Переход от (1) к (2) называется *свертыванием кванторов*. Он может также применяться для свертывания (замены) двух смежных соседних кванторов всеобщности одним квантором всеобщности.

Вследствие RE2 мы можем употреблять кванторы существования по числовым переменным в явных определениях рекурсивно перечислимых отношений.

*) Определение функции In см. в § 6.4 — Прим. ред.

RE3. Если Q и R рекурсивно перечислимы, то $Q \vee R$ и $Q \& R$ рекурсивно перечислимы.

Доказательство. Пусть P есть $Q \vee R$. Пусть $Q(\mathfrak{A}) \leftrightarrow \exists x Q_1(\overline{\mathfrak{A}}(x), x)$, $R(\mathfrak{A}) \leftrightarrow \exists y R_1(\overline{\mathfrak{A}}(y), y)$, где Q_1 и R_1 рекурсивны. Тогда при помощи пренексных операций и свертывания кванторов получаем

$$\begin{aligned} P(\mathfrak{A}) &\leftrightarrow \exists x Q_1(\overline{\mathfrak{A}}(x), x) \vee \exists y R_1(\overline{\mathfrak{A}}(y), y) \\ &\leftrightarrow \exists x \exists y (Q_1(\overline{\mathfrak{A}}(x), x) \vee R_1(\overline{\mathfrak{A}}(y), y)) \\ &\leftrightarrow \exists z (Q_1(\overline{\mathfrak{A}}((z)_0), (z)_0) \vee R_1(\overline{\mathfrak{A}}((z)_1), (z)_1)) \\ &\leftrightarrow \exists z (Q_1(\text{In}(\overline{\mathfrak{A}}(z), (z)_0), (z)_0) \vee R_1(\text{In}(\overline{\mathfrak{A}}(z), (z)_1), (z)_1)). \end{aligned}$$

Следовательно, P рекурсивно перечислимо. С $Q \& R$ мы поступаем аналогично.

Вследствие RE3 мы можем использовать $\vee$ и $\&$ в явных определениях рекурсивно перечислимых отношений.

Отметим, что

$$\forall x_{x < a} \exists y P(x, y, a) \leftrightarrow \exists z \forall x_{x < a} P(x, (z)_x, a). \quad (3)$$

Действительно, обе части утверждают, что существуют такие числа $y_0, y_1, \dots, y_{a-1}$, что $P(x, y_x, a)$ для всех $x < a$.

RE4. Если Q рекурсивно перечислимо и P определено следующим образом:

$$P(a, \mathfrak{A}) \leftrightarrow \forall x_{x < a} Q(\mathfrak{A}, x),$$

то P рекурсивно перечислимо.

Доказательство. Пусть $Q(\mathfrak{A}, x) \leftrightarrow \exists y R(\overline{\mathfrak{A}}(y), x, y)$, где R рекурсивно. Тогда, используя (3), получаем

$$\begin{aligned} P(a, \mathfrak{A}) &\leftrightarrow \forall x_{x < a} \exists y R(\overline{\mathfrak{A}}(y), x, y) \\ &\leftrightarrow \exists z \forall x_{x < a} R(\overline{\mathfrak{A}}((z)_x), x, (z)_x) \\ &\leftrightarrow \exists z \forall x_{x < a} R(\text{In}(\overline{\mathfrak{A}}(z), (z)_x), x, (z)_x). \end{aligned}$$

Отсюда следует, что P рекурсивно перечислимо. Вследствие RE4 мы можем употреблять ограниченные кванторы всеобщности в явных определениях рекурсивно перечислимых отношений.

Теперь мы обобщим R1—R14 на частичные функционалы и отношения. Так как эти обобщения включают

предшествующие результаты, то мы снова назовем их R1—R14. В случае прямых обобщений мы опустим доказательства, а иногда и формулировки правил.

Пусть $1 \leq i \leq n$; определим (m, n) -арный функционал $I_i^{m, n}$ следующим образом:

$$I_i^{m, n}(\alpha_1, \dots, \alpha_m, a_1, \dots, a_n) = a_i.$$

Определим также $(1, 1)$ -арный функционал Ap :

$$\text{Ap}(\alpha, a) = \alpha(a).$$

R1. Функционалы $I_i^{m, n}$, $+$, $\cdot$, $K_<$ и Ap рекурсивны.

Доказательство. Нам надо рассмотреть лишь $I_i^{m, n}$ и Ap . Обозначая $I_i^{m, n}$ через I , имеем

$$\mathfrak{G}_I(\alpha_1, \dots, \alpha_m, a_1, \dots, a_n, b) \leftrightarrow a_i = b.$$

Таким образом, $\mathfrak{G}_I$ рекурсивно перечислимо. Аналогично,

$$\begin{aligned} \mathfrak{G}_{\text{Ap}}(\alpha, a, b) &\leftrightarrow \alpha(a) = b \\ &\leftrightarrow \exists x (x > a \& (\overline{\alpha}(x))_a = b), \end{aligned}$$

поэтому $\mathfrak{G}_{\text{Ap}}$ рекурсивно перечислимо.

R2. Если $G, H_1, \dots, H_k$ рекурсивны, а F определен следующим образом:

$$\begin{aligned} F(\alpha_1, \dots, \alpha_m, a) &\simeq G(\alpha_{i_1}, \dots, \alpha_{i_r}, H_1(\alpha_1, \dots, \alpha_m, a), \dots \\ &\dots, H_k(\alpha_1, \dots, \alpha_m, a)), \end{aligned}$$

где числа $i_1, \dots, i_r$ находятся среди $1, \dots, m$, то F рекурсивен.

Доказательство. Мы имеем

$$\begin{aligned} \mathfrak{G}_F(\alpha_1, \dots, \alpha_m, a, a) &\leftrightarrow \exists z_1 \dots \\ &\dots \exists z_k (\mathfrak{G}_{H_1}(\alpha_1, \dots, \alpha_m, a, z_1) \& \dots \\ &\dots \& \mathfrak{G}_{H_k}(\alpha_1, \dots, \alpha_m, a, z_k) \& \mathfrak{G}_G(\alpha_{i_1}, \dots, \alpha_{i_r}, z_1, \dots, z_k, a)). \end{aligned}$$

Из полученных ранее результатов следует, что $\mathfrak{G}_F$ рекурсивно перечислимо.

R3. Если G рекурсивен, а F определен следующим образом:

$$F(\mathfrak{A}) \simeq \mu x (G(\mathfrak{A}, x) = 0),$$

то F рекурсивен.

Доказательство. Мы имеем

$$\mathfrak{G}_F(\mathfrak{A}, a) \leftrightarrow \mathfrak{G}_G(\mathfrak{A}, a, 0) \& \forall x_{x < a} \exists y (y > 0 \& \mathfrak{G}_G(\mathfrak{A}, x, y)).$$

Из полученных ранее результатов следует, что $\mathfrak{G}_F$ рекурсивно перечислимо.

R4. Если $Q, H_1, \dots, H_k$ рекурсивны, а P определено следующим образом:

$$P(\alpha_1, \dots, \alpha_m, a) \rightleftharpoons Q(\alpha_{i_1}, \dots, \alpha_{i_r}, H_1(\alpha_1, \dots, \alpha_m, a), \dots, H_k(\alpha_1, \dots, \alpha_m, a)),$$

где числа $i_1, \dots, i_r$ находятся среди $1, \dots, m$, то P рекурсивно.

R5. Если P рекурсивно, а F определен следующим образом:

$$F(\mathfrak{A}) \simeq \mu x P(\mathfrak{A}, x),$$

то F рекурсивен.

Применяя R1—R5, мы можем почти точно так же, как и ранее, показать, что явно определенные частичные функционалы и отношения рекурсивны. Например, предположим, что F определен следующим образом:

$$F(\alpha, \beta, x) \simeq \beta(G(\alpha, x) + \alpha(x)),$$

где G рекурсивен. Тогда мы можем последовательно определить рекурсивные частичные функционалы:

$$F_1(\alpha, \beta, x) \simeq G(\alpha, x) \simeq G(\alpha, I_1^{2,1}(\alpha, \beta, x)),$$

$$F_2(\alpha, \beta, x) \simeq \alpha(x) \simeq \text{Ap}(\alpha, x),$$

$$F_3(\alpha, \beta, x) \simeq G(\alpha, x) + \alpha(x) \simeq F_1(\alpha, \beta, x) + F_2(\alpha, \beta, x),$$

$$F(\alpha, \beta, x) \simeq \beta(G(\alpha, x) + \alpha(x)) \simeq \text{Ap}(\beta, F_3(\alpha, \beta, x)).$$

В обобщении R7 подразумевается, что $P \vee Q$ определено следующим образом:

$$(P \vee Q)(\mathfrak{A}) \rightleftharpoons P(\mathfrak{A}) \vee Q(\mathfrak{A}),$$

и поэтому определено на $\mathfrak{A}$ тогда и только тогда, когда как $P(\mathfrak{A})$, так и $Q(\mathfrak{A})$ определены. Поэтому мы имеем

$$K_{P \vee Q}(\mathfrak{A}) \simeq K_P(\mathfrak{A}) \cdot K_Q(\mathfrak{A}).$$

Аналогичные замечания применимы к $\neg P, P \rightarrow Q, P \& Q$ и $P \leftrightarrow Q$.

Мы можем трактовать ограниченные μ -операторы и ограниченные кванторы так же, как ранее. Однако ограниченный μ -оператор или ограниченный квантор по x имеет свое обычное значение только тогда, когда следующее выражение определено для каждого x .

R12. Пусть $G_1, \dots, G_k$ рекурсивны. Пусть $R_1, \dots, R_k$ — либо рекурсивные частичные отношения, либо рекурсивно перечислимые отношения такие, что для каждого $\mathfrak{A}$ не более чем одно из отношений $R_1(\mathfrak{A}), \dots, R_k(\mathfrak{A})$ определено и истинно. Если F определен следующим образом:

$$F(\mathfrak{A}) \simeq \begin{cases} G_1(\mathfrak{A}), & \text{если } R_1(\mathfrak{A}), \\ \dots & \dots \\ G_k(\mathfrak{A}), & \text{если } R_k(\mathfrak{A}) \end{cases}$$

(где подразумевается, что $F(\mathfrak{A})$ не определен, если никакое из отношений $R_1(\mathfrak{A}), \dots, R_k(\mathfrak{A})$ не будет определено и истинно), то F рекурсивен.

Доказательство. Если R_i — рекурсивное частичное отношение, а R'_i определено следующим образом:

$$R'_i(\mathfrak{A}) \leftrightarrow \mathfrak{G}_{K_{R_i}}(\mathfrak{A}, 0),$$

то R'_i рекурсивно перечислимо и $R'_i(\mathfrak{A})$ истинно тогда и только тогда, когда $R_i(\mathfrak{A})$ определено и истинно. Поэтому мы можем предположить, что R_i — рекурсивно перечислимое отношение. Тогда

$$\mathfrak{G}_F(\mathfrak{A}, a) \leftrightarrow (\mathfrak{G}_{G_1}(\mathfrak{A}, a) \& R_1(\mathfrak{A})) \vee \dots \vee (\mathfrak{G}_{G_k}(\mathfrak{A}, a) \& R_k(\mathfrak{A}));$$

поэтому $\mathfrak{G}_F$ рекурсивно перечислимо.

R13. Пусть $Q_1, \dots, Q_k$ рекурсивны. Пусть $R_1, \dots, R_k$ — или рекурсивные частичные отношения, или рекурсивно перечислимые отношения такие, что для каждого $\mathfrak{A}$ не более чем одно из отношений $R_1(\mathfrak{A}), \dots, R_k(\mathfrak{A})$ определено и истинно. Если P определено следующим образом:

$$P(\mathfrak{A}) \rightleftharpoons \begin{cases} Q_1(\mathfrak{A}), & \text{если } R_1(\mathfrak{A}), \\ \dots & \dots \\ Q_k(\mathfrak{A}), & \text{если } R_k(\mathfrak{A}) \end{cases}$$

(где подразумевается, что $P(\mathfrak{A})$ не определено, если ни одно из отношений $R_1(\mathfrak{A}), \dots, R_k(\mathfrak{A})$ не будет определено и истинно), то P рекурсивно.

Определим $\bar{F}$ следующим образом:

$$\bar{F}(b, \mathfrak{A}) \simeq \langle F(0, \mathfrak{A}), \dots, F(b-1, \mathfrak{A}) \rangle.$$

Явное определение (14) из § 6.4 все еще корректно, поэтому, если F рекурсивен, то $\bar{F}$ рекурсивен. Определение (15) из § 6.4 не имеет силы, если функционал частичный.

Мы можем очевидным образом обобщить R14 на рекурсивные частичные функционалы.

Заметим, что

$$\overline{\text{Ar}}(\alpha, a) = \overline{\alpha}(a);$$

следовательно, употребляя $\overline{\text{Ar}}$ таким же образом, как мы прежде использовали Ar , мы видим, что надчеркнутые функциональные переменные можно употреблять в явных определениях рекурсивных частичных функционалов и отношений.

Следствием наших результатов о явных определениях является то, что если $G(\mathfrak{A}, x)$ и $H(\mathfrak{A})$ рекурсивны и мы подставим $H(\mathfrak{A})$ вместо x в $G(\mathfrak{A}, x)$, то мы получим рекурсивный частичный функционал от $\mathfrak{A}$. Мы намерены доказать подобное правило подстановки вместо функциональных переменных. Очевидно, мы не можем подставить $H(\mathfrak{A})$ вместо α , потому что $H(\mathfrak{A})$ — число. Поэтому мы сначала введем некоторое обозначение.

Пусть $\dots x \dots$ — выражение, которое, когда оно определено, представляет число. Тогда мы используем $\lambda x \dots x \dots$ для обозначения унарной частичной функции F , определенной следующим образом: $F(x) \simeq \dots x \dots$. Отметим, что x в $\lambda x \dots x \dots$ связано. Например, $\lambda x(x+y)$ — это функция F , определенная как $F(x) = x+y$; это функция, зависящая от значения y , но не зависящая от значения x . Частичная функция $\lambda x \dots x \dots$ всюду определена, если $\dots x \dots$ определено для всех x .

Теорема о подстановке. Пусть G и H — рекурсивные частичные функционалы; тогда существует такой рекурсивный частичный функционал F , что

$$F(\mathfrak{A}) \simeq G(\lambda x H(x, \mathfrak{A}), \mathfrak{A})$$

для всех таких $\mathfrak{A}$, что $\lambda x H(x, \mathfrak{A})$ является всюду определенной функцией.

Доказательство. Определим F' следующим образом:

$$F'(\mathfrak{A}) \simeq G(\lambda x H(x, \mathfrak{A}), \mathfrak{A}).$$

Пусть R — такой рекурсивный предикат, что

$$\mathfrak{G}_a(\alpha, \mathfrak{A}, y) \leftrightarrow \exists x R(\overline{\alpha}(x), \overline{\mathfrak{A}}(x), y, x).$$

Тогда, если $\mathfrak{A}$ таково, что $\lambda x H(x, \mathfrak{A})$ всюду определена, то

$$\mathfrak{G}_{F'}(\mathfrak{A}, y) \leftrightarrow \exists x R(\overline{H}(x, \mathfrak{A}), \overline{\mathfrak{A}}(x), y, x);$$

поэтому вследствие (1) из § 7.2 получаем, что

$$F'(\mathfrak{A}) \simeq (\mu z R(\overline{H}((z)_1, \mathfrak{A}), \overline{\mathfrak{A}}((z)_1), z_1))_0.$$

Следовательно, мы можем явно определить F , полагая $F(\mathfrak{A})$ равным правой части последнего выражения.

Замечание. Если $\mathfrak{A}$ таково, что $\lambda x H(x, \mathfrak{A})$ определена не всюду, то $F'(\mathfrak{A})$, конечно, не определен, однако $F(\mathfrak{A})$ может быть определен.

Теперь рассмотрим явное определение

$$F(\mathfrak{A}) \simeq \lambda x (\dots x \dots), \quad (4)$$

содержащее λ , и предположим, что для всех остальных имеющихся символов уже было показано, что они могут употребляться в явных определениях рекурсивных частичных функционалов.

Мы можем определить рекурсивные частичные функционалы G и H следующим образом:

$$G(\alpha, \mathfrak{A}) = \alpha;$$

$$H(x, \mathfrak{A}) \simeq \dots x \dots$$

Тогда (4) превращается в

$$F(\mathfrak{A}) \simeq G(\lambda x H(x, \mathfrak{A}), \mathfrak{A}).$$

Мы не можем сделать вывод, что функционал F рекурсивен; однако по теореме о подстановке существует такой рекурсивный функционал F , что (4) имеет место, если $\dots x \dots$ определено для всех x . Если $\dots x \dots$ определено при всех значениях x и $\mathfrak{A}$, то мы можем сделать вывод, что определенный в (4) функционал F рекурсивен. Справедливы точно такие же замечания об употреблении λ в явных определениях рекурсивных частичных отношений.

Функцию $\lambda x \alpha(\langle i, x \rangle)$ мы обозначаем через $(\alpha)_i$. Ввиду сказанного выше $(\alpha)_i$ может применяться в явных определениях рекурсивных частичных функционалов и отношений. Если $\alpha_0, \alpha_1, \dots$ — бесконечная последовательность функций, то существует такое α , что $(\alpha)_i = \alpha_i$ для всех i , потому что мы можем определить α следующим образом: $\alpha(x) = \alpha_{(x)_0}((x)_1)$.

7.4. Индексы

Теперь мы сопоставим каждому рекурсивному частичному функционалу число таким образом, чтобы по этому числу можно было восстановить этот частичный функционал.

Пусть $z_1, z_2, \dots$ — переменные теории N , расположенные в алфавитном порядке. Если A — формула теории N , то пусть $E_n(A)$ — множество таких n -ок $(a_1, \dots, a_n)$, что

$$\vdash_N A_{z_1, \dots, z_n} [k_{a_1}, \dots, k_{a_n}].$$

Точно так же, как и в § 6.8, мы можем показать, что каждый рекурсивный n -арный всюду определенный предикат есть $E_n(A)$ для некоторого A .

Теперь мы получим явное определение $E_n(A)$. Определим рекурсивную функцию S_n следующим образом:

$$S_n(e, a) = \text{Sub}(e, \langle 2n \rangle, \text{Num}(a)).$$

Тогда

$$S_n(\ulcorner A \urcorner, a) = \ulcorner A_{z_1, \dots, z_n} [k_a] \urcorner.$$

Теперь мы определим такую рекурсивную функцию Sb_n , что

$$\text{Sb}_n(\ulcorner A \urcorner, a_1, \dots, a_n) = \ulcorner A_{z_1, \dots, z_n} [k_{a_1}, \dots, k_{a_n}] \urcorner.$$

Пользуясь индукцией по n , определяем

$$\text{Sb}_0(e) = e$$

и

$$\text{Sb}_{n+1}(e, a_1, \dots, a_{n+1}) = \text{Sb}_n(S_n(e, a_{n+1}), a_1, \dots, a_n). \quad (1)$$

Тогда мы имеем

$$(a_1, \dots, a_n) \in E_n(A) \leftrightarrow \exists v \text{Pr}_N(\text{Sb}_n(\ulcorner A \urcorner, a_1, \dots, a_n), v). \quad (2)$$

Пусть теперь F — рекурсивный (m, n) -арный частичный функционал. Тогда мы можем выбрать такой рекурсивный предикат R , что

$$\mathfrak{G}_F(\mathfrak{A}, y) \leftrightarrow \exists w R(y, w, \bar{\mathfrak{A}}(w)).$$

Выберем A такое, что R есть $E_{m+n+2}(A)$, и пусть $f = \ulcorner A \urcorner$. Тогда, свертывая кванторы, вследствие (2) имеем

$$\begin{aligned} \mathfrak{G}_F(\mathfrak{A}, y) &\leftrightarrow \exists w \exists v \text{Pr}_N(\text{Sb}_{m+n+2}(f, y, w, \bar{\mathfrak{A}}(w)), v) \\ &\leftrightarrow \exists x \text{Pr}_N(\text{Sb}_{m+n+2}(f, y, (x)_0, \bar{\mathfrak{A}}((x)_0)), (x)_1). \end{aligned}$$

Вследствие (1) из § 7.2

$$F(\mathfrak{A}) \simeq (\mu z \text{Pr}_N(\text{Sb}_{m+n+2}(f, (z)_0, (z)_{1,0}, \bar{\mathfrak{A}}((z)_{1,0})), (z)_{1,1}))_0.$$

Определим рекурсивное отношение $T_{m,n}$ и рекурсивную функцию U следующим образом:

$$\begin{aligned} T_{m,n}(f, \mathfrak{A}, z) &\leftrightarrow \text{Pr}_N(\text{Sb}_{m+n+2}(f, (z)_0, (z)_{1,0}, \bar{\mathfrak{A}}((z)_{1,0})), (z)_{1,1}), \\ U(z) &= (z)_0 \end{aligned}$$

(вместо $T_{0,n}$ мы пишем T_n). Тогда мы имеем

$$F(\mathfrak{A}) \simeq U(\mu z T_{m,n}(f, \mathfrak{A}, z)). \quad (3)$$

Число f называется *индексом* (m, n) -арного частичного функционала F , если (3) верно для всех $\mathfrak{A}$. Мы доказали, что каждый рекурсивный частичный функционал имеет индекс. Обратно, если f является индексом функционала F , то функционал F имеет явное определение (3) и поэтому рекурсивен. Таким образом, мы имеем следующий результат.

Теорема о нормальной форме (Клини). Частичный функционал рекурсивен тогда и только тогда, когда он имеет индекс.

Каждое число f является индексом единственного (m, n) -арного частичного функционала, а именно, того F , который определен в (3). Этот частичный функционал мы обозначим через $\{f\}^{m,n}$, опуская верхние индексы, если это не вызывает путаницы. Таким образом,

$$\{f\}^{m,n}(\mathfrak{A}) \simeq U(\mu z T_{m,n}(f, \mathfrak{A}, z)) \quad (4)$$

и, следовательно,

$$\{f\}^{m,n}(\mathfrak{A}) \text{ определено} \leftrightarrow \exists z T_{m,n}(f, \mathfrak{A}, z). \quad (5)$$

Вследствие (4) $\{f\}(\mathfrak{A})$ является рекурсивным частичным функционалом от аргументов $f, \mathfrak{A}$. Отсюда видно, что мы можем употреблять $\{f\}(\mathfrak{A})$ в явных определениях рекурсивных частичных функционалов и отношений. Отсюда также видно (ввиду определения рекурсивного частичного функционала), что $\{f\}(\mathfrak{A}) \simeq b$ является рекурсивно перечислимым отношением от аргументов $f, \mathfrak{A}, b$.

Пусть теперь P — рекурсивно перечислимое (m, n) -арное отношение, например,

$$P(\mathfrak{A}) \leftrightarrow \exists x R(\bar{\mathfrak{A}}(x), x),$$

где R рекурсивно. Определим рекурсивный частичный функционал F следующим образом: $F(\mathfrak{A}) \simeq \mu x R(\bar{\mathfrak{A}}(x), x)$, и пусть p является индексом функционала F . Тогда значение $\{p\}(\mathfrak{A})$ определено тогда и только тогда, когда $P(\mathfrak{A})$. Отсюда и из (5) имеем

$$P(\mathfrak{A}) \leftrightarrow \exists z T_{m,n}(p, \mathfrak{A}, z). \quad (6)$$

Число p называется **RE-индексом** (m, n) -арного отношения P , если (6) справедливо для всех $\mathfrak{A}$. Мы видели, что каждое рекурсивно перечислимое отношение имеет RE-индекс. Отношение P , имеющее RE-индекс p , имеет явное определение (6) и потому рекурсивно перечисливо. Отсюда получается

Теорема о перечислении (Клини). *Отношение рекурсивно перечисливо тогда и только тогда, когда оно имеет RE-индекс.*

Каждое число p является RE-индексом единственного (m, n) -арного отношения P , определенного в (6). Мы обозначим это отношение через $W_e^{m,n}$, опуская верхние индексы, если это не приводит к путанице.

Пусть F — $(m, n+k)$ -арный частичный функционал; для каждой k -ки α определим (m, n) -арный частичный функционал $F_{(\alpha)}$ следующим образом:

$$F_{(\alpha)}(\mathfrak{A}) \simeq F(\mathfrak{A}, \alpha).$$

Пусть P есть $(m, n+k)$ -арное отношение; для каждой k -ки $\mathfrak{A}$ мы определим (m, n) -арное отношение $P_{(\alpha)}$ следующим образом:

$$P_{(\alpha)}(\mathfrak{A}) \leftrightarrow P(\mathfrak{A}, \alpha).$$

(Мы могли бы дать аналогичное определение для частичного отношения P , однако оно нам не потребуется.) Мы говорим, что $(m, n+1)$ -арное отношение P *перечисляет* класс (m, n) -арных отношений, состоящий из $P_{(0)}, P_{(1)}, \dots$

Теперь мы покажем, что существует такая рекурсивная функция $S_{m,n,k}$, что

$$T_{m,n+k}(f, \mathfrak{A}, \alpha, z) \leftrightarrow T_{m,n}(S_{m,n,k}(f, \alpha), \mathfrak{A}, z). \quad (7)$$

Мы можем положить $S_{m,n,0}(f) = f$. Сравнивая (1) и определение $T_{m,n}$, мы видим, что мы можем определить

$$S_{m,n,1}(f, \alpha) = S_{m+n+2}(f, \alpha).$$

Далее, проводя индукцию по k , определяем

$$S_{m,n,k+1}(f, \alpha, a) = S_{m,n,k}(S_{m,n+k,1}(f, a), \alpha).$$

Иногда мы опускаем нижние индексы у $S_{m,n,k}$.

Из (7) мы получаем

$$\{f\}^{m,n+k}(\mathfrak{A}, \alpha) \simeq \{S_{m,n,k}(f, \alpha)\}(\mathfrak{A})$$

и

$$W_p^{m,n+k}(\mathfrak{A}, \alpha) \leftrightarrow W_{S_{m,n,k}(p, \alpha)}(\mathfrak{A}). \quad (8)$$

Вследствие этого, если f является индексом функционала F , то $S(f, \alpha)$ является индексом функционала $F_{(\alpha)}$; если p является RE-индексом отношения P , то $S(p, \alpha)$ является RE-индексом отношения $P_{(\alpha)}$.

Теперь мы используем индексы для получения еще одного метода определения рекурсивных частичных функционалов. В неявном определении частичного функционала F значение $F(\mathfrak{A})$ дается в терминах F и $\mathfrak{A}$. Таким образом, мы полагаем

$$F(\mathfrak{A}) \simeq \Phi(F, \mathfrak{A}), \quad (9)$$

где Φ — отображение, значениями которого являются числа. Конечно, это на самом деле не определяет функционал F , это просто означает, что мы искали такой функционал F , что уравнение справедливо для всех $\mathfrak{A}$. Это уравнение может не иметь решения, или иметь единственное решение, или много решений.

Мы хотим показать, что при подходящих предположениях о Φ существует по крайней мере одно рекурсивное решение. Мы не можем предполагать, что отображение Φ рекурсивно, так как Φ не является функционалом. Поэтому мы заменим в правой части (9) функционал F на индекс функционала F . Иначе говоря, мы определим частичный функционал Φ' следующим образом:

$$\Phi'(f, \mathfrak{A}) \simeq \Phi(\{f\}, \mathfrak{A}).$$

Теперь мы можем предполагать, что Φ' рекурсивен. Мы хотим показать, что существует такой рекурсивный функционал F с индексом f , что $F(\mathfrak{A}) \simeq \Phi'(f, \mathfrak{A})$ для всех $\mathfrak{A}$.

Теорема о рекурсии (Клини). *Пусть G — рекурсивный $(m, n+1)$ -арный частичный функционал; существует такой (m, n) -арный частичный функционал F с*

индексом f , что

$$F(\mathfrak{A}) \simeq G(\mathfrak{A}, f)$$

для всех $\mathfrak{A}$.

Доказательство. Определим рекурсивный функционал H следующим образом:

$$H(\mathfrak{A}, e) \simeq G(\mathfrak{A}, S_{m,n,1}(e, e)),$$

и пусть h — индекс функционала H . Пусть F есть $H_{(h)}$ и $f = S_{m,n,1}(h, h)$. Тогда f есть индекс функционала F и

$$\begin{aligned} F(\mathfrak{A}) &\simeq H(\mathfrak{A}, h) \\ &\simeq G(\mathfrak{A}, S_{m,n,1}(h, h)) \\ &\simeq G(\mathfrak{A}, f). \end{aligned}$$

Теорема о рекурсии является ценным средством для доказательства рекурсивности частичных функционалов. По данному функционалу F мы пытаемся построить отображение Φ так, чтобы (9) имело в качестве единственного решения F , и так, чтобы соответствующий функционал был рекурсивен. Тогда мы можем заключить, что F рекурсивен. Примером такой техники служит задача 1.

При употреблении теоремы о рекурсии мы обычно будем говорить: определим рекурсивный частичный функционал F с индексом f следующим образом: $F(\mathfrak{A}) \simeq G(\mathfrak{A}, f)$. Конечно, в общем случае F и f не являются единственными; мы подразумеваем, что какие-то F и f , обладающие этими свойствами, могут быть выбраны. Обычно функционал G будет задаваться явным определением или определением разбором случаев. Поэтому $F(\mathfrak{A}) \simeq G(\mathfrak{A}, f)$ будет иметь вид явного определения функционала F или определения функционала F разбором случаев, за исключением того, что индекс f функционала F может встречаться в правой части. Мы также будем допускать появление выражений $F(\dots)$ в правой части; такое выражение считается сокращением для $\{f\}(\dots)$. Мы можем определить

$$F(\mathfrak{A}) \simeq \begin{cases} H(F(\mathfrak{A})), & \text{если } P(\mathfrak{A}), \\ K(\mathfrak{A}, f) & \text{в остальных случаях,} \end{cases}$$

где H и K — рекурсивные частичные функционалы, а P — рекурсивное отношение.

Мы можем также использовать теорему о рекурсии для того, чтобы определить рекурсивное частичное отношение P следующим образом: $P(\mathfrak{A}) \stackrel{\sim}{\leftrightarrow} Q(\mathfrak{A}, p)$, где p — индекс функ-

ционала K_p ; действительно, это определение эквивалентно определению $K_p(\mathfrak{A}) \simeq K_Q(\mathfrak{A}, p)$. И снова в общем случае Q может быть задано явным определением или определением разбором случаев. Тогда мы допускаем наличие в правой части выражений $P(\dots)$; такое выражение считается сокращением для $\{p\}(\dots) = 0$.

7.5. Арифметическая иерархия

Мы уже видели, что применение кванторов в явных определениях выводит за пределы класса рекурсивных отношений. Мы собираемся изучить отношения, которые могут быть получены навешиванием кванторов на рекурсивные отношения. В этом параграфе мы рассматриваем только кванторы по числовым переменным, кванторы по функциональным переменным будут рассмотрены позже.

Отношение P называется *арифметическим*, если оно имеет явное определение

$$P(\mathfrak{A}) \leftrightarrow \alpha x_1 \dots \alpha x_n R(\mathfrak{A}, x_1, \dots, x_n), \quad (1)$$

где R — рекурсивное отношение и каждое αx_i есть либо $\exists x_i$, либо $\forall x_i$.

Два квантора имеют *одинаковый вид*, если они оба являются кванторами существования или оба являются кванторами всеобщности. Если нам дано определение (1), в котором имеются два смежных квантора одинакового вида, то мы можем воспользоваться свертыванием кванторов для замены их одним квантором. Так, если первоначальным определением является

$$P(\mathfrak{A}) \leftrightarrow \exists x \forall y \forall z \exists w R(\mathfrak{A}, x, y, z, w),$$

то мы имеем новое определение

$$P(\mathfrak{A}) \leftrightarrow \exists x \forall v \exists w R'(\mathfrak{A}, x, v, w),$$

где R' — рекурсивное отношение, определенное следующим образом:

$$R'(\mathfrak{A}, x, v, w) \leftrightarrow R(\mathfrak{A}, x, (v)_0, (v)_1, w).$$

Если $n \geq 1$, то отношение называется *отношением рода* Σ_n^0 (Π_n^0), если оно имеет явное определение (1), где отношение R рекурсивно, нет двух смежных кванторов одинакового вида и где первый квантор — квантор существования

(всеобщности). Таким образом, мы видим, что каждое арифметическое отношение либо рекурсивно, либо является отношением рода Σ_n^0 или Π_n^0 для некоторого $n \geq 1$. Эта классификация арифметических отношений называется *арифметической иерархией*.

Мы дадим несколько правил получения отношений рода Σ_n^0 и Π_n^0 .

A1. Если отношение P рекурсивно, то P — отношение рода Σ_n^0 и Π_n^0 для любых n . Если P — отношение рода Σ_m^0 или Π_m^0 , то P — отношение рода Σ_n^0 и Π_n^0 для любых $n > m$.

Доказательство. Используется добавление лишних кванторов. Предположим, например, что P — отношение рода Σ_2^0 и имеет определение

$$P(\mathfrak{A}) \leftrightarrow \exists x \forall y R(\mathfrak{A}, x, y).$$

Покажем, что P — отношение рода Σ_3^0 и Π_3^0 . Действительно,

$$\begin{aligned} P(\mathfrak{A}) &\leftrightarrow \exists x \forall y \exists z R(\mathfrak{A}, x, y) \\ &\leftrightarrow \forall z \exists x \forall y R(\mathfrak{A}, x, y). \end{aligned}$$

A2. Если Q — отношение рода Σ_n^0 (Π_n^0) и $F_1, \dots, F_r, G_1, \dots, G_k$ — рекурсивные функционалы, то отношение P , определенное следующим образом:

$$P(\mathfrak{A}) \leftrightarrow Q(\lambda x F_1(\mathfrak{A}, x), \dots, \lambda x F_r(\mathfrak{A}, x), G_1(\mathfrak{A}), \dots, G_k(\mathfrak{A})),$$

является отношением рода Σ_n^0 (Π_n^0).

Доказательство. Предположим, что Q — отношение рода Σ_2^0 и имеет определение

$$Q(\mathfrak{A}) \leftrightarrow \exists y \forall z R(\mathfrak{A}, y, z).$$

Тогда $P(\mathfrak{A}) \leftrightarrow \exists y \forall z R'(\mathfrak{A}, y, z)$, где R' — рекурсивное отношение, определенное следующим образом:

$$\begin{aligned} R'(\mathfrak{A}, y, z) &\leftrightarrow R(\lambda x F_1(\mathfrak{A}, x), \dots, \lambda x F_r(\mathfrak{A}, x), \\ &\quad G_1(\mathfrak{A}), \dots, G_k(\mathfrak{A}), y, z). \end{aligned}$$

A3. Если Q — отношение рода Σ_n^0 и отношение P определено следующим образом: $P(\mathfrak{A}) \leftrightarrow \exists x Q(\mathfrak{A}, x)$, то P — отношение рода Σ_n^0 . Если Q — отношение рода Π_n^0 и отношение P определено следующим образом: $P(\mathfrak{A}) \leftrightarrow \forall x Q(\mathfrak{A}, x)$, то P — отношение рода Π_n^0 .

Доказательство. Используется свертывание кванторов. Так, если Q — отношение рода Σ_2^0 и определено

следующим образом:

$$Q(\mathfrak{A}, x) \leftrightarrow \exists y \forall z R(\mathfrak{A}, x, y, z),$$

то

$$P(\mathfrak{A}) \leftrightarrow \exists x \exists y \forall z R(\mathfrak{A}, x, y, z),$$

и, следовательно, P — отношение рода Σ_2^0 , если свернуть кванторы.

A4. Если P и Q — отношения рода Σ_n^0 (Π_n^0), то $P \vee Q$ и $P \& Q$ — отношения рода Σ_n^0 (Π_n^0).

Доказательство. Предположим, что P и Q — отношения рода Σ_2^0 , например, что

$$P(\mathfrak{A}) \leftrightarrow \exists x \forall y P_1(\mathfrak{A}, x, y), \quad Q(\mathfrak{A}) \leftrightarrow \exists z \forall w Q_1(\mathfrak{A}, z, w).$$

Свертывая кванторы, видим, что $P \vee Q$ — отношение рода Σ_2^0 .

A5. Если P — отношение рода Σ_n^0 (Π_n^0), то $\neg P$ — отношение рода Π_n^0 (Σ_n^0).

Доказательство. Используются пренексные операции. Например, если P — отношение рода Σ_2^0 и имеет определение

$$P(\mathfrak{A}) \leftrightarrow \exists x \forall y R(\mathfrak{A}, x, y),$$

то

$$\begin{aligned} \neg P(\mathfrak{A}) &\leftrightarrow \neg \exists x \forall y R(\mathfrak{A}, x, y) \\ &\leftrightarrow \forall x \exists y \neg R(\mathfrak{A}, x, y). \end{aligned}$$

Для изучения ограниченных кванторов нам необходимы следующие эквивалентности:

$$\exists x_{x < a} \exists y P(x, y, a) \leftrightarrow \exists y \exists x_{x < a} P(x, y, a), \quad (2)$$

$$\forall x_{x < a} \forall y P(x, y, a) \leftrightarrow \forall y \forall x_{x < a} P(x, y, a), \quad (3)$$

$$\forall x_{x < a} \exists y P(x, y, a) \leftrightarrow \exists y \forall x_{x < a} P(x, (y)_x, a), \quad (4)$$

$$\exists x_{x < a} \forall y P(x, y, a) \leftrightarrow \forall y \exists x_{x < a} P(x, (y)_x, a). \quad (5)$$

Первые две очевидны, а (4) есть (3) из § 7.3. Чтобы получить (5), мы в (4) заменим P на $\neg P$ и вынесем знаки отрицания вперед с помощью пренексных операций. Мы получим, что отрицания обеих частей в (5) эквивалентны, отсюда следует (5).

A6. Если P — отношение рода Σ_n^0 (Π_n^0), а отношения Q и R определены следующим образом:

$$Q(a, \mathfrak{A}) \leftrightarrow \exists x_{x < a} P(\mathfrak{A}, x), \quad R(a, \mathfrak{A}) \leftrightarrow \forall x_{x < a} P(\mathfrak{A}, x),$$

то Q и R — отношения рода Σ_n^0 (Π_n^0).

Доказательство. Предположим, что P — отношение рода Σ_2^0 , например, что

$$P(\mathfrak{A}, x) \leftrightarrow \exists y \forall z R(\mathfrak{A}, x, y, z).$$

Тогда вследствие (2) и (5) имеем

$$\begin{aligned} Q(a, \mathfrak{A}) &\leftrightarrow \exists x_{x < a} \exists y \forall z R(\mathfrak{A}, x, y, z) \\ &\leftrightarrow \exists y \exists x_{x < a} \forall z R(\mathfrak{A}, x, y, z) \\ &\leftrightarrow \exists y \forall z \exists x_{x < a} R(\mathfrak{A}, x, y, (z)_x). \end{aligned}$$

Эти результаты могут применяться для доказательства того, что различные явно определенные отношения являются отношениями рода Σ_n^0 или Π_n^0 ; при этом техника такая же, как при употреблении рекурсивных частичных отношений и рекурсивно перечислимых отношений.

Отношения рода Σ_1^0 — это в точности рекурсивно перечислимые отношения. Действительно, отношение рода Σ_1^0 рекурсивно перечисливо в силу результатов из § 7.3, а обратное очевидно.

Если P — отношение рода Σ_1^0 , имеющее хотя бы один функциональный аргумент, то P имеет определение

$$P(\alpha, \mathfrak{A}) \leftrightarrow \exists x R(\bar{\alpha}(x), \mathfrak{A}), \quad (6)$$

где отношение R рекурсивно. Действительно, так как P рекурсивно перечисливо, то

$$P(\alpha, \mathfrak{A}) \leftrightarrow \exists x Q(\bar{\alpha}(x), \bar{\mathfrak{A}}(x), x),$$

где Q рекурсивно, а тогда мы можем определить R следующим образом:

$$R(a, \mathfrak{A}) \leftrightarrow Q(a, \bar{\mathfrak{A}}(lh(a)), lh(a)).$$

Отсюда и из А5 мы видим, что если P — отношение рода Π_1^0 , имеющее хотя бы один функциональный аргумент, то

$$P(\alpha, \mathfrak{A}) \leftrightarrow \neg \exists x Q(\bar{\alpha}(x), \mathfrak{A}),$$

где отношение Q рекурсивно. Применяя пренексную операцию к правой части, мы видим, что P имеет явное определение

$$P(\alpha, \mathfrak{A}) \leftrightarrow \forall x R(\bar{\alpha}(x), \mathfrak{A}), \quad (7)$$

где R рекурсивно.

Теорема об арифметическом перечислении (Клини). Для любых m и n и любого $k \geq 1$ существует

вует $(m, n+1)$ -арное отношение рода Σ_k^0 (Π_k^0), которое перечисляет множество (m, n) -арных отношений рода Σ_k^0 (Π_k^0).

Доказательство. Предположим, например, что $k=3$. Если P — отношение рода Σ_3^0 , то

$$P(\mathfrak{A}) \leftrightarrow \exists x \forall y \exists z R(x, y, z, \mathfrak{A}),$$

где R рекурсивно. По теореме о нумерации существует такое p , что

$$\exists z R(x, y, z, \mathfrak{A}) \leftrightarrow \exists z T_{m, n+2}(p, x, y, \mathfrak{A}, z),$$

так что

$$P(\mathfrak{A}) \leftrightarrow \exists x \forall y \exists z T_{m, n+2}(p, x, y, \mathfrak{A}, z).$$

Наоборот, определенное этой эквивалентностью отношение P имеет род Σ_3^0 . Поэтому перечисляющее отношение для отношений рода Σ_3^0 определяется следующим образом:

$$Q(\mathfrak{A}, p) \leftrightarrow \exists x \forall y \exists z T_{m, n+2}(p, x, y, \mathfrak{A}, z).$$

По А5 отношения рода Π_3^0 — это в точности отрицания отношений рода Σ_3^0 . Вследствие этого $\neg Q$ является перечисляющим отношением для отношений рода Π_3^0 .

Теперь мы можем показать, что единственными соотношениями между отношениями рода Σ_n^0 и Π_n^0 являются соотношения, полученные по А1.

Теорема об арифметической иерархии (Клини). Для каждого $n \geq 1$ существует унарный предикат P рода Σ_n^0 , который не имеет рода Π_n^0 и, следовательно, не имеет рода Σ_m^0 или Π_m^0 при $m < n$. Кроме того, $\neg P$ имеет род Π_n^0 , но не Σ_n^0 и, следовательно, не Σ_m^0 или Π_m^0 при $m < n$.

Доказательство. Пусть Q — бинарный предикат рода Σ_n^0 , перечисляющий множество унарных предикатов рода Σ_n^0 , определим P следующим образом: $P(a) \leftrightarrow Q(a, a)$. Тогда P имеет род Σ_n^0 по А2, в то время как $\neg P$ не имеет рода Σ_n^0 по диагональной лемме. Поэтому требуемое заключение следует из А5 и А1.

Отношение P имеет род Δ_n^0 , если оно одновременно имеет род Σ_n^0 и Π_n^0 . Согласно А5 P имеет род Δ_n^0 тогда и только тогда, когда как P , так и $\neg P$ имеют род Σ_n^0 , и тогда и только тогда, когда как P , так и $\neg P$ имеют род Π_n^0 . В частности, P имеет род Δ_1^0 тогда и только тогда, когда как P , так и $\neg P$ рекурсивно перечислимы.

Следовательно, по теореме об отрицании предикаты рода Δ_1^0 — это в точности рекурсивные предикаты. Мы можем легко использовать доказательство теоремы об отрицании, чтобы показать, что отношения рода Δ_1^0 — это в точности рекурсивные отношения; на этот результат мы будем также ссылаться как на *теорему об отрицании*. В следующем параграфе мы получим аналогичную характеристику предикатов рода Δ_n^0 для $n > 1$.

7.6. Относительная рекурсивность

Пусть Φ — некоторое множество всюду определенных функций. Определим функции, *рекурсивные в Φ* (или *рекурсивные относительно Φ*) с помощью обобщенного определения, состоящего из четырех правил $R0_\Phi$, $R1_\Phi$, $R2_\Phi$ и $R3_\Phi$. Последние три правила получены из $R1$, $R2$ и $R3$ заменой слова *рекурсивные* на *рекурсивные в Φ* . Первое правило:

$R0_\Phi$. Каждая функция из Φ рекурсивна в Φ .

Пусть теперь Φ — некоторое множество всюду определенных функций и предикатов, и пусть Φ' — множество, состоящее из функций, принадлежащих Φ , и из представляющих функций предикатов, принадлежащих Φ . Мы говорим, что функция *рекурсивна в Φ* , если она рекурсивна в Φ' . Если Φ состоит из $F_1, \dots, F_m, R_1, \dots, R_n$, то мы говорим «рекурсивна в $F_1, \dots, F_m, R_1, \dots, R_n$ » вместо «рекурсивна в Φ ».

Так как все понятия теории рекурсии определены в терминах понятия рекурсивной функции, то мы можем из каждого из этих понятий получить новое понятие относительно Φ заменой слова *рекурсивно* на *рекурсивно в Φ* в определении старого понятия. Это приводит к следующим определениям.

Предикат *рекурсивен в Φ* , если его представляющая функция рекурсивна в Φ (очевидно, отсюда следует, что каждый предикат, принадлежащий Φ , рекурсивен в Φ). Отношение R *рекурсивно перечислимо в Φ* , если существует рекурсивный в Φ предикат R такой, что

$$P(\mathfrak{A}) \leftrightarrow \exists x R(\bar{\mathfrak{A}}(x), x)$$

для всех $\mathfrak{A}$. Частичный функционал *рекурсивен в Φ* , если его график рекурсивно перечислим в Φ . Частичное отно-

шение *рекурсивно в Φ* , если его представляющий частичный функционал рекурсивен в Φ . Мы предоставляем читателю самому определить арифметичность, Σ_n^0 , Π_n^0 и Δ_n^0 в Φ .

Многие доказанные нами результаты зависят только от того обстоятельства, что рекурсивные функции удовлетворяют правилам $R1$ — $R3$. Очевидно, эти результаты также справедливы в релятивизованном случае (когда используется понятие относительной рекурсивности). Таким способом обобщаются правила $R1$ — $R14$ (в обоих вариантах) и $RE1$ — $RE4$, а также теорема о подстановке. Обобщаются правила $A1$ — $A6$, а также утверждения о том, что каждое арифметическое отношение рекурсивно, имеет род Σ_n^0 или Π_n^0 , и утверждение о том, что отношения рода Σ_1^0 — это в точности рекурсивно перечислимые отношения. Теорема об отрицании также обобщается. Разумеется, результаты, доказываемые индукцией по рекурсивным функциям (подобно теореме о представлении), не могут быть обобщены столь просто.

Если Φ пусто, то функции, рекурсивные в Φ , — это в точности рекурсивные функции. Таким образом, релятивизованная теория рекурсии содержит в себе как частный случай обычную теорию рекурсии.

Пусть Ψ — другое множество всюду определенных функций и предикатов. Мы говорим, что Φ *рекурсивно в Ψ* , если каждый элемент, принадлежащий Φ , рекурсивен в Ψ .

Лемма о транзитивности. Если Φ *рекурсивно в Ψ* , то каждая функция, рекурсивная в Φ , рекурсивна в Ψ .

Доказательство. Используется индукция по функциям, рекурсивным в Φ .

Следствие 1. Всякая функция, рекурсивная в Φ , рекурсивна в каждом множестве, включающем Φ .

В частности, каждая рекурсивная функция рекурсивна в Φ для любого Φ .

Следствие 2. Если функция F рекурсивна в множестве, каждый элемент которого либо рекурсивен, либо принадлежит Φ , то F рекурсивна в Φ .

Лемма о транзитивности обобщается для частичных рекурсивных функционалов и отношений, рекурсивно перечислимых и арифметических отношений, а также отношений рода Σ_n^0 , Π_n^0 и Δ_n^0 . Это значит, например, что если Φ рекурсивно в Ψ , то каждое отношение, арифме-

тическое в Φ , является арифметическим в Ψ . Следствия также могут быть обобщены для этих случаев.

Лемма о конечности. Если функция рекурсивна в Φ , то она рекурсивна в некотором конечном подмножестве множества Φ .

Доказательство. Используется индукция по функциям, рекурсивным в Φ .

Лемма о конечности обобщается также для всех рассмотренных выше понятий.

Теперь мы рассмотрим случай, когда Φ конечно. При этом полезно предположить, что элементы множества Φ каким-то образом упорядочены, так что Φ является конечной последовательностью, а не конечным множеством. Затем мы определим унарную функцию Φ^* , называемую *сверткой* Φ , следующим образом. Пусть $F_0, \dots, F_{k-1}$ — последовательность, полученная из Φ заменой каждой функции ее сверткой и каждого предиката сверткой его представляющей функции, тогда

$$\Phi^*(a) = \langle F_0(a), \dots, F_{k-1}(a) \rangle.$$

Очевидно,

$$F_i(x) = (\Phi^*(x))_i.$$

Эти равенства показывают, что функция Φ^* рекурсивна в $F_0, \dots, F_{k-1}$ и что каждая функция F_i рекурсивна в Φ^* . Из формул свертывания следует, что каждый член из Φ рекурсивен в $F_0, \dots, F_{k-1}$ и что каждая функция F_i рекурсивна в Φ . Комбинируя эти факты с леммой о транзитивности, получаем, что Φ^* рекурсивна в Φ , и наоборот. Тогда по лемме о транзитивности функции, рекурсивные в Φ , — это в точности функции, рекурсивные в Φ^* ; аналогичные утверждения справедливы для рекурсивных частичных функционалов, рекурсивно перечислимых отношений и т. д.

Лемма о замене. Частичный функционал F рекурсивен в конечной последовательности Φ тогда и только тогда, когда существует такой рекурсивный частичный функционал F' , что $F(\mathfrak{A}) \simeq F'(\Phi^*, \mathfrak{A})$ для всех $\mathfrak{A}$. Отношение R рекурсивно перечисливо в конечной последовательности Φ тогда и только тогда, когда существует такое рекурсивно перечислимое отношение R' , что $R(\mathfrak{A}) \leftrightarrow R'(\Phi^*, \mathfrak{A})$ для всех $\mathfrak{A}$.

Доказательство. Если такой функционал F' существует, то явное определение

$$F(\mathfrak{A}) \simeq F'(\lambda x \Phi^*(x), \mathfrak{A})$$

показывает, что функционал F рекурсивен в Φ^* и, следовательно, в Φ . Утверждение «тогда» во второй части леммы доказывается аналогично.

Теперь мы докажем утверждение «только тогда» для случая, когда F является всюду определенной функцией. Так как F рекурсивна в Φ^* , то мы можем воспользоваться индукцией по функциям, рекурсивным в Φ^* . Рассматривая правило $R0_{\Phi^*}$, заметим, что

$$\Phi^*(a) = \text{Ap}(\Phi^*, a).$$

Доказательство для правила $R1_{\Phi^*}$ тривиально. Так как правила $R2_{\Phi^*}$ и $R3_{\Phi^*}$ рассматриваются аналогично, то мы рассмотрим лишь последнее из них. Предположим, что функция F определена следующим образом: $F(a) = \mu x (G(a, x) = 0)$. По индуктивному предположению

$$G(a, x) = G'(\Phi^*, a, x)$$

для некоторого рекурсивного частичного функционала G' . Определяя F' следующим образом:

$$F'(\alpha, a) \simeq \mu x (G'(\alpha, a, x) = 0),$$

мы получаем, что $F(a) = F'(\Phi^*, a)$.

Предположим теперь, что R рекурсивно перечисливо в Φ , и пусть

$$R(\mathfrak{A}) \leftrightarrow \exists x R(\bar{\mathfrak{A}}(x), x),$$

где R рекурсивно в Φ . Выберем рекурсивный функционал F' так, что

$$K_R(a, x) = F'(\Phi^*, a, x).$$

Тогда

$$\begin{aligned} R(\mathfrak{A}) &\leftrightarrow \exists x (F'(\Phi^*, \bar{\mathfrak{A}}(x), x) = 0) \\ &\leftrightarrow \exists x \mathfrak{G}_{F'}(\Phi^*, \bar{\mathfrak{A}}(x), x, 0). \end{aligned}$$

Определяя R' следующим образом:

$$R'(\alpha, \mathfrak{A}) \leftrightarrow \exists x \mathfrak{G}_{F'}(\alpha, \bar{\mathfrak{A}}(x), x, 0),$$

мы убеждаемся, что R' рекурсивно перечисливо и $R(\mathfrak{A}) \leftrightarrow R'(\Phi^*, \mathfrak{A})$.

Наконец, пусть F — частичный функционал, рекурсивный в Φ . Пользуясь только что доказанным результатом и тем, что рекурсивно перечислимые отношения имеют род Σ_1^0 , мы получаем, что

$$\mathcal{G}_F(\mathcal{A}, a) \leftrightarrow \exists x R'(\Phi^*, \mathcal{A}, a, x),$$

где R' — рекурсивное отношение. Тогда вследствие (1) из § 7.2 имеем

$$F(\mathcal{A}) \simeq (\mu z R'(\Phi^*, \mathcal{A}, (z)_0, (z)_1))_0;$$

поэтому мы можем определить F' следующим образом:

$$F'(\alpha, \mathcal{A}) \simeq (\mu z R'(\alpha, \mathcal{A}, (z)_0, (z)_1))_0.$$

Следствие 1. Частичное отношение R рекурсивно в конечной последовательности Φ тогда и только тогда, когда существует такое рекурсивное частичное отношение R' , что $R(\mathcal{A}) \approx R'(\Phi^*, \mathcal{A})$ для всех $\mathcal{A}$.

Следствие 2. Отношение R является арифметическим отношением рода Σ_n^0 (Π_n^0) в конечной последовательности Φ тогда и только тогда, когда существует такое арифметическое отношение R' рода Σ_n^0 (Π_n^0), что $R(\mathcal{A}) \leftrightarrow R'(\Phi^*, \mathcal{A})$ для всех $\mathcal{A}$.

Доказательство. В случае Σ_1^0 это следует из теоремы (потому что Σ_1^0 означает то же самое, что и рекурсивно перечислимое). Затем мы получаем случай Π_1^0 , используя отрицания. Оставшиеся случаи получаются из этих двух навешиванием кванторов.

Замечание. Подобные утверждения неверны для рекурсивных всюду определенных функционалов, рекурсивных всюду определенных отношений и отношений рода Δ_n^0 ; см. задачи 11 (г) и 21 (б).

Теперь мы используем понятие относительной рекурсивности, чтобы охарактеризовать предикаты рода Δ_n^0 при $n > 1$.

Лемма. Предикат R имеет род Σ_{n+1}^0 тогда и только тогда, когда он рекурсивно перечислим в множестве предикатов рода Π_n^0 .

Доказательство. Если R имеет род Σ_{n+1}^0 , то $R(a) \leftrightarrow \exists x Q(a, x)$, где Q имеет род Π_n^0 , поэтому R рекурсивно перечислим в множестве предикатов рода Π_n^0 . Теперь предположим, что R рекурсивно перечислим в указанном множестве. Формулы свертывания показывают, что свертка

предиката рода Π_n^0 имеет род Π_n^0 и что каждый предикат рекурсивен в своей свертке. Таким образом, R рекурсивно перечислим в множестве унарных предикатов рода Π_n^0 и по лемме о конечности — в некоторой конечной последовательности Φ таких предикатов. Пусть Φ состоит из предикатов $R_1, \dots, R_k$, и пусть Q_i является графиком K_{R_i} . Тогда

$$Q_i(a, b) \leftrightarrow (R_i(a) \& b = 0) \vee (\neg R_i(a) \& b = 1),$$

поэтому Q_i имеет род Σ_{n+1}^0 вследствие A1—A6. Далее,

$$\begin{aligned} \mathcal{G}_{\Phi^*}(a, b) \leftrightarrow b = \\ = \langle (b)_0, \dots, (b)_{k-1} \rangle \& Q_1(a, (b)_0) \& \dots \& Q_k(a, (b)_{k-1}); \end{aligned}$$

поэтому $\mathcal{G}_{\Phi^*}$ имеет род Σ_{n+1}^0 .

По лемме о замене существует такой рекурсивный предикат M , что

$$\begin{aligned} R(\mathcal{A}) \leftrightarrow \exists x M(\overline{\Phi^*}(x), a, x) \\ \leftrightarrow \exists x \exists y (y = \overline{\Phi^*}(x) \& M(y, a, x)) \\ \leftrightarrow \exists x \exists y (\text{Seq}(y) \& \text{lh}(y) = \\ = x \& \forall z < x \mathcal{G}_{\Phi^*}(z, (y)_z) \& M(y, a, x)). \end{aligned}$$

Следовательно, по A1—A6 R имеет род Σ_{n+1}^0 .

Комбинируя лемму с релятивизованной теоремой об отрицании, мы получаем такой результат.

Теорема Поста. Предикат имеет род Δ_{n+1}^0 тогда и только тогда, когда он рекурсивен в множестве предикатов рода Π_n^0 .

Используя A5 и то, что каждый из предикатов R и $\neg R$ рекурсивен в другом, мы видим, что в теореме Поста Π_n^0 можно заменить на Σ_n^0 .

Пусть Φ — конечная последовательность. Число f является индексом (m, n) -арного частичного функционала F по Φ , если для всех $\mathcal{A}$

$$F(\mathcal{A}) \simeq \{f\}^{m+1, n}(\Phi^*, \mathcal{A}). \quad (1)$$

Вследствие теоремы о нормальной форме и леммы о замене частичный функционал рекурсивен в Φ тогда и только тогда, когда он имеет некоторый индекс по Φ . Каждое число f является индексом по Φ единственного (m, n) -арного функционала F , а именно, того F , который определен в (1). Этот функционал F обозначим через $\{f\}^\Phi$.

Пусть снова Φ — конечная последовательность. Число p является *RE-индексом* (m, n) -арного отношения P по Φ , если для всех $\mathfrak{A}$

$$P(\mathfrak{A}) \leftrightarrow W_p^{m+1, n}(\Phi^*, \mathfrak{A}).$$

Тогда отношение является рекурсивно перечислимым в Φ в том и только в том случае, когда оно имеет некоторый *RE-индекс* по Φ . И снова каждое число p является *RE-индексом* по Φ единственного отношения; это отношение мы обозначим через W_p^Φ .

Мы имеем

$$\begin{aligned} \{f\}^\Phi(\mathfrak{A}, a) &\simeq \{S_{m+1, n, k}(f, a)\}^\Phi(\mathfrak{A}), \\ W_p^\Phi(\mathfrak{A}, a) &\leftrightarrow W_{S_{m+1, n, k}^\Phi}^\Phi(p, a)(\mathfrak{A}). \end{aligned}$$

Далее мы можем сформулировать релятивизованный вариант теоремы о рекурсии.

Частичный функционал называется *функционально рекурсивным*, если он рекурсивен в множестве всех всюду определенных функций. Аналогично мы определяем *функционально рекурсивное* частичное отношение и понятия *функционально рекурсивно перечислимого* и *функционально арифметического* отношения. Отношение имеет род Σ_n^0 , если оно имеет род Σ_n^0 в множестве всех функций; аналогично мы определяем отношения рода Π_n^0 и Δ_n^0 . Очевидно, каждая функция функционально рекурсивна и каждый предикат функционально рекурсивен.

Предположим, что F — функционально рекурсивный (m, n) -арный частичный функционал. По лемме о конечности F рекурсивен в некоторой конечной последовательности Φ . Пусть f — индекс F по Φ , а α — функция, определенная равенствами $\alpha(0) = f$, $\alpha(n+1) = \Phi^*(n)$. Тогда

$$F(\mathfrak{A}) \simeq \{\alpha(0)\}^{m+1, n}(\lambda x \alpha(x+1), \mathfrak{A}). \quad (2)$$

Функциональным индексом функционала F мы называем такую унарную функцию α , что (2) выполняется для всех $\mathfrak{A}$. Так как определенный в (2) функционал F рекурсивен в α и потому функционально рекурсивен, то мы видим, что частичный функционал функционально рекурсивен тогда и только тогда, когда он имеет некоторый функциональный индекс. Каждая унарная функция α является индексом единственного (m, n) -арного частичного

функционала F , а именно, того функционала F , который определен в (2). Этот функционал F мы обозначаем через $\{\alpha\}^{m, n}$ или, проще, через $\{\alpha\}$.

Из (2) следует, что

$$\{\alpha\}^{m, n}(\mathfrak{A}) \simeq U(\mu z T_{m+1, n}(\alpha(0), \lambda x \alpha(x+1), \mathfrak{A}, z)).$$

Определим рекурсивный функционал $T_{m, n}$ следующим образом:

$$T_{m, n}(\alpha, \mathfrak{A}, z) \leftrightarrow T_{m+1, n}(\alpha(0), \lambda x \alpha(x+1), \mathfrak{A}, z).$$

Тогда

$$\{\alpha\}^{m, n}(\mathfrak{A}) \simeq U(\mu z T_{m, n}(\alpha, \mathfrak{A}, z)). \quad (3)$$

Функциональным RE-индексом отношения P мы назовем такую функцию α , что для всех $\mathfrak{A}$

$$P(\mathfrak{A}) \leftrightarrow \exists z T_{m, n}(\alpha, \mathfrak{A}, z).$$

Используя доказательство теоремы о нумерации, мы покажем, что отношение функционально рекурсивно перечислимо тогда и только тогда, когда оно имеет некоторый функциональный RE-индекс.

Если P является $(m+1, n)$ -арным отношением, то мы для каждой функции α определим (m, n) -арное отношение $P_{(\alpha)}$ следующим образом:

$$P_{(\alpha)}(\mathfrak{A}) \leftrightarrow P(\mathfrak{A}, \alpha).$$

Мы говорим, что P *функционально перечисляет* класс отношений, состоящий из $P_{(\alpha)}$.

Теперь мы можем получить аналог теоремы об арифметическом перечислении для случая функциональной перечислимости. Отсюда мы получим аналог теоремы об арифметической иерархии для $(1, 0)$ -арных отношений. (Разумеется, мы не можем получить подобный аналог для унарных предикатов, так как каждый предикат функционально рекурсивен.)

Лемма о проекции. Если $F_{(\alpha)}$ функционально рекурсивен для каждого α , то F функционально рекурсивен.

Доказательство. Пусть α_a является функциональным индексом $F_{(\alpha)}$ для каждого α ; выберем α так, что $(\alpha)_a = \alpha_a$ для всех α . Определим рекурсивный функционал G следующим образом:

$$G(\beta, \mathfrak{A}, a) \simeq \{(\beta)_a\}(\mathfrak{A}).$$

Тогда

$$\begin{aligned} F(\mathbb{N}, a) &\simeq F_{(a)}(\mathbb{N}) \\ &\simeq \{\alpha_a\}(\mathbb{N}) \\ &\simeq G(\alpha, \mathbb{N}, a). \end{aligned}$$

Таким образом, F рекурсивен в α , а отсюда и по лемме о замене он функционально рекурсивен.

Лемма о проекциях обобщается на функционально рекурсивные частичные отношения, потому что $(K_p)_{(a)}$ является представляющим частичным функционалом для $P_{(a)}$. Она обращается также на отношения рода Σ_n^0 (в частности, на функционально рекурсивно перечислимые отношения), отношения рода Π_n^0 и отношения рода Δ_n^0 , а потому и на функционально арифметические отношения. Например, предположим, что $P_{(a)}$ имеет род Σ_2^0 для всех a . Тогда

$$P_{(a)}(\mathbb{N}) \leftrightarrow \exists x \forall y R_a(\mathbb{N}, x, y),$$

где R_a функционально рекурсивно. Определим

$$R(\mathbb{N}, x, y, a) \leftrightarrow R_a(\mathbb{N}, x, y).$$

Тогда $R_{(a)} = R_a$ функционально рекурсивно для каждого a , поэтому R функционально рекурсивно. Также имеем

$$P(\mathbb{N}, a) \leftrightarrow \exists x \forall y R(\mathbb{N}, x, y, a);$$

поэтому P имеет род Σ_2^0 .

7.7. Степени

Пусть Φ — множество всех всюду определенных функций и предикатов. Мы говорим, что два элемента из Φ эквивалентны, если каждый из них рекурсивен в другом. Пользуясь леммой о транзитивности, мы легко проверим, что это отношение эквивалентности. Классы эквивалентности называются *степенями рекурсивной неразрешимости* или просто *степенями*. Для обозначения степеней мы пользуемся полужирными строчными латинскими буквами.

Грубо говоря, два элемента из Φ эквивалентны, если их одинаково трудно вычислять. Таким образом, степень функции или предиката является мерой трудности их вычисления.

Очевидно, P эквивалентен K_P и F эквивалентна $\mathfrak{G}_F$. Следовательно, каждая степень содержит и функцию и предикат. Формулы свертывания показывают, что каждая функция и каждый предикат эквивалентны своей свертке, поэтому каждая степень содержит унарную функцию и множество. По этой причине мы часто имеем дело только с множествами.

Пусть a и b — степени; запись $a \leq b$ означает, что существуют множество A в a и множество B в b такие, что A рекурсивно в B . Если это так, то по лемме о транзитивности любая функция и любой предикат из a рекурсивен в любой функции и любом предикате из b . Подбываясь этим, а также леммой о транзитивности, мы легко проверим, что $\leq$ обладает основными свойствами частичного порядка:

$$\begin{aligned} a &\leq a, \\ a \leq b \rightarrow b \leq a &\rightarrow a = b, \\ a \leq b \rightarrow b \leq c &\rightarrow a \leq c. \end{aligned}$$

Мы пишем $a < b$, если $a \leq b$ и $a \neq b$.

Очевидно, множество всех рекурсивных функций и предикатов является степенью, эту степень мы обозначим через 0 . Для любых a мы имеем $0 \leq a$; это значит, что 0 является наименьшей степенью.

Мы говорим, что a *рекурсивно перечислима* в b , если существуют множество A в a и множество B в b такие, что A рекурсивно перечислимо в B . В таком случае по лемме о транзитивности A рекурсивно перечислимо в каждом множестве из b . Степень a *рекурсивно перечислима*, если она рекурсивно перечислима в 0 , иначе говоря, если она содержит некоторое рекурсивно перечислимое множество. Если a рекурсивно перечислима в b и $b \leq c$, то a рекурсивно перечислима в c по лемме о транзитивности. В частности, каждая рекурсивно перечислимая степень рекурсивно перечислима в любой степени.

Среди рекурсивно перечислимых в a степеней имеется наибольшая. Действительно, пусть A — множество из a , и пусть

$$B(a) \leftrightarrow \exists x T_{1,1}((a)_0, K_A, (a)_1, x).$$

Тогда степень b , содержащая B , рекурсивно перечислима в a . Мы покажем, что среди таких степеней она является

наибольшей. Пусть c рекурсивно перечислима в a . В таком случае c содержит множество C , которое рекурсивно перечислимо в A . По релятивизованной теореме о нумерации существует такое e , что для любых a

$$\begin{aligned} C(a) &\leftrightarrow \exists x T_{1,1}(e, K_A, a, x) \\ &\leftrightarrow B(\langle e, a \rangle). \end{aligned}$$

Таким образом, C рекурсивно в B ; следовательно, $c \leq b$.

Наибольшая рекурсивно перечислимая в a степень называется *скачком* a и обозначается через a' . Таким образом, $0'$ является наибольшей рекурсивно перечислимой степенью. Если $a \leq b$, то a' рекурсивно перечислима в a и, следовательно, в b , поэтому $a' \leq b'$. Так как каждое множество, рекурсивное в A , рекурсивно перечислимо в A , но не наоборот (вследствие релятивизованной теоремы об арифметической иерархии), то мы имеем $a < a'$. Отсюда следует, что не существует наибольшей степени.

Сказанное выше наводит на два вопроса. Первый: является ли множество степеней линейно упорядоченным? Второй, известный как проблема Поста: существуют ли рекурсивно перечислимые степени, отличные от 0 и $0'$? Сейчас мы докажем теорему, отвечающую на оба вопроса.

Теорема Фридберга — Мучника. *Существуют такие рекурсивно перечислимые множества A и B , что A не рекурсивно в B и B не рекурсивно в A .*

Предположим, что теорема верна, и пусть a и b — степени, содержащие A и B соответственно. Тогда неверно как $a \leq b$, так и $b \leq a$, поэтому множество степеней не является линейно упорядоченным. Так как для каждой рекурсивно перечислимой степени c $0 \leq c \leq 0'$, то a и b являются рекурсивно перечислимыми степенями, отличными от 0 и $0'$, этим решается проблема Поста.

Вначале мы дадим общую схему доказательства. Мы будем строить A и B по этапам. На каждом этапе мы либо ничего не будем делать, либо добавим в точности одно число в A или в B . По данному n можно будет в точности установить, что происходит на n -м шаге. Вследствие этого A и B будут позитивно вычислимыми, а потому и рекурсивно перечислимыми.

Чтобы быть уверенным, что B не рекурсивно в A , мы должны быть уверены, что K_B отлична от всех $\{e\}^A$.

Наша идея состоит в следующем. Мы непрерывно стараемся вычислить $\{e\}^A(x_{2e})$ для некоторого числа x_{2e} . Если нам это удастся и значением будет 1, то мы относим x_{2e} к множеству B . Таким образом, $K_B(x_{2e}) = 0$ тогда и только тогда, когда $\{e\}^A(x_{2e}) \simeq 1$, поэтому K_B отлично от $\{e\}^A$. Аналогично, мы гарантируем, что K_A отлично от $\{e\}^B$, относя некоторое число x_{2e+1} к множеству A тогда и только тогда, когда $\{e\}^B(x_{2e+1}) \simeq 1$.

Трудностью в проведении этой идеи является то, что на n -м этапе нам еще не известно множество A , а известно только конечное множество A_n чисел, которые были отнесены к A до n -го этапа. Поэтому мы пытаемся вычислить $\{e\}^{A_n}(x_{2e})$; если это нам удастся и значение равно 1, то мы относим x_{2e} к множеству B . Однако неприятность заключается в том, что позже мы можем отнести к множеству A еще несколько чисел и, таким образом, изменить значение $\{e\}^A(x_{2e})$ на 0; тогда мы получим $\{e\}^A(x_{2e}) = K_B(x_{2e})$. Мы можем исправить положение, допуская, что x_e может измениться. При вычислении

$$\{e\}^{A_n}(x_{2e}) = 1$$

мы используем только конечное число значений функции K_{A_n} . Пусть y больше любого из значений этих аргументов. Если мы никогда в дальнейшем не будем относить к множеству A числа, меньшие y , то всё будет в порядке. Далее, к множеству A причисляются лишь числа x_{2f+1} . Следовательно, мы просто изменяем все числа x_{2f+1} так, чтобы они были больше y .

Имеется еще одно затруднение. x_e может изменять свое значение бесконечное число раз, так что мы никогда не решим, какое же значение x_e нам взять. Мы обойдем это затруднение, изменив нашу процедуру; если мы относим x_{2e} к B , то мы изменяем x_{2f+1} только в том случае, если $2f+1 > 2e$. Таким образом, x_{2f+1} может изменять значение только из-за конечного числа значений x_{2e} , где $2e < 2f+1$, поэтому оно изменяет свое значение только конечное число раз. Но что можно сказать о x_{2f+1} , где $2f+1 < 2e$, которое мы не изменяем? Если x_{2f+1} никогда не будет отнесено к A , то это не приведет ни к каким трудностям. Если же оно отнесено к A , то мы одновременно изменяем x_{2e} , потому что $2e > 2f+1$. Таким образом, тот факт, что мы для прежних значений

x_{2e} можем иметь $\{e\}^A(x_{2e}) = K_B(x_{2e})$, не имеет никакого значения.

Теперь мы приведем доказательство. Если $F(\alpha, e, a) \simeq \{e\}^\alpha(a)$, то F рекурсивен, поэтому $\mathfrak{G}_F$ рекурсивно перечислим и потому имеет род Σ_1^0 . Согласно (6) из § 7.5 существует такой рекурсивный предикат R , что

$$\{e\}^\alpha(a) \simeq b \leftrightarrow \exists y R(\bar{\alpha}(y), e, a, b).$$

Множества A_n и B_n и функции F_n мы определим индукцией по n . ($F_n(e)$ будет значением x_e до n -го этапа.) В качестве A_0 и B_0 мы возьмем пустые множества и положим $F_0(e) = 2^e$. Теперь предположим, что A_n, B_n и F_n уже выбраны. Допустим вначале, что $(n)_0$ четно, например, $(n)_0 = 2e$. Мы ищем такое число y , что

$$y < n \text{ \& } R(\bar{K}_{A_n}(y), e, F_n(2e), 1) \text{ \& } F_n(2e) \notin B_n. \quad (1)$$

Если такого y не существует, то $A_{n+1} = A_n$, $B_{n+1} = B_n$, $F_{n+1} = F_n$. В противном случае мы выберем среди таких y наименьшее. Отнесем $F_n(2e)$ к B_{n+1} и положим

$$F_{n+1}(2f+1) = 3^{y+1} \cdot F_n(2f+1)$$

для $2f+1 > 2e$. Во всем остальном A_{n+1}, B_{n+1} и F_{n+1} совпадают с A_n, B_n и F_n . Теперь предположим, что $(n)_0$ нечетно, например, что $(n)_0 = 2f+1$. Тогда мы опять поступаем так, как написано выше, меняя местами A и B и $f, 2e$ и $2f+1$.

Мы утверждаем, что $K_{A_n}(x)$, $K_{B_n}(x)$ и $F_n(x)$ являются рекурсивными функциями от n и x . Это очевидно вследствие тезиса Чёрча. Простейший способ дать точное доказательство — положить $G(n, x) = \langle K_{A_n}(x), K_{B_n}(x), F(x) \rangle$ и определить G с помощью теоремы о рекурсии. Мы предоставляем это читателю.

Теперь мы покажем, что для каждого e значение $F_n(e)$ изменяется только конечное число раз. Доказательство ведется индукцией по e . Если $F_{n+1}(e) \neq F_n(e)$, то мы имеем $F_n(f) \in A_{n+1}$ и $F_n(f) \notin A_n$ для некоторого $f < e$. (Это верно для четного e ; если e нечетно, то мы должны поменять местами A и B .) По индуктивному предположению число значений $F_n(f)$, где $f < e$, конечно. Следовательно, $F_n(e)$ может изменяться только конечное число раз.

Пусть A — объединение всех A_n , а B — объединение всех B_n . Так как

$$A(x) \leftrightarrow \exists n (K_{A_n}(x) = 0)$$

и аналогичное выражение верно для B , то A и B рекурсивно перечислимы. Пусть x_e — заключительное значение $F_n(e)$. Мы покажем, что $x_{2e} \in B$ тогда и только тогда, когда $\{e\}^A(x_{2e}) \simeq 1$. Это доказывает, что B не рекурсивно в A , а симметричное рассуждение доказывает, что A не рекурсивно в B .

Предположим, что $\{e\}^A(x_{2e}) \simeq 1$. Тогда существует такое y , что

$$R(\bar{K}_A(y), e, x_{2e}, 1).$$

Далее, существует бесконечно много n , для которых $(n)_0 = 2e$. Выберем одно из этих n такое, что $n > y$, $F_n(2e) = x_{2e}$ и $\bar{K}_{A_n}(y) = \bar{K}_A(y)$. Тогда либо x_{2e} принадлежит B_n , либо оно отнесено к B_{n+1} . Следовательно, $x_{2e} \in B$.

Теперь предположим, что $x_{2e} \notin B$. Выберем такое n , что $x_{2e} \in B_{n+1}$ и $x_{2e} \notin B_n$. Тогда мы получим, что $(n)_0 = 2e$ и $F_n(e) = x_{2e}$ и (1) будет истинно для некоторого y . (Мы воспользовались тем, что $F_n(e)$ всегда имеет вид $2^e 3^z$ и потому для разных e принимает разные значения.) Если $\bar{K}_{A_n}(y) = \bar{K}_A(y)$, то из (1) следует, что $\{e\}^A(x_{2e}) \simeq 1$. В противном случае существует такое число z , что $z < y$ и $K_{A_n}(z) \neq K_A(z)$. Это означает, что существует такое $m > n$, что $z \in A_{m+1}$, $z \notin A_m$. Тогда мы имеем

$$(m)_0 = 2f+1 \text{ и } z = F_m(2f+1).$$

Если при этом $2f+1 > 2e$, то мы получим

$$z = F_m(2f+1) \geq F_{n+1}(2f+1) = 3^{y+1} \cdot F_n(2f+1) > y,$$

т. е. противоречие. Следовательно, $2f+1 < 2e$, поэтому

$$F_{m+1}(2e) > F_m(2e) \geq F_n(2e) = x_{2e}.$$

Однако это невозможно по определению x_{2e} .

С помощью развитой выше техники могут быть доказаны многие другие утверждения о степенях, однако мы не будем здесь этим заниматься.

7.8. Аналитическая иерархия

Теперь мы изучим результат навешивания кванторов по функциональным переменным на рекурсивные отношения.

Отношение P называется *аналитическим*, если оно имеет явное определение вида

$$P(\mathfrak{A}) \leftrightarrow Q_1 \dots Q_k R(\mathfrak{A}, \mathfrak{B}), \quad (1)$$

где отношение R рекурсивное, а $Q_1, \dots, Q_k$ — кванторы, по одному на каждую переменную из $\mathfrak{B}$.

Мы говорим, что два квантора имеют *одинаковый вид*, если они оба являются кванторами существования или оба являются кванторами всеобщности. Мы говорим, что два квантора имеют *одинаковый тип*, если они оба связывают функциональные переменные или оба связывают числовые переменные.

Теперь предположим, что мы имеем определение вида (1), и перечислим некоторые упрощения, которые можно делать в цепочке кванторов $Q_1 \dots Q_k$. В каждом случае подразумевается, что упрощение требует замены отношения R новым рекурсивным отношением (как это было при свертывании кванторов в арифметическом случае).

(i) Числовой квантор может быть заменен функциональным квантором того же вида.

Это следует из эквивалентностей

$$\exists x P(x) \leftrightarrow \exists \alpha P(\alpha(0)),$$

$$\forall x P(x) \leftrightarrow \forall \alpha P(\alpha(0)).$$

(ii) Два смежных квантора одинакового вида и типа могут быть заменены одним квантором того же вида и типа.

Для числовых кванторов это является свертыванием кванторов. Для функциональных кванторов мы пользуемся тем же методом, заменяя $(a)_i$ на $(\alpha)_i$.

(iii) Если функциональный квантор следует непосредственно за числовым квантором, то он может быть переставлен вперед этого числового квантора.

Это следует из эквивалентностей

$$\exists x \exists \alpha P(\alpha, x) \leftrightarrow \exists \alpha \exists x P(\alpha, x),$$

$$\forall x \forall \alpha P(\alpha, x) \leftrightarrow \forall \alpha \forall x P(\alpha, x),$$

$$\forall x \exists \alpha P(\alpha, x) \leftrightarrow \exists \alpha \forall x P((\alpha)_x, x),$$

$$\exists x \forall \alpha P(\alpha, x) \leftrightarrow \forall \alpha \exists x P((\alpha)_x, x).$$

Первые две из них очевидны, а две другие доказываются так же, как (4) и (5) из § 7.5.

Приставка $Q_1 \dots Q_k$ в (1) называется *нормализованной*, если $k \geq 2$, $Q_1, \dots, Q_{k-1}$ — функциональные кванторы, а Q_k — числовой квантор и все кванторы чередуются по видам. Мы покажем, что, исходя из определения (1), в котором имеется хотя бы один функциональный квантор, мы можем упростить приставку до нормализованной приставки. Сначала мы переставим все функциональные кванторы вперед согласно (iii). Если теперь найдутся числовые кванторы того же вида, что и последний функциональный квантор, то мы элиминируем каждый из этих кванторов, начиная с первого, следующим образом: мы заменяем этот квантор функциональным квантором согласно (i), переносим его вперед всех числовых кванторов согласно (iii) и свертываем его с последним функциональным квантором согласно (ii). Теперь все числовые кванторы находятся в конце и все имеют вид, противоположный виду последнего функционального квантора. Если же таких числовых кванторов не найдется, то мы добавим в конце фиктивный числовой квантор вида, противоположного виду последнего функционального квантора. Если мы теперь выполним все возможные свертывания согласно (ii), то получим нормализованную приставку. Заметим, что мы могли бы получить тот же самый конечный результат, если бы мы поступили следующим образом: вычеркнули все числовые кванторы, выполнили все возможные свертывания согласно (ii) и присоединили в конце новый числовой квантор вида, противоположного виду последнего функционального квантора.

Отношение имеет род $\Sigma_n^1(\Pi_n^1)$ при $n \geq 1$, если оно удовлетворяет определению (1), в котором приставка нормализована, число функциональных кванторов равно n и первым стоит квантор существования (всеобщности). Отсюда мы видим, что каждое аналитическое отношение либо является арифметическим, либо имеет род Σ_n^1 или Π_n^1 при некотором n . Эта классификация аналитических отношений называется *аналитической иерархией*.

Теперь мы приведем аналоги утверждений A1 — A6. Если при этом не дается доказательства, то это доказательство такое же, как и в арифметическом случае.

Y1. Если отношение P — арифметическое, то P имеет род Σ_n^1 и Π_n^1 для каждого n . Если P имеет род Σ_m^1 или Π_m^1 , то P имеет род Σ_n^1 и Π_n^1 для каждого $n > m$.

Доказательство. Используется добавление фиктивных кванторов с последующим упрощением, как это было показано ранее. Так, если P — отношение рода Σ_2^1 , то

$$\begin{aligned} P(\mathfrak{A}) &\leftrightarrow \exists \alpha \forall \beta \exists x R(\mathfrak{A}, \alpha, \beta, x) \\ &\leftrightarrow \forall \gamma \exists \alpha \forall \beta \exists x R(\mathfrak{A}, \alpha, \beta, x) \\ &\leftrightarrow \exists \alpha \forall \beta \exists \gamma \exists x R(\mathfrak{A}, \alpha, \beta, x). \end{aligned}$$

После упрощения вторая строка показывает, что P — отношение рода Π_3^1 , а третья строка показывает, что P — отношение рода Σ_3^1 .

Y2. Если Q — отношение рода Σ_n^1 (Π_n^1), а $F_1, \dots, F_r, G_1, \dots, G_k$ — рекурсивные функционалы, то отношение P , определенное следующим образом: $P(\mathfrak{A}) \leftrightarrow Q(\lambda x F_1(\mathfrak{A}, x), \dots, \lambda x F_r(\mathfrak{A}, x), G_1(\mathfrak{A}), \dots, G_k(\mathfrak{A}))$, имеет род Σ_n^1 (Π_n^1).

Y3. Если Q — отношение рода Σ_n^1 , а отношение P определено следующим образом: $P(\mathfrak{A}) \leftrightarrow \exists \alpha Q(\mathfrak{A}, \alpha)$, то P имеет род Σ_n^1 . Если отношение Q — отношение рода Π_n^1 , а отношение P определено следующим образом: $P(\mathfrak{A}) \leftrightarrow \forall \alpha Q(\mathfrak{A}, \alpha)$, то P имеет род Π_n^1 .

Y4. Если P и Q — отношения рода Σ_n^1 (Π_n^1), то $P \vee Q$ и $P \& Q$ — отношения рода Σ_n^1 (Π_n^1).

Y5. Если P — отношение рода Σ_n^1 (Π_n^1), то $\neg P$ — отношение рода Π_n^1 (Σ_n^1).

Y6. Если P — отношение рода Σ_n^1 (Π_n^1), а отношения Q и R определены следующим образом: $Q(\mathfrak{A}) \leftrightarrow \exists x P(\mathfrak{A}, x)$ и $R(\mathfrak{A}) \leftrightarrow \forall x P(\mathfrak{A}, x)$, то Q и R — отношения рода Σ_n^1 (Π_n^1).

Доказательство. Проводится при помощи упрощения, как это описано выше.

Отметим, что из Y6 следует аналогичный результат для ограниченных кванторов, так как мы можем переписать $\exists x_{x < b} P(\mathfrak{A}, x)$ и $\forall x_{x < b} P(\mathfrak{A}, x)$ как $\exists x (x < b \& P(\mathfrak{A}, x))$ и $\forall x (x < b \rightarrow P(\mathfrak{A}, x))$.

Если P имеет род Π_1^1 , то $P(\mathfrak{A}) \leftrightarrow \forall \alpha Q(\mathfrak{A}, \alpha)$, где Q имеет род Σ_1^1 . Поэтому вследствие (6) из § 7.5 P определяется формулой

$$P(\mathfrak{A}) \leftrightarrow \forall \alpha \exists x R(\bar{\alpha}(x), \mathfrak{A}), \quad (2)$$

где R рекурсивно. Аналогично, применяя (7) из § 7.5, мы видим, что любое отношение P рода Σ_1^1 определяется

формулой

$$P(\mathfrak{A}) \leftrightarrow \exists \alpha \forall x R(\bar{\alpha}(x), \mathfrak{A}), \quad (3)$$

где R рекурсивно.

Теми же самыми методами, что и в арифметическом случае, можно доказать теорему об аналитическом перечислении и теорему об аналитической иерархии. Мы предоставляем это читателю.

Отношение имеет род Δ_n^1 , если оно имеет как род Σ_n^1 , так и род Π_n^1 . Вследствие Y5 P имеет род Δ_n^1 тогда и только тогда, когда как P , так и $\neg P$ имеют род Σ_n^1 , и тогда и только тогда, когда как P , так и $\neg P$ имеют род Π_n^1 .

Мы определим понятие *аналитичности* в Φ , рода Σ_n^1 в Φ , рода Π_n^1 в Φ и рода Δ_n^1 в Φ с помощью обычного метода определения релятивизованных понятий. Например, отношение P является аналитическим в Φ , если оно определяется формулой вида (1), где отношение R рекурсивно в Φ . Утверждение, что каждое аналитическое отношение является арифметическим, либо имеет род Σ_n^1 или Π_n^1 для некоторого n , обобщается на релятивизованный случай по образцу Y1 — Y6. Теорема об аналитическом перечислении и теорема об аналитической иерархии обобщаются при условии, что Φ — конечная последовательность. При этом условии истинны также лемма о транзитивности и лемма о конечности. Лемма о замене истинна для понятий аналитичности в Φ , рода Σ_n^1 в Φ и рода Π_n^1 в Φ (но не для рода Δ_n^1 в Φ).

Отношение P называется *проективным* (отношением рода Σ_n^1 , Π_n^1 , Δ_n^1), если оно аналитично (имеет род Σ_n^1 , Π_n^1 , Δ_n^1) в множестве всех функций. Мы можем обобщить теорему об аналитическом перечислении и теорему об аналитической иерархии на этот случай, пользуясь функциональной перечислимостью точно так же, как и в арифметическом случае. Лемма о проекциях обобщается на все эти понятия. Следствием является то, что если мы определим P следующим образом:

$$P(\mathfrak{A}) \leftrightarrow \exists x Q_x(\mathfrak{A}),$$

где каждое Q_x — отношение рода Σ_n^1 (Π_n^1), то P — отношение рода Σ_n^1 (Π_n^1). Действительно, если мы определим Q

следующим образом:

$$Q(\mathbb{N}, x) \leftrightarrow Q_x(\mathbb{N}),$$

то по лемме о проекциях Q — отношение рода $\Sigma_n^1(\Pi_n^1)$, а затем мы можем применить У6.

7.9. Гиперарифметические отношения

Теорема об отрицании говорит нам, что отношения рода Δ_1^1 , для определения которых, казалось бы, требуются кванторы, на самом деле рекурсивны и потому могут быть определены без кванторов. Это наводит на мысль поискать такую характеристику отношений рода Δ_1^1 , которая показывает, что эти отношения, для определения которых, казалось бы, требуются кванторы по функциям, могут на самом деле быть определены без кванторов. Вначале можно было бы предположить, что отношения рода Δ_1^1 — это в точности арифметические отношения; однако оказывается, что арифметические отношения образуют собственный подкласс отношений рода Δ_1^1 . Чтобы получить действительную характеристику отношений рода Δ_1^1 , мы должны обобщить арифметическую иерархию.

Так как любое отношение является подмножеством множества $N_{m,n}$, то мы можем выполнять теоретико-множественные операции над отношениями. Таким образом, А4 и А5 могут рассматриваться как правила, показывающие, что получается из арифметических отношений при взятии объединений, пересечений и дополнений. Кроме того, каждое отношение рода $\Sigma_{n+1}^0(\Pi_{n+1}^0)$ является объединением (пересечением) счетного числа отношений рода $\Pi_n^0(\Sigma_n^0)$. Например, если P — отношение рода Σ_{n+1}^0 , то существует такое отношение Q рода Π_n^0 , что

$$\begin{aligned} P(\mathbb{N}) &\leftrightarrow \exists x Q(\mathbb{N}, x) \\ &\leftrightarrow \exists x Q_{(x)}(\mathbb{N}). \end{aligned}$$

Таким образом, P является объединением отношений $Q_{(x)}$, а $Q_{(x)}$ — отношение рода Π_n^0 , потому что $Q_{(x)}(\mathbb{N}) \leftrightarrow Q(\mathbb{N}, x)$. Тем не менее только очень простые объединения и пересечения счетного числа арифметических отношений являются арифметическими. Например, каждое множество является объединением счетного числа конечных, а потому рекурсивных множеств.

Мы будем получать гиперарифметические отношения, отправляясь от рекурсивно перечислимых отношений и неоднократно беря дополнения и некоторые объединения счетного числа множеств. Чтобы описать эти объединения, мы сопоставим каждому гиперарифметическому отношению некоторый индекс. Тогда если A является рекурсивно перечислимым множеством индексов, то мы берем объединение тех отношений, индексы которых принадлежат A .

Три следующие правила образуют обобщенное индуктивное определение H -индекса:

11. $\langle 0, e \rangle$ является H -индексом для каждого e .

12. Если e является H -индексом, то $\langle 1, e \rangle$ является H -индексом.

13. Если каждое число из $W_e^{0,1}$ является H -индексом, то $\langle 2, e \rangle$ является H -индексом.

Для каждого H -индекса i мы определяем (m, n) -арное отношение $J_i^{m,n}$ следующим образом. Если $i = \langle 0, e \rangle$, то $J_i^{m,n}$ есть $W_e^{m,n}$. Если $i = \langle 1, e \rangle$, где e — некоторый H -индекс, то $J_i^{m,n}$ есть $\neg J_e^{m,n}$. Если $i = \langle 2, e \rangle$, где каждое число из $W_e^{0,1}$ является H -индексом, то $J_i^{m,n}$ является объединением отношений $J_x^{m,n}$, где x принадлежит $W_e^{0,1}$, т. е.

$$J_i^{m,n}(\mathbb{N}) \leftrightarrow \exists x (W_e^{0,1}(x) \& J_x^{m,n}(\mathbb{N})). \quad (1)$$

Нам надо показать, что это является законным методом определения $J_i^{m,n}$. Чтобы определить эти отношения, очевидно, достаточно определить для каждого m и n множество $\Phi_{m,n}$ пар $(i, J_i^{m,n})$. Теперь три части приведенного выше определения могут рассматриваться как три правила в обобщенном индуктивном определении множества $\Phi_{m,n}$. Например, правилом, соответствующим случаю $i = \langle 2, e \rangle$, является следующее: если $i = \langle 2, e \rangle$ является некоторым H -индексом, если (x, P_x) принадлежит $\Phi_{m,n}$ для каждого x из $W_e^{0,1}$ и если P является объединением всех P_x , то (i, P) принадлежит $\Phi_{m,n}$.

(m, n) -арное отношение P является гиперарифметическим, если $P = J_i^{m,n}$ для некоторого H -индекса i ; при этом всякое такое i называется H -индексом отношения P .

Теперь мы установим некоторые правила получения гиперарифметических отношений и H -индексов таких отно-

шений. Если это не вносит путаницы, то мы опускаем верхние индексы у W_e и J_i .

Н1. Если R — рекурсивно перечислимый предикат, то существует такая рекурсивная функция F , что

$$J_{F(a)}(\mathfrak{A}) \leftrightarrow \exists x (R(x, a) \& J_x(\mathfrak{A}))$$

всякий раз, когда a такова, что для каждого x из $R(x, a)$ следует, что x является H -индексом.

Доказательство. Выберем e так, что R есть W_e . Имеем

$$W_{S(e, a)}(x) \leftrightarrow W_e(x, a).$$

Полагая $F(a) = \langle 2, S(e, a) \rangle$, мы для a , описанного в Н1, имеем

$$\begin{aligned} J_{F(a)}(\mathfrak{A}) &\leftrightarrow \exists x (W_{S(e, a)}(x) \& J_x(\mathfrak{A})) \\ &\leftrightarrow \exists x (R(x, a) \& J_x(\mathfrak{A})). \end{aligned}$$

Н2. Пусть $F_1, \dots, F_r, G_1, \dots, G_k$ — рекурсивные функционалы. Тогда существует такая рекурсивная функция H , что для каждого H -индекса i

$$\begin{aligned} J_{H(i, a)}(\mathfrak{A}) &\leftrightarrow J_i(\lambda x F_1(\mathfrak{A}, a, x), \dots \\ &\dots, \lambda x F_r(\mathfrak{A}, a, x), G_1(\mathfrak{A}, a), \dots, G_k(\mathfrak{A}, a)). \end{aligned}$$

Доказательство. Сначала мы докажем эквивалентность, замечая, какие свойства H необходимы, а затем мы определим H , обладающую этими свойствами.

Доказательство эквивалентности мы будем вести индукцией по H -индексам. Вместо множества аргументов у J_i в правой части эквивалентности мы будем писать ... Тогда $W_e(\dots)$ является рекурсивно перечислимым отношением от аргументов $\mathfrak{A}, a, e$ по А1. Следовательно, по (8) из § 7.4 существует такая рекурсивная функция L , что

$$W_{L(a, e)}(\mathfrak{A}) \leftrightarrow W_e(\dots).$$

Тогда, если $i = \langle 0, e \rangle$, то

$$\begin{aligned} J_i(\dots) &\leftrightarrow W_{L(a, e)}(\mathfrak{A}) \\ &\leftrightarrow J_{\langle 0, L(a, e) \rangle}(\mathfrak{A}). \end{aligned}$$

Следовательно, чтобы получить эквивалентность $J_{H(i, a)}(\mathfrak{A}) \leftrightarrow J_i(\dots)$ в этом случае, достаточно иметь

$$H(i, a) = \langle 0, L(a, (i)_1) \rangle, \text{ если } (i)_0 = 0. \quad (2)$$

Пусть теперь $i = \langle 1, e \rangle$. Тогда, используя индуктивное предположение, мы получаем

$$\begin{aligned} J_i(\dots) &\leftrightarrow \neg J_e(\dots) \\ &\leftrightarrow \neg J_H(e, a)(\mathfrak{A}) \\ &\leftrightarrow J_{\langle 1, H(e, a) \rangle}(\mathfrak{A}). \end{aligned}$$

Следовательно, в этом случае достаточно иметь

$$H(i, a) = \langle 1, H((i)_1, a) \rangle, \text{ если } (i)_0 = 1. \quad (3)$$

Теперь пусть $i = \langle 2, e \rangle$. Тогда, пользуясь индуктивным предположением, мы получаем

$$\begin{aligned} J_i(\dots) &\leftrightarrow \exists x (W_e(x) \& J_x(\dots)) \\ &\leftrightarrow \exists x (W_e(x) \& J_H(x, a)(\mathfrak{A})) \\ &\leftrightarrow \exists y (\exists x (W_e(x) \& H(x, a) = y) \& J_y(\mathfrak{A})). \end{aligned}$$

Пусть h — некоторый индекс функции H . Тогда из сказанного выше следует, что

$$J(\dots) \leftrightarrow \exists y (\exists x (W_e(x) \& \{h\}(x, a) = y) \& J_y(\mathfrak{A})).$$

Далее, $\exists x (W_e(x) \& \{h\}(x, a) = y)$ является рекурсивно перечислимым предикатом от аргументов y, e, h, a . Следовательно, по Н1 существует такая рекурсивная функция K (не зависящая от H и h), что

$$J_i(\dots) \leftrightarrow J_{K(e, h, a)}(\mathfrak{A}).$$

Таким образом, в этом случае достаточно получить

$$H(i, a) = K((i)_1, h, a), \text{ если } (i)_0 > 1. \quad (4)$$

Остается определить такую рекурсивную функцию H с индексом h , что (2), (3) и (4) выполняются. По теореме о рекурсии мы можем так определить рекурсивную частичную функцию H с индексом h , что (2), (3) и (4) выполняются, если $=$ заменено на $\simeq$. Далее, вследствие (8) из § 6.4 мы имеем в (3) $(i)_1 < i$. Пользуясь этим, легко доказать индукцией по i , что $H(i, a)$ определена для всех i и a . Это завершает доказательство.

Н3. Существует такая рекурсивная функция F , что $J_{F(i)}$ есть $\neg J_i$ для всех H -индексов i . Существует такая рекурсивная функция G , что $J_{G(i, j)}$ есть $J_i \vee J_j$ для всех H -индексов i и j . Существуют аналогичные функции для $\rightarrow$, $\&$ и $\leftrightarrow$.

Доказательство. Мы можем положить $F(i) = \langle 1, i \rangle$. Далее,

$$(J_i \vee J_j)(\mathcal{A}) \leftrightarrow \exists x ((x=i \vee x=j) \& J_x(\mathcal{A})).$$

Отсюда и по Н1 мы получаем G . Остальные функции получаются, если воспользоваться определениями $\rightarrow$, $\&$ и $\leftrightarrow$ в терминах $\neg$ и $\vee$. Например, функция H для $\rightarrow$ определена следующим образом: $H(i, j) = G(F(i), j)$.

Н4. Существуют такие рекурсивные функции H и K , что

$$\begin{aligned} J_{H(i)}(\mathcal{A}) &\leftrightarrow \exists x J_i(\mathcal{A}, x), \\ J_{K(i)}(\mathcal{A}) &\leftrightarrow \forall x J_i(\mathcal{A}, x) \end{aligned}$$

для каждого H -индекса i .

Доказательство. По Н2 существует такая рекурсивная функция G , что $J_{G(i, x)}(\mathcal{A}) \leftrightarrow J_i(\mathcal{A}, x)$. Тогда

$$\begin{aligned} \exists x J_i(\mathcal{A}, x) &\leftrightarrow \exists x J_{G(i, x)}(\mathcal{A}) \\ &\leftrightarrow \exists y (\exists x (y = G(i, x)) \& J_y(\mathcal{A})). \end{aligned}$$

Затем нужную функцию H мы получим по Н1. Чтобы получить K , положим $K(i) = F(H(F(i)))$, где F — такая же, как и в Н3.

Н5. Каждое арифметическое отношение является гиперарифметическим.

Доказательство. Индукцией по n мы покажем, что каждое отношение рода Σ_n^0 или Π_n^0 является гиперарифметическим. Любое отношение рода Σ_1^0 является рекурсивно перечислимым и, следовательно, гиперарифметическим, поэтому любое отношение рода Π_1^0 является гиперарифметическим по Н3. Шаг от n к $n+1$ следует из Н4.

Замечание. Обращение Н5 ложно; см. задачу 22.

Так как определение гиперарифметичности использует RE -индексы, то мы не можем для произвольного множества Φ получить релятивизованный вариант этого определения, поэтому мы сначала рассмотрим конечную последовательность Φ . Мы определим H -индекс по Φ и J_i^Φ для H -индекса i по Φ так же, как и прежде, за исключением того, что W_e заменено на W_e^Φ . Мы говорим, что P является гиперарифметическим в Φ , если существует такое i , что P есть J_i^Φ ; тогда всякое такое i называется H -индексом отношения P по Φ . Затем мы можем релятивизовать Н1 — Н5.

Пусть теперь Φ является некоторым классом всюду определенных функций и отношений. Мы говорим, что P является гиперарифметическим в Φ , если оно является гиперарифметическим в некоторой конечной последовательности элементов из Φ . Отношение называется борелевским, если оно является гиперарифметическим в классе всех функций.

7.10. Теорема характеристики

Теперь мы можем перейти к характеристизации отношений рода Δ_1^1 .

Пусть $J(i, \mathcal{A})$ означает, что i есть H -индекс и что имеет место $J_i(\mathcal{A})$. (Мы опускаем верхние индексы.) Мы хотим получить явное определение для J .

Пусть $Q(\mathcal{A}, \alpha, \beta, e)$ — конъюнкция утверждений

$$\begin{aligned} \alpha(\langle 0, e \rangle) &= 0, \\ \beta(\langle 0, e \rangle) &= 0 \leftrightarrow W_e(\mathcal{A}), \\ \alpha(e) &= 0 \rightarrow \alpha(\langle 1, e \rangle) = 0, \\ \alpha(\langle 1, e \rangle) &= 0 \rightarrow (\beta(\langle 1, e \rangle) = 0 \leftrightarrow \beta(e) \neq 0), \\ \forall x (W_e(x) \rightarrow \alpha(x) = 0) &\rightarrow \alpha(\langle 2, e \rangle) = 0, \\ \alpha(\langle 2, e \rangle) &= 0 \rightarrow (\beta(\langle 2, e \rangle) = 0 \leftrightarrow \exists x (W_e(x) \& \beta(x) = 0)). \end{aligned}$$

Покажем, что

$$\begin{aligned} J(i, \mathcal{A}) &\leftrightarrow \forall \alpha \forall \beta (\forall e Q(\mathcal{A}, \alpha, \beta, e) \rightarrow \\ &\rightarrow \alpha(i) = 0 \& \beta(i) = 0). \end{aligned} \quad (1)$$

Предположим, что имеет место $J(i, \mathcal{A})$. Пусть α и β таковы, что выполняется $\forall e Q(\mathcal{A}, \alpha, \beta, e)$. Пользуясь индукцией по H -индексам, мы получим, что $\alpha(j) = 0$ и $\beta(j) = 0 \leftrightarrow J_j(\mathcal{A})$ для каждого H -индекса j . Полагая $j = i$, мы убеждаемся, что $\alpha(i) = \beta(i) = 0$. Теперь предположим, что правая часть (1) истинна. Пусть α — представляющая функция множества H -индексов, и пусть β — представляющая функция множества таких H -индексов j , что справедливо $J_j(\mathcal{A})$. Очевидно, что $Q(\mathcal{A}, \alpha, \beta, e)$ для всех e ; следовательно, по предположению $\alpha(i) = \beta(i) = 0$. Вследствие этого имеем $J(i, \mathcal{A})$.

Так как отношение Q — арифметическое, то вследствие (1) J — отношение рода Π_1^1 . Если i есть H -индекс, то $J_i(\mathcal{A}) \leftrightarrow J(i, \mathcal{A})$ для всех $\mathcal{A}$ и, следовательно, J_i — отно-

шение рода Π_1^1 . Таким образом, каждое гиперарифметическое отношение имеет род Π_1^1 . Если отношение P — гиперарифметическое, то и отношение $\neg P$ — гиперарифметическое, поэтому P и $\neg P$ оба имеют род Π_1^1 . Отсюда получается

Лемма 1. *Каждое гиперарифметическое отношение имеет род Δ_1^1 .*

Номер последовательности $\langle a_1, \dots, a_n \rangle$ называется *расширением* номера последовательности $\langle b_1, \dots, b_m \rangle$, если $n \geq m$ и $a_i = b_i$ при $i = 1, \dots, m$. Если к тому же $n > m$, то мы говорим, что $\langle a_1, \dots, a_n \rangle$ — собственное расширение $\langle b_1, \dots, b_m \rangle$. Мы будем писать $a <^* b$, если a — собственное расширение b .

Очевидно,

$$a <^* b \rightarrow b <^* c \rightarrow a <^* c. \quad (2)$$

Предикат $<^*$ рекурсивен, так как он имеет явное определение

$$a <^* b \leftrightarrow \text{Seq}(a) \& \exists x_{x < \text{lh}(a)} (b = \text{In}(a, x)).$$

Последовательностью, убывающей относительно $<^*$, называется такая бесконечная последовательность $a_0, a_1, \dots$, что $a_{n+1} <^* a_n$ для любого n . Множество A , состоящее из номеров последовательностей, называется *деревом*, если не существует последовательности, убывающей относительно $<^*$, все члены которой содержатся в A . Ясно, что каждое подмножество дерева является деревом.

Обозначим через SS класс представляющих функций множеств, состоящих из номеров последовательностей, а через Tr — класс представляющих функций деревьев. Оба они являются $(1, 0)$ -арными отношениями. Мы имеем явные определения

$$\begin{aligned} \text{SS}(\alpha) &\leftrightarrow \forall x (\alpha(x) \leq 1) \& \forall x (\alpha(x) = 0 \rightarrow \text{Seq}(x)), \\ \text{Tr}(\alpha) &\leftrightarrow \text{SS}(\alpha) \& \neg \exists \beta \forall x (\alpha(\beta(x)) = 0 \& \beta(x+1) <^* \beta(x)). \end{aligned}$$

Вследствие этого SS имеет род Π_1^1 , а Tr — род Π_1^1 .

Теорема о дереве. *Если P — отношение рода Π_1^1 , то существует такой рекурсивный функционал F , что для всех $\mathcal{A}$ имеем $\text{SS}(\lambda x F(\mathcal{A}, x))$ и*

$$P(\mathcal{A}) \leftrightarrow \text{Tr}(\lambda x F(\mathcal{A}, x)).$$

Доказательство. Вследствие (2) из § 7.8 существует такое рекурсивное отношение R , что

$$P(\mathcal{A}) \leftrightarrow \forall \alpha \exists x R(\bar{\alpha}(x), \mathcal{A}). \quad (3)$$

Пусть $U(\mathcal{A})$ — множество номеров последовательностей $\langle x_0, \dots, x_{n-1} \rangle$ таких, что

$$\neg R(\langle x_0, \dots, x_{i-1} \rangle, \mathcal{A}) \quad \text{для всех } i \leq n.$$

Мы утверждаем, что

$$\exists \alpha \forall x \neg R(\bar{\alpha}(x), \mathcal{A}) \leftrightarrow U(\mathcal{A}) \text{ не является деревом.} \quad (4)$$

Предположим, что верна левая часть, и выберем такое α , что $\neg R(\bar{\alpha}(x), \mathcal{A})$ для всех x . Тогда $\bar{\alpha}(0), \bar{\alpha}(1), \dots$ — убывающая последовательность из $U(\mathcal{A})$. Предположим теперь, что $a_0, a_1, \dots$ — убывающая последовательность из $U(\mathcal{A})$. По определению $<^*$ существует такая функция α , что каждая $\bar{\alpha}(x)$ имеет в качестве доопределения некоторое a_i . Так как a_i принадлежит $U(\mathcal{A})$, то мы имеем $\neg R(\bar{\alpha}(x), \mathcal{A})$.

Если в (4) мы перенесем знак отрицания вперед при помощи пренексных операций, возьмем отрицание обеих частей и воспользуемся (3), то получим

$$P(\mathcal{A}) \leftrightarrow U(\mathcal{A}) \text{ является деревом.}$$

Поэтому достаточно выбрать такой рекурсивный функционал F , что $\lambda x F(\mathcal{A}, x)$ — представляющая функция $U(\mathcal{A})$. Такой функционал определяется следующим образом:

$$F(\mathcal{A}, x) = \begin{cases} 0, & \text{если } \text{Seq}(x) \& \forall i \leq \text{lh}(x) \neg R(\text{In}(x, i), \mathcal{A}), \\ 1 & \text{в остальных случаях.} \end{cases}$$

Если A — множество номеров последовательностей и a принадлежит A , то $A_{[a]}$ — множество таких b из A , что $b <^* a$. Вследствие (2)

$$b \in A_{[a]} \rightarrow A_{[a][b]} = A_{[b]}. \quad (5)$$

Мы также определим

$$\alpha_{[a]}(b) = \begin{cases} \alpha(b), & \text{если } b <^* a \& \alpha(a) = 0, \\ 1 & \text{в остальных случаях.} \end{cases}$$

Тогда если α — представляющая функция множества A и a принадлежит A , то $\alpha_{[a]}$ — представляющая функция множества $A_{[a]}$. Заметим, что $\alpha_{[a]}$ есть $\lambda x F(\alpha, a, x)$ для неко-

торого рекурсивного функционала F и поэтому может использоваться в явных определениях рекурсивных частичных функционалов и отношений.

Далее мы будем предполагать, что читатель знаком с элементарными свойствами ординалов. (Весь необходимый материал можно найти в главе 9.) Для обозначения ординалов мы используем буквы σ , τ и ρ .

Для каждого ординала σ мы при помощи трансфинитной индукции по σ определим класс $\text{ТО}(\sigma)$ множеств номеров последовательностей. Множество номеров последовательностей A принадлежит $\text{ТО}(\sigma)$, если $A_{[a]}$ принадлежит $\text{ТО}(\tau)$ для некоторого $\tau < \sigma$ и для каждого a из A . Ясно, что

$$\sigma \leq \tau \rightarrow \text{ТО}(\sigma) \subset \text{ТО}(\tau). \quad (6)$$

Теперь мы покажем, что множество принадлежит некоторому $\text{ТО}(\sigma)$ тогда и только тогда, когда оно является деревом. Докажем сначала при помощи трансфинитной индукции по σ , что каждое множество из $\text{ТО}(\sigma)$ является деревом. Предположим, что некоторое множество A из $\text{ТО}(\sigma)$ имеет убывающую последовательность $a_0, a_1, \dots$. Тогда $A_{[a_0]}$ принадлежит $\text{ТО}(\tau)$ для некоторого $\tau < \sigma$ и вследствие (2) $a_1, a_2, \dots$ — убывающая последовательность из $A_{[a_0]}$. Это противоречит индуктивному предположению.

Теперь предположим, что A не принадлежит ни одному $\text{ТО}(\sigma)$. Мы покажем, что A — не дерево, определив индуктивно такую убывающую последовательность $a_0, a_1, \dots$ из A , что каждое $A_{[a_n]}$ не принадлежит ни одному $\text{ТО}(\sigma)$. Предположим, что a_i выбрано при $i < n$. Пусть $B = A$, если $n = 0$, и пусть $B = A_{[a_{n-1}]}$ в противном случае. Вследствие (5) достаточно так выбрать a_n из B , что $B_{[a_n]}$ не принадлежит ни одному $\text{ТО}(\sigma)$. Если это невозможно, то для каждого a из B существует такое σ_a , что $B_{[a]} \in \text{ТО}(\sigma_a)$. Выбирая σ больше любого из σ_a , мы получим, что $B \in \text{ТО}(\sigma)$; это противоречит тому, что B не принадлежит ни одному $\text{ТО}(\sigma)$.

Если A — дерево, то наименьший ординал σ такой, что $A \in \text{ТО}(\sigma)$, называется *ординалом дерева* A и обозначается через $\|A\|$. Запись $\|A\| \leq \sigma$ означает, что A — дерево и $\|A\| \leq \sigma$, аналогично используется запись $\|A\| < \sigma$. Тогда

$$A \in \text{ТО}(\sigma) \leftrightarrow \|A\| \leq \sigma. \quad (7)$$

То, что из левой части следует правая, очевидно. Если A — дерево, то $A \in \text{ТО}(\|A\|)$; поэтому если $\|A\| \leq \sigma$, то $A \in \text{ТО}(\sigma)$ вследствие (6). Из (7) и из определения ТО мы получаем

$$\|A\| \leq \sigma \leftrightarrow \forall x (A(x) \rightarrow \|A_{[x]}\| < \sigma) \quad (8)$$

для каждого множества A номеров последовательностей. Отсюда следует, что если A — дерево, то

$$A(x) \rightarrow \|A_{[x]}\| < \|A\|. \quad (9)$$

Мы также имеем обратное к (9): если A — дерево, то

$$\sigma < \|A\| \rightarrow \exists x (A(x) \& \sigma = \|A_{[x]}\|). \quad (10)$$

Мы докажем это трансфинитной индукцией по $\|A\|$. Если $\sigma < \|A\|$, то вследствие (8) существует такое x , принадлежащее A , что $\sigma \leq \|A_{[x]}\|$. Если $\sigma = \|A_{[x]}\|$, то всё доказано. В противном случае $\sigma < \|A_{[x]}\| < \|A\|$ вследствие (9), поэтому по индуктивному предположению и вследствие (5) существует такое y , принадлежащее $A_{[x]}$, что $\sigma = \|A_{[x][y]}\| = \|A_{[y]}\|$.

Пусть A и B — множества номеров последовательностей. Отображение F множества A в B является *монотонным*, если для любых a и a' из A

$$a <^* a' \rightarrow F(a) <^* F(a').$$

Лемма 2. Пусть A — множество номеров последовательностей, а B — дерево. Тогда $\|A\| \leq \|B\|$ тогда и только тогда, когда существует монотонное отображение A в B .

Доказательство. Мы воспользуемся трансфинитной индукцией по $\|B\|$. Предположим, что F — монотонное отображение A в B . Если a принадлежит множеству A , то некоторое ограничение отображения F является монотонным отображением $A_{[a]}$ в $B_{[F(a)]}$, поэтому $\|A_{[a]}\| \leq \|B_{[F(a)]}\|$ вследствие (9) и индуктивного предположения. Отсюда, а также из (9) и (8) мы получаем $\|A\| \leq \|B\|$.

Теперь предположим, что $\|A\| \leq \|B\|$. Фиксируя a из A , мы вследствие (9) имеем $\|A_{[a]}\| < \|A\| \leq \|B\|$. Вследствие (10) для некоторого b из B справедливо $\|A_{[a]}\| = \|B_{[b]}\|$. Вследствие (9) и индуктивного предположения существует монотонное отображение F_a множества $A_{[a]}$ в $B_{[b]}$, а потому и в B . Если мы положим $F_a(a) = b$, то F_a будет монотонным отображением A_a в B , где A_a — множество расширений a , принадлежащих A .

Элемент из A называется *максимальным*, если он не является собственным расширением никакого элемента из A . Очевидно, каждый элемент из A принадлежит A_a для единственного максимального элемента a из A . Следовательно, существует такое отображение F множества A в B , что для каждого максимального элемента a ограничение F на A_a есть F_a . Если a и a' — различные максимальные элементы, то никакой элемент из A_a не может быть расширением элемента из $A_{a'}$. Отсюда следует, что F монотонно.

Если α — представляющая функция дерева A , то вместо $\|A\|$ мы пишем $\|\alpha\|$. Мы пишем $\|\alpha\| \leq \sigma$ или $\|\alpha\| < \sigma$, подразумевая, что $\bar{\alpha}$ — представляющая функция дерева.

Следствие. *Существуют такие отношения $T \leq$ и $T <$ рода Σ_1^1 , что если $\text{Tr}(\beta)$, то*

$$T \leq (\alpha, \beta) \leftrightarrow \|\alpha\| \leq \|\beta\|$$

и

$$T < (\alpha, \beta) \leftrightarrow \|\alpha\| < \|\beta\|.$$

Доказательство. Согласно лемме мы можем положить

$$T \leq (\alpha, \beta) \leftrightarrow SS(\alpha) \& \exists \gamma (\forall x (\alpha(x) = 0 \rightarrow \beta(\gamma(x)) = 0) \& \forall x \forall y (\alpha(x) = 0 \rightarrow \alpha(y) = 0 \rightarrow x <^* y \rightarrow \gamma(x) <^* \gamma(y))).$$

Вследствие (10) мы можем положить

$$T < (\alpha, \beta) \leftrightarrow \exists x (\beta(x) = 0 \& T \leq (\alpha, \beta_{[x]})).$$

Оба отношения имеют род Σ_1^1 вследствие Y1 — Y6.

Ординал σ называется *рекурсивным*, если $\sigma = \|A\|$ для некоторого рекурсивного дерева A . Каждый ординал, меньший некоторого рекурсивного ординала, рекурсивен. Действительно, пусть $\tau < \sigma = \|A\|$, где A — рекурсивное дерево. Вследствие (10) $\tau = \|A_{[a]}\|$ для некоторого a из A . Однако $A_{[a]}$ — рекурсивное дерево, так как

$$A_{[a]}(x) \leftrightarrow A(x) \& x <^* a.$$

Первый нерекурсивный ординал обозначается через k . Согласно только что доказанному утверждению ординал рекурсивен тогда и только тогда, когда он меньше k .

Замечание. Мы имеем $\omega < k$. Чтобы это доказать, обозначим через A множество всех таких $\langle a_1, \dots, a_n \rangle$,

что $a_1 > a_2 > \dots > a_n$. Легко заметить, что A — дерево, и оно рекурсивно, потому что

$$A(a) \leftrightarrow \text{Seq}(a) \& \forall i < \text{lh}(a) \forall j < i ((a)_i < (a)_j).$$

Фиксируя n , положим $a_i = \langle n, n-1, \dots, i \rangle$ для $i \leq n$. Тогда a_i принадлежит A и

$$a_0 <^* a_1 <^* \dots <^* a_n.$$

Вследствие (9) и (5)

$$\|A_{[a_0]}\| < \|A_{[a_1]}\| < \dots < \|A_{[a_n]}\| < \|A\|.$$

Отсюда следует, что $n < \|A\|$. Так как это верно при всех n , то отсюда следует, что $\omega \leq \|A\| < \kappa$.

Для каждого σ мы определяем

$$\begin{aligned} \text{Tr}_\sigma(\alpha) &\leftrightarrow \|\alpha\| \leq \sigma, \\ \text{Tr}'_\sigma(\alpha) &\leftrightarrow \|\alpha\| < \sigma. \end{aligned}$$

Вследствие (8)

$$\text{Tr}_\sigma(\alpha) \leftrightarrow SS(\alpha) \& \forall x (\alpha(x) = 0 \rightarrow \text{Tr}'_\sigma(\alpha_{[x]})).$$

Отсюда и из H1 — H5 следует, что существует такая рекурсивная функция L , что если Tr'_σ есть J_i , то Tr_σ есть $J_{L(i)}$.

Лемма 3. *Если σ рекурсивен, то отношения Tr'_σ и Tr_σ гиперарифметические.*

Доказательство. Из только что доказанного утверждения следует, что нам достаточно рассмотреть лишь Tr'_σ . Пусть A — такое рекурсивное дерево, что $\sigma = \|A\|$, и пусть для x из A ординал $\sigma_x = \|A_{[x]}\|$. Вследствие (9) и (10)

$$\text{Tr}'_\sigma(\alpha) \leftrightarrow \exists x (A(x) \& \text{Tr}_{\sigma_x}(\alpha)).$$

Мы покажем, что существует такая рекурсивная функция F , что для каждого x из A отношение Tr_{σ_x} есть $J_{F(x)}$. Отсюда будет следовать, что

$$\begin{aligned} \text{Tr}'_\sigma(\alpha) &\leftrightarrow \exists x (A(x) \& J_{F(x)}(\alpha)) \\ &\leftrightarrow \exists y (\exists x (A(x) \& F(x) = y) \& J_y(\alpha)). \end{aligned}$$

Поэтому отношение Tr'_σ гиперарифметическое по H1.

Сначала трансфинитной индукцией по σ_x мы докажем, что Tr_{σ_x} есть $J_{F(x)}$, замечая, какие свойства F необходимы, а затем мы определим F с этими свойствами. Вследствие (9), (10) и (5) ординалами, меньшими σ_x , являются σ_y для y из A и $y <^* x$. Следовательно,

$$\text{Tr}'_{\sigma_x}(\alpha) \leftrightarrow \exists y (A(y) \& y <^* x \& J_{F(y)}(\alpha))$$

по индуктивному предположению. Если f — индекс функции F , то мы можем записать

$$\text{Tr}'_{\sigma_x}(\alpha) \leftrightarrow \exists z (\exists y (A(y) \& y <^* x \& \{f\}(y) = z) \& J_z(\alpha)).$$

По Н1 отсюда следует, что существует такая рекурсивная функция M (не зависящая от F и f), что

$$\text{Tr}'_{\sigma_x}(\alpha) \leftrightarrow J_{M(f, x)}(\alpha).$$

Если L та же, что и раньше, то

$$\text{Tr}_{\sigma_x}(\alpha) \leftrightarrow J_{L(M(f, x))}(\alpha).$$

Следовательно, чтобы заключить, что Tr_{σ_x} есть $J_{F(x)}$, достаточно иметь $F(x) = L(M(f, x))$. Теперь, пользуясь теоремой о рекурсии, мы можем определить такую рекурсивную частичную функцию F с индексом f , что

$$F(x) \simeq L(M(f, x))$$

для всех x . Так как функции L и M — всюду определенные, то функция F также всюду определена и $F(x) = L(M(f, x))$.

Теорема ограниченности. Если P — подкласс рода Σ_1^1 класса Tr , то существует такой рекурсивный ординал σ , что P — подмножество множества Tr_σ .

Доказательство. Мы предположим, что такого σ не существует, и докажем, что каждый унарный предикат Q рода Π_1^1 имеет род Σ_1^1 ; это будет противоречить теореме об аналитической иерархии. По теореме о дереве существует такая рекурсивная функция F , что

$$Q(a) \leftrightarrow \text{Tr}(\lambda x F(a, x)). \quad (11)$$

Мы покажем, что

$$Q(a) \leftrightarrow \exists \alpha (P(\alpha) \& T_{\leq}(\lambda x F(a, x), \alpha)),$$

отсюда будет следовать, что Q — предикат рода Σ_1^1 .

Предположим, что имеет место $Q(a)$. Тогда вследствие (11) получаем $\text{Tr}(\lambda x F(a, x))$. Пусть $\sigma = \|\lambda x F(a, x)\|$. Так как F рекурсивна, то ординал σ рекурсивен, поэтому в P существует такая α , что $\neg \text{Tr}_\sigma(\alpha)$. Тогда мы имеем $\text{Tr}(\alpha)$ и $\sigma \leq \|\alpha\|$, поэтому $T_{\leq}(\lambda x F(a, x), \alpha)$. Теперь предположим, что в P существует такая α , что $T_{\leq}(\lambda x F(a, x), \alpha)$. Тогда $\text{Tr}(\alpha)$ и, следовательно, $\text{Tr}(\lambda x F(a, x))$. Следовательно, по (11) выполняется $Q(a)$.

Пусть P , Q и R — (m, n) -арные отношения. Мы говорим, что P и Q не пересекаются, если $\neg (P(\mathfrak{A}) \& Q(\mathfrak{A}))$ для

всех $\mathfrak{A}$. Мы говорим, что R отделяет P от Q , если $P(\mathfrak{A}) \rightarrow R(\mathfrak{A})$ для всех $\mathfrak{A}$ и R и Q не пересекаются; очевидно, отсюда следует, что P и Q не пересекаются.

Теорема делимости (Лузин — Аддисон). Если P и Q — непересекающиеся отношения рода Σ_1^1 , то существует гиперарифметическое отношение R , отделяющее P от Q .

Доказательство. По теореме о дереве существует такой рекурсивный функционал F , что

$$\neg Q(\mathfrak{A}) \leftrightarrow \text{Tr}(\lambda x F(\mathfrak{A}, x)).$$

Пусть S — класс всех $\lambda x F(\mathfrak{A}, x)$, где $\mathfrak{A}$ таково, что $P(\mathfrak{A})$. Так как P и Q не пересекаются, то S — подмножество множества Tr . Так как

$$S(\alpha) \leftrightarrow \exists \mathfrak{A} (P(\mathfrak{A}) \& \forall x (\alpha(x) = F(\mathfrak{A}, x))),$$

то S имеет род Σ_1^1 . По теореме ограниченности отсюда следует, что существует такой рекурсивный ординал σ , что S является подклассом класса Tr_σ . Мы определим R следующим образом:

$$R(\mathfrak{A}) \leftrightarrow \text{Tr}_\sigma(\lambda x F(\mathfrak{A}, x)).$$

Так как класс Tr_σ — гиперарифметический по лемме 3, то отношение R — гиперарифметическое. Если $P(\mathfrak{A})$, то $\lambda x F(\mathfrak{A}, x)$ принадлежит S и, следовательно, классу Tr_σ , поэтому $R(\mathfrak{A})$. Если $Q(\mathfrak{A})$, то $\lambda x F(\mathfrak{A}, x)$ не принадлежит множеству Tr и, следовательно, не принадлежит классу Tr_σ , поэтому $\neg R(\mathfrak{A})$. Таким образом, R отделяет P от Q .

Теорема характеристики (Суслин — Клини). Отношение имеет род Δ_1^1 тогда и только тогда, когда оно гиперарифметическое.

Доказательство. Если отношение P — гиперарифметическое, то оно имеет род Δ_1^1 по лемме 1. Если P — отношение рода Δ_1^1 , то P и $\neg P$ — непересекающиеся множества рода Σ_1^1 . По теореме делимости существует гиперарифметическое отношение R , отделяющее P от $\neg P$. Отсюда следует, что $R = P$, поэтому P — гиперарифметическое отношение.

Для любой конечной последовательности Φ мы можем релятивизовать все рассуждения этого параграфа. Из релятивизованной теоремы характеристики и леммы о конечности следует, что отношение имеет род Δ_1^1 тогда и только тогда, когда оно борелевское.

Получив такой аналог теоремы об отрицании, соблазнительно предположить истинность следующего аналога теоремы Поста: предикат имеет род Δ_{n+1}^1 тогда и только тогда, когда он является гиперарифметическим в классе предикатов рода Π_n^1 . Однако это неверно; предикаты, гиперарифметические в классе предикатов рода Π_n^1 , образуют собственный подкласс класса предикатов рода Δ_{n+1}^1 (задача 18). Известны некоторые полезные характеристики предикатов рода Δ_2^1 (см. задачу 27), однако при $n > 2$ подобные характеристики предикатов рода Δ_n^1 неизвестны.

7.11. Теоремы о базисе

Функция имеет род Σ_n^i (Π_n^i , Δ_n^i), если ее график имеет род Σ_n^i (Π_n^i , Δ_n^i) (где $i=1$ или $i=0$). Далее, для любой всюду определенной функции F имеем

$$\neg \mathcal{G}_F(a, a) \leftrightarrow \exists x (x \neq a \& \mathcal{G}_F(a, x)).$$

Следовательно, если F — функция рода Σ_n^0 , то $\neg \mathcal{G}_F$ имеет род Σ_n^0 и потому F — функция рода Δ_n^0 , тогда как если F — функция рода Σ_n^1 или Π_n^1 , то $\neg \mathcal{G}_F$ имеет род Σ_n^1 или Π_n^1 соответственно и F — функция рода Δ_n^1 . По этой причине мы будем рассматривать только функции рода Δ_n^i .

Функция F имеет род Δ_1^0 тогда и только тогда, когда $\mathcal{G}_F$ рекурсивен (по теореме об отрицании), и, следовательно, тогда и только тогда, когда F рекурсивна. Функция F имеет род Δ_1^1 тогда и только тогда, когда $\mathcal{G}_F$ — гиперарифметический (по теореме характеристики); в этом случае мы говорим, что функция F — *гиперарифметическая*.

Нас интересует следующая проблема. Предположим, что P — некоторый класс унарных функций, т. е. некоторое $(1,0)$ -арное отношение. Предположим, что нам что-нибудь известно о классификации P в одной из иерархий. Что можно сказать о классификации функций из P ? Мы не можем надеяться узнать что-либо о всех функциях из P ; например, если P — множество всех функций, то P рекурсивно, однако некоторые элементы из P не имеют классификации. Самое большее, что мы можем надеяться доказать, — это что если P имеет простую классификацию, то некоторый элемент класса P имеет простую классификацию.

В соответствии с этим мы приходим к следующему определению. Класс B унарных функций*) называется *базисом* совокупности Φ классов унарных функций, если для каждого P из Φ

$$\exists \alpha P(\alpha) \rightarrow \exists \alpha (B(\alpha) \& P(\alpha)).$$

Пример. Класс функций, равных нулю везде, кроме конечного числа значений аргумента, является базисом совокупности функциональных классов рода Σ_1^0 (*). Действительно, предположим, что P есть непустой класс рода Σ_1^0 . Имеем $P(\alpha) \leftrightarrow \exists x R(\alpha(x))$ для некоторого R . Так как класс P — непустой, то существует такой номер последовательности s , что $R(s)$. Полагая $\alpha(x) = (s)_x$ при $x < \text{lh } s$ и $\alpha(x) = 0$ при $x \geq \text{lh } (s)$, мы получаем, что α принадлежит P .

Отметим, что если B является базисом совокупности функциональных классов рода Π_1^0 , то класс функций $(\gamma)_0$, где γ принадлежит B , является базисом совокупности функциональных классов рода Σ_1^1 . Действительно, пусть класс P имеет род Σ_1^1 и непуст. Тогда $P(\alpha) \leftrightarrow \exists \beta Q(\alpha, \beta)$, где Q имеет род Π_1^0 . Определим отношение R рода Π_1^0 следующим образом: $R(\gamma) \leftrightarrow Q((\gamma)_0, (\gamma)_1)$. Так как класс P непуст, то Q непуст, поэтому непустым является R . Таким образом, R содержит функцию γ из B , а $(\gamma)_0$ является функцией из P . Аналогичным способом мы убеждаемся, что если B является базисом совокупности функциональных классов рода Π_n^1 , то класс функций $(\gamma)_0$, где γ принадлежит B , является базисом совокупности функциональных классов рода Σ_{n+1}^1 .

Для произвольного класса функций P через I_P мы обозначим множество всех чисел $\bar{\alpha}(x)$, где α принадлежит P , а x произвольно. Оно имеет явное определение

$$I_P(a) \leftrightarrow \exists \alpha (P(\alpha) \& \bar{\alpha}(\text{lh}(a)) = a). \quad (1)$$

Лемма. Если P — непустой функциональный класс рода Π_1^0 , то P содержит функцию, рекурсивную в I_P .

Доказательство. Определим F индуктивно следующим образом:

$$F(n) \simeq \mu z I_P(F(n) * \langle z \rangle).$$

*) Термины «класс функций» и «функциональный класс» употребляются как синонимы ради удобства. — *Прим. ред.*

По R14F рекурсивна в I_P . Индукцией по n мы покажем, что $\bar{F}(n)$ определено и принадлежит I_P . Так как P непуст, то $\bar{F}(0) = \langle \rangle$ принадлежит I_P . Теперь предположим, что $\bar{F}(n)$ определено и принадлежит I_P . Тогда $\bar{F}(n) = \bar{\alpha}(n)$ для некоторого α из P . Так как

$$I_P(\bar{\alpha}(n+1)) \text{ и } \bar{\alpha}(n+1) = \bar{\alpha}(n) * \langle \alpha(n) \rangle,$$

то $F(n)$ определено и $I_P(\bar{F}(n) * \langle F(n) \rangle)$. Следовательно, $\bar{F}(n+1)$ определено и принадлежит I_P .

Остается показать, что F принадлежит P . Для некоторого предиката R мы имеем $P(\alpha) \leftrightarrow \forall x R(\bar{\alpha}(x))$. Очевидно, I_P является подмножеством множества R , поэтому $\forall x R(\bar{F}(x))$ и, следовательно, F принадлежит P .

Теорема Клини о базисе. *Класс функций, рекурсивных в классе всех предикатов рода Σ_1^1 , является базисом совокупности функциональных классов рода Π_1^0 и, следовательно, совокупности функциональных классов рода Σ_1^1 . Класс гиперарифметических функций не является базисом совокупности функциональных классов рода Π_1^0 .*

Доказательство. Если P имеет род Π_1^0 , то вследствие (1) I_P имеет род Σ_1^1 , поэтому первое утверждение следует из леммы. Чтобы доказать второе утверждение, достаточно показать, что класс H всех гиперарифметических функций не является базисом совокупности функциональных классов рода Σ_1^1 . Так как $\neg H$ непуст и не содержит элементов из H , то достаточно показать, что $\neg H$ имеет род Σ_1^1 , или, что равносильно, что H имеет род Π_1^1 . Для этого мы воспользуемся явным определением

$$H(\alpha) \leftrightarrow \exists i \forall x \forall y ((\alpha(x) = y \rightarrow J(i, x, y)) \& \& (\alpha(x) \neq y \rightarrow J(\langle 1, i \rangle, x, y))). \quad (2)$$

(Отметим, что из правой части следует, что i является H -индексом, потому что она означает, что $J(i, x, y)$ дл некоторых x и y .)

Мы также можем применить наши соображения к классам множеств. Чтобы не вводить новую терминологию, мы вместо этих классов рассматриваем классы представляющих функций множеств, т. е. унарных функций, значениями которых являются только 0 и 1. В качестве переменных, изменяющихся на множестве таких функций мы используем строчные греческие буквы со звездочкой

Лемма бесконечности (Брауэр — Кёниг). *Для любого предиката P*

$$\exists \alpha^* \forall x P(\bar{\alpha}^*(x)) \leftrightarrow \forall n \exists \alpha^* \forall x_{x \leq n} P(\bar{\alpha}^*(x)).$$

Доказательство. Очевидно, что из левой части вытекает правая. Предположим, что правая часть истинна. Пусть A — такое множество номеров последовательностей $\langle a_0, \dots, a_n \rangle$, что $a_i \leq 1$ и $P(\langle a_0, \dots, a_i \rangle)$ для всех $i \leq n$. Индукцией по x мы так определим $\alpha^*(x)$, что $\bar{\alpha}^*(x)$ для всех x имеет бесконечно много расширений в A ; отсюда следует, что $\forall x P(\bar{\alpha}^*(x))$. Из правой части эквивалентности следует, что $\bar{\alpha}^*(0) = \langle \rangle$ имеет бесконечно много расширений в A . Теперь предположим, что $\bar{\alpha}^*(x)$ определено и имеет бесконечно много расширений в A . Каждое собственное расширение $\bar{\alpha}^*(x)$ в A есть расширение либо $\bar{\alpha}^*(x) * \langle 0 \rangle$, либо $\bar{\alpha}^*(x) * \langle 1 \rangle$. Отсюда следует, что при подходящем выборе $\bar{\alpha}^*(x)$

$$\bar{\alpha}^*(x+1) = \bar{\alpha}^*(x) * \langle \alpha(x) \rangle$$

имеет бесконечно много расширений в A .

Следствие. *Если P имеет род Π_1^0 , а Q определено следующим образом:*

$$Q(\mathfrak{A}) \leftrightarrow \exists \alpha^* P(\mathfrak{A}, \alpha^*),$$

то Q имеет род Π_1^0 .

Доказательство. Мы имеем $P(\mathfrak{A}, \alpha) \leftrightarrow \forall x R(\bar{\alpha}(x), \mathfrak{A})$, где R рекурсивно. Отсюда по лемме получаем

$$Q(\mathfrak{A}) \leftrightarrow \forall n \exists \alpha^* \forall x_{x < n} R(\bar{\alpha}^*(x), \mathfrak{A}).$$

Поэтому достаточно доказать, что часть, следующая за $\forall n$, является рекурсивным отношением от $\mathfrak{A}$, n .

Определим рекурсивную функцию F следующим образом:

$$F(0) = \langle \rangle,$$

$$F(n+1) = \mu z \forall y_{y \leq F(n)} (y^* \langle 0 \rangle \leq z \& y^* \langle 1 \rangle \leq z).$$

Тогда если $a_i \leq 1$ при $i < n$, то мы имеем $\langle a_0, \dots, a_{n-1} \rangle \leq F(n)$. Поэтому

$$\begin{aligned} \exists \alpha^* \forall x_{x \leq n} R(\bar{\alpha}^*(x), \mathfrak{A}) &\leftrightarrow \exists s_{s \leq F(n)} (\text{Seq}(s) \& \text{lh}(s) = \\ &= n \& \forall i_{i < n} ((s)_i \leq 1) \& \forall i_{i \leq n} R(\text{In}(s, i), \mathfrak{A})). \end{aligned}$$

Это дает нужный результат.

Теорема Крайзеля о базисе. Класс функций рода Δ_2^0 является базисом совокупности классов рода Π_1^0 представляющих функций.

Доказательство. Пусть P — непустой класс рода Π_1^0 представляющих функций. Из (1) и из следствия к лемме бесконечности вытекает, что I_P имеет род Π_1^0 . По лемме и по теореме Поста P содержит функцию рода Δ_2^0 .

Если P — класс, единственным элементом которого является унарная функция F , то мы говорим, что P неявно определяет F . Тогда F имеет род Δ_n^1 тогда и только тогда, когда P имеет род Δ_n^1 . Действительно, предположим, что P имеет род Δ_n^1 и, следовательно, Σ_n^1 . Так как

$$\begin{aligned}\mathfrak{G}_F(a, b) &\leftrightarrow \exists \alpha (P(\alpha) \& \alpha(a) = b) \\ &\leftrightarrow \forall \alpha (P(\alpha) \rightarrow \alpha(a) = b),\end{aligned}$$

то F имеет род Δ_n^1 . Теперь предположим, что F имеет род Δ_n^1 . Тогда $\mathfrak{G}_F$ и $\neg \mathfrak{G}_F$ имеют род Δ_n^1 . Так как

$$\begin{aligned}P(\alpha) &\leftrightarrow \forall x \forall y (\alpha(x) = y \leftrightarrow \mathfrak{G}_F(x, y)) \\ &\leftrightarrow \forall x \forall y ((\alpha(x) = y \& \mathfrak{G}_F(x, y)) \vee (\alpha(x) \neq y \& \neg \mathfrak{G}_F(x, y))),\end{aligned}$$

то P имеет род Δ_n^1 .

Отсюда следует, что для того, чтобы доказать, что функциональный класс рода Δ_n^1 является базисом совокупности Φ , достаточно доказать, что каждый непустой класс из Φ содержит функцию, неявно определенную классом рода Δ_n^1 , или, что эквивалентно, что в каждом непустом классе из Φ имеется подкласс рода Δ_n^1 , содержащий в точности одну функцию. Мы воспользуемся этим методом, чтобы показать, что функциональный класс рода Δ_2^1 является базисом совокупности функциональных классов рода Π_1^1 .

Теорема униформизации (Новиков — Кондо — Аддисон). Если P — отношение рода Π_1^1 , то существует такое отношение Q рода Π_1^1 , что для всех $\mathfrak{A}$, α и β

- (а) $Q(\alpha, \mathfrak{A}) \rightarrow P(\alpha, \mathfrak{A})$,
- (б) $Q(\alpha, \mathfrak{A}) \& Q(\beta, \mathfrak{A}) \rightarrow \alpha = \beta$,
- (в) $\exists \alpha P(\alpha, \mathfrak{A}) \rightarrow \exists \alpha Q(\alpha, \mathfrak{A})$.

Доказательство. Так как $\mathfrak{A}$ остается фиксированным, то для простоты обозначений мы будем его опускать. По теореме о дереве существует такой рекурсивный функционал F , что $P(\alpha) \leftrightarrow \text{Tr}(\lambda x F(\alpha, x))$. Мы будем писать F_α вместо $\lambda x F(\alpha, x)$ и $F_{\alpha, n}$ вместо $(F_\alpha)_n$.

Если отношение P пусто, то Q мы возьмем также пустым. Теперь предположим, что P непусто. Индукцией по n мы определим для каждого n непустой подкласс P_n из P . Пусть σ — наименьший из ординалов $\|F_\alpha\|$, где α принадлежит P , и пусть P_0 — класс таких α из P , что $\|F_\alpha\| = \sigma$. Теперь предположим, что P_n уже определен. Пусть s_n — наименьшее из чисел $\bar{\alpha}(n)$, где α принадлежит P_n , и пусть σ_n — наименьший из ординалов $\|F_{\alpha, n}\|$, где α принадлежит P_n и $\bar{\alpha}(n) = s_n$. Тогда в качестве P_{n+1} мы возьмем множество таких α из P_n , что $\bar{\alpha}(n) = s_n$ и $\|F_{\alpha, n}\| = \sigma_n$. В таком случае мы имеем

$$\alpha \in P_n \& \bar{\alpha}(n) \leq s_n \& \|F_{\alpha, n}\| \leq \sigma_n \rightarrow \alpha \in P_{n+1}. \quad (3)$$

Возьмем в качестве Q пересечение всех P_n . Свойство (а) очевидно. Если α принадлежит Q , то $\bar{\alpha}(n) = s_n$ для всех n , это доказывает (б). Чтобы доказать (в), нам надо показать, что Q непусто. Выбирая α в P_{n+2} , мы получаем, что $\alpha \in P_{n+1}$, поэтому $\bar{\alpha}(n+1) = s_{n+1}$ и $\bar{\alpha}(n) = s_n$. Следовательно s_{n+1} является расширением s_n . Так как к тому же $\text{lh}(s_n) = n$, то существует единственная функция γ такая, что $\bar{\gamma}(n) = s_n$ для всех n . Покажем, что γ принадлежит Q .

Сначала мы покажем, что

$$F_\gamma(m) = F_\gamma(n) = 0 \& m <^* n \rightarrow \sigma_m < \sigma_n. \quad (4)$$

Так как функционал F рекурсивен, то мы имеем $F(\alpha, a) \simeq b \leftrightarrow \exists z R(\bar{\alpha}(z), a, b)$. Отсюда и из того, что $F_\gamma(m) = F_\gamma(n) = 0$, мы видим, что существует такое число k , что если $\bar{\alpha}(k) = \bar{\gamma}(k)$, то $F_\alpha(m) = F_\alpha(n) = 0$. Мы можем также предполагать, что $k > m, k > n$. Выберем α в P_{k+1} . Тогда $\bar{\alpha}(k) = s_k = \bar{\gamma}(k)$, поэтому $F_\alpha(m) = F_\alpha(n) = 0$. Отсюда и из $m <^* n$ мы получаем $\|F_{\alpha, m}\| = \|(F_{\alpha, n})_m\| < \|F_{\alpha, n}\|$. Так как α принадлежит P_{m+1} и P_{n+1} , то это неравенство превращается в $\sigma_m < \sigma_n$. Аналогичное (однако несколько более простое) доказательство показывает, что

$$F_\gamma(n) = 0 \rightarrow \sigma_n < \sigma. \quad (5)$$

Далее, мы покажем, что γ принадлежит P . В противном случае существовала бы такая убывающая последовательность $m_0, m_1, \dots$, что $F_\gamma(m_i) = 0$ для всех i . Тогда вследствие (4) $\sigma_{m_0} > \sigma_{m_1} > \dots$, что невозможно.

Теперь трансфинитной индукцией по σ_n мы докажем, что

$$F_\gamma(n) = 0 \rightarrow \|F_{\gamma,n}\| \leq \sigma_n. \quad (6)$$

Если $F_{\gamma,n}(m) = 0$, то $F_\gamma(m) = 0$ и $m <^* n$, поэтому $\sigma_m < \sigma_n$ вследствие (4). Следовательно, по индуктивному предположению

$$\|(F_{\gamma,n})[m]\| = \|F_{\gamma,m}\| \leq \sigma_m < \sigma_n.$$

Вследствие (8) из § 7.10 отсюда вытекает, что $\|F_{\gamma,n}\| \leq \sigma_n$.

Вследствие (5) и (6) $\|F_\gamma\| \leq \sigma$, поэтому γ принадлежит P_0 . Если γ принадлежит P_n , то из (3) и (6) следует, что γ принадлежит P_{n+1} . Таким образом, по индукции γ принадлежит всем P_n и, следовательно, Q .

Остается показать, что Q — отношение рода Π_1^1 . Вследствие (3) мы имеем

$$P_n(\beta) \leftrightarrow \|F_\beta\| \leq \sigma \ \& \ \forall m_{m < n} (\bar{\beta}(m) \leq s_m \ \& \ \|F_{\beta,m}\| \leq \sigma_m).$$

Следовательно, если α принадлежит P_n , то

$$P_n(\beta) \leftrightarrow T \leq (F_\beta, F_\alpha) \ \& \ \forall m_{m < n} (\bar{\beta}(m) \leq \bar{\alpha}(m) \ \& \ T \leq (F_{\beta,m}, F_{\alpha,m})).$$

Правую часть этой эквивалентности можно переписать как $R(\alpha, \beta, n)$, где R — отношение рода Σ_1^1 . Тогда для α из P_n

$$\begin{aligned} \neg P_{n+1}(\alpha) &\leftrightarrow \exists \beta (P_n(\beta) \ \& \ [\bar{\beta}(n) < \bar{\alpha}(n) \vee (\bar{\beta}(n) = \\ &= \bar{\alpha}(n) \ \& \ \|F_{\beta,n}\| < \|F_{\alpha,n}\|)]) \\ &\leftrightarrow \exists \beta (R(\alpha, \beta, n) \ \& \ [\bar{\beta}(n) < \bar{\alpha}(n) < (\bar{\beta}(n) = \\ &= \bar{\alpha}(n) \ \& \ T < (F_{\beta,n}, F_{\alpha,n}))]) \\ &\leftrightarrow R'(\alpha, n), \end{aligned}$$

где R' — отношение рода Σ_1^1 . Отсюда

$$\begin{aligned} Q(\alpha) &\leftrightarrow P_0(\alpha) \ \& \ \forall n \neg R'(\alpha, n) \\ &\leftrightarrow P(\alpha) \ \& \ \forall \beta \neg T < (F_\beta, F_\alpha) \ \& \ \forall n \neg R'(\alpha, n). \end{aligned}$$

Таким образом, Q — отношение рода Π_1^1 . Если P и Q пусты, то мы можем использовать такое же определение для Q .

Следствие 1. Класс функций рода Δ_2^1 является базисом для совокупности функциональных классов рода Π_1^1 .

Следствие 2. Класс функций рода Δ_2^1 является базисом для совокупности функциональных классов рода Σ_2^1 .

Следующей задачей должна бы быть такая: найти базис совокупности функциональных классов рода Π_2^1 . Однако Леви показал, что при обычных аксиомах теории множеств нельзя доказать, что класс функций, определимых в теории множеств, является базисом этой совокупности. Так как среди определимых функций содержатся, например, все функции, рекурсивные в множестве аналитических предикатов, то мы видим, что эту проблему нельзя удовлетворительно решить, не рассматривая новые аксиомы. С другой стороны, Аддисон показал, что предположение о том, что класс функций рода Δ_2^1 является базисом совокупности функциональных классов рода Π_2^1 , не противоречит имеющимся аксиомам.

Так как теперь мы, очевидно, далеко ушли от проблемы разрешимости, которая вначале привела нас к рекурсивным функциям, то естественно спросить, чего мы надеемся достичь при изучении иерархий? Одним из ответов является такой: мы надеемся прояснить понятие множества. С этой точки зрения мы рассматриваем иерархии как классификацию некоторых важных множеств в соответствии со сложностью их определения. Поэтому не является неожиданным, что, как только что было указано, многие из нерешенных проблем в теории иерархий связаны с проблемами в аксиоматической теории множеств.

Задачи

1. (а) Пусть F определена индуктивно следующим образом:

$$\begin{aligned} F(0, a) &= G(a), \\ F(b+1, a) &= H(F(b, K(F(b, a), b, a)), b, a), \end{aligned}$$

где G , H и K — рекурсивные функции. Показать, что F рекурсивна. [Определить с помощью теоремы о рекурсии рекурсивную частичную функцию F' , удовлетворяющую равенствам, в которых $=$ заменено на $\simeq$, а затем доказать индукцией по b , что $F'(b, a) \simeq F(b, a)$.]

(б) Показать, что существует такая бинарная рекурсивная функция F , что для каждой n -арной примитивно рекурсивной функции G существует такое число g , что $F_{(g)} = \langle G \rangle$. [Сопоставить индекс g каждой примитивно рекурсивной функции G . Положить $F(a, g) = \langle G \rangle(a)$, если g является индексом функции G , и $F(a, g) = 0$, если g не является индексом. Пользуясь методом из (а), показать, что F рекурсивна.] Затем показать, что F не является примитивно рекурсивной. [Показать, что функция H , определенная следующим образом: $H(a) = F(a, a) + 1$, не является примитивно рекурсивной.]

2. (а) Показать, что область определения любого рекурсивного частичного функционала рекурсивно перечислима.

(б) Пусть F — рекурсивный частичный функционал, а A — некоторое подмножество области определения функционала F . Показать, что ограничение функционала F на A рекурсивно тогда и только тогда, когда A рекурсивно перечислимо. [Использовать (а) и R12.]

(в) Пусть P — такой рекурсивный предикат, что $\forall x P(x, a)$ не является рекурсивно перечислимым предикатом от a . Пусть $H(x, a) \simeq \mu z P(x, a) = 0, F(a) \simeq G(\lambda x H(a, x), a)$. Показать, что F не рекурсивна. [Использовать (а)].

3. Частичный функционал F называется *селектором* для отношения P , если для любых $\mathbb{N}$ таких, что $\exists x P(x, \mathbb{N})$, $F(\mathbb{N})$ определено и $P(F(\mathbb{N}), \mathbb{N})$.

(а) Показать, что если отношение P рекурсивно перечислимо, то для P существует рекурсивный селектор. [Если $P(x, \mathbb{N}) \leftrightarrow \exists y R(x, \mathbb{N}, y)$, то пусть $F(\mathbb{N}) \simeq (\mu z R((z)_0, \mathbb{N}, (z)_1))_0$.]

(б) Показать, что можно найти такое рекурсивно перечислимое отношение P , что селектор $\mu x P(x, a)$ для P не рекурсивен. [Определить P следующим образом: $P(x, a) \leftrightarrow R(a) \vee x = 1$, где отношение P рекурсивно перечислимо, но не рекурсивно.]

(в) Предположим, что отношение P рекурсивно. Показать, что существует рекурсивный всюду определенный функционал, являющийся селектором для P тогда и только тогда, когда $\exists x P(x, \mathbb{N})$ является рекурсивным отношением от $\mathbb{N}$.

(г) Пусть $F_1, \dots, F_n$ — рекурсивные частичные функционалы. Показать, что существует такой рекурсивный функционал F , что $F(\mathbb{N})$ для каждого $\mathbb{N}$ определено тогда и только тогда, когда хотя бы одно из $F_i(\mathbb{N})$ определено, и в этом случае $F(\mathbb{N}) = F_i(\mathbb{N})$ для некоторого i . [Использовать (а).]

4. Рекурсивная частичная функция F называется *креативной функцией* для множества A , если для каждого e такого, что A и W_e не пересекаются, $F(e)$ определено и не принадлежит ни A , ни W_e . Рекурсивно перечислимое множество A *креативно*, если оно имеет креативную функцию. Рекурсивно перечислимое множество A называется *простым*, если его дополнение бесконечно, но не содержит никакого бесконечного рекурсивно перечислимого подмножества.

(а) Показать, что креативное множество существует. [Рассмотреть $A(e) \leftrightarrow W_e(e)$.]

(б) Показать, что креативное множество не может быть рекурсивным. [Воспользоваться теоремой об отрицании.]

(в) Показать, что каждое креативное множество A имеет всюду определенную креативную функцию. [Ввести рекурсивную функцию G , областью определения которой является множество таких e , что пересечение множеств W_e и A непусто, и воспользоваться 3(г).]

(г) Показать, что простое множество существует. [Ввести $P(x, e) \leftrightarrow \neg W_e(x) \& x > 2e$. Пусть F является рекурсивным селектором для P , и пусть A — множество значений функционала F . Показать, что для каждого k в A найдется не более k чисел, не превосходящих $2k$.]

(д) Показать, что простое множество не может быть рекурсивным. [Воспользоваться теоремой об отрицании.]

(е) Показать, что простое множество не может быть креативным.

5. Множество A называется *много-односводимым* к множеству B , если существует такая рекурсивная функция F , что для каждого a

$$A(a) \leftrightarrow B(F(a)).$$

Если к тому же можно F выбрать так, что она окажется инъективной (биективной), то A называется *одно-односводимым* к B (соответственно *рекурсивно изоморфным* B).

(а) Показать, что если множества A и B рекурсивно изоморфны, то каждое из них одно-односводимо к другому.

(б) Пусть A одно-односводимо к B , и пусть $R(a, b)$ означает, что $a = \langle a_1, \dots, a_n \rangle$, $b = \langle b_1, \dots, b_n \rangle$, $a_i = a_j \leftrightarrow b_i = b_j$ для всех i, j и $A(a_i) \leftrightarrow B(b_i)$. Показать, что существует такая рекурсивная функция G , что

$$R(a, b) \rightarrow R(a^* \langle x \rangle, b^* \langle G(a, b, x) \rangle).$$

[Пусть $A(a) \leftrightarrow B(F(a))$, где F инъективна. Если $x = a_i$, то пусть $G(a, b, x) = b_i$. В противном случае, если $F(x)$ не равно b_i , то пусть $G(a, b, x) = F(x)$; если $F(x) = b_{i_1}$ и $F(a_{i_1})$ не равно b_i , то пусть $G(a, b, x) = F(a_{i_1})$ и т. д.]

(в) Показать, что если каждое из множеств A и B одно-односводимо к другому, то A рекурсивно изоморфно B . [Использовать (б) и технику доказательства теоремы Риль-Нардзевского.]

(г) Показать, что существуют такие рекурсивно перечислимые множества A и B , что A одно-односводимо к B , B много-односводимо к A и B не одно-односводимо к A . [Взять в качестве A простое множество и сформировать B , исключив из A некоторое бесконечное рекурсивное подмножество.]

6. (а) Показать, что если P — рекурсивно перечислимый предикат, то существует такая рекурсивная функция H , что $W_{H(x)}(a) \leftrightarrow P(a, x, H(x))$ для любых a и x . [Определить такую рекурсивную функцию G с индексом g , что $G(a, x) = 0$, если $P(a, x, S(g, x))$, и $G(a, x)$ не определена в противном случае, и положить $H(x) = S(g, x)$.]

(б) Показать, что если A креативно, а P рекурсивно перечислим, то существует такая рекурсивная функция F , что $P(x, F(x)) \leftrightarrow A(F(x))$ для всех x . [Пусть G — всюду определенная креативная функция для A . Выбрать H из (а) так, чтобы

$$W_{H(x)}(a) \leftrightarrow a = G(H(x)) \& P(x, G(H(x))),$$

и положить $F(x) = G(H(x))$.]

(в) Показать, что если A креативно, то существует такая всюду определенная креативная функция F для A , что если пересечение A с W_e непусто, то $A(F(e))$. [Ввести $P(e, y) \leftrightarrow W_e(y) \vee \exists x (W_e(x) \& A(x))$ и применить (б).]

(г) Пусть A креативно. Показать, что существует такая рекурсивная функция F , что если $A(x)$, то $W_{F(x)} \subset A$, а если $\neg A(x)$, то $W_{F(x)}$ бесконечно и не пересекается с A . [Использовать (в).]

(д) Показать, что если A креативно, то существует такая рекурсивная функция F , что $F(x, y) \geq y$ и $A(x) \leftrightarrow A(F(x, y))$ для всех x и y . [Использовать (г) и 3(а).]

(е) Показать, что если A креативно, а B много-односводимо к A , то B одно-односводимо к A . [Пусть F рекурсивна, пользуясь

(д), определить индуктивно такую инъективную рекурсивную функцию F' , что $A(F(a)) \leftrightarrow A(F'(a))$.]

(ж) Показать, что для рекурсивно перечислимого множества A следующие утверждения эквивалентны:

- (i) A креативно;
- (ii) каждое рекурсивно перечислимое множество много-односводимо к A ;
- (iii) каждое рекурсивно перечислимое множество одно-односводимо к A .

[Использовать (б), (е) и 4 (а).]

7. Два непересекающихся множества A и B эффективно рекурсивно неотделимы, если существует такая рекурсивная частичная функция F , что если $A \subset W_e$ и $B \subset W_f$, то $F(e, f)$ определено и не принадлежит ни W_e , ни W_f .

(а) Показать, что эффективно рекурсивно неотделимые множества рекурсивно неотделимы. [Использовать теорему об отрицании.]

(б) Показать, что существуют эффективно рекурсивно неотделимые рекурсивно перечислимые множества. [Ввести

$$A(x) \leftrightarrow \exists y (T_1((x)_1, x, y) \& \forall z \leq y \neg T_1((x)_0, x, z)),$$

$$B(x) \leftrightarrow \exists y (T_1((x)_0, x, y) \& \forall z < y \neg T_1((x)_1, x, z))$$

и $F(e, f) = \langle e, f \rangle$.]

(в) Показать, что если A и B — эффективно рекурсивно неотделимые рекурсивно перечислимые множества, то A , B и $A \vee B$ креативны.

(г) Показать, что существуют рекурсивно неотделимые рекурсивно перечислимые множества A и B , не являющиеся эффективно рекурсивно неотделимыми. [Построить A и B следующим образом. На n -м шаге положить $e = (n)_0$, $x = (n)_1$, $y = (n)_2$. Если условие $T_1(e, x, y) \& x > 3e$ не выполняется, то на этом шаге больше ничего не делать. Если же оно выполняется, то отнести число x к A , если оно не было отнесено к B и никакое число не было отнесено к A на шаге $m < n$, где $(m)_0 = e$. В противном случае отнести x к B , если оно не было отнесено к A и никакое число не было отнесено к B на шаге $m < n$, где $(m)_0 = e$. Показать, что $A \vee B$ является простым и что если $W_e \& \neg(A \vee B)$ бесконечно, то каждое из множеств A и B содержит элемент из W_e . Использовать (в) и 4 (е).]

8. Пусть Ux означает для бесконечно многих x . Предикат P называется предикатом рода $U_n(V_n)$, если

$$P(a) \leftrightarrow Ux_1 \dots Ux_n R(a, x_1, \dots, x_n),$$

где предикат R рекурсивен (рода Π_1^0).

(а) Показать, что каждый предикат рода U_n имеет род Π_{2n}^0 и что каждый предикат рода V_n имеет род Π_{2n+1}^0 .

(б) Пусть P — предикат рода Π_{n+1}^0 ; показать, что $P(a) \leftrightarrow \exists x Q(a, x)$ для предиката Q рода Σ_n^0 . [Воспользоваться эквивалентностью $\forall z R(z) \leftrightarrow \exists w \forall z_{z < w} R(w)$.]

(в) Пусть P — предикат рода Π_{n+2}^0 (Π_2^0); показать, что

$$P(a) \leftrightarrow Ux (P_1(a, x) \& P_2(a, x)),$$

где P_1 — предикат рода Π_n^0 (рекурсивный), а P_2 — предикат рода Σ_n^0 (рекурсивный). [Использовать (б) и эквивалентность

$$Ux \exists y Q(x, y) \leftrightarrow \exists z (Q((z)_0, (z)_1) \& \forall w_{w < (z)_1} \neg Q((z)_0, w)).$$

(г) Пусть P — предикат рода Π_{n+2}^0 ; показать, что $P(a) \leftrightarrow \exists x P_1(a, x)$, где P_1 — предикат рода Π_n^0 . [Использовать (в) и эквивалентность

$$Ux (\exists y Q(x, y) \& \forall v R(x, v)) \leftrightarrow \exists z (Q((z)_0, (z)_1) \& \forall w_{w < (z)_1} \neg Q((z)_0, w) \& \forall v R((z)_0, v)).]$$

(д) Пусть P — предикат рода Π_n^0 . Показать, что если $n = 2m$, то P — предикат рода U_m , а если $n = 2m + 1$, то P — предикат рода V_m . [Воспользоваться (в), (г) и индукцией по m .]

9. Полным множеством рода Σ_n^0 (Π_n^0) называется такое множество A рода Σ_n^0 (Π_n^0), что каждое множество рода Σ_n^0 (Π_n^0) много-односводимо к A .

(а) Пусть P — бинарный предикат рода Σ_n^0 (Π_n^0), перечисляющий класс унарных предикатов рода Σ_n^0 (Π_n^0), и пусть $A(a) \leftrightarrow P((a)_0, (a)_1)$. Показать, что A — полное множество рода Σ_n^0 (Π_n^0).

(б) Показать, что множество таких e , что W_e бесконечно, является полным множеством рода Π_2^0 . [Использовать 8 (д).]

(в) Показать, что множество таких e , что $\neg W_e$ бесконечно, является полным множеством рода Π_2^0 . [Использовать 8 (а) и 8 (д).]

(г) Показать, что множество таких e , что W_e рекурсивно, является полным множеством рода Σ_2^0 . [Пользуясь теоремой об отрицании, показать, что это множество рода Σ_2^0 . Пусть A — нерекурсивное рекурсивно перечислимое множество. Определить такую рекурсивную функцию F , что

$$W_{F(e)}(x) \leftrightarrow (W_e((x)_0) \& (x)_1 = 0) \vee ((x)_0 < (x)_1 \& A((x)_0)) \vee \neg((x)_1 > 0 \& W_e((x)_1)).$$

Показать, что $W_{F(e)}$ рекурсивно тогда и только тогда, когда $\neg W_e$ конечно, и использовать (в).]

10. Множество A таблично сводимо к множеству B , если существуют рекурсивная функция F и рекурсивный предикат P такие, что $A(x) \leftrightarrow P(\bar{K}_B(F(x)))$ для всех x .

(а) Показать, что если A много-односводимо к B , то A таблично сводимо к B .

(б) Показать, что для каждого рекурсивно перечислимого множества A существует такое простое множество B , что A таблично сводимо к B . [Мы можем предполагать, что $\neg A$ бесконечно. Пусть C — такое простое множество, что для каждого n в C существуют самое большее n чисел, меньших $2n + 2$. Пусть D_n — множество таких x , что $2^n \leq x < 2^{n+1}$, а B — объединение множеств C и D_n , где n принадлежит множеству A .] Затем показать, что обращение (а) ложно даже для рекурсивно перечислимых множеств. [Использовать 4 (е).]

(в) Показать, что A таблично сводимо к B тогда и только тогда, когда существует такой всюду определенный функционал F , что

$K_A(x) = F(K_B, x)$ для всех x . [Предположим, что такой функционал F существует. Выберите такой рекурсивный предикат R , что $\mathcal{G}_F(\alpha, x, a) \leftrightarrow \exists z R(\bar{\alpha}(z), x, a)$. Обратите внимание на то, что для каждого x

$$\forall \alpha^* \exists z R(\bar{\alpha}^*((z)_0), x, (z)_1),$$

и воспользуйтесь леммой о бесконечности.]

11. Рекурсивно перечислимое множество A называется *гиперпростым*, если дополнение множества A бесконечно и не существует такой рекурсивной функции F , что $\forall x \exists y (\neg A(y) \& x < y < F(x))$.

(а) Показать, что если A гиперпросто, то A просто и потому не рекурсивно.

(б) Предположим, что креативное множество A таблично сводимо к рекурсивно перечислимому множеству B . Показать, что B не может быть гиперпростым. [Пусть $A(a) \leftrightarrow P(\bar{K}_B(F(x)))$, где P и F рекурсивны. Выберем рекурсивную функцию G из 6 (б) так, что $A(G(e)) \leftrightarrow \neg W_e(G(e))$. Пусть $J_n(x) = (n)_x$, если $x < lh_n$, $J_n(x) = 0$ в противном случае. Выберем рекурсивную функцию H так, что

$$W_{H(n)}(a) \leftrightarrow \neg P(\bar{J}_n(F(a))).$$

Пусть $L(n) = F(G(H(n)))$. Показать, что

$$\neg P(\bar{J}_n(L(n))) \leftrightarrow P(\bar{K}_B(L(n))),$$

а затем показать, что $J_n(i) \neq K_B(i)$ для некоторого $i < L(n)$. Используя L , определить такую рекурсивную функцию M , что $\forall x \exists y (\neg B(y) \& x < y < M(x))$.

(в) Показать, что для каждого нерекурсивного рекурсивно перечислимого множества A существует такое гиперпростое множество B , что B таблично сводимо к A и A рекурсивно в B . [Пусть F — инъективная рекурсивная функция, перечисляющая A ; определить B следующим образом:

$$B(a) \leftrightarrow \exists x (a < x \& F(x) < F(a)).$$

Показать, что дополнение множества B бесконечно и что

$$\neg B(w) \& F(w) > x \rightarrow (A(x) \leftrightarrow \exists z_{z < w} (x = F(z))).$$

Предположим, что G — такая рекурсивная функция, что $\forall x \exists y (\neg B(y) \& x < y < G(x))$. Показать, что мы можем установить, принадлежит ли a множеству A , отыскивая такое x , что

$$a < \min(F(x), F(x+1), \dots, F(G(x))).$$

(г) Показать, что существуют такие рекурсивно перечислимые множества A и B , что A рекурсивно в B , однако не является таблично сводимым к B . [Использовать (б) и (в).] Затем показать, что лемма о замене неверна для рекурсивных всюду определенных функций и предикатов. [Использовать 10 (в).]

12. Пусть $\mathcal{F}$ — класс всех рекурсивных унарных частичных функций. Подкласс $\mathcal{F}'$ класса $\mathcal{F}$ называется *вполне рекурсивно перечислимым* (вполне рекурсивным), если множество индексов частичных функций из $\mathcal{F}'$ рекурсивно перечислимо (рекурсивно). Отображение Φ из подкласса $\mathcal{F}'$ класса $\mathcal{F}$ в множество чисел называется *эффективной опе-*

рацией, если существует такая рекурсивная частичная функция F , что $F(e) \simeq \Phi(\{e\})$, как только $\{e\}$ принадлежит $\mathcal{F}'$.

(а) Показать, что если $\mathcal{F}'$ вполне рекурсивно перечислим, то каждое расширение любой частичной функции из $\mathcal{F}'$, принадлежащее $\mathcal{F}$, принадлежит $\mathcal{F}'$. [Предположим, что G принадлежит $\mathcal{F}'$, а ее расширение H не принадлежит ему. Пусть A — нерекурсивное рекурсивно перечислимое множество, и пусть F_1 и F_2 определены следующим образом:

$$F_1(x, y) \simeq H(x), \text{ если } A(y),$$

$$F_2(x, y) \simeq G(x).$$

Определим F так же, как в 3 (г), и выберем рекурсивную функцию K так, что $\{K(y)\}(x) \simeq F(x, y)$. Показать, что $\{K(y)\}$ принадлежит $\mathcal{F}'$ тогда и только тогда, когда $\neg A(y)$.

(б) Показать, что если $\mathcal{F}'$ вполне рекурсивно перечислим и G принадлежит $\mathcal{F}'$, то G является расширением некоторой частичной функции G' из $\mathcal{F}'$, имеющей конечную область определения. [Предположим, что такой функции G' не существует. Выберем такое e , что W_e нерекурсивно. Определим F следующим образом:

$$F(y, x) \simeq G(x), \text{ если } \neg \exists z_{z < x} T_1(e, y, z),$$

и выберем такую рекурсивную функцию K , что $\{K(y)\}(x) \simeq F(x, y)$. Показать, что $\{K(y)\}$ принадлежит $\mathcal{F}'$ тогда и только тогда, когда $\neg W_e(y)$.

(в) Пусть $\mathcal{F}_{s, t, n}$ — множество таких G из $\mathcal{F}$, что $G((s)_i) \simeq (t)_i$ при $i < n$. Показать, что подмножество $\mathcal{F}'$ множества $\mathcal{F}$ вполне рекурсивно перечислимо тогда и только тогда, когда существует такой рекурсивно перечислимый предикат P , что $\mathcal{F}'$ является объединением $\mathcal{F}_{s, t, n}$, где s, t и n таковы, что $P(s, t, n)$. [Использовать (а) и (б).]

(г) Показать, что вполне рекурсивными подклассами класса $\mathcal{F}$ является лишь $\mathcal{F}$ и пустой класс. [Использовать (а) и теорему об отрицании.]

(д) Показать, что отображение Φ вполне рекурсивно перечислимого класса $\mathcal{F}'$ в множество чисел является эффективной операцией тогда и только тогда, когда существует такая рекурсивная частичная функция H , что для F из $\mathcal{F}'$

$$\Phi(F) \simeq a \leftrightarrow \exists s \exists t \exists n (F \in \mathcal{F}_{s, t, n} \& H(s, t, n) \simeq a).$$

[Если Φ — эффективная операция, то множество таких F , что $\Phi(F) \simeq a$, вполне рекурсивно перечислимо. Пользуясь этим, скопируйте доказательство (в).]

(е) Показать, что условие в (д), говорящее, что $\mathcal{F}'$ — вполне рекурсивно перечислимое множество, нельзя заменить условием, говорящим, что каждая частичная функция из $\mathcal{F}'$ всюду определена. [Пусть $\Phi(F) = 0$, если $F(x) = 0$ для всех x , и $\Phi(F) = 1$, если F — рекурсивная всюду определенная функция и $\exists x (x \leq e \& F(x) \neq 0)$ для каждого индекса e из F . Показать, что для каждого k существует такая F , что $F(x) = 0$ при $x \leq k$ и $\Phi(F) = 1$.]

13. Пусть $\mathcal{R}$ — класс всех рекурсивных унарных функций. Подкласс $\mathcal{R}'$ класса $\mathcal{R}$ называется *тотально рекурсивно перечислимым* (тотально рекурсивным), если существует такое рекурсивно перечислимое множество A (существуют непересекающиеся рекурсивно перечис-

лимые множества A и B), что $\{e\} \in \mathfrak{N}' \Leftrightarrow A(e)$ (и $\{e\} \notin \mathfrak{N}' \Leftrightarrow B(e)$) как только $\{e\}$ всюду определена.

(а) Пусть класс $\mathfrak{N}'$ totally рекурсивно перечислим. Показать, что для каждой G из $\mathfrak{N}'$ и каждого z существует такая G' из $\mathfrak{N}'$, что $G'(x) = G(x)$ при $x < z$ и $G'(x) = 0$ везде, кроме конечного числа значений x . [Доказывать подобно 12 (б).]

(б) Пусть Φ — отображение некоторого totally рекурсивно перечислимого класса $\mathfrak{N}'$ в множество чисел. Показать, что Φ является эффективной операцией тогда и только тогда, когда оно имеет расширение, являющееся рекурсивным частичным функционалом. [Предположим, что Φ — эффективная операция, например, $F(e) \simeq \Phi(\{e\})$, где $\{e\}$ принадлежит $\mathfrak{N}'$. Пусть K — такая рекурсивная функция, что $\{K(n)\}(x) = (n)_x$, если $\text{Seq}(n) \& x < \text{lh}(n)$, и $\{K(n)\}(x) = 0$ в противном случае. Пользуясь 3 (а), определить такую рекурсивную частичную функцию M , что $M(f, y)$ является таким числом n , что $\{K(n)\}$ принадлежит $\mathfrak{N}'$ и является расширением $\{f\}(y)$, и $F(f) \neq F(K(n))$, если только такое n существует. Выберем такую рекурсивную функцию L , что

$$\{L(e, f)\}(x) \simeq \begin{cases} \{f\}(x), & \text{если } \forall y_{y < x} \neg T_1(e, e, y), \\ (M(f, \mu y T_1(e, e, y)))_x & \text{в противном случае.} \end{cases}$$

Если $\neg W_e(e)$, то $\{L(e, f)\} = \{f\}$; если $y = \mu y T_1(e, e, y)$ и $M(f, y)$ определено, то

$$\{L(e, f)\} = \{K(M(f, y))\}.$$

Выберем рекурсивную функцию N так, чтобы $W_{N(f)}$ являлось множеством таких e , что $F(L(e, f)) \simeq F(f)$. Показать, что если $\{f\} \in \mathfrak{N}'$, то $N(f) \in W_{N(f)}$. Если $F(f)$ определено и

$$y = \mu y T_1(N(f), N(f), y),$$

а G принадлежит $\mathfrak{N}'$ и $\bar{G}(y) = \{f\}(y)$, то $\Phi(G) = F(f)$; действительно, в противном случае $M(f, y)$ определено по (а), поэтому $F(L(N(f)), f) = F(K(M(f, y))) \neq F(f)$ и потому $N(f) \notin W_{N(f)}$. Пусть $Q(f, \alpha)$ означает, что существует такое y , что $F(f)$ определено, $y = \mu y T_1(N(f), N(f), y)$ и $\bar{\alpha}(y) = \{f\}(y)$. Пусть H — рекурсивный селектор для Q . Показать, что $\Phi(\alpha) = F(H(\alpha))$ для α из $\mathfrak{N}'$.

(в) Показать, что подкласс $\mathfrak{N}'$ класса $\mathfrak{N}$ totally рекурсивен тогда и только тогда, когда существуют такие непересекающиеся рекурсивно перечислимые множества A и B , что для $\alpha \in \mathfrak{N}$ имеем

$$\alpha \in \mathfrak{N}' \leftrightarrow \exists x A(\bar{\alpha}(x)) \text{ и } \alpha \notin \mathfrak{N}' \leftrightarrow \exists x B(\bar{\alpha}(x)).$$

[Пусть $\mathfrak{N}'$ totally рекурсивен, пользуясь (б), найти такую рекурсивную функцию H , что $H(\alpha) = 0$, если α принадлежит $\mathfrak{N}'$, и $H(\alpha) \neq 1$, если α рекурсивна и не принадлежит $\mathfrak{N}'$. Выразить $\mathfrak{G}_H$ на языке рекурсивных предикатов.]

(г) Показать, что если A рекурсивно перечислимо, то множество таких α из $\mathfrak{N}$, что $\exists x A(\bar{\alpha}(x))$, является totally рекурсивно перечислимым. Показать, что не каждый totally рекурсивно перечислимый класс может быть получен таким образом. [Пусть F из $\mathfrak{N}$ принадлежит $\mathfrak{N}'$, если либо $\forall x (F(x) = 0)$, либо $\exists e < z \forall x_{x \leq z} (\{e\}(x) =$

$= F(x)$), где $z = \mu x (F(x) \neq 0)$. Показать, что если $\{f\}$ принадлежит $\mathfrak{N}$ и $\{f\}(x) = 0$ при $x \leq f$, то $\{f\}$ принадлежит $\mathfrak{N}'$, а затем показать, что $\mathfrak{N}'$ totally рекурсивно перечислим. Показать, что для каждого k существует функция F , принадлежащая $\mathfrak{N}$, но не принадлежащая $\mathfrak{N}'$, такая, что для всех $x \leq k$ $F(x) = 0$.]

14. (а) Показать, что если a и b — степени, то множество, состоящее из a и b , имеет наименьшую верхнюю грань (относительно частичного упорядочения степеней $\leq$). [Пусть A и B — множества из a и b соответственно, и пусть c — степень множества C , определенного следующим образом:

$$\begin{aligned} C(x) &\leftrightarrow A((x)_0), & \text{если } (x)_1 = 0, \\ C(x) &\leftrightarrow B((x)_0) & \text{в противном случае.} \end{aligned}$$

Эту степень мы обозначим через $a \cup b$.

(б) Пусть A и B — непересекающиеся рекурсивно перечислимые множества, имеющие степени a и b соответственно. Показать, что $A \cup B$ имеет степень $a \cup b$.

(в) Показать, что если $0' \leq a$, то существует такая степень b , что $a = b' = b \cup 0'$. [Пусть A — множество из a . Выберем рекурсивный предикат R так, что

$$\exists x T_{1,1}((a)_0, \alpha, (a)_1, x) \leftrightarrow \exists x R(\bar{\alpha}(x), a),$$

и положим

$$Q(s, a) \leftrightarrow \exists t (t <^* s \& R(t, a)).$$

Положим $G(0) = \langle \quad \rangle$ и

$$G(a+1) = \begin{cases} \mu t (t <^* G(a) * \langle K_A(a) \rangle \& R(t, a)), & \text{если } Q(G(a) * \langle K_A(a) \rangle, a), \\ G(a) * \langle K_A(a) \rangle & \text{в противном случае.} \end{cases}$$

Пользуясь тем, что Q рекурсивен в A , показать, что G и A эквивалентны. Пусть

$$F(a) = (G(a+1))_a,$$

и пусть b — степень функции F . Показать, что $\exists x R(\bar{F}(x), a)$ рекурсивен в G , а затем показать, что $b' \leq a$. Показать, что G рекурсивна в F и Q , а затем показать, что $a \leq b \cup 0'$.]

15. (а) Пусть A — нерекурсивное рекурсивно перечислимое множество. Показать, что существуют непересекающиеся рекурсивно перечислимые множества A_0 и A_1 , объединение которых A не рекурсивно ни в A_0 , ни в A_1 . [Пусть F — инъективная рекурсивная функция, перечисляющая A , и пусть предикат R такой же, как и в доказательстве теоремы Фридберга — Мучника. Определим A_0 и A_1 по шагам, одновременно определяя множества B_k . Пусть $A_{i,n}$ — множество чисел, отнесенных к A_i до n -го шага, и пусть D_n — множество значений функции $F(x)$ при $x < n$. На n -м шаге для $j < n$ и $i = 0, 1$ пусть $x_{j,i}$ является таким наибольшим числом, меньшим n , что для всех $x < x_{j,i}$ имеем

$$\exists y_{y < n} R(\bar{K}_{A_{i,n}}(y), i, x, K_{D_n}(x)).$$

Если $x < x_{j,i}$, то отнесем каждое число, меньшее

$$x + \mu y R(\bar{K}_{A_{i,n}}(y), j, x, K_{D_n}(x)),$$

к B_{2j+i} . Теперь выберем такое наименьшее $2j+i$, что $F(n)$ принадлежит множеству B_{2j+i} , и отнесем $F(n)$ к A_{1-i} или, если $F(n)$ не принадлежит B_k , отнесем $F(n)$ к A_0 . Показать, что если $\{j\}^{A_i} \neq K_A$, то B_{2j+i} конечно. Затем индукцией по $2j+i$ доказать, что $\{j\}^{A_i} \neq K_A$, следующим образом. Показать, что существует шаг n_0 , после которого уже никакое число B_{2j+i} не относится к A_i . Предположить, что $\{j\}^{A_i} = K_A$, и показать, что $K_A(x)$ можно вычислить, проверяя на шаге $n > n_0$, выполняется ли $x < x_{i,j}$, и полагая $K_A(x) = K_{D_n}(x)$.]

(б) Показать, что каждое нерекурсивное рекурсивно перечислимое множество является объединением двух непересекающихся нерекурсивных рекурсивно перечислимых множеств. [Использовать (а) и 14 (б).]

(в) Показать, что если a — отличная от 0 рекурсивно перечислимая степень, то существует такая рекурсивно перечислимая степень b , что $0 < b < a$. [Использовать (а) и 14 (б).]

16. Зададим на каждом множестве $N_{m,n}$ топологию следующим образом. Зададим на $N_{0,1}$ дискретную топологию. Рассматривая $N_{1,0}$ как произведение счетного числа копий множества $N_{0,1}$, зададим на нем топологию произведения. Рассматривая $N_{m,n}$ как произведение m копий множества $N_{1,0}$ и n копий множества $N_{0,1}$, зададим на нем топологию произведения.

(а) Пусть B_s — класс все таких $\mathfrak{A}$ из $N_{m,n}$, что $\bar{\mathfrak{A}}((s)_0) = ((s)_1, \dots, (s)_{m+n})$. Показать, что B_s образуют базу для $N_{m,n}$.

(б) Показать, что подмножество P множества $N_{m,n}$ открыто тогда и только тогда, когда оно представляет собой отношение рода Σ_1^0 . [Если P открыто, то согласно (а) P есть объединение всех $B_{\alpha(n)}$ для некоторого α . Если P имеет род Σ_1^0 , то $P(\mathfrak{A}) \leftrightarrow \exists x R(\alpha(x), \mathfrak{A}(x))$ для некоторых R и α .]

(в) Показать, что отображение Φ множества $N_{m,n}$ в $N_{1,0}$ непрерывно тогда и только тогда, когда функционал F , определенный следующим образом: $F(\mathfrak{A}, b) = (\Phi(\mathfrak{A}))(b)$, является функционально рекурсивным. [Если F функционально рекурсивно, то использовать (б), чтобы доказать, что множество, являющееся прообразом открытого множества относительно Φ , само является открытым. Если отображение Φ непрерывно, то показать, что график функционала F открыт, и использовать (б).]

(г) Показать, что класс (m, n) -арных борелевских отношений является наименьшим классом подмножества множеств $N_{m,n}$, содержащим открытые множества и замкнутым относительно взятия дополнений и счетных объединений. [Использовать (б).]

17. (а) Показать, что если P — множество рода Σ_1^1 , то существует такое рекурсивное отношение R , что

$$P(\mathfrak{A}) \leftrightarrow \exists \alpha^* \forall x \exists y R(\mathfrak{A}, \alpha^*, x, y).$$

[Пусть $P(\mathfrak{A}) \leftrightarrow \exists \alpha \forall x Q(\bar{\mathfrak{A}}(x), \bar{\alpha}(x))$, где Q рекурсивно. Тогда $P(\mathfrak{A})$

в том и только в том случае, когда существует α^* , являющаяся представляющей функцией для некоторого $\langle \mathfrak{G}_\beta \rangle$ такого, что

$$\forall x \exists y (\alpha^*(\langle x, y \rangle) = 0 \ \& \ Q(\bar{\mathfrak{A}}(x), y)).]$$

(б) Показать, что если P определено следующим образом: $P(\mathfrak{A}) \leftrightarrow \exists \alpha R(\mathfrak{A}, \alpha)$, где отношение R рекурсивно, то P рекурсивно перечислимо. [Записать правую часть так: $\exists \alpha \exists x Q(\mathfrak{A}, \alpha(x))$, где Q рекурсивно.]

18. (а) Показать, что если Φ — конечная последовательность предикатов рода Δ_n^1 , то Φ^* — предикат рода Δ_n^1 .

(б) Предположим, что P — предикат рода Σ_k^1 (Π_k^1, Δ_k^1) в множестве всех предикатов. Показать, что если $k \geq n$, то P — предикат рода Σ_k^1 (Π_k^1, Δ_k^1), и что если $k < n$, то P — отношение рода Δ_n^1 . [Заметим, что если $P(\mathfrak{A}) \leftrightarrow Q(\Phi^*, \mathfrak{A})$ и R — класс, единственным членом которого является Φ^* , то

$$\begin{aligned} P(\mathfrak{A}) &\leftrightarrow \exists \alpha (R(\alpha) \ \& \ Q(\alpha, R)) \\ &\leftrightarrow \forall \alpha (R(\alpha) \rightarrow Q(\alpha, \mathfrak{A})). \end{aligned}$$

Воспользоваться этим, леммой о конечности и (а).]

(в) Показать, что каждое гиперарифметическое в множестве гиперарифметических предикатов отношение является гиперарифметическим. [Использовать (б) и теорему характеристики.]

(г) Показать, что предикаты, гиперарифметические в множестве предикатов рода Π_n^1 , образуют собственный подкласс класса предикатов рода Δ_{n+1}^1 . [Показать, что существует предикат P рода Π_n^1 , в котором рекурсивен каждый предикат рода Π_n^1 , и выбрать предикат, имеющий род Π_1^1 в P , однако не имеющий рода Σ_1^1 в P . К этому предикату применить (б) и релятивизированную теорему характеристики.]

19. Реляционное множество состоит из множества A и бинарного предиката $<_A$. Убывающей последовательностью в таком реляционном множестве является такая последовательность $a_0, a_1, \dots$ элементов из A , что $a_{n+1} <_A a_n$ для всех n . Реляционное множество вполне фундировано, если в нем нет убывающих последовательностей. Таким образом, дерево является вполне фундированным реляционным множеством с предикатом $<^*$. Реляционное множество называется вполне упорядоченным, если оно вполне фундировано и $<_A$ линейно упорядочивает A . Если x принадлежит A , то $A_{[x]}$ является множеством таких y из A , что $y <_A x$, рассматриваемым в качестве реляционного множества с предикатом $<_A$.

(а) Показать, что ординалы можно сопоставить вполне фундированным реляционным множествам таким же образом, как и деревьям. Ординал, сопоставленный вполне фундированному реляционному множеству A , обозначается через $|A|$.

(б) Если A — реляционное множество, то $DS(A)$ является множеством всех таких чисел $\langle a_1, \dots, a_n \rangle$, что $a_n <_A a_{n-1} <_A \dots <_A a_1$. Показать, что A вполне фундировано тогда и только тогда, когда $DS(A)$ является деревом, и что в этом случае $|A| = \|DS(A)\|$. [Пусть A вполне фундировано и $a = \langle a_1, \dots, a_n \rangle$ принадлежит $DS(A)$,

показать трансфинитной индукцией по $|A[a_n]|$, что $|A[a_n]| = \|DS(A)_{[a]}\|$.

(в) Показать, что для каждого счетного σ существует дерево, имеющее ординал σ . [Использовать (б).]

(г) Реляционное множество A называется *рекурсивным* (гиперарифметическим), если рекурсивными (гиперарифметическими) являются как множество A , так и предикат $<_A$. Показать, что если A — вполне фундированное гиперарифметическое реляционное множество, то $|A|$ рекурсивно. [Показать, что $DS(A)$ — гиперарифметическое множество, и применить теорему ограниченности к классу, неявно определяющему $K_{DS(A)}$.]

(д) Если a и b — номера последовательностей, то $a <^o b$ означает, что либо $a <^* b$, либо существует такое j , что $j < lh(a)$, $j < lh(b)$, $(a)_j < (b)_j$ и $\forall i < j ((a)_i = (b)_i)$. Показать, что если $a_0, a_1, \dots$ — такая последовательность, что $a_{n+1} <^o a_n$ для всех n , то существует такая убывающая относительно $<^*$ последовательности $b_0, b_1, \dots$, что для каждого n при всех достаточно больших m мы имеем $a_m <^* b_n$. [Определить b_n индукцией по n .] Показать, что $<^o$ линейно упорядочивает множество Seq.

(е) Пусть A — реляционное множество; рассмотрим $DS(A)$ как реляционное множество с предикатом $<^o$. Показать, что A вполне фундировано тогда и только тогда, когда $DS(A)$ вполне упорядочено, и что в этом случае $|A| \leq |DS(A)|$. [Использовать (д) и метод из (б).] Затем показать, что рекурсивные ординалы — это в точности ординалы рекурсивных вполне упорядоченных реляционных множеств.

(ж) Показать, что если ординалы σ и τ рекурсивны, то $\sigma + \tau$ и $\sigma \cdot \tau$ также рекурсивны. [Использовать (е).] Затем показать, что κ является предельным числом.

20. Два предиката называются *H-эквивалентными*, если каждый из них является гиперарифметическим в другом.

(а) Показать, что *H-эквивалентность* является отношением эквивалентности. [Использовать релятивизованный вариант 18 (в).] Классы эквивалентности называются *гиперстепенями*. Определим для гиперстепеней отношения $\leq$ и $<$ так же, как и для степеней. Показать, что класс гиперарифметических предикатов является гиперстепенью 0 и что $0 \leq a$ для каждой гиперстепени a .

(б) Гиперстепень a имеет род Π_1^1 в гиперстепени b , если существуют множество A из a и множество B из b такие, что A имеет род Π_1^1 в B . Показать, что отсюда следует, что A имеет род Π_1^1 в каждом множестве из b . Показать, что среди гиперстепеней, имеющих род Π_1^1 в a , существует наибольшая. Она называется *гиперскачком* a и обозначается через a' . Показать, что $a \leq b \rightarrow a' \leq b'$ и что $a < a'$.

(в) Для произвольной конечной последовательности Φ обозначим через κ^Φ наименьший не рекурсивный в Φ ординал. Показать, что если a — гиперстепень, то κ^A один и тот же для всех множеств A из a . [Использовать релятивизованный вариант 19 (г).] Этот ординал обозначается через κ^a . Показать, что $a \leq b \rightarrow \kappa^a \leq \kappa^b$.

(г) Показать, что если a имеет род Π_1^1 в 0 и $\kappa^a = \kappa$, то $a = 0$. [Пусть A — множество рода Π_1^1 из a . Тогда $A(a) \leftrightarrow \text{Tr}(\lambda x F(a, x))$,

где F рекурсивна. Как и в доказательстве теоремы делимости, показать, что существует такой рекурсивный в A ординал σ , что $A(a) \leftrightarrow \text{Tr}_\sigma(\lambda x F(a, x))$. Заметить, что ординал σ рекурсивен, и показать, что множество A гиперарифметическое.]

(д) Показать, что $\kappa^a \neq \kappa \leftrightarrow 0' \leq a$. [Если $\kappa < \kappa^a$, то Tr_κ является гиперарифметическим в каждом множестве из a . Пользуясь теоремой о дереве, показать, что $0' \leq a$. Чтобы доказать обратное утверждение, заметить, что по (г) $\kappa < \kappa^{0'}$, и применить (в).]

(е) Показать, что степенями, имеющими род Π_1^1 в 0, являются лишь 0 и $0'$. [Использовать (г) и (д).]

21. (а) Показать, что если ординал σ рекурсивен, то существует такое гиперарифметическое множество A , что для любой рекурсивной функции F неверно, что $A(a) \leftrightarrow \text{Tr}_\sigma(\lambda x F(a, x))$ для всех a . [Пусть $Q(e, a)$ означает, что $\{e\}^{0,2}$ всюду определена и что $\text{Tr}_\sigma(\lambda x \{e\}(a, x))$. Показать, что Q — гиперарифметический предикат, и применить диагональную лемму.]

(б) Показать, что лемма о замене не верна для гиперарифметических отношений. [Пользуясь 19 (в), выберем Φ так, что $\kappa^\Phi > \kappa$. Предположим, что $P(a) \leftrightarrow P'(\Phi^*, a)$, где P' — гиперарифметический предикат. Выберем такой рекурсивный функционал F , что

$$P'(\alpha, a) \leftrightarrow \text{Tr}(\lambda x F(\alpha, a, x)).$$

Как и в доказательстве теоремы делимости, показать, что $P'(\alpha, a) \leftrightarrow \text{Tr}_\kappa(\lambda x F(\alpha, a, x))$ и, следовательно, $P(a) \leftrightarrow \text{Tr}_\kappa(\lambda x F(\Phi^*, a, x))$, и применить релятивизованный вариант (а).]

22. Определим L_n индуктивно следующим образом:

$$L_0(a) \leftrightarrow a = a, \quad L_{n+1}(a) \leftrightarrow \exists z T_{1,1}((a)_0, K_{L_n}(a)_1, z).$$

Введем $L(n, a) \leftrightarrow L_n(a)$.

(а) Показать, что если множество P рекурсивно перечислимо в L_n , то P рекурсивно в L_{n+1} . [Использовать релятивизованную теорему о нумерации.]

(б) Показать, что каждый арифметический предикат рекурсивен в L . [Используя (а), индукцией по n показать, что каждый предикат рода Σ_n^0 рекурсивен в L_n .] Затем показать, что предикат L неарифметический. [Воспользоваться теоремой об арифметической иерархии и теоремой Поста.]

(в) Показать, что существует такая рекурсивная функция F , что $F(n)$ является *H-индексом* предиката L_n для каждого n . Затем показать, что предикат L гиперарифметический. [Использовать H1.]

23. Пусть Q — такое (1,1)-арное отношение, что для любых множеств A и B

$$A \subset B \rightarrow \forall x (Q(K_A, x) \rightarrow Q(K_B, x)).$$

Множество A называется *Q-замкнутым*, если $\forall x (Q(K_A, x) \rightarrow A(x))$. Пусть A — множество всех чисел, входящих в каждое Q -замкнутое множество.

(а) Показать, что A является Q -замкнутым.

(б) Показать, что

$$A(a) \leftrightarrow \forall \alpha (\forall x (Q(\alpha, x) \rightarrow \alpha(x) = 0) \rightarrow \alpha(a) = 0).$$

Затем показать, что если Q имеет род Π_1^1 , то A имеет род Π_1^1 .

(в) Показать, что в эквивалентности из (б) мы можем α заменить на α^* . Затем показать, что если Q рекурсивно перечислимо, то A рекурсивно перечислимо. [Использовать следствие леммы бесконечности.]

(г) Применяя трансфинитную индукцию по σ , определим для каждого σ множество A_σ следующим образом:

$$A_\sigma(a) \leftrightarrow \exists \tau (\tau < \sigma \ \& \ Q(K_{A_\tau}, a)).$$

Показать, что $\sigma \leq \tau \rightarrow A_\sigma \subset A_\tau$, а затем показать, что существует такой счетный ординал σ , что $A_\sigma = A_{\sigma+1}$. Пусть ρ — наименьший среди таких ординалов. Показать, что $A_\sigma = A$ при $\sigma \geq \rho$.

(д) Показать, что A_0 — пустое множество, что $A_{\sigma+1}$ является множеством таких a , что $Q(K_{A_\sigma}, a)$, и что если σ — предельный ординал, то A_σ — объединение всех A_τ при $\tau < \sigma$.

(е) Показать, что если Q рекурсивно перечислимо, то $\rho \leq \omega$. [Заметить, что для некоторого R

$$Q(K_A, a) \leftrightarrow \exists x R(\bar{K}_A(x), a),$$

и воспользоваться (д), чтобы показать, что $A_{\omega+1} \subset A_\omega$.]

(ж) Пусть для каждого σ дано отношение P_σ ; мы говорим, что P_σ является Π_1^1 -равномерным по σ , если существует такое отношение P' рода Π_1^1 , что $P_{\|B\|}(\mathfrak{A}) \leftrightarrow P'(K_B, \mathfrak{A})$ для каждого дерева B . Показать, что если Q — отношение рода Π_1^1 , то A_σ будет Π_1^1 -равномерным по σ . [Для произвольного дерева B определим P_B следующим образом:

$$P_B(0, a) \leftrightarrow A_{\|B\|}(a),$$

$$P_B(b+1, a) \leftrightarrow B(b) \ \& \ A_{\|B[b]\|}(a).$$

Показать, что для подходящего Π_1^1 -отношения Q'_B множество $\langle P_B \rangle$ является множеством чисел, принадлежащих каждому Q'_B -замкнутому множеству, и воспользоваться эквивалентностью из (б).]

(з) Если P_σ является Π_1^1 -равномерным по σ и

$$\forall \mathfrak{A} \exists \sigma (\sigma < k \ \& \ P_\sigma(\mathfrak{A})),$$

то существует такой рекурсивный ординал τ , что

$$\forall \mathfrak{A} \exists \sigma (\sigma < \tau \ \& \ P_\sigma(\mathfrak{A})).$$

[Пусть $V(\alpha) \rightarrow \exists \mathfrak{A} \forall \sigma (\sigma < k \ \& \ P_\sigma(\mathfrak{A}) \leftrightarrow \|\alpha\| \leq \sigma)$. Применить к V теорему ограниченности.]

(и) Пусть

$$R_\sigma(\alpha, a) \leftrightarrow (\forall x (A_\sigma(x) \rightarrow \alpha(x) = 0) \rightarrow Q(\alpha, a)).$$

Показать, что $\sigma \leq \tau \rightarrow R_\sigma(\alpha, a) \rightarrow R_\tau(\alpha, a)$. Показать, что

$$A_{\sigma+1}(a) \leftrightarrow \forall \alpha R_\sigma(\alpha, a)$$

и что для предельного ординала σ

$$R_\sigma(\alpha, a) \rightarrow \exists \tau (\tau < \sigma \ \& \ R_\tau(\alpha, a)).$$

[Использовать (д).] Показать, что если Q — отношение рода Π_1^1 , то R_σ является Π_1^1 -равномерным по σ . [Использовать (ж).]

(к) Показать, что если Q — отношение рода Π_1^1 , то $\rho \leq k$. [Пользуясь (и), (з) и 19(ж), показать, что $A_{k+1} \subset A_k$.] Затем показать, что если Q — отношение рода Π_1^1 , то A_σ имеет род Π_1^1 для всех σ . [Использовать (ж), (г) и (б).]

24. (а) Показать, что если P — отношение рода Π_1^1 , то существует такое Π_1^1 -отношение Q , что

$$Q(x, \mathfrak{A}) \rightarrow P(x, \mathfrak{A}),$$

$$Q(x, \mathfrak{A}) \ \& \ Q(y, \mathfrak{A}) \rightarrow x = y$$

и

$$\exists x P(x, \mathfrak{A}) \rightarrow \exists x Q(x, \mathfrak{A}).$$

[Использовать теорему униформизации.]

(б) Показать, что если P — отношение рода Π_1^1 и $\forall x \exists y P(y, x)$, то существует такая гиперарифметическая функция α , что $\forall x P(\alpha(x), x)$. [Используя (а), показать, что существует такая α , что $\forall x P(\alpha(x), x)$ и $\mathfrak{G}_\alpha$ имеет род Π_1^1 .]

(в) Показать, что если P — отношение рода Π_1^1 и если для каждого x существует такая гиперарифметическая функция α , что $P(\alpha, x)$, то существует такая гиперарифметическая функция α , что $\forall x P((\alpha)_x, x)$. [Пусть $Q(i, x)$ означает, что i является H -индексом графика такой функции α , что $P(\alpha, x)$. Показать, что Q — отношение рода Π_1^1 . Выбрать согласно (б) гиперарифметическую функцию β так, что $\forall x Q(\beta(x), x)$, и, используя β , построить такую функцию α , что $\forall x P((\alpha)_x, x)$ и $\mathfrak{G}_\alpha$ — отношение рода Π_1^1 .]

25. Пусть $\mathfrak{F}$ — совокупность подклассов некоторого пространства, $\mathfrak{F}_c$ — совокупность дополнений классов из $\mathfrak{F}$. Мы говорим, что $\mathfrak{F}$ удовлетворяет *принципу редукции*, если для каждой пары A и B классов из $\mathfrak{F}$ существуют такие непересекающиеся классы A_1 и B_1 из $\mathfrak{F}$, что $A_1 \subset A$, $B_1 \subset B$ и $A_1 \cup B_1 = A \cup B$. Мы говорим, что $\mathfrak{F}$ удовлетворяет *принципу делимости*, если каждую пару непересекающихся классов из $\mathfrak{F}$ можно разделить с помощью класса, принадлежащего одновременно $\mathfrak{F}$ и $\mathfrak{F}_c$.

(а) Показать, что если $\mathfrak{F}$ удовлетворяет принципу редукции, то $\mathfrak{F}_c$ удовлетворяет принципу делимости.

(б) Показать, что совокупность подмножеств рода Σ_k^0 множества $N_{m,n}$ удовлетворяет принципу редукции. [Пусть $A(\mathfrak{A}) \leftrightarrow \exists x P(\mathfrak{A}, x)$, $B(\mathfrak{A}) \leftrightarrow \exists x Q(\mathfrak{A}, x)$. Определить

$$A_1(\mathfrak{A}) \leftrightarrow \exists x (P(\mathfrak{A}, x) \ \& \ \forall y_{y < x} \neg Q(\mathfrak{A}, y))$$

и аналогично определить B_1 , заменив $<$ на $\leq$.]

(в) Показать, что совокупность подмножеств рода Π_1^1 множества $N_{m,n}$ удовлетворяет принципу редукции. [Пусть $A(\mathfrak{A}) \leftrightarrow \neg \text{Tr}(\lambda x F(\mathfrak{A}, x))$, $B(\mathfrak{A}) \leftrightarrow \text{Tr}(\lambda x G(\mathfrak{A}, x))$. Определить

$$A_1(\mathfrak{A}) \leftrightarrow \text{Tr}(\lambda x F(\mathfrak{A}, x)) \ \& \ \neg \text{Tr}(\lambda x G(\mathfrak{A}, x), \lambda x F(\mathfrak{A}, x))$$

и аналогично определить B_1 , заменив $<$ на $\leq$.]

(г) Показать, что совокупность подмножеств рода Σ_2^1 множества $N_{m,n}$ удовлетворяет принципу редукции. [Пусть

$$A(\mathfrak{A}) \leftrightarrow \exists \beta \text{Tr}(\lambda x F(\mathfrak{A}, \beta, x)),$$

$$B(\mathfrak{A}) \leftrightarrow \exists \beta \text{Tr}(\lambda x G(\mathfrak{A}, \beta, x)).$$

Положить

$$A_1(\mathfrak{M}) \leftrightarrow \exists \beta [\text{Tg}(\lambda x F(\mathfrak{M}, \beta, x)) \& \neg \exists \alpha T_{<}(\lambda x G(\mathfrak{M}, \alpha, x), \lambda x F(\mathfrak{M}, \beta, x))].$$

(д) Показать, что совокупность подмножеств рода Σ_k^0 (Π_1^1 , Σ_2^1) множества $N_{0,2}$ не удовлетворяет принципу отделимости. [Пусть P — бинарный предикат рода Σ_k^0 , перечисляющий класс унарных предикатов рода Σ_k^0 . Пусть $A(a, b) \leftrightarrow P(a, (b)_0)$, $B(a, b) \leftrightarrow P(a, (b)_1)$. Возьмем A_1 и B_1 , о которых говорится в определении принципа редукции. Если некоторый предикат рода Δ_k^0 отделяет A_1 от B_1 , то он должен перечислять класс унарных предикатов рода Δ_k^0 . Однако это невозможно по диагональной лемме.]

26. (а) Показать, что класс функций, степени которых меньше $0'$, является базисом для совокупности классов рода Π_1^0 представляющих функций. [Пусть P — непустой класс рода Π_1^0 представляющих функций. Пусть Q — класс таких α^* , что если $\beta = (\alpha^*)_0$ и $\gamma = (\alpha^*)_1$, то $P(\beta)$ и $\gamma(e) \neq \{e\}(\beta, e)$, как только $\{e\}(\beta, e)$ определено. Применить к Q теорему Крайзеля о базисе.]

(б) Показать, что класс функций, гиперстепени которых меньше $0'$, образуют базис для совокупности функциональных классов рода Π_1^0 . [Пусть P — непустой функциональный класс рода Π_1^0 . Пусть Q — класс таких α , что если $\beta = (\alpha)_0$ и $\gamma = (\alpha)_1$, то $P(\beta)$ и $\gamma(e) \neq K_R(e)$ при условии, что e является H -индексом для R по β . Пользуясь релятивизованным вариантом J , показать, что Q имеет род Σ_1^1 , и применить теорему Клини о базисе.]

(в) Показать, что существует такая гиперстепень a , что $0 < a < 0'$. [Использовать (б) и теорему Клини о базисе.]

(г) Показать, что класс представляющих функций рекурсивно перечислимых множеств не является базисом для совокупности классов рода Π_1^0 представляющих функций. [Показать, что если P и Q рекурсивно перечислимы, то класс представляющих функций множеств, отделяющих P от Q , имеет род Π_1^0 , и применить 7(б).]

27. Для произвольного H -индекса i определим A_i следующим образом:

$$A_i(x) \leftrightarrow \begin{cases} x = i \vee A_{(i)_1}(x), & \text{если } (i)_0 = 1, \\ x = i \vee \exists y (y \in W_{(i)_1} \& A_y(x)), & \text{если } (i)_0 = 2, \\ x = i & \text{в остальных случаях.} \end{cases}$$

(а) Показать, что существует такая рекурсивная функция F , что $A_i = W_{F(i)}$ для каждого H -индекса i . [Использовать теорему о рекурсии.]

(б) Пусть для произвольного H -индекса i

$$J_i(j, a) \leftrightarrow A_i(j) \& J(j, x).$$

Показать, что существует такое арифметическое отношение Q , что $Q(i)$ неявно определяет $\langle K_{J_i} \rangle$ для каждого H -индекса i . [Использовать (а).]

(в) Показать, что каждый гиперарифметический предикат рекурсивен в некоторой функции, неявно определенной некоторым арифметическим классом. [Использовать (б).]

(г) Показать, что если F неявно определена классом рода Π_{2n+1}^0 , то F рекурсивна в функции G , неявно определенной классом рода Π_{2n-1}^0 . [Положить $\alpha = F \leftrightarrow \forall x \exists y R(\alpha, x, y)$ и ввести $G(x) = \langle F(x), \mu y R(F, x, y) \rangle$.]

(д) Показать, что предикат является гиперарифметическим тогда и только тогда, когда он рекурсивен в функции, неявно определенной классом рода Π_1^0 . [Использовать (в) и (г).]

(е) Показать, что предикат имеет род Δ_2^1 тогда и только тогда, когда он гиперарифметический в функции, неявно определенной классом рода Π_1^1 . [Чтобы доказать часть «тогда», применить 18(б). Предположим, что

$$P(a) \leftrightarrow \exists \alpha R(\alpha, a) \quad \text{и} \quad \neg P(a) \leftrightarrow \exists \alpha Q(\alpha, a),$$

где R и Q имеют род Π_1^1 . По теореме униформизации мы можем предполагать, что для каждого a существует единственное α_a такое, что $R(\alpha_a, a) \vee Q(\alpha_a, a)$. Выбрать F так, что $(F)_a = \alpha_a$ для всех a , и показать, что P имеет род Δ_1^1 в F .]

28. Пусть предикат $J(i, a)$ такой же, как и в § 7.10, и пусть H — множество H -индексов.

(а) Показать, что J — негиперарифметический предикат. [Применить диагональную лемму.]

(б) Показать, что H имеет род Π_1^1 , однако не является гиперарифметическим. [Использовать (а) и эквивалентности

$$\begin{aligned} H(i) &\leftrightarrow \exists x (J(i, x) \vee J(\langle 1, i \rangle, x)), \\ J(i, a) &\leftrightarrow H(i) \& \neg J(\langle 1, i \rangle, a). \end{aligned}$$

НАТУРАЛЬНЫЕ ЧИСЛА

8.1. Арифметика Пеано

До сих пор мы изучали общую теорию аксиоматических систем. В этой и следующей главах мы будем изучать аксиоматические системы для двух фундаментальных математических понятий: *натурального числа и множества*.

Теория N не совсем подходит для изучения натуральных чисел. Она содержит лишь немногие из основных функций и предикатов теории чисел и даже для них она содержит лишь некоторые из очевидных аксиом. В частности, отсутствует аксиома индукции, которая необходима для большинства доказательств из теории чисел. Мы покажем, что, присоединив аксиому индукции в подходящем виде, мы получим более удовлетворительную теорию.

Одним из вариантов аксиомы индукции является утверждение о том, что если множество содержит 0 и содержит последователь для каждого натурального числа из этого множества, то оно содержит каждое натуральное число. Мы не можем выразить это утверждение в языке $L(N)$, потому что у нас нет переменных, областью изменения которых являются множества натуральных чисел. В другой форме аксиома индукции утверждает, что если 0 обладает некоторым свойством и если последователь каждого натурального числа, обладающего этим свойством, сам обладает этим свойством, то этим свойством обладает каждое натуральное число. Мы также не можем это выразить в языке $L(N)$, так как у нас нет переменных, областью изменения которых состоит из свойств натуральных чисел. Однако мы можем это выразить для каждого свойства натуральных чисел, которое может быть выражено в языке $L(N)$.

Если A — формула языка $L(N)$, то формула

$$A_x[0] \& \forall x (A \rightarrow A_x[Sx]) \rightarrow A \quad (1)$$

называется *аксиомой индукции*. Теория, полученная из N

выбрасыванием аксиомы $N9$ и присоединением в качестве новых нелогических аксиом всех аксиом индукции, называется *арифметикой Пеано* и обозначается через P .

Нашим первым наблюдением является то, что многие обычные доказательства, использующие индукцию, могут быть формализованы в P . В качестве примера мы докажем в P аксиому $N9$, доказав тем самым, что P является расширением теории N . Пусть формула A есть $0 = y \vee 0 < y$. Тогда по аксиоме тождества $\vdash A_y[0]$. Вследствие $N8$ имеем $\vdash A \leftrightarrow 0 < Sy$, поэтому $\vdash A \rightarrow A_y[Sy]$. Следовательно, $\vdash A$ по аксиомам индукции. Пусть теперь B есть $x < y \rightarrow \rightarrow Sx < Sy$. Тогда $\vdash B_y[0]$ по $N7$. По $N8$

$$\vdash B_y[Sy] \leftrightarrow (x < y \vee x = y \rightarrow Sx < Sy \vee Sx = Sy).$$

Отсюда и из теоремы равенства мы получаем $\vdash B \rightarrow B_y[Sy]$. Таким образом, по аксиомам индукции $\vdash B$. Пусть теперь C есть $x < y \vee x = y \vee y < x$. Из $\vdash A$ мы получаем $\vdash C_x[0]$. Из $\vdash B$ и $N8$

$$\vdash x < y \rightarrow Sx < y \vee Sx = y,$$

$$\vdash y < x \vee y = x \rightarrow y < Sx.$$

Отсюда $\vdash C \rightarrow C_x[Sx]$. Следовательно, $\vdash C$ по аксиомам индукции.

Теперь заметим, что в P могут быть доказаны некоторые обычные следствия аксиомы индукции. Так, мы имеем *принцип полной индукции*

$$\vdash \forall x (\forall y (y < x \rightarrow A_x[y]) \rightarrow A) \rightarrow \forall x A \quad (2)$$

при условии, что y отлично от x и не встречается в A . Для доказательства обозначим $\forall y (y < x \rightarrow A_x[y])$ через B . Тогда $\vdash B_x[0]$ по $N7$. Из $N8$ с помощью элементарных преобразований получаем

$$\vdash B_x[Sx] \leftrightarrow B \vee A. \quad (3)$$

Если теперь C есть левая часть в (2), то по теореме подстановки

$$\vdash C \rightarrow B \rightarrow A. \quad (4)$$

Из (3), (4) и правила $\forall$ -введения

$$\vdash C \rightarrow \forall x (B \rightarrow B_x[Sx]).$$

Отсюда, из $\vdash B_x[0]$ и из аксиом индукции следует $\vdash C \rightarrow B$. Используя это, (4) и правило $\forall$ -введения, мы получаем (2).

Теперь мы можем получить *принцип наименьшего числа*:

$$\exists x A \rightarrow \exists x (A \& \forall y (y < x \rightarrow \neg A_x[y])), \quad (5)$$

где y отлично от x и не встречается в A . Для этого мы в (2) заменим A на $\neg A$ и произведем некоторые элементарные преобразования.

Заметим, что (1), (2) и (5) истинны также в каждом расширении теории P с помощью определений. Действительно, перевод формулы вида (1) в теорию снова имеет вид (1), аналогично для (2) и (5).

Теперь рассмотрим проблему введения новых функций и предикатов. Предположим, что при неформальном построении теории чисел из аксиом Пеано мы имеем определение новой функции или нового предиката u . Если это определение может быть выражено в P , то мы можем ввести расширение P' теории P с помощью определений, в котором некоторый новый нелогический символ u обозначает u ; определяющая аксиома для u будет формально выражать данное неформальное определение символа u . Тогда мы скажем, что мы *ввели* u в P' . Неформальные доказательства свойств u можно тогда заменить формальными доказательствами в теории P' при условии, что техника доказательства не выходит за пределы того, что возможно в P' . (Разумеется, при этом существенно формализовать данное неформальное определение символа u или хотя бы формализовать некоторое неформальное определение, о котором можно доказать в P' , что оно эквивалентно данному.)

Мы покажем, что многие фундаментальные функции и предикаты из теории чисел можно ввести в специального типа расширение теории P с помощью определений. Прежде, чем описать этот тип расширения, мы введем формальный аналог μ -оператора.

Предположим, что P' — расширение теории P с помощью определений и что A — формула теории P' , в которой нет свободных переменных, отличных от $x_1, \dots, x_n, y$. Предположим также, что $\vdash_{P'} \exists y A$. Тогда мы можем получить расширение P'' теории P' с помощью определений, вводя n -арный символ f и определяющую аксиому

$$A_y[f x_1 \dots x_n] \& \forall y (y < f x_1 \dots x_n \rightarrow \neg A). \quad (6)$$

Чтобы убедиться в этом, нам надо доказать условия существования и единственности для f в P' . Условие существования следует из $\vdash_{P'} \exists y A$ и (5); условие единственности является простым следствием аксиомы N9. Обычно мы сокращаем (6) до

$$f x_1 \dots x_n = \mu y A \quad (7)$$

и называем $\exists y A$ *условием существования* для f .

Под *рекурсивным расширением* теории P мы понимаем расширение теории P с помощью определений, в котором определяющие аксиомы для предикатных символов открытые, а определяющие аксиомы для функциональных символов имеют вид (7), где формула A открытая. Простым следствием результатов из § 6.3 является то, что функции и предикаты, введенные в рекурсивных расширениях теории P , рекурсивны. Теперь мы покажем, что в таких расширениях можно ввести большое количество важных рекурсивных функций и предикатов.

Вначале мы заметим, что условие существования для определения

$$f x_1 \dots x_n = \mu x (x = a)$$

есть $\exists x (x = a)$, доказуемое в силу аксиом тождества и теоремы подстановки. Кроме того, из этой аксиомы следует, что

$$f x_1 \dots x_n = a. \quad (8)$$

Обычно мы будем просто говорить, что мы вводим f с помощью аксиомы (8).

Теперь мы проверим R1 — R14. Делая это, мы позволим себе употреблять все латинские буквы (возможно, с верхними индексами) так, как если бы они были переменными теории P . Если функции или предикату неформально было дано имя, то мы пользуемся этим именем как нелогическим символом, обозначающим эту функцию или этот предикат.

Сначала мы отметим, что если R уже введен, то K_R можно ввести с помощью аксиомы

$$K_R(a_1, \dots, a_n) = \mu x ((R(a_1, \dots, a_n) \& x = 0) \vee \vee (\neg R(a_1, \dots, a_n) \& x = 1))$$

(где 1 является сокращением для S0). Условие существования для K_R легко доказывается. Из аксиомы для K_R

где $Q_1, \dots, Q_k, P_1, \dots, P_k$ введены ранее, а (12) и (13) доказуемы, то мы вводим R следующим образом:

$$R(a_1, \dots, a_n) \leftrightarrow ((P_1(a_1, \dots, a_n) \& Q_1(a_1, \dots, a_n)) \vee \dots \vee (P_k(a_1, \dots, a_n) \& Q_k(a_1, \dots, a_n))).$$

С помощью явных определений, данных в § 6.4, мы можем ввести OP , Div и β . Основное свойство функции β можно выразить следующим образом:

$$\exists x \forall y (y < z \rightarrow \beta(x, y) = a), \quad (14)$$

где x, y и z различны, а x и z не входят в a . Это можно доказать, формализовав доказательство, данное в § 6.4. Это дает условие существования для введения функций $\langle a_1, \dots, a_n \rangle$. Остальные функции и предикаты, связанные с номерами последовательностей, можно ввести без всяких трудностей.

Если F уже введена, то мы вводим $\bar{F}$, пользуясь явным определением (14) из § 6.4. Опять же (14) дает нам условие существования. Предположим, что F определена следующим образом:

$$F(b, a_1, \dots, a_n) = G(\bar{F}(b, a_1, \dots, a_n), b, a_1, \dots, a_n), \quad (15)$$

где G уже была введена. Тогда мы вводим F , пользуясь определениями (16) и (17) из § 6.4. Затем, пользуясь элементарными свойствами используемых там функций, мы можем доказать (15). В дальнейшем мы будем просто говорить, что мы ввели F с помощью аксиомы (15).

Если F определена следующим образом:

$$F(0, a_1, \dots, a_n) = G(a_1, \dots, a_n), \\ F(b+1, a_1, \dots, a_n) = H(F(b, a_1, \dots, a_n), b, a_1, \dots, a_n), \quad (16)$$

где G и H введены ранее, то мы можем ввести F с помощью определения вида (15), как это изложено в § 6.4; затем мы можем доказать (16).

Этими средствами мы можем вводить функции из обычной теории чисел (экспоненты, факториалы и т. д.) и формализовать наиболее элементарные доказательства, данные в учебниках по теории чисел. Фактически можно формализовать и много более сложных доказательств, если их несколько модифицировать. Так, многие доказательства в теории чисел используют контурные интегралы в комплексной плоскости. Такие доказательства зачастую

можно формализовать, заменяя интегралы подходящими аппроксимирующими римановыми суммами. Мы не будем вдаваться в подробности, а лишь отметим, что такие методы можно применить с тем, чтобы усилить утверждения, доказанные в оставшейся части этой главы.

8.2. Теорема о доказательствах непротиворечивости

Мы видели, что значительная часть теории чисел может быть формализована в теории P . Теперь мы изучим свойства теории P .

Очевидно, что $\mathcal{N}$ является моделью теории P . Мы называем ее *стандартной* моделью теории P и говорим, что формула теории P *истинна*, если она истинна в $\mathcal{N}$.

Теперь применим результаты главы 6. Так как $\mathcal{N}$ является моделью теории P , то P является непротиворечивым расширением теории N , поэтому по теореме Чёрча теория P неразрешима. Легко привести явное определение множества номеров аксиом индукции, которое показывает, что это множество рекурсивно, а отсюда следует, что теория P рекурсивно аксиоматизированная. Таким образом, по теореме о неполноте теория P неполна. Эти результаты непосредственно обобщаются на рекурсивные расширения теории P .

Пусть P' — некоторое рекурсивное расширение теории P , а $\mathcal{N}'$ — обогащение модели $\mathcal{N}$ до модели теории P' . Мы говорим, что формула теории P' *истинна*, если она истинна в $\mathcal{N}'$. Таким образом, каждая теорема теории P' истинна. Если A — замкнутая формула теории P' , то либо A , либо $\neg A$ истинно. Поэтому ввиду неполноты теории P' существует истинная формула теории P' , не являющаяся теоремой теории P' . Мы изучим эту ситуацию подробнее.

Пусть P' — некоторое рекурсивное расширение теории P . Определим R -формулы теории P' с помощью обобщенного индуктивного определения.

(i) Каждая формула вида $fx_1 \dots x_n = y$, или $px_1 \dots x_n$, или $\neg px_1 \dots x_n$ является R -формулой.

(ii) Если A и B — R -формулы, то $A \vee B$ и $A \& B$ являются R -формулами.

(iii) Если A — R -формула, а x и y различны, то $\forall x (x < y \rightarrow A)$ является R -формулой.

(iv) Если A является R -формулой, то $\exists x A$ является R -формулой.

Лемма 1. Если теория P' является рекурсивным расширением теории P , то каждая экзистенциальная формула теории P' эквивалентна в P' некоторой R -формуле.

Доказательство. Сначала мы докажем это для формул вида $x=a$, пользуясь индукцией по длине a . Если a — переменная, то $x=a$ является R -формулой. В противном случае a есть $fa_1 \dots a_n$. Тогда по следствию 3 теоремы равенства

$$\vdash x=a \leftrightarrow \exists y_1 \dots \exists y_n (y_1 = a_1 \& \dots \& y_n = a_n \& x = fy_1 \dots y_n).$$

По индуктивному предположению формула $y_i = a_i$ эквивалентна некоторой R -формуле, а по теореме симметрии формула $x = fy_1 \dots y_n$ также эквивалентна некоторой R -формуле. Таким образом, формула $x=a$ эквивалентна некоторой R -формуле по теореме эквивалентности.

Очевидно, достаточно доказать, что каждая открытая формула A эквивалентна некоторой R -формуле. Мы докажем это индукцией по длине формулы A . Если A — атомная формула $pa_1 \dots a_n$, то

$$\vdash A \leftrightarrow \exists y_1 \dots \exists y_n (y_1 = a_1 \& \dots \& y_n = a_n \& py_1 \dots y_n).$$

Так как по доказанному выше формула $y_i = a_i$ эквивалентна некоторой R -формуле, то формула A эквивалентна некоторой R -формуле. Аналогичное доказательство справедливо и тогда, когда A является отрицанием атомной формулы *). Осталось рассмотреть случаи, в которых A есть $\neg \neg B$, $\neg(B \vee C)$ и $B \vee C$. Если A есть $\neg \neg B$, то формула B эквивалентна некоторой R -формуле по индуктивному предположению; так как A эквивалентна B , то она эквивалентна некоторой R -формуле. Если A есть $\neg(B \vee C)$, то A эквивалентна $\neg B \& \neg C$. По индуктивному предположению формулы $\neg B$ и $\neg C$ эквивалентны R -формулам, поэтому по теореме эквивалентности формула A эквивалентна некоторой R -формуле. Аналогичное доказательство справедливо, если A есть $B \vee C$.

*) Если A — отрицание атомной формулы вида $\neg(f(a_1, \dots, a_n) = b)$, то $\vdash A \leftrightarrow \exists y_1 \dots \exists y_n \exists z_1 \exists z_2 (y_1 = a_1 \& \dots \& y_n = a_n \& f(y_1, \dots, y_n) = z_1 \& z_2 = b \& \neg(z_1 = z_2))$. — Прим. ред.

Лемма 2. Если P' — рекурсивное расширение теории P , то каждая R -формула теории P' эквивалентна в P' некоторой R -формуле теории P .

Доказательство. Очевидно, достаточно показать, что если P' получена из P'' присоединением одного нового нелогического символа, то каждая R -формула теории P' эквивалентна некоторой R -формуле теории P'' . Также достаточно рассмотреть только R -формулы вида $fx_1 \dots x_n = y$, или $px_1 \dots x_n$, или $\neg px_1 \dots x_n$, где f или p — новый нелогический символ. Из вида определяющей аксиомы для p , правила подстановки и теоремы эквивалентности мы видим, что $px_1 \dots x_n$ и $\neg px_1 \dots x_n$ эквивалентны открытым формулам теории P'' . Вследствие этого по лемме 1 они эквивалентны R -формулам теории P'' . Аналогично, формула $fx_1 \dots x_n = y$ эквивалентна некоторой формуле теории P'' вида $A \& \forall z (z < y \rightarrow A')$, где формулы A и A' открытые. Таким образом, по лемме 1 и теореме эквивалентности она эквивалентна некоторой R -формуле теории P'' .

Численным частным случаем формулы A называется замкнутая формула вида

$$A[k_{a_1}, \dots, k_{a_n}].$$

Лемма 3. Если A — R -формула теории P , то каждый истинный численный частный случай формулы A является теоремой теории P .

Доказательство. Мы пользуемся индукцией по длине формулы A . Если A есть $0=y$, то единственным численным частным случаем является $0=0$, и он доказуем. Если A есть $Sx=y$, то каждый истинный численный частный случай имеет вид $k_{n+1}=k_{n+1}$ и потому доказуем. Если A есть $x+x'=y$, $x \cdot x'=y$, $x=y$, $x \neq y$, $x < y$ или $\neg(x < y)$, то утверждение следует из (1) — (6) из § 6.7. Если A есть $B \vee C$ или $B \& C$, то утверждение следует из индуктивного предположения и теоремы тавтологии. Предположим, что A есть $\forall x (x < y \rightarrow B)$. Истинный численный частный случай формулы A имеет вид $\forall x (x < k_n \rightarrow B')$. Для каждого $i < n$ формула $B'[k_i]$ является истинным численным частным случаем формулы B и, следовательно, доказуема по индуктивному предположению. Таким образом, $\vdash \forall x (x < k_n \rightarrow B)$ по лемме 2 из § 6.7, правилу $\forall$ -введения и правилу отделения.

Наконец предположим, что A есть $\exists xB$. Истинный численный частный случай формулы A имеет вид $\exists xB'$. Так как формула $\exists xB'$ истинна, то при некотором i истинна формула $B'_i[k_i]$. Так как она является численным частным случаем формулы B , то по индуктивному предположению она доказуема. Следовательно, по теореме подстановки $\vdash \exists xB'$.

Комбинируя эти три леммы, мы получаем следующий результат.

Теорема. Если P' — рекурсивное расширение теории P , то каждая истинная замкнутая экзистенциальная формула теории P' является теоремой теории P' .

Мы покажем, что это утверждение нельзя распространить на универсальные формулы. Наша методика получения истинной, но недоказуемой формулы основана на доказательстве теоремы Чёрча. В этом доказательстве мы строим предикат Q , отличный от всех $E(A)$. Мы построим такую формулу A , что $A[k_n]$ истинно тогда и только тогда, когда $Q(n)$. Так как $Q \neq E(A)$, то существует такое n , что $\vdash_P A[k_n]$ не эквивалентно $Q(n)$. Так как доказуемые формулы истинны, то $A[k_n]$ истинна и недоказуема.

Напомним, что Q был определен следующим образом:

$$Q(a) \leftrightarrow \neg \text{Thm}_P(\text{Sub}(a, \ulcorner z \urcorner, \text{Num}(a))).$$

Тогда если $a = \ulcorner A \urcorner$, то $Q(a)$ истинен тогда и только тогда, когда $A[k_a]$ не является теоремой теории P .

Пусть теперь P' является рекурсивным расширением теории P , в котором введены все функции и предикаты из § 6.6 (для теории P). Пусть B есть формула

$$\neg \exists y \text{Pr}_P(\text{Sub}(z, k_{\ulcorner z \urcorner}, \text{Num}(z)), y)$$

(где y отлично от z), и пусть A — перевод формулы B в P . Тогда $B[k_n]$ и $A[k_n]$ истинны тогда и только тогда, когда $Q(n)$. Если $a = \ulcorner A \urcorner$, то $A[k_a]$ истинна тогда и только тогда, когда $Q(a)$, и потому, ввиду сказанного выше, тогда и только тогда, когда $A[k_a]$ не является теоремой теории P . Так как все теоремы теории P истинны, то отсюда следует, что $A[k_a]$ истинна и не является теоремой теории P . Следовательно, $B[k_a]$ истинна и не является теоремой теории P' . Тогда пренексной формой формулы $B[k_a]$ является некоторая истинная универсальная формула теории P' , не являющаяся теоремой теории P' .

Наше доказательство того, что $A[k_a]$ истинна, зависит от того факта, что теоремы теории P истинны. Пользуясь нашими леммами, мы вместо этого можем дать другое доказательство, основанное на непротиворечивости теории P . Согласно леммам 1 и 2 существует некоторая R -формула C теории P , эквивалентная в P' формуле $\neg B[k_a]$. В таком случае C эквивалентна $\neg A[k_a]$ в P' и, следовательно, в P . Таким образом, если $A[k_a]$ ложна, то C истинна, поэтому по лемме 3 $\vdash_P C$ и потому $\vdash_P \neg A[k_a]$. Однако если $A[k_a]$ ложна, то $Q(a)$ ложен и потому $\vdash_P A[k_a]$. Из этих двух результатов и непротиворечивости теории P мы заключаем, что $A[k_a]$ истинно.

Формализуем эти шаги в теории P' . Пусть $\text{Thm}_P(a)$ является сокращением для $\exists y \text{Pr}_P(a, y)$. Пусть $c = \ulcorner C \urcorner$, $d = \ulcorner A[k_a] \urcorner$. Тогда утверждение *если $A[k_a]$ ложно, то C истинно* превращается в

$$\neg A[k_a] \rightarrow C. \quad (1)$$

Утверждение *если C истинно, то $\vdash_P C$* превращается в

$$C \rightarrow \text{Thm}_P(c). \quad (2)$$

Утверждение *если $\vdash_P C$, то $\vdash_P \neg A[k_a]$* превращается в

$$\text{Thm}_P(c) \rightarrow \text{Thm}_P(\text{Neg}(k_d)), \quad (3)$$

где $\text{Neg}(a)$ является сокращением для $\langle k_{\text{SN}(\neg)}, a \rangle$. Утверждение *если $A[k_a]$ ложно, то $\vdash_P A[k_a]$* превращается в

$$\neg A[k_a] \rightarrow \text{Thm}_P(k_d). \quad (4)$$

Утверждение (молчаливо использованное) *если $\vdash_P A[k_a]$ и $\vdash_P \neg A[k_a]$, то теория P противоречива* превращается в

$$\text{Thm}_P(k_d) \rightarrow \text{Thm}_P(\text{Neg}(k_d)) \rightarrow \neg \text{Con}_P, \quad (5)$$

где Con_P является сокращением для $\neg \forall x (\text{For}_P(x) \rightarrow \text{Thm}_P(x))$. Заключительный вывод о том, что *если теория P непротиворечива, то $A[k_a]$ истинно* превращается в

$$\text{Con}_P \rightarrow A[k_a]. \quad (6)$$

Покажем, что все эти утверждения доказуемы в теории P' . Для (1) это следует из того, что $\neg A[k_a]$ эквивалентна C . Рассмотрение (2) мы ненадолго отложим. Рассматривая (3), заметим, что так как $\vdash_P C \rightarrow \neg A[k_a]$,

то

$$\text{Thm}_P(\langle k_{\text{SN}(\vee)}, \text{Neg}(k_c), \text{Neg}(k_d) \rangle) \quad (7)$$

является истинной замкнутой экзистенциальной формулой теории P' и, следовательно, теоремой теории P' . Если мы также формализуем доказательство правила отделения в P' , то (3) мы можем получить из (7). Чтобы доказать (4), заметим, что

$$k_d = \text{Sub}(k_a, k_{\neg z \neg}, \text{Num}(k_a))$$

является истинной свободной от переменных формулой теории P' и, следовательно, теоремой теории P' . Поэтому мы получаем (4) по теореме равенства и по выбору формулы A . Доказательство (5) в P' является просто формализацией очень простой синтаксической леммы. Наконец, (6) является тавтологическим следствием (1) — (5).

Теперь рассмотрим доказательство (2). Пусть $S(a, b_1)$ является сокращением для

$$\text{Sub}(a, k_{\neg x_1 \neg}, \text{Num}(b_1));$$

$S(a, b_1, b_2)$ является сокращением для

$$\text{Sub}(S(a, b_1), k_{\neg x_2 \neg}, \text{Num}(b_2))$$

и т. д. (Разумеется, S зависит от выбора $x_1, x_2, \dots$, однако мы не считаем нужным отмечать это с помощью специальных обозначений.) Докажем, что если D — некоторая R -формула теории P , а $x_1, \dots, x_n$ — переменные, свободные в D , то

$$\vdash_{P'} D \rightarrow \text{Thm}_P(S(k_{\neg D \neg}, x_1, \dots, x_n)); \quad (8)$$

тогда (2) получается отсюда как частный случай. Доказательство проводится индукцией по длине формулы D . Поскольку оно является просто формализацией доказательства леммы 3, то мы лишь кратко рассмотрим несколько случаев.

Предположим, что D есть $0=x$. Опираясь на свойства Sub , мы можем доказать

$$S(k_{\neg D \neg}, x) = \langle k_{\text{SN}(=)}, \text{Num}(0), \text{Num}(x) \rangle.$$

Следовательно, нам надо доказать

$$0=x \rightarrow \text{Thm}_P(\langle k_{\text{SN}(=)}, \text{Num}(0), \text{Num}(x) \rangle).$$

Ввиду теоремы равенства достаточно доказать

$$\text{Thm}_P(\langle k_{\text{SN}(=)}, \text{Num}(0), \text{Num}(0) \rangle).$$

Однако это истинная замкнутая экзистенциальная формула, и потому она доказуема.

Предположим, что D есть $x+y=z$. Как и выше, достаточно доказать

$$\begin{aligned} x+y &= \\ &= z \rightarrow \text{Thm}(\langle k_{\text{SN}(=)}, \langle k_{\text{SN}(+)}, \text{Num}(x), \text{Num}(y) \rangle, \text{Num}(z) \rangle), \end{aligned}$$

а для этого достаточно доказать

$$\text{Thm}_P(\langle k_{\text{SN}(=)}, \langle k_{\text{SN}(+)}, \text{Num}(x), \text{Num}(y) \rangle, \text{Num}(x+y) \rangle).$$

Это формализованный вариант (3) из § 6.7, доказываемый индукцией по y .

Предположим, что D есть $\exists z D'$. Если a есть $S(k_{\neg D' \neg}, x_1, \dots, x_n)$, то по свойствам Sub имеем

$$\vdash S(k_{\neg D \neg}, x_1, \dots, x_n) = \langle k_{\text{SN}(\exists)}, k_{\neg z \neg}, a \rangle. \quad (9)$$

По индуктивному предположению

$$\vdash D' \rightarrow \text{Thm}_P(\text{Sub}(a, k_{\neg z \neg}, \text{Num}(z)));$$

следовательно, по правилу дистрибутивности

$$\vdash D \rightarrow \exists z \text{Thm}_P(\text{Sub}(a, k_{\neg z \neg}, \text{Num}(z))). \quad (10)$$

С другой стороны,

$$\begin{aligned} \vdash \exists z \text{Thm}_P(\text{Sub}(a, k_{\neg z \neg}, \text{Num}(z))) &\rightarrow \\ &\rightarrow \text{Thm}_P(\langle k_{\text{SN}(\exists)}, k_{\neg z \neg}, a \rangle); \end{aligned} \quad (11)$$

действительно, это просто формальное утверждение, говорящее, что если $\vdash D'_z[k_n]$ для некоторого n , то $\vdash \exists z D'$. Из (10), (11) и (9) получаем (8). В остальных случаях следует действовать аналогично, используя формализацию леммы 2 из § 6.7, где D есть $\forall z (z < x_i \rightarrow D')$.

Итак, мы показали, что $\text{Con}_P \rightarrow A[k_a]$ является теоремой теории P' . Так как $A[k_a]$ не является теоремой теории P' , то отсюда следует, что Con_P не является теоремой теории P' . Если мы будем называть перевод формулы Con_P в P формулой теории P , утверждающей, что теория P непротиворечива, то получим следующий результат.

Теорема о доказательствах непротиворечивости (Гёдель). *Формула теории P , утверждающая, что теория P непротиворечива, не является теоремой теории P .*

Как и теорему Чёрча и теорему неполноты, это утверждение можно обобщить на более общие теории, и, не вполне строго говоря, мы можем утверждать, что оно обобщается на более общие аксиоматические системы. Основным выводом является то, что если некоторая аксиоматическая система содержит теорию чисел в том же объеме, что и P , то мы не можем доказать непротиворечивость этой аксиоматической системы из аксиом этой системы.

Теорема о доказательствах непротиворечивости накладывает ограничения на типы доказательств непротиворечивости, которые мы можем дать для теории P . Чтобы они имели какое-нибудь значение, нам надо знать, что некоторые типы доказательств непротиворечивости можно формализовать в P . Разумно предполагать, что каждое финитное доказательство непротиворечивости можно формализовать в P (или, что эквивалентно, в некотором рекурсивном расширении теории P). Во-первых, финитное доказательство имеет дело только с конкретными объектами, а их можно заменить натуральными числами, сопоставляя такое число каждому объекту (как мы это проделали с выражениями). Во-вторых, это доказательство имеет дело с такими объектами конструктивным способом, поэтому мы можем ожидать, что возникающие функции и предикаты могут быть введены в некоторых рекурсивных расширениях теории P .

Изучение конкретных финитных доказательств непротиворечивости подтверждает это предположение. Например, приведенное в главе 4 доказательство непротиворечивости теории N может быть формализовано в P . Формализация доказательства теоремы непротиворечивости является скучным, но элементарным упражнением. Затем следует проверить, что множество номеров истинных свободных от переменных формул теории N можно ввести в некотором рекурсивном расширении теории P ; это также несложно.

Конечно, мы не можем гарантировать, что каждое финитное доказательство непротиворечивости можно формализовать в P , поскольку мы не указали точно, какие методы являются финитными. Можно попытаться доказать

это утверждение из тех аксиом, описывающих финитные методы, которые очевидны даже при нашем неточном определении, но в этом направлении не было достигнуто большого прогресса. Однако исследованиями Крайзеля было показано, что в тех доказательствах непротиворечивости, которые нельзя формализовать в P , должны бы использоваться некоторые принципы, полностью отличные от принципов, использующихся в известных финитных доказательствах.

Мы пришли к заключению, что разумно отказаться от попыток отыскать финитное доказательство непротиворечивости теории P . Однако это не означает, что мы должны удовлетвориться доказательством непротиворечивости посредством стандартной модели. Основной неприятностью в таком доказательстве является не то, что оно не финитно, а то, что оно столь неинформативно. Доказательство непротиворечивости теории N из главы 4 сопровождалось побочными результатами, которые в конечном счете вели к решению проблемы характеристики. Доказательство непротиворечивости теории P посредством стандартной модели не содержит таких побочных результатов. Оно даже не увеличивает наше понимание теории P , потому что не содержит ничего такого, чего бы мы не заложили в P с самого начала.

Существует вторая причина для продолжения поисков доказательства непротиворечивости теории P . Любое финитное доказательство имеет две характерные черты: оно имеет дело с конкретными объектами, и оно обращается с ними конструктивным способом. Теперь мы можем надеяться найти некоторое доказательство непротиворечивости, имеющее дело с абстрактными объектами, однако по-прежнему конструктивное. Первое такое доказательство было найдено Генценом; позднее было найдено несколько других доказательств. Мы приведем одно из таких доказательств, принадлежащее Гёделю.

8.3. Доказательство непротиворечивости

Теперь мы введем формальную систему P' , являющуюся фактически только видоизменением теории P . Символы системы P' те же самые, что и символы теории P , за исключением того, что $\exists$ заменен на $\forall$. Термы и

формулы, свободные и связанные вхождения переменных определены так же, как и в P , только опять $\exists$ заменен на $\forall$.

Аксиомы и правила системы P' получены из аналогичных аксиом и правил теории P с тремя изменениями. Во-первых, аксиомы подстановки теории P заменены на аксиомы подстановки системы P' , которые являются формулами вида $\forall x A \rightarrow A_x[a]$. Во-вторых, правило $\exists$ -введения заменено на следующее правило $\forall$ -введения: из $A \vee B$ выводима $\forall x A \vee B$, если только x не входит свободно в B . В-третьих, аксиомы индукции заменены правилом индукции: из $A_x[0]$ и $A \rightarrow A_x[Sx]$ выводима A .

Очевидно, что теорема тавтологии истинна в P' , потому что модифицированные правила и аксиомы теории P не используются в ее доказательстве.

Мы вводим $\exists$ как сокращение в P' , считая $\exists x A$ сокращением для $\neg \forall x \neg A$. Тогда каждая формула теории P является определяемой формулой системы P' . Покажем, что если $\vdash_P A$, то $\vdash_{P'} A$. Очевидно, для этого достаточно показать, что аксиомы подстановки теории P и аксиомы индукции доказуемы в P' и что правило $\exists$ -введения справедливо в P' .

Согласно аксиомам подстановки системы P' имеем $\vdash_{P'} \forall x \neg A \rightarrow \neg A_x[a]$. Тогда по теореме тавтологии $\vdash_{P'} A_x[a] \rightarrow \neg \forall x \neg A$, т. е. $\vdash_{P'} A_x[a] \rightarrow \exists x A$.

Предположим, что $\vdash_{P'} A \rightarrow B$ и что x не входит свободно в B . По определению $\rightarrow$ и по правилу $\forall$ -введения $\vdash_{P'} \forall x \neg A \vee B$. По теореме тавтологии $\vdash_{P'} \neg \forall x \neg A \rightarrow B$, т. е. $\vdash_{P'} \exists x A \rightarrow B$.

Предположим, что A является аксиомой индукции

$$B_x[0] \& \forall x (B \rightarrow B_x[Sx]) \rightarrow B.$$

Легко заметить, что $A_x[0]$ и $A \rightarrow A_x[Sx]$ доказуемы в P без использования аксиом индукции, следовательно, как уже было доказано, они являются теоремами системы P' . По правилу индукции $\vdash_{P'} A$.

Теорема о доказательствах непротиворечивости показывает, что каждое доказательство непротиворечивости теории P должно использовать что-нибудь такое, что не формализуемо в P . В доказательстве Генцена использована трансфинитная индукция. Мы вместо этого вос-

пользуемся функционалами высших типов, которые мы теперь и опишем.

Определим типовые символы при помощи обобщенного индуктивного определения:

(а) o — типовой символ;

(б) если r и s — типовые символы, то $(r \rightarrow s)$ — типовой символ.

Теперь мы для каждого типового символа r индукцией по длине символа r определим функционалы типа r . Функционалом типа o является натуральное число. Функционалом типа $(r \rightarrow s)$ является отображение множества функционалов типа r в множество функционалов типа s . Впредь функционал будет означать функционал некоторого типа.

Если F — функционал типа $(r \rightarrow (s \rightarrow t))$, а x — функционал типа r , то $F(x)$ является функционалом типа $(s \rightarrow t)$, поэтому если y — функционал типа s , то $F(x)(y)$ является функционалом типа t . Более общо, если F — функционал типа

$$(r_1 \rightarrow (r_2 \rightarrow \dots \rightarrow (r_n \rightarrow s) \dots)), \quad (1)$$

а $x_1, \dots, x_n$ — функционалы типов $r_1, \dots, r_n$ соответственно, то $F(x_1) \dots (x_n)$ является функционалом типа s . Если мы положим

$$F'(x_1, \dots, x_n) = F(x_1) \dots (x_n),$$

то получим отображение F' множества A , состоящего из всех n -ок $(x_1, \dots, x_n)$, где x_i имеет тип r_i при $i = 1, \dots, n$, в множество B всех функционалов типа s . Кроме того, каждое отображение множества A в B может быть получено таким способом из единственного функционала F типа (1). Поэтому мы отождествим F и F' . В смысле обозначений это означает, что вместо $F(x_1) \dots (x_n)$ мы можем писать $F(x_1, \dots, x_n)$. Чтобы подчеркнуть это отождествление, мы будем иногда записывать тип (1) как $(r_1, \dots, r_n \rightarrow s)$.

Ясно, что (m, n) -арный функционал в смысле определения из предшествующей главы является функционалом типа

$$(r_1, \dots, r_m, s_1, \dots, s_n \rightarrow o),$$

где каждое r_i есть $(o \rightarrow o)$ и каждое s_i есть o .

Теперь для рассматриваемых функционалов мы введем язык Y . Язык Y имеет следующие символы.

(i) Для каждого типового символа r переменные типа r

$$x_r, y_r, z_r, \omega_r, x'_r, \dots$$

(ii) Для каждого типового символа r константы типа r . Они будут описаны ниже.

(iii) Символы Λ_r , $=$, $\neg$ и $\vee$.

Переменные типа r будут изменяться на множестве функционалов типа r . Каждая константа типа r будет обозначать конкретный функционал типа r , как это будет разъяснено ниже. Символ Λ_r мы вводим для того, чтобы обозначать результат применения какой-либо функции к ее аргументу; так, мы сокращаем $\Lambda_r uv$ до $u(v)$ и $u(v_1) \dots (v_n)$ до $u(v_1, \dots, v_n)$. Символы $=$, $\neg$ и $\vee$ имеют свой обычный смысл.

Мы применяем x , y и z в качестве синтаксических переменных, областью изменения которых являются переменные языка Y .

Константы и термы языка Y определяются при помощи следующего обобщенного индуктивного определения.

(а) Символ 0 является константой типа o , символ S является константой типа $(o \rightarrow o)$.

(б) Каждая переменная или константа типа r является термом типа r .

(в) Если u — терм типа $(r \rightarrow s)$, а v — терм типа r , то $u(v)$ — терм типа s .

(г) Предположим, что $x_1, \dots, x_n$ — различные переменные типов $r_1, \dots, r_n$ соответственно и что u — терм типа s , в котором нет вхождений переменных, отличных от $x_1, \dots, x_n$. Мы вводим новую константу v типа $(r_1, \dots, r_n \rightarrow s)$ с помощью определяющего равенства $vx_1 \dots x_n = u$.

(д) Предположим, что x — переменная типа o , u — константа типа r , а u' — константа типа $(r, o \rightarrow r)$. Мы вводим новую константу v типа $(o \rightarrow r)$ с помощью определяющих равенств $v(0) = u$ и $v(S(x)) = u'(v(x), x)$.

Константа 0 обозначает натуральное число нуль, а константа S обозначает функцию-последователь. Значения остальных констант даются их определяющими равенствами.

(Это является единственным назначением определяющих равенств. Они не являются определениями в смысле § 1.2, потому что константы не являются определяемыми символами.)

Мы употребляем f , g и h в качестве синтаксических переменных, областью изменения которых являются константы; a , b и c — в качестве синтаксических переменных, областью изменения которых являются термы.

Атомной формулой называется выражение $a = b$, где a и b имеют тип o . Формулы определяются при помощи следующего обобщенного индуктивного определения:

(i) любая атомная формула является формулой;

(ii) если u — формула, то и $\neg u$ — формула;

(iii) если u и v — формулы, то и $\vee uv$ — формула.

(Отметим, что определяющие равенства, вообще говоря, не являются формулами, потому что они являются равенствами между термами, не обязательно имеющими тип o .)

Поскольку мы разъяснили значение всех символов языка Y , то должно быть ясно, что подразумевается, когда говорят, что некоторая формула языка Y истинна при каких-то значениях ее переменных. Мы пишем $\vdash_Y A$ для обозначения того, что A истинна при любых значениях ее переменных, опуская иногда нижний индекс.

Подходящие сокращения, применявшиеся в теориях, можно применять и в языке Y . Чтобы избежать ссылок на типы констант, мы примем следующее соглашение: типы всех переменных и констант таковы, что все выражения, в которых они встречаются, образованы в соответствии с правилами образования термов, формул и определяющих равенств. Так, например, если мы упоминаем о формуле $f(x) = a$, то подразумевается, что для некоторого r символ f имеет тип $(r \rightarrow o)$, x имеет тип r , а a имеет тип o .

Через $u_x[a]$ мы обозначим выражение, полученное из u заменой всех вхождений x на a . Если встречается такой символ, то подразумевается, что x и a имеют одинаковый тип. Аналогично мы употребляем $u_{x_1, \dots, x_n}[a_1, \dots, a_n]$.

Заметим, что существует по крайней мере одна константа каждого типа. Действительно, 0 является константой типа o , и если f имеет тип s , а x является переменной типа r , то мы можем ввести некоторое g типа $(r \rightarrow s)$ с помощью определяющего равенства $g(x) = f$.

Пусть $x_1, \dots, x_n, y, z$ — различные переменные, причем y имеет тип o . Пусть a и b — такие термы типа o , что a не содержит переменных, отличных от $x_1, \dots, x_n$, а b не содержит переменных, отличных от $x_1, \dots, x_n, y, z$. Тогда мы можем найти такую константу f , что

$$\begin{aligned} \vdash f(0, x_1, \dots, x_n) &= a, \\ \vdash f(S(y), x_1, \dots, x_n) &= b_z[f(y, x_1, \dots, x_n)]. \end{aligned} \quad (2)$$

Для этого мы введем f при помощи определяющих равенств $f(0) = g$, $f(S(y)) = h(f(y), y)$, где g и h имеют определяющие равенства

$$\begin{aligned} g(x_1, \dots, x_n) &= a, \\ h(w, y, x_1, \dots, x_n) &= b_z[w(x_1, \dots, x_n)]. \end{aligned}$$

Если мы выбрали некоторое f , удовлетворяющее (2), то мы говорим, что мы *ввели* f при помощи (2). В частности, мы вводим $+$ следующим образом:

$$\begin{aligned} 0 + x &= x, \\ S(y) + x &= S(x + y), \end{aligned}$$

а затем вводим $\cdot$ следующим образом:

$$\begin{aligned} 0 \cdot x &= 0, \\ S(y) \cdot x &= (y \cdot x) + x. \end{aligned}$$

Кроме того, мы введем P следующим образом:

$$\begin{aligned} P(0) &= 0, \\ P(S(y)) &= y, \end{aligned}$$

а затем введем L следующим образом:

$$\begin{aligned} L(0, x) &= x, \\ L(S(y), x) &= P(L(y, x)). \end{aligned}$$

После этого сократим выражение $L(a, b) \neq 0$ до $a < b$. Очевидно, это придает символу $<$ его обычное значение.

Переменные из P' мы отождествляем с переменными типа o языка Y . Тогда каждый терм из P' является термом типа o языка Y , а каждая открытая формула из P' является (возможно, определяемой) формулой языка Y . Кроме того, такая формула имеет в P' то же значение, что и в Y .

Теперь заметим, что для каждой формулы A языка Y существует такой терм a типа o , все переменные которого

входят в A , что

$$\vdash_Y A \leftrightarrow a = 0.$$

Мы легко можем получить a , воспользовавшись индукцией по длине формулы A , если мы имеем такие константы E , N и D , что

$$\begin{aligned} a = b &\leftrightarrow E(a, b) = 0, \\ a \neq 0 &\leftrightarrow N(a) = 0, \\ a = 0 \vee b = 0 &\leftrightarrow D(a, b) = 0. \end{aligned}$$

Последние можно ввести следующим образом:

$$\begin{aligned} E(x, y) &= L(x, y) + L(y, x), \\ N(0) &= 1, \quad N(S(y)) = 0, \\ D(x, y) &= x \cdot y. \end{aligned}$$

По данным различным переменным $x_1, \dots, x_n$, среди которых находятся все переменные, входящие в A , a и b , мы можем найти такую константу f , что

$$\begin{aligned} \vdash A \rightarrow f(x_1, \dots, x_n) &= a, \\ \vdash \neg A \rightarrow f(x_1, \dots, x_n) &= b. \end{aligned} \quad (3)$$

Действительно, воспользовавшись сказанным выше, выберем c так, что $\vdash A \leftrightarrow c = 0$, и введем f с помощью определяющего равенства

$$f(x_1, \dots, x_n) = a \cdot N(c) + b \cdot N(N(c)).$$

Если мы выбрали f , удовлетворяющую (3), то мы говорим, что мы *ввели* f при помощи (3).

Обобщенной формулой называется выражение $\forall x_1 \dots \forall x_m \exists y_1 \dots \exists y_n A$, где $x_1, \dots, x_m, y_1, \dots, y_n$ различны, а A — формула языка Y . Разумеется, оно не является выражением языка Y (исключая случай $m = n = 0$), однако ясно, что оно должно означать. Две обобщенные формулы мы считаем одинаковыми, если они отличаются только выбором подкванторных переменных (т. е. если они являются вариантами).

Для удобства изменим порядок употребления синтаксических переменных до конца этого параграфа. Мы будем употреблять x, y и z для обозначения последовательностей (возможно, пустых) различных переменных. (Областью изменения для w будут по-прежнему переменные из P' .) Если x и y встречаются в одном контексте, то переменные,

входящие в x , отличны от переменных, входящих в y ; аналогично и для других пар синтаксических переменных. Если x есть последовательность $x_1, \dots, x_n$, то $\exists x$ есть $\exists x_1 \dots \exists x_n$ и $\forall x$ есть $\forall x_1 \dots \forall x_n$. Мы применяем a, b и c для обозначения последовательностей (не обязательно различных) термов, а f, g и h для обозначения последовательностей констант. (Областью изменения для d по-прежнему являются термы из P' .) Если a есть последовательность $a_1, \dots, a_n$, а b есть последовательность $b_1, \dots, b_m$, то $a(b)$ есть последовательность

$$a_1(b_1, \dots, b_m), \dots, a_n(b_1, \dots, b_m).$$

Аналогичное значение будут иметь $f(a)$, $b(x)$ и т. д. Если a есть последовательность $a_1, \dots, a_n$, а b есть последовательность $b_1, \dots, b_n$, то $a=b$ означает последовательность равенств $a_1=b_1, \dots, a_n=b_n$. Таким образом, мы можем ввести некоторую последовательность констант f с помощью последовательности определяющих равенств $f(x)=a$.

Чтобы сократить число нижних индексов, мы будем записывать обобщенную формулу $\forall x \exists y A$ в виде $\forall x \exists y A[x, y, z]$, где z состоит из переменных, свободных в A , и, возможно, переменных, не встречающихся в A . Далее, мы пишем $A[a, b, c]$ вместо $A_{x, y, z}[a, b, c]$. Поскольку мы разрешаем переменным, не встречающимся в A , входить в z , и так как мы можем изменять подкванторные переменные, не меняя обобщенной формулы, то мы видим, что любые две обобщенные формулы можно записать в виде $\forall x \exists y A[x, y, z]$ и $\forall x' \exists y' B[x', y', z]$ с обычным соглашением, что все переменные, входящие в x, y, x', y' и z , различны.

Теперь мы сопоставим каждой формуле A из P' некоторую обобщенную формулу A^* . Определение формулы A^* производится индукцией по длине формулы A .

(i) Если A — атомная формула, то A^* есть A .

(ii) Если A есть $\neg B$ и B^* есть $\forall x \exists y B'[x, y, z]$, то A^* есть $\forall y' \exists x \neg B'[x, y'(x), z]$, где y' — последовательность новых переменных соответствующих типов.

(iii) Если A есть $B \vee C$, B^* есть $\forall x \exists y B'[x, y, z]$ и C^* есть $\forall x' \exists y' C'[x', y', z]$, то A^* есть

$$\forall x \forall x' \exists y \exists y' (B'[x, y, z] \vee C'[x', y', z]).$$

(iv) Если A есть $\forall w B$ и B^* есть $\forall x \exists y B'[x, y, z]$, то A^* есть $\forall w \forall x \exists y B'[x, y, z]$.

Хотя это и не будет использоваться в нашем доказательстве, легко заметить, что формулы A и A^* имеют одинаковое значение. Это является очевидным, быть может, за исключением случая (ii). В случае (ii) заметим, что B^* имеет то же самое значение, что и $\exists y' \forall x B'[x, y'(x), z]$, поэтому A имеет то же самое значение, что и $\neg \exists y' \forall x B'[x, y'(x), z]$, а затем воспользуемся пренебрежными операциями.

Если формула A открытая, то A^* есть A . Индукцией по длине формулы A легко проверить, что $A_w[d]^*$ есть $A_w^*[d]$.

Обобщенная формула $\forall x \exists y A[x, y, z]$ называется *верной*, если существует такая последовательность термов a , что $\vdash_{\mathcal{U}} A[x, a, z]$. (Разумеется, отсюда следует, что эта обобщенная формула будет истинной для всех значений своих переменных.)

Теорема. Если $\vdash_{P'} A$, то A^* верна.

Доказательство. Воспользуемся индукцией по теоремам P' . Сначала предположим, что A является пропозициональной аксиомой $\neg B \vee B$. Если B^* есть $\forall x \exists y B'[x, y, z]$, то $(\neg B)^*$ есть (после замены переменных) $\forall y' \exists x' \neg B'[x', y'(x'), z]$, поэтому A^* есть

$$\forall y' \forall x \exists x' \exists y (\neg B'[x', y'(x'), z] \vee B'[x, y, z]).$$

Таким образом, мы должны найти такую последовательность термов a и b , что

$$\vdash \neg B'[a, y'(a), z] \vee B'[x, b, z].$$

Положим a равным x и b равным $y'(x)$.

Теперь предположим, что A является аксиомой подстановки $\forall w B \rightarrow B_w[d]$. Если B^* есть

$$\forall x \exists y B'[x, y, z, w],$$

то $(\neg \forall w B)^*$ есть

$$\forall y' \exists w \exists x' \neg B'[x', y'(w, x'), z, w]$$

и $B_w[d]^*$ есть

$$\forall x \exists y B'[x, y, z, d].$$

Следовательно, A^* есть

$$\forall y' \forall x \exists w \exists x' \exists y (B'[x', y'(w, x'), z, w] \rightarrow B'[x, y, z, d]).$$

Нам надо найти такой терм a и такие последовательности термов b и c , что

$$\vdash B'[b, y'(a, b), z, a] \rightarrow B'[x, c, z, d].$$

Положим a равным d , b равным x и c равным $y'(a, b)$.

Если A является аксиомой равенства, аксиомой тождества или одной из аксиом N1—N8, то формула A открытая и, следовательно, A^* есть A . Очевидно, $\vdash_y A$.

Предположим, что A получена из B по правилу расширения, например, что A есть $C \vee B$. Если B^* есть $\forall x \exists y B'[x, y, z]$ и C^* есть $\forall x' \exists y' C'[x', y', z]$, то A^* есть

$$\forall x' \forall x \exists y' \exists y (C'[x', y', z] \vee B'[x, y, z]).$$

По индуктивному предположению B^* верна, поэтому существует такая последовательность термов a , что $\vdash B'[x, a, z]$. Таким образом, для любой последовательности термов b

$$\vdash C'[x', b, z] \vee B'[x, a, z].$$

Отсюда следует, что A^* верна.

Теперь предположим, что A получена из $A \vee A$ по правилу сокращения. Если A есть $\forall x \exists y A'[x, y, z]$, то $(A \vee A)^*$ есть

$$\forall x \forall x' \exists y \exists y' (A'[x, y, z] \vee A'[x', y', z]).$$

Так как $(A \vee A)^*$ верна, то существуют такие последовательности термов a и a' , что

$$\vdash A'[x, a, z] \vee A'[x', a', z].$$

Подставляя x вместо x' , для подходящих b и b' имеем

$$\vdash A'[x, b, z] \vee A'[x, b', z]. \quad (4)$$

С помощью (3) мы можем найти такую последовательность термов c , что

$$\begin{aligned} A'[x, b, z] &\rightarrow c = b, \\ \neg A'[x, b, z] &\rightarrow c = b'. \end{aligned}$$

Отсюда и из (4) следует, что $\vdash A'[x, c, z]$. Таким образом, A^* верна.

Предположим, что A получена из B по правилу ассоциативности. Тогда матрица формулы A^* может быть получена из матрицы формулы B^* по правилу ассоциативности.

Отсюда сразу следует, что из верности формулы B^* следует верность формулы A^* .

Предположим, что A получена по правилу сечения, например, что A есть $C \vee D$, и получена из формул $B \vee C$ и $\neg B \vee D$. Пусть B^* , C^* и D^* имеют вид

$$\forall x \exists y B'[x, y, z], \quad \forall x' \exists y' C'[x', y', z]$$

и

$$\forall x'' \exists y'' D'[x'', y'', z].$$

Тогда $(B \vee C)^*$ есть

$$\forall x \forall x' \exists y \exists y' (B'[x, y, z] \vee C'[x', y', z]),$$

а $(\neg B \vee D)^*$ есть

$$\forall y_1 \forall x'' \exists x \exists y'' (\neg B'[x, y_1(x), z] \vee D'[x'', y'', z]).$$

Поскольку обе они верны по индуктивному предположению, то мы имеем такие последовательности термов a , a' , b и b' , что

$$\vdash B'[x, a, z] \vee C'[x', a', z], \quad (5)$$

$$\vdash \neg B'[b, y_1(b), z] \vee D'[x'', b', z]. \quad (6)$$

Можно предполагать, что a не содержит переменных, не встречающихся в x , z или x' ; действительно, такие переменные можно было бы заменить константой такого же типа. Далее, мы можем ввести последовательность f при помощи определяющих равенств $f(x', z, x) = a$. Полагая в (5) a равным $f(x', z, x)$, получаем

$$\vdash B'[x, f(x', z, x), z] \vee C'[x', a', z]. \quad (7)$$

Подставляя в (6) $f(x', z)$ вместо y_1 , получаем

$$\vdash \neg B'[b_1, f(x', z, b_1), z] \vee D'[x'', b'_1, z]. \quad (8)$$

Подставляя в (7) b_1 вместо x , имеем

$$\vdash B'[b_1, f(x', z, b_1), z] \vee C'[x', a_1, z]. \quad (9)$$

Из (8) и (9) получаем

$$\vdash C'[x', a_1, z] \vee D'[x'', b'_1, z].$$

Так как A^* есть

$$\forall x' \forall x'' \exists y' \exists y'' (C'[x', y', z] \vee D'[x'', y'', z]),$$

то отсюда следует, что A^* верна.

Теперь предположим, что A получена из $B \vee C$ по правилу $\vee$ -введения. Тогда A есть $\forall w B \vee C$, где w не свободна в C . Легко проверить, что A^* есть $\forall w ((B \vee C)^*)$. Таким образом, если $(B \vee C)^*$ верна, то верна и A^* .

Наконец, предположим, что A получена из $A_w[0]$ и $A \rightarrow A_w[S w]$ по правилу индукции. Пусть A^* есть $\forall x \exists y A'[x, y, z, w]$. Тогда $(A_w[0])^*$ есть

$$\forall x \exists y A'[x, y, z, 0];$$

поэтому по индуктивному предположению существует такая последовательность термов a , что $\vdash A'[x, a, z, 0]$. Как и выше, мы можем определить последовательность g следующим образом: $g(z, x) = a$, и получить, что

$$\vdash A'[x, g(z, x), z, 0]. \quad (10)$$

Теперь $(A \rightarrow A_w[S z])^*$ есть

$$\forall y' \forall x' \exists x' \exists y (A'[x', y', (x'), z, w] \rightarrow A'[x, y, z, S(w)]).$$

По индуктивному предположению существуют такие последовательности b и c , что

$$\vdash A'[b, y'(b), z, w] \rightarrow A'[x, c, z, S(w)].$$

Подставляя $x'(z)$ вместо y' , получаем, что

$$\vdash A'[b', x'(z, b'), z, w] \rightarrow A'[x, c', z, S(w)].$$

Как и ранее, мы можем переписать это следующим образом:

$$\vdash A'[b', x'(z, b'), z, w] \rightarrow A'[x, h(x', w, z, x), z, S(w)]. \quad (11)$$

Пусть f имеет определяющие равенства $f(0) = g$, $f(S(w)) = h(f(w), w)$. Тогда (10) превращается в

$$\vdash A'[x, f(0, z, x), z, 0]; \quad (12)$$

в то же время, подставляя $f(w)$ вместо x' в (11), получаем

$$\vdash A'[b_1, f(w, z, b_1), z, w] \rightarrow A'[x, f(S(w), z, x), z, S(w)]. \quad (13)$$

Теперь покажем, что $\vdash A'[x, f(w, z, x), z, w]$; отсюда будет следовать, что A^* верна. Мы хотим показать, что для каждого n если w имеет значение n , то $A'[x, f(w, z, x), z, w]$ истинна при всех значениях x и z . Докажем это индукцией по n . Для $n=0$ это верно след-

ствие (12). Теперь предположим, что это верно для некоторого n . Если w имеет значение n , а x и z имеют произвольные значения, то

$$A'[b_1, f(w, z, b_1), z, w]$$

истинна; таким образом, вследствие (13)

$$A'[x, f(S(w), z, x), z, S(w)]$$

истинна. Отсюда следует, что если w имеет значение $n+1$, а x и z имеют произвольные значения, то $A'[x, f(w, z, x), z, w]$ истинна. Это завершает доказательство.

Наше доказательство данной теоремы было конструктивным. Действительно, мы показали, как построить последовательность a , показывающую, что A^* верна, по доказательству формулы A в P' .

Теперь доказательство непротиворечивости стало простым. Пусть A есть $0 \neq 0$. Если $\vdash_P A$, то $\vdash_{P'} A$, поэтому A^* верна. Однако A^* есть $0 \neq 0$, которая не верна, следовательно, $0 \neq 0$ не является теоремой теории P , и потому теория P непротиворечива.

8.4. Применения доказательства непротиворечивости

Ранее мы уже отмечали, что финитное доказательство часто дает больше информации, чем нефинитное, потому что оно требует от нас доказать больше, чем на самом деле сформулировано. Это верно и по отношению к конструктивным доказательствам непротиворечивости; хорошим примером служит наше доказательство непротиворечивости теории P . По смыслу стандартной модели из доказательства непротиворечивости мы получаем необходимое условие того, что A является теоремой теории P , а именно, A должна быть истинной. Из нашего конструктивного доказательства мы получаем другое необходимое условие, а именно, A^* должна быть верной. Далее, если A^* верна, то она истинна, и, следовательно, истинна A , однако обратное не всегда выполняется (см. задачу 9 (б)). Таким образом, наше конструктивное доказательство привело к дополнительной информации неконструктивного характера.

Достаточное условие того, что A является теоремой теории P , можно рассматривать как частичное решение

проблемы характеристики для P . Полученное нами решение не является вполне удовлетворительным в одном отношении: если формула A очень сложная, то отношение между A и верностью формулы A^* не вполне ясно. Мы увидим, как можно преодолеть это препятствие.

Как обычно, достаточно рассмотреть замкнутые формулы, находящиеся в пренексной форме. Пусть A — такая формула, и пусть P_0 и P'_0 получены из P и P' присоединением новых функциональных символов из формулы A_H . Доказывая теорему Эрбрана, мы показали, что формула $A \rightarrow A_H$ доказуема без использования нелогических аксиом. Отсюда следует, что если $\vdash_P A$, то A_H является теоремой теории P_0 , а потому и системы P'_0 .

Теперь будем смотреть на каждый из новых функциональных символов из A_H как на переменную языка Y соответствующего типа. Тогда можно определить B^* для произвольной формулы B из P'_0 , как это делалось прежде, и доказать для P'_0 теорему из предыдущего параграфа. Мы приходим к выводу, что если $\vdash_P A$, то A_H^* верна.

Предположим, что $f_1, \dots, f_n$ — новые функциональные символы из A_H и что A_H есть $\exists x_1 \dots \exists x_m B$, где формула B открытая. Легко заметить, что A_H^* есть $\exists x_1 \dots \exists x_m B'$, где B' получена из B приписыванием к ней слева $2m$ знаков отрицания. Отсюда следует, что если $\vdash_P A$, то существуют такие термы $a_1, \dots, a_m$ языка Y , что $\vdash_Y B'[a_1, \dots, a_m]$, и, следовательно, $\vdash_Y B[a_1, \dots, a_m]$. Мы можем предполагать, что a_i не содержит переменных, отличных от $f_1, \dots, f_n$, а тогда мы можем ввести некоторую константу F_i при помощи определяющего равенства $F_i(f_1, \dots, f_n) = a_i$. Отсюда

$$\vdash_Y B[F_1(f_1, \dots, f_n), \dots, F_m(f_1, \dots, f_n)].$$

Мы называем функционал функционалом *рекурсивного типа*, если он обозначен некоторой константой языка Y . Утверждение, которое мы доказали, можно сформулировать следующим образом.

Интерпретация опровержением контрпримера (Крайзель). Пусть A — замкнутая формула в пренексной форме, являющаяся теоремой теории P . Пусть формула A_H есть $\exists x_1 \dots \exists x_m B$, где формула B открытая, и пусть $f_1, \dots, f_n$ — новые функциональные символы из A_H . Тогда существуют такие функционалы $F_1, \dots, F_m$

рекурсивного типа, что

$$B_{x_1, \dots, x_m}[F_1(f_1, \dots, f_n), \dots, F_m(f_1, \dots, f_n)]$$

истинна при любом выборе символов $f_1, \dots, f_n$.

Чтобы пояснить, что это означает, предположим, что A есть

$$\exists x \forall y \exists z \forall w B[x, y, z, w].$$

Тогда A_H есть $\exists x \exists z B[x, f(x), z, g(x, z)]$. Отсюда следует, что если $\vdash_P A$, то существуют такие функционалы F и G рекурсивного типа, что

$$B[F(f, g), f(F(f, g)), G(f, g), g(F(f, g), G(f, g))]. \quad (1)$$

Далее, $\neg A$ эквивалентна формуле $\forall x \exists y \forall z \exists w \neg B[x, y, z, w]$, поэтому A ложна тогда и только тогда, когда существуют такие функции f и g , что для всех x и z

$$\neg B[x, f(x), z, g(x, z)].$$

Подобные функции f и g мы будем называть *контрпримером* к A . Далее, A истинна тогда и только тогда, когда не существует контрпримера к A , т. е. тогда и только тогда, когда для любых f и g мы можем найти такие $F(f, g)$ и $G(f, g)$, что (1) истинно. Дополнительная информация, которую мы получаем, когда A доказуема в P , заключается в том, что F и G можно выбрать среди функционалов рекурсивного типа.

Замечание. Если A истинна, то существуют такая константа e и такая функция f , что $B[e, y, f(y), z]$ для всех y и z . Кажется правдоподобным, что если A доказуема, то функцию f можно выбрать рекурсивной. Однако это неверно; см. задачу 9.

Мы расширим интерпретацию опровержением контрпримера на рекурсивные расширения теории P . Очевидно, для этого достаточно распространить наше доказательство непротиворечивости на такие расширения. (Отметим, что такое обобщение доказательства непротиворечивости бессмысленно для доказательства собственно непротиворечивости, потому что непротиворечивость каждого рекурсивного расширения теории P следует из непротиворечивости теории P ввиду предшествующих результатов.)

Очевидно, достаточно предположить, что мы распространили доказательство непротиворечивости на рекурсивное

расширение P' , и показать, что его можно распространить также на рекурсивное расширение P'' , содержащее на один нелогический символ больше, чем P' . Сначала предположим, что присоединяемый символ есть предикатный символ p с определяющей аксиомой $px_1 \dots x_n \leftrightarrow A$. Тогда формула A открытая, поэтому A^* есть A . Мы вводим p в качестве определяемого символа языка Y , считая $pa_1 \dots a_n$ сокращением для $A[a_1, \dots, a_n]$. Очевидно, p имеет в Y такой же смысл, что и в P'' . Кроме того, $(px_1 \dots x_n \leftrightarrow A)^*$ есть $px_1 \dots x_n \leftrightarrow A$, которая наверняка верна; таким образом, наше доказательство непротиворечивости обобщено.

Теперь предположим, что новым нелогическим символом является функциональный символ f с определяющей аксиомой

$$fx_1 \dots x_n = \mu y A. \quad (2)$$

Тогда формула A открытая и $\vdash_{P'} \exists y A$. Поскольку наше доказательство непротиворечивости было обобщено на P' , то $(\exists y A)^*$, которая есть не что иное, как $\exists y \neg \neg A$, верна. Отсюда следует, что существует такой терм a , что $\vdash_Y \neg \neg A_y[a]$ и, следовательно, $\vdash_Y A_y[a]$. Если g имеет определяющее равенство

$$g(x_1, \dots, x_n) = a,$$

то мы получаем, что

$$\vdash_Y A_y[g(x_1, \dots, x_n)]. \quad (3)$$

Введем теперь константу h следующим образом:

$$\begin{aligned} A \rightarrow h(y, w, x_1, \dots, x_n) &= y, \\ \neg A \rightarrow h(y, w, x_1, \dots, x_n) &= S(w), \end{aligned}$$

и константу f' следующим образом:

$$\begin{aligned} f'(0, x_1, \dots, x_n) &= 0, \\ f'(S(w), x_1, \dots, x_n) &= h(f'(w, x_1, \dots, x_n), w, x_1, \dots, x_n). \end{aligned}$$

Тогда

$$\begin{aligned} \vdash_Y A_y[f'(w, x_1, \dots, x_n)] \vee f'(w, x_1, \dots, x_n) &= w, \quad (4) \\ \vdash_Y y < f'(w, x_1, \dots, x_n) \rightarrow \neg A. \quad (5) \end{aligned}$$

Будем считать f константой языка Y с определяющим равенством

$$f(x_1, \dots, x_n) = f'(g(x_1, \dots, x_n), x_1, \dots, x_n).$$

Тогда из (3), (4) и (5) получаем, что

$$\vdash_Y A_y[f(x_1, \dots, x_n)], \quad (6)$$

$$\vdash_Y y < f(x_1, \dots, x_n) \rightarrow \neg A. \quad (7)$$

Отсюда следует, что f имеет в Y тот же смысл, что и в P'' .

Нам еще надо показать, что если B есть аксиома (2), то B^* верна. Однако B есть

$$A_y[f x_1 \dots x_n] \& \forall y (y < f x_1 \dots x_n \rightarrow \neg A);$$

поэтому B^* есть

$$\forall y (A_y[f(x_1, \dots, x_n)] \& (y < f(x_1, \dots, x_n) \rightarrow \neg A)).$$

Она верна вследствие (6) и (7).

В процессе расширения доказательства непротиворечивости мы показали, что каждая функция, которую можно ввести в некотором рекурсивном расширении теории P , имеет рекурсивный тип. Теперь мы увидим, что, наоборот, каждую функцию рекурсивного типа можно ввести в некотором рекурсивном расширении теории P .

Введем формальную систему F . Символами системы F являются константы языка Y и символы Ar и $=$. Сокращение $u(v_1 \dots, v_n)$ мы вводим так же, как и в Y . Термы системы F определены при помощи следующего обобщенного индуктивного определения:

(а) константа типа r является термом типа r ;

(б) если u — терм типа $(r \rightarrow s)$, а v — терм типа r , то $u(v)$ — терм типа s .

Синтаксическими переменными f, g, h, a, b и c мы пользуемся так же, как и в Y . Формулами системы F являются выражения $a = b$, где a и b имеют одинаковый тип.

Каждая формула $a = a$ является аксиомой системы F . Если f имеет определяющее равенство

$$f(x_1, \dots, x_n) = a,$$

а $g_1, \dots, g_n$ имеют тип $x_1, \dots, x_n$ соответственно, то

$$f(g_1, \dots, g_n) = a[g_1, \dots, g_n]$$

является аксиомой системы F . Если f имеет определяющие равенства $f(0) = g$ и $f(S(x)) = h(f(x), x)$, то $f(0) = g$ является аксиомой системы F и все формулы $f(k_{n+1}) = h(f(k_n), k_n)$ являются аксиомами системы F . Этим множество аксиом системы F исчерпывается. Единственным

правилом системы F является следующее правило: B выводима из A и $a=b$, если B получена из A заменой некоторого вхождения a на b или наоборот.

Определим понятие *сводимого* терма типа r индукцией по длине r . Терм a типа o является сводимым, если $\vdash_F a = k_n$ для некоторого n . Терм a типа $(r \rightarrow s)$ является сводимым, если $a(b)$ является сводимым для каждого сводимого терма b типа r .

Докажем теперь некоторые простые факты о сводимости.

(i) Если каждая входящая в a константа сводима, то a сводим. Докажем это индукцией по длине терма a . Если a — константа, то утверждение тривиально. В противном случае a есть $b(c)$, где b и c сводимы по индуктивному предположению. Тогда a сводим по определению сводимости для b .

(ii) Если $\vdash a = b$ и b сводим, то a сводим. Воспользуемся индукцией по типу терма b . Если b имеет тип o , то $\vdash b = k_n$ для некоторого n , и, следовательно, $\vdash a = k_n$ по правилу системы F . Таким образом, a сводим. Пусть b имеет тип $(r \rightarrow s)$, и пусть c — сводимый терм типа r . Так как $\vdash a(c) = a(c)$ и $\vdash a = b$, то получаем, что $\vdash a(c) = b(c)$. Поскольку терм b сводимый, сводимым будет и $b(c)$, так что $a(c)$ сводим по индуктивному предположению. Таким образом, a сводим.

(iii) Если $a(k_n)$ сводим для каждого n , то a сводим. Действительно, пусть b — сводимый терм типа o , тогда $\vdash b = k_n$ для некоторого n . Так как $\vdash a(b) = a(b)$, то $\vdash a(b) = a(k_n)$. Терм $a(b)$ сводим по условию и (ii).

Теперь индукцией по константам покажем, что каждая константа сводима. Очевидно, константа 0 сводима. Так как $S(k_n)$ есть k_{n+1} , то она сводима, следовательно, S сводима по (iii). Пусть f имеет определяющее равенство $f(x_1, \dots, x_n) = a$, где каждая константа из a сводима. Очевидно, чтобы доказать, что f сводима, достаточно показать, что $f(g_1, \dots, g_n)$ сводима для всех сводимых констант $g_1, \dots, g_n$ (*). Однако

$$\vdash f(g_1, \dots, g_n) = a[g_1, \dots, g_n]$$

*) Действительно, если b_i — сводимый терм, то, вводя константу g_i определяющим равенством $g_i = b_i$, имеем по (ii), что g_i — сводимая константа. Далее, из $\vdash f(b_1, \dots, b_n) = f(g_1, \dots, g_n)$ следует по (ii), что из сводимости $f(g_1, \dots, g_n)$ следует сводимость $f(b_1, \dots, b_n)$. — Прим. ред.

и $a[g_1, \dots, g_n]$ сводима по (i). Отсюда следует, что $f(g_1, \dots, g_n)$ сводима по (ii).

Пусть теперь f имеет определяющие равенства $f(0) = g$, $f(x) = h(f(x), x)$, где g и h сводимы. Индукцией по n покажем, что $f(k_n)$ сводима, тогда сводимость f будет следовать из (iii). Так как $\vdash f(0) = g$, то $f(0)$ сводима в силу (ii). Далее, предположим, что $f(k_n)$ сводима. Из сводимости h следует сводимость $h(f(k_n), k_n)$. Ввиду сводимости k_n отсюда следует, что $h(f(k_n), k_n)$ сводима. Так как

$$\vdash f(k_{n+1}) = h(f(k_n), k_n),$$

то из (ii) следует, что $f(k_{n+1})$ сводима.

Следующим шагом является сопоставление номеров выражениям системы F и введение определений, аналогичных определениям, введенным для F в § 6.6. Поскольку в этом нет ничего нового, то мы это пропустим. Пусть f — константа, обозначающая некоторую n -арную функцию рекурсивного типа, тогда мы можем определить такой предикат R , что $R(a_1, \dots, a_n, b)$ означает, что b есть номер доказательства формулы вида $fk_{a_1} \dots k_{a_n} = k_c$, и такую функцию G , что если b является номером такого доказательства, то $G(b) = c$. Так как f сводима, то для всех $a_1, \dots, a_n$ мы имеем $\exists b R(a_1, \dots, a_n, b)$, и ясно, что

$$G(\mu b R(a_1, \dots, a_n, b)) \quad (8)$$

является как раз функцией, обозначенной через f .

Воспользовавшись результатами из § 8.1, мы можем ввести R и G в некотором рекурсивном расширении P' теории P . Чтобы ввести функцию (8), мы должны уметь доказать в P' условие существования $\exists y R(x_1, \dots, x_n, y)$. По существу это означает, что мы должны уметь доказать сводимость f в P' .

Для каждого типового символа r в некотором (нерекурсивном) расширении системы P' с помощью определений мы можем ввести такой предикат Red_r , что $\text{Red}_r(x)$ означает, что x является номером какого-то сводимого терма типа r . Затем мы можем доказать (i) отдельно для каждого типа, т. е. для каждого r мы можем доказать формулу, утверждающую, что (i) истинно для всех термов a типа r . Аналогично, (ii) и (iii) можно доказать отдельно для каж-

дого типа. Затем индукцией по константам мы можем показать, что если a — номер некоторой константы типа r , то $\vdash \text{Red}_r(k_a)$.

Полагая a равным номеру константы f , мы получаем нужный результат *).

8.5. Арифметика второго порядка

Мы убедились в том, что не существует аксиоматической системы, в которой можно доказать все истинные формулы теории P и ни одной ложной. Однако весьма естественно искать такой способ расширения теории P , который позволит нам доказать больше истинных утверждений о натуральных числах. Один из способов сделать это — это присоединить переменные, областью изменения которых являются функционалы высших типов. Мы рассмотрим несколько упрощенную систему, в которой мы присоединяем переменные, областью изменения которых являются множества чисел; это разъяснит возникающие проблемы и в то же время позволит избежать некоторых трудностей.

Наиболее естественным путем было бы присоединение к P нового вида переменных. Однако при этом мы не получили бы теории, а потому не могли бы воспользоваться полученными ранее результатами. Вместо этого мы будем придерживаться процедуры, предложенной в § 2.1 для работы с двумя видами индивидов.

Опишем теорию S , называемую *арифметикой второго порядка*. Нелогическими символами теории S являются нелогические символы теории P , бинарный предикатный символ $\in$ и унарные предикатные символы N и C . Примем соглашение, что Nx будет означать, что x есть некоторое число, и что Cx будет означать, что x есть некоторое множество чисел.

Договоримся применять строчные латинские буквы так, как если бы они были переменными из S . Кроме того, мы вообще будем предпочитать использовать буквы из этого алфавита в тех случаях, когда переменная обозначает число,

*) Нам нужно получить доказательство $\exists y R(x_1, \dots, x_n, y)$ в P' . Для этого замечаем, что $\text{Red}_r(k_a) \rightarrow \exists y R(x_1, \dots, x_n, y)$ доказуема в рассматриваемом расширении P' , тогда и $\exists y R(x_1, \dots, x_n, y)$ доказуема в этом расширении. Но это расширение консервативно (см. § 4.6), поэтому $\vdash_{P'} \exists y R(x_1, \dots, x_n, y)$. — Прим. ред.

а не множество. Это соглашение вводится только затем, чтобы облегчить чтение, и имеет неофициальный характер.

Наши первые две нелогические аксиомы утверждают, что каждый индивид есть либо число, либо множество, но не то и другое одновременно:

$$Nx \vee Cx, \quad (1)$$

$$\neg (Nx \& Cx). \quad (2)$$

Следующие три аксиомы говорят о том, что некоторые индивиды являются числами или множествами:

$$N0, \quad (3)$$

$$Na \rightarrow NSa, \quad (4)$$

$$a \in x \rightarrow Na \& Cx. \quad (5)$$

Определим интерпретацию I языка $L(P)$ в языке $L(S)$, считая, что U_I есть N и что u_I есть u для нелогического символа u теории P . Тогда в качестве новых нелогических аксиом мы возьмем интерпретации аксиом N1 — N8 относительно I .

Аксиомой индукции теории S является

$$Cx \& 0 \in x \& \forall a (Na \& a \in x \rightarrow Sa \in x) \rightarrow \forall a (Na \rightarrow a \in x).$$

Аксиомой объемности является

$$Cx \& Cy \& \forall a (a \in x \leftrightarrow a \in y) \rightarrow x = y;$$

она утверждает, что два множества, имеющие одни и те же элементы, совпадают.

Теперь нам нужны такие аксиомы, которые позволят нам получить некоторые множества. Основной способ получить некоторое множество — это взять множество всех чисел, имеющих некоторое свойство. Введем некоторые аксиомы, называемые *аксиомами выделения*, которые показывают, что множества, определенные таким способом, существуют. Ими являются все формулы вида

$$\exists y (Cy \& \forall x (x \in y \leftrightarrow Nx \& A)),$$

где y отлично от x и не встречается в A .

Так как функция, обозначенная некоторым функциональным символом, должна быть определена для всех индивидов, то Sx должна иметь смысл даже тогда, когда x является множеством. В этом случае мы положим $Sx = 0$.

Аналогичное соглашение мы примем и относительно поведения $+$, $\cdot$ и $<$, если их аргументами являются не числа. Это выражается следующими аксиомами:

$$Cx \rightarrow Sx = 0, \quad (6)$$

$$Cx \vee Cy \rightarrow x + y = 0 \& x \cdot y = 0 \& \neg(x < y). \quad (7)$$

Этим наш список нелогических аксиом теории S завершается.

Построим модель $\mathcal{N}'$ теории S следующим образом. Пусть $N_{\mathcal{N}'}$ является множеством натуральных чисел, а $C_{\mathcal{N}'}$ является множеством всех множеств натуральных чисел. Обозначим через $|\mathcal{N}'|$ объединение $N_{\mathcal{N}'}$ и $C_{\mathcal{N}'}$. Пусть $a \in {}_{\mathcal{N}'}x$ истинно, если a является числом, x является множеством и $a \in x$. Пусть u — нелогический символ теории P , придадим $u_{\mathcal{N}'}$ то же самое значение, что и $u_{\mathcal{N}}$, если аргументами являются числа, и значение, данное согласно (6) и (7), при других аргументах. Ясно, что $\mathcal{N}'$ на самом деле является моделью теории S . Мы называем ее *стандартной* моделью теории S и говорим, что формула теории S *истинна*, если она истинна в $\mathcal{N}'$.

Изучим теперь некоторые синтаксические свойства теории S . Предположим, что $x_1, \dots, x_n, y$ — различные переменные, и среди них находятся все свободные переменные формулы A . Тогда мы можем ввести новый функциональный символ f с помощью определяющей аксиомы

$$Cfx_1 \dots x_n \& \forall y (y \in fx_1 \dots x_n \leftrightarrow Ny \& A). \quad (8)$$

Действительно, условием существования для f является аксиома выделения, а условие единственности является простым следствием аксиомы объемности и (5). Из аксиомы индукции следует, что

$$\begin{aligned} \vdash 0 \in fx_1 \dots x_n \& \forall y (Ny \& y \in fx_1 \dots x_n \rightarrow \\ \rightarrow Sy \in fx_1 \dots x_n) \rightarrow \forall y (Ny \rightarrow y \in fx_1 \dots x_n), \end{aligned}$$

поэтому вследствие (8) и теоремы эквивалентности получаем

$$\begin{aligned} \vdash N0 \& A_y[0] \& \forall y (Ny \& A \rightarrow NSy \& A_y[Sy]) \rightarrow \\ \rightarrow \forall y (Ny \rightarrow Ny \& A). \end{aligned}$$

Ввиду (3) и (4) это можно упростить до

$$\vdash A_y[0] \& \forall y (Ny \& A \rightarrow A_y[Sy]) \rightarrow \forall y (Ny \rightarrow A). \quad (9)$$

Отсюда мы получаем *правило индукции*: если $\vdash A_y[0]$ и $\vdash Ny \& A \rightarrow A_y[Sy]$, то $\vdash Ny \rightarrow A$.

Теперь докажем, что I является интерпретацией теории P в теории S . Вследствие (3)

$$\vdash \exists a Na. \quad (10)$$

Интерпретациями аксиом N3 и N4 являются

$$Na \rightarrow a + 0 = a, \quad (11)$$

$$Na \rightarrow Nb \rightarrow a + Sb = S(a + b). \quad (12)$$

Вследствие (12) и (4)

$$\vdash Nb \rightarrow (Na \rightarrow N(a + b)) \rightarrow (Na \rightarrow N(a + Sb)). \quad (13)$$

Из (11), (13) и правила индукции получаем, что

$$\vdash Nb \rightarrow Na \rightarrow N(a + b). \quad (14)$$

Аналогично, используя (14) и интерпретации аксиом N5 и N6, получаем, что

$$\vdash Nb \rightarrow Na \rightarrow N(a \cdot b). \quad (15)$$

Вследствие (10), (3), (4), (14) и (15) I является интерпретацией языка $L(P)$ в теории S . Остается показать, что интерпретация аксиомы индукции теории P доказуема в S . Эта интерпретация имеет вид

$$\begin{aligned} Ny_1 \rightarrow \dots \rightarrow Ny_n \rightarrow (A_x[0] \& \forall x (Nx \rightarrow A \rightarrow A_x[Sx])) \rightarrow \\ \rightarrow \forall x (Nx \rightarrow A) \end{aligned}$$

и, таким образом, доказуема вследствие (9).

Комбинируя это с результатами из § 4.7, мы видим, что I можно расширить до интерпретации любого рекурсивного расширения теории P в некотором расширении теории S с помощью определений. Таким образом, те функции и предикаты, которые могут быть введены в рекурсивном расширении теории P , могут быть также введены в расширении теории S с помощью определений. Иногда мы будем молчаливо предполагать, что некоторые из этих функций и предикатов уже введены.

Разумеется, эти результаты позволяют вводить лишь те функции, значениями которых являются числа. Укажем, как можно вводить функции, значениями которых являются множества, если они определены индуктивно. Для простоты рассмотрим лишь унарные функции.

Предположим, что в некотором расширении S' теории S с помощью определений имеется константа A и бинарный функциональный символ G и что мы можем доказать $C(A)$ и $C(G(x, a))$. Мы покажем, что в некотором расширении теории S' с помощью определений можно ввести функциональный символ F и доказать

$$F(0) = A,$$

$$Na \rightarrow F(Sa) = G(F(a), a).$$

Используя (8), определим функциональный символ Cut определяющей аксиомой

$$\forall b (b \in \text{Cut}(x, a) \leftrightarrow Nb \ \& \ \langle a, b \rangle \in x).$$

Тогда мы можем выписать определяющую аксиому для функционального символа H , говорящую следующее. Если x — множество, то $H(x) = 0$. Если a — число, то $H(a)$ — множество чисел вида $\langle b, c \rangle$, где $b \leq a$. Кроме того, $\text{Cut}(H(a), 0) = A$ и для каждого $b < a$ выполняется $\text{Cut}(H(a), Sb) = G(\text{Cut}(H(a), b), b)$. Условие существования и единственности для H мы можем доказать индукцией, используя аксиомы выделения при доказательстве существования и аксиому объемности при доказательстве единственности. Воспользовавшись индукцией по b , мы можем также доказать, что $\text{Cut}(H(Sa), b) = \text{Cut}(H(a), b)$ при $b \leq a$. Введем F с помощью определяющей аксиомы $F(a) = \text{Cut}(H(a), a)$. Тогда

$$F(0) = \text{Cut}(H(0), 0) = A,$$

$$\begin{aligned} F(Sa) &= \text{Cut}(H(Sa), Sa) = G(\text{Cut}(H(Sa), a), a) = \\ &= G(\text{Cut}(H(a), a), a) = G(F(a), a). \end{aligned}$$

Правильный путь «доказать» формулу A теории P в теории S — это доказать $A^{(1)}$. Мы видим, что каждую теорему теории P можно доказать в этом смысле в S . Как уже говорилось в начале этого параграфа, не каждая истинная формула теории P может быть доказана в S (см. задачу 10). Однако существуют истинные формулы теории P , которые недоказуемы в P , но доказуемы в S . Мы проиллюстрируем это, набросав план доказательства $\text{Con}_P^{(1)}$ в S .

Идея заключается в формализации доказательства непротиворечивости теории P с помощью стандартной

модели. Другими словами, мы индукцией по теоремам докажем, что каждая теорема теории P истинна, и придем к заключению, что $0 \neq 0$ не является теоремой теории P . Сделать это очень просто, как только мы получим определение истинных формул теории P . Для этого достаточно определить истинные замкнутые формулы. Это можно сделать индукцией по высоте формулы после того, как мы определим истинные свободные от переменных атомные формулы. Однако множество номеров истинных свободных от переменных атомных формул можно определить в некотором рекурсивном расширении теории P , а потому и в S . Тогда описанным выше методом мы можем ввести такое F , что $F(a)$ является множеством номеров истинных замкнутых формул высоты, не превосходящей a . Затем легко определить множество номеров истинных замкнутых формул.

З а м е ч а н и е. Разумеется, это доказательство нельзя провести в P . Причиной является то, что истинность истинного замкнутого утверждения зависит от истинности или ложности бесконечного числа формул меньшей высоты. Мы не можем определить в P функцию, если ее значения зависят от бесконечного числа прежних значений.

Перейдем теперь к моделям теории S . Если $\mathcal{A}$ — модель теории S , то $\mathcal{A}_1$ (в обозначениях из § 6.9) — структура для $L(P)$. Если A — аксиома теории P , то $\vdash_S A^{(1)}$, поэтому $A^{(1)}$ истинна в $\mathcal{A}$, следовательно, A истинна в $\mathcal{A}_1$. Таким образом, $\mathcal{A}_1$ — модель теории P .

Модель $\mathcal{A}$ теории S называется *регулярной*, если $C_{\mathcal{A}}$ является множеством подмножеств множества $N_{\mathcal{A}}$ и $a \in_{\mathcal{A}} x \leftrightarrow a \in x$, где a принадлежит $N_{\mathcal{A}}$, а x принадлежит $C_{\mathcal{A}}$. Мы покажем, что каждая модель $\mathcal{A}$ теории S изоморфна некоторой регулярной модели. Заменяя $\mathcal{A}$ на какую-нибудь изоморфную модель, мы можем предполагать, что никакой элемент из $|\mathcal{A}|$ не является подмножеством множества $|\mathcal{A}|$. Определим отображение φ следующим образом: если a принадлежит $N_{\mathcal{A}}$, то $\varphi(a) = a$; если x принадлежит $C_{\mathcal{A}}$, то $\varphi(x)$ является таким множеством элементов a из $N_{\mathcal{A}}$, что $a \in_{\mathcal{A}} x$. Используя (1), (2) и аксиому объемности, мы видим, что φ — биективное отображение $|\mathcal{A}|$ в некоторое множество. Отсюда следует, что существует такая модель $\mathcal{B}$, что φ является изоморфизмом между $\mathcal{A}$ и $\mathcal{B}$. Очевидно, $\mathcal{B}$ регулярна.

Регулярная модель $\mathcal{A}$ полностью определяется по $\mathcal{A}_I$ и $S_{\mathcal{A}}$. Действительно, $\mathcal{A}_I$ определяет $N_{\mathcal{A}} = |\mathcal{A}_I|$ и значения функций и предикатов, отличных от $\in_{\mathcal{A}}$, для аргументов из $N_{\mathcal{A}}$. Согласно (1) $|\mathcal{A}|$ должно быть объединением $N_{\mathcal{A}}$ и $S_{\mathcal{A}}$, а (5) и условие регулярности определяют $\in_{\mathcal{A}}$. Остальные функции и предикаты для аргументов, не принадлежащих $N_{\mathcal{A}}$, определены согласно (6) и (7).

Лемма. Модель $\mathcal{A}$ теории P изоморфна $\mathcal{N}$ тогда и только тогда, когда каждый индивид модели $\mathcal{A}$ есть $\mathcal{A}(k_n)$ для некоторого n .

Доказательство. Очевидно, условие необходимо. Предположим, что оно выполнено. Определим сюръективное отображение φ из $|\mathcal{N}|$ в $|\mathcal{A}|$ следующим образом: $\varphi(n) = \mathcal{A}(k_n)$. Если $m \neq n$, то $\vdash_P k_m \neq k_n$, поэтому $\mathcal{A}(k_m) \neq \mathcal{A}(k_n)$. Это показывает, что φ инъективно. Теперь условие изоморфизма следует из леммы 3 из § 8.2. Например, чтобы доказать, что

$$\varphi(m) +_{\mathcal{A}} \varphi(n) = \varphi(m+n),$$

заметим, что $\vdash_P k_m + k_n = k_{m+n}$ и потому

$$\mathcal{A}(k_m) +_{\mathcal{A}} \mathcal{A}(k_n) = \mathcal{A}(k_{m+n}).$$

Если $\mathcal{A}$ — регулярная модель теории S , то $\mathcal{A}(k_n) = \mathcal{A}_I(k_n)$ для всех n . Отсюда и из леммы 2 следует, что $\mathcal{A}_I$ изоморфна $\mathcal{N}$ тогда и только тогда, когда каждый элемент из $|\mathcal{A}_I| = N_{\mathcal{A}}$ есть $\mathcal{A}(k_n)$ для некоторого n . Если это так, то мы говорим, что $\mathcal{A}$ является ω -моделью теории S .

Регулярная модель $\mathcal{A}$ теории S называется *тотальной*, если $S_{\mathcal{A}}$ является множеством всех подмножеств множества $N_{\mathcal{A}}$. Покажем, что каждая тотальная модель теории S изоморфна $\mathcal{N}'$. (Это является известным доказательством того, что аксиомы Пеано категоричны.) Пусть $\mathcal{A}$ — тотальная модель теории S , и пусть x — множество всех $\mathcal{A}(k_n)$. Тогда $0_{\mathcal{A}} \in x$, и если $a \in x$, то $S_{\mathcal{A}}a \in x$. По аксиоме индукции отсюда следует, что $a \in x$ для каждого a из $N_{\mathcal{A}}$, поэтому $\mathcal{A}$ является ω -моделью. Вследствие этого мы можем предполагать, что $\mathcal{A}_I = \mathcal{N}$. Но тогда $S_{\mathcal{A}} = S_{\mathcal{N}'}$ и потому $\mathcal{A} = \mathcal{N}'$.

Теперь мы получим синтаксическую характеристику тех формул, которые являются истинными в каждой ω -модели. Формальная система S_{ω} получена из S добавлением

следующего ω -правила: из $A[k_0], A[k_1], \dots$ выводима $Nx \rightarrow A$. Заметим, что в отличие от всех рассматривавшихся нами ранее правил, ω -правило не конечно; для получения заключения требуется бесконечно много посылок.

Теорема Генкина—Оре. Формула теории S является теоремой системы S_{ω} тогда и только тогда, когда она истинна в каждой ω -модели теории S .

Доказательство. Чтобы доказать, что каждая теорема системы S_{ω} истинна в каждой ω -модели $\mathcal{A}$ теории S , достаточно показать, что если все посылки ω -правила истинны в $\mathcal{A}$, то и заключение истинно в $\mathcal{A}$, а это очевидно.

Предположим теперь, что A — не теорема системы S_{ω} . Пусть S' — теория языка $L(S)$, нелогическими аксиомами которой являются все теоремы системы S_{ω} . Тогда каждая теорема теории S' будет теоремой системы S_{ω} , поэтому A — не теорема теории S' . Отсюда следует, что если A' — замыкание формулы A , то $T = S'[\neg A']$ непротиворечива.

Пусть Γ — подмножество множества $S_1(T)$, состоящее из формулы Nz_1 и всех формул $z_1 \neq k_n$. Покажем, что множество Γ не является главным. Предположим, что B — образующая для Γ . Для каждого n имеем $\vdash_T B \rightarrow z_1 \neq k_n$. Подставляя k_n вместо z_1 и используя аксиомы тождества, получаем, что $\vdash_T \neg B[k_n]$. По теореме дедукции $\neg A' \rightarrow \neg B[k_n]$ — теорема теории S' , а потому и системы S_{ω} . По ω -правилу $Nz_1 \rightarrow \neg A' \rightarrow \neg B$ — теорема системы S_{ω} , а потому и теории S' . Таким образом, $\vdash_T Nz_1 \rightarrow \neg B$. Однако $\vdash_T B \rightarrow Nz_1$, поэтому $\vdash_T \neg B$ по теореме тавтологии. Это невозможно по определению образующей.

Из теоремы Эренфойхта следует, что существует такая модель $\mathcal{A}$ теории T , что никакой 1-тип из $\mathcal{A}$ не включает Γ . Мы можем предполагать, что модель $\mathcal{A}$ регулярная. Тогда $\mathcal{A}$ является ω -моделью теории S , в которой A не является истинной.

Если A — истинная формула теории P , то для каждой ω -модели $\mathcal{A}$ мы имеем

$$\mathcal{A}(A^{(I)}) = \mathcal{A}_I(A) = N(A) = \mathbf{I},$$

поэтому $A^{(I)}$ — теорема системы S_{ω} . Это не противоречит выводу, который мы сделали из теоремы о неполноте, поскольку S_{ω} не является аксиоматической системой в упомянутом там смысле.

Формула A теории S является теоремой системы S_ω тогда и только тогда, когда она принадлежит каждому классу Γ формул теории S такому, что

- (i) каждая аксиома системы S_ω принадлежит Γ ;
 - (ii) если все посылки некоторого правила из S_ω принадлежат Γ , то и заключение этого правила принадлежит Γ .
- Если мы заменим все формулы их номерами, то мы сможем сформулировать это определение в теории S . Другими словами, существует такая формула D теории S , что $D[k_n]$ истинна тогда и только тогда, когда n является номером некоторой теоремы системы S_ω . Пользуясь этим, мы так же, как и в § 8.2, можем доказать следующее утверждение.

Теорема Россера. *Существует истинная формула теории S , не являющаяся теоремой системы S_ω .*

В заключение сделаем несколько замечаний о доказательствах непротиворечивости теории S . Если исключить тривиальные доказательства, то единственное такое доказательство принадлежит Спектору. Это доказательство по существу является обобщением доказательства непротиворечивости, проведенного нами для P . Для того чтобы позаботиться об аксиомах выделения, необходимо присоединить к Y новые константы. То, что определяющие равенства для них определяют функционалы, не так очевидно, как в рассмотренных ранее определяющих равенствах. Это можно доказать довольно легко, однако доказательство не конструктивно. Таким образом, чтобы сделать доказательство конструктивным, надо дать конструктивное доказательство того, что эти равенства определяют функционалы. Недавние исследования показывают, что это вряд ли возможно. Таким образом, в настоящее время неизвестно, существует ли конструктивное доказательство непротиворечивости теории S .

Все сказанное вызывает следующий более общий вопрос: что такое, собственно говоря, конструктивное доказательство и каковы свойства таких доказательств? Это главный вопрос, изучаемый интуиционизмом. Хотя пока окончательные ответы на эти вопросы не найдены, в этом направлении достигнуты значительные успехи. Однако мы не будем здесь углубляться в этот предмет.

Задачи

Предполагается, что все теории имеют только конечное число нелогических символов.

1. Предикатный символ p из расширения P' теории P с помощью определений называется *R-символом*, если $px_1 \dots x_n$ эквивалентно некоторой R -формуле теории P .

(а) Показать, что если предикат Q можно ввести как некоторый R -символ в P' , то $Qx_1 \dots x_n$ от $x_1, \dots, x_n$ слабо представляет Q в P' . [Использовать лемму 3 из § 8.2.] Затем показать, что Q рекурсивно перечислим.

(б) Показать, что каждую примитивно рекурсивную функцию (примитивно рекурсивный предикат) можно ввести в некотором рекурсивном расширении теории P . В частности, так можно ввести T_n .

(в) Показать, что каждый рекурсивно перечислимый предикат можно ввести как R -символ в некотором расширении теории P с помощью определений. [Использовать (б) и теорему о нумерации.]

2. Пусть T — такая теория, что $NLAx_T$ рекурсивно перечислим. Согласно 1 (в) $NLAx_T$ можно ввести как R -символ в некотором расширении теории P с помощью определений. Тогда мы строим Thm_T и Con_T подобно Thm_P и Con_P , используя $NLAx_T$ вместо $NLAx_P$. (Заметим, что Thm_T и Con_T зависят не только от T , но также и от выбора R -символа $NLAx_T$.)

(а) Показать, что Thm_T является R -символом.

(б) Введем $NLAx_N$ с помощью определения

$$NLAx_N(x) \leftrightarrow x = k_{a_1} \vee \dots \vee x = k_{a_n}.$$

Показать, что (8) из § 8.2 выполняется, если Thm_P заменить на Thm_N .

(в) Показать, что если T — расширение теории N , то $\vdash Thm_N(x) \rightarrow \rightarrow Thm_T(x)$.

(г) Показать, что если T — непротиворечивое расширение теории P , то Con_T не является теоремой теории T . [Следовать доказательству из § 8.2, используя (а) — (в).]

3. (а) Пусть S и T — такие теории, что $NLAx_S$ и $NLAx_T$ рекурсивно перечислимы. Предположим, что S имеет интерпретацию I в T . Показать, что для каждого выбора R -символа $NLAx_T$ можно так выбрать R -символ $NLAx_S$, что $\vdash Con_T \rightarrow Con_S$. [Ввести такую функцию I' , что $I'(\ulcorner A \urcorner) = \ulcorner A^{(I)} \urcorner$ в некотором рекурсивном расширении теории P . Ввести $NLAx_S$ как R -символ и определить новый R -символ следующим образом:

$$NLAx'_S(x) \leftrightarrow NLAx_S(x) \& Thm_T(I'(x)).$$

Следуя доказательству теоремы об интерпретации, показать, что $\vdash Thm'_S(x) \rightarrow Thm_T(I'(x))$.]

(б) Пусть T — такая теория, что $NLAx_T$ рекурсивно перечислим. Показать, что если теория T непротиворечива, то $P[Con_T]$ не интер-

претируема в T . [Предположить, что это не так, и, пользуясь (а) и 1(г), показать, что $P[\text{Соп}_T]$ противоречива, и, следовательно, что Соп_T ложен.]

(в) Пусть T — такая теория, что NLAx_T рекурсивно перечислим. Показать, что если теория T непротиворечива и если I является интерпретацией теории P в теории T , то $\text{Соп}_T^{(I)}$ не является теоремой теории T . [Использовать (б).]

4. (а) Показать, что если Q — унарный R -символ из P' , то существует такая замкнутая R -формула A , что $\vdash_P A \leftrightarrow Q(k_{\neg A})$. [Взять в качестве A формулу $B_z[k_{\neg B}]$, где B есть R -формула, эквивалентная $Q(\text{Sub}(z, k_{\neg z}, \text{Num}(z)))$.]

(б) Показать, что если B — замкнутая формула теории P такая, что $\vdash_P \text{Thm}(k_{\neg B}) \rightarrow B$, то имеем $\vdash_P B$. [Определим $Q(a) \leftrightarrow \text{Thm}_P(\text{Imp}(a, \neg B))$, где $\text{Imp}(\neg A, \neg B) = \neg A \rightarrow B$. Введем Q как R -символ, и пусть A такая же, как и в (а), Показать, что

$$\vdash A \rightarrow \text{Thm}(k_{\neg A}) \rightarrow \text{Thm}(k_{\neg B}) \text{ и } \vdash A \rightarrow \text{Thm}(k_{\neg A}),$$

а затем последовательно доказать, что $\vdash A \rightarrow B, \vdash Q(k_{\neg A}), \vdash A, \vdash B$.]

(в) Показать, что если Q есть Thm_P и A такая же, как в (а), то $\vdash_P A$. [Использовать (б).]

5. Пусть A — не разрешимая в P замкнутая формула.

(а) Пусть B — множество номеров теорем теории $P[A]$, не являющихся теоремами теории P . Показать, что B не является рекурсивно перечислимым. [Предположить обратное и воспользоваться теоремой об отрицании, чтобы показать, что теория $P[\neg A]$ разрешима.]

(б) Пусть F — рекурсивная функция. Показать, что существует такая теорема B теории P , что если m и n — наименьшие номера доказательств теоремы B в P и $P[A]$ соответственно, то $m > F(n)$. [Предположить обратное и прийти к противоречию с (а).]

6. Пусть $\mathcal{A}$ — такая модель теории P , что $|\mathcal{A}| = |\mathcal{A}^*|$, однако $\mathcal{A}$ не изоморфна $\mathcal{A}^*$. По лемме из § 8.5 существуют элементы из $|\mathcal{A}|$, отличные от $\mathcal{A}(k_n)$; такие элементы называются *бесконечными* элементами.

(а) Показать, что если x является бесконечным элементом из $|\mathcal{A}|$, то $\mathcal{A}(k_n) <_A x$ для всех n . [Использовать N9 и лемму 2 из § 6.7.]

(б) Показать, что если в A нет свободных переменных, за исключением x , то

$$\vdash_P \exists z \exists y \forall x (x < \omega \rightarrow (\exists x' (y = x' \cdot (1 + x) \cdot z) \leftrightarrow A)).$$

[Аналогично лемме из § 6.4.]

(в) Пусть Φ — последовательность всех функций и предикатов из $\mathcal{A}$. Показать, что если в A нет свободных переменных, за исключением x , то множество A таких n , что $\mathcal{A}(A_x[k_n]) = \text{И}$, является рекурсивным в Φ . [Показать, что $\mathcal{A}(k_n)$, рассматриваемая как функция от n , рекурсивна в Φ . Взять бесконечный элемент ω , и

выбрать z, y, z' и y' согласно (а) и (б) так, чтобы в $\mathcal{A}$ выполнялось

$$\exists x' (y = x' \cdot (1 + \mathcal{A}(k_n) \cdot z) \leftrightarrow A[k_n],$$

$$\exists x' (y' = x' \cdot (1 + \mathcal{A}(k_n) \cdot z') \leftrightarrow \neg A[k_n].$$

Воспользоваться теоремой об отрицании.]

(г) Показать, что любые два непересекающиеся рекурсивно перечислимые множества могут быть отделены некоторым множеством, рекурсивным в Φ . [Использовать (в) и задачу 8(б) из главы 6.] Затем показать, что некоторый элемент из Φ является нерекурсивным. [Использовать задачу 13(в) из главы 6.]

(д) Показать, что если $\mathcal{A}$ элементарно эквивалентна $\mathcal{A}^*$, то некоторый элемент из Φ не является арифметическим. [Показать, что каждое арифметическое множество представимо в $\text{Th}(\mathcal{A}^*)$ и потому вследствие (в) рекурсивно в Φ . Затем применить теорему об арифметической иерархии.]

7. P -теорией называется такое расширение теории P , в котором каждая формула вида

$$A_x[0] \rightarrow \forall x (A \rightarrow A_x[Sx]) \rightarrow A$$

является теоремой. Пусть T — некоторая P -теория; определим рекурсивные расширения так же, как и для P , тогда мы можем доказать все результаты из § 8.1.

(а) Показать, что всякое расширение P -теории с помощью определений является P -теорией.

(б) Унарный функциональный символ f доминирует над n -арным функциональным символом g в P -теории T , если

$$\vdash_T x_1 < x \rightarrow \dots \rightarrow x_n < x \rightarrow gx_1 \dots x_n < fx.$$

Показать, что если T — P -теория, то существует расширение T' теории T с помощью определений, содержащее функциональный символ f , доминирующий над каждым функциональным символом теории T . [Пусть g — n -арный функциональный символ теории T , определить $h_1, \dots, h_n$ в рекурсивном расширении теории T так, что

$$\vdash x_1 < y_1 \rightarrow \dots \rightarrow x_i < y_i \rightarrow gx_1 \dots x_n < hy_1 \dots y_i x_{i+1} \dots x_n.]$$

(в) Пусть T — P -теория. Показать, что в подходящем расширении T' теории T с помощью определений существует бинарный функциональный символ g такой, что если a — терм теории T , содержащий самое большее m функциональных символов, а $x_1, \dots, x_n$ — все переменные из a , то

$$\vdash_T x_1 < x \rightarrow \dots \rightarrow x_n < x \rightarrow a < g(x, k_m),$$

и такой, что

$$\vdash_T y < z \rightarrow g(x, y) < g(x, z).$$

[Используя f из (б), индукцией по y определить $g(x, y)$.]

(г) Пусть $\exists y A$ — теорема некоторой P -теории T , и пусть $x_1, \dots, x_n$ — все переменные, свободные в $\exists y A$. Показать, что существует функциональный символ f из расширения T' теории T с помощью определений такой, что $\vdash_T A_y[f x_1 \dots x_n]$. [Использовать принцип наименьшего числа.]

(д) Показать, что если существует конечно аксиоматизируемая непротиворечивая P -теория, то существует конечно аксиоматизируемая непротиворечивая открытая P -теория. [Доказывать аналогично доказательству теоремы Скулема, используя (г).]

(е) Пусть $\mathcal{A}$ — модель некоторой P -теории; элемент x из $\mathcal{A}$ такой, что $\mathcal{A}(k_n) \neq x$ для всех n , называется *бесконечным* элементом. Показать, что если x — бесконечный элемент, то $\mathcal{A}(k_n) <_{\mathcal{A}} x$ для всех n . [Подобно 6 (а).] Показать, что если T — непротиворечивая P -теория, то T имеет модель, содержащую бесконечный элемент. [Использовать теорему о мощностях.]

(ж) Показать, что не существует конечно аксиоматизируемой непротиворечивой P -теории. [Предположим, что T — такая теория. Вследствие (д) мы можем предполагать, что теория T открытая. Согласно (е) существует модель $\mathcal{A}$ теории T , имеющая бесконечный элемент x . По теореме Лоса — Тарского мы можем предполагать, что каждый элемент из $|\mathcal{A}|$ есть $\mathcal{A}(a)$, где a — свободный от переменных терм языка $L(\mathcal{A})$, не содержащий имени, отличного от имени x . Выберем g и T' так же, как и в (в), и обогатим $\mathcal{A}$ до модели теории T' . Показать, что $y <_{\mathcal{A}} g_{\mathcal{A}}(S_{\mathcal{A}}(x), x)$ для каждого индивида y из $\mathcal{A}$.]

8. (а) Пользуясь теоремой из § 8.3, показать, что не существует замкнутой теоремы $\neg \forall w A$ теории P такой, что $\vdash_P A_w[k_n]$ для всех n . [Предположим противное, и пусть A^* есть $\forall x \exists y A^*[x, y, z]$. Тогда существуют такие функции f, g и h_w рекурсивного типа, что

$$\neg A^*[f(y'), y'(f(y'), g(y')), g(y')]$$

и

$$A^*[x, h_w(x), w]$$

истинны при всех y', x и w . Получить противоречие при помощи подходящего выбора y', x и w .]

(б) Показать, что существует такая замкнутая теорема $\exists w A$ теории P , что $A_w[k_n]$ не является теоремой теории P для каждого n . [Пусть B является такой R -формулой, что $\forall w B$ истинна, но не доказуема в P , и пусть A есть $\neg B \vee \forall w B$.]

9. (а) Показать, что существует такая бинарная рекурсивная функция F , что каждая унарная функция рекурсивного типа есть $F(e)$ для некоторого e . [Использовать (8) из § 8.4.] Затем показать, что существует унарная рекурсивная функция, не являющаяся функцией рекурсивного типа. [Взять $G(x) = F(x, x) + 1$.]

(б) Показать, что существует предикатный символ R из некоторого рекурсивного расширения P' теории P такой, что $\forall x \exists y R(x, y)$ истинно, но такой, что для каждой унарной функции рекурсивного типа F существует такое x , что $R(x, F(x))$ ложно. [Положить $R(x, y) \leftrightarrow T_1(e, x, y)$, где e — индекс рекурсивной функции, не являющейся функцией рекурсивного типа.] Затем показать, что $\forall x \exists y R(x, y)$ неразрешима в P' .

(в) Показать, что существует предикатный символ R из рекурсивного расширения P' теории P такой, что $\vdash_{P'} \forall x \exists y \forall z R(x, y, z)$, но такой, что не существует такой рекурсивной функции F , что $R(x, F(x), z)$ истинно для всех x и z . [Пусть $R(x, y, z) \leftrightarrow T_1(x, x, y) \vee$

$\vee \neg T_1(x, x, z)$. Если существует такая рекурсивная функция F , что $\forall x \forall z R(x, F(x), z)$, то $\exists y T_1(x, x, y)$ является рекурсивным предикатом от x , а это противоречит диагональной лемме.]

10. (а) Показать, что если T имеет точную интерпретацию в некоторой рекурсивно аксиоматизированной теории, то T рекурсивно аксиоматизируема. [Использовать задачу 5 (а) из главы 6.]

(б) Показать, что если полная теория T имеет интерпретацию в непротиворечивой рекурсивно аксиоматизированной теории T' , то T разрешима. [Показать, что интерпретация должна быть точной, и воспользоваться (а) и леммой из § 6.8.] Затем показать, что $\text{Th}(\mathcal{N})$ не может иметь интерпретации в непротиворечивой рекурсивно аксиоматизированной теории.

(в) Показать, что существует такая истинная формула A теории P , что $A^{(1)}$ не является теоремой теории S . [Использовать (б).]

11. (а) Показать, что если Q есть $(1, n)$ -арное арифметическое отношение, то существует такое предложение A теории S , что для каждой ω -модели $\mathcal{A}$ имеем $\mathcal{A}(A[i, k_{a_1}, \dots, k_{a_n}]) = \text{И}$ тогда и только тогда, когда i — имя такого множества A , что $Q(K_A, a_1, \dots, a_n)$. [Свести к случаю, когда Q рекурсивно перечислимо. Затем заметить, что

$$Q(\alpha, a) \leftrightarrow \exists x R(\bar{\alpha}(x), a) \\ \leftrightarrow \exists x \exists y (y = \bar{\alpha}(x) \& R(y, a)),$$

где R рекурсивно. Воспользоваться тем, что R представим в теории S .]

(б) Показать, что каждый предикат рода Π_1^1 слабо представим в S_ω . [Использовать (а), задачу 17 (а) из главы 7 и теорему Генкина — Оре.]

(в) Показать, что множество номеров теорем системы S_ω имеет род Π_1^1 . Вывести, что каждый слабо представимый в S_ω предикат имеет род Π_1^1 .

12. Множество натуральных чисел A находится в ω -модели $\mathcal{A}$ (где $\mathcal{A}_1 = \mathcal{N}$), если A принадлежит $S_{\mathcal{A}}$.

(а) Показать, что если A представимо в S_ω , то A находится в каждой ω -модели. [Использовать аксиому выделения и теорему Генкина — Оре.]

(б) Показать, что каждое гиперарифметическое множество представимо в S_ω . [Использовать 11 (а), задачу 27 (б) из главы 7 и теорему Генкина — Оре.]

(в) Пусть T — счетная непротиворечивая теория, и пусть Γ и Δ — подмножества множества $S_1(T)$, ни одно из которых не является главным. Показать, что существует счетная модель $\mathcal{A}$ теории T такая, что никакой 1-тип из $\mathcal{A}$ не включает либо Γ , либо Δ . [Подобно теореме Эренфойхта.]

(г) Показать, что множество A , находящееся в каждой ω -модели, является гиперарифметическим. [Пусть S' и Γ такие же, как и в доказательстве теоремы Генкина — Оре, и пусть Δ состоит из $Cz_1, k_n \in z_1$, где $n \in A$, и $k_n \notin z_1$, где $n \notin A$. Используя (в), показать, что Δ имеет образующую. Используя это и 11 (в), показать, что A и $\neg A$ имеют род Π_1^1 .]

9.1. Аксиомы для множеств

Обратимся теперь к исследованию теории множеств. Большой интерес к множествам отчасти вызван той важной ролью, которую они сыграли в современной математике. Но даже без этого понятие множества так естественно, что оно само привлекает внимание исследователя.

Множество (или *класс*) есть некоторое семейство объектов. Этими объектами могут быть числа, функции, физические объекты или даже множества. Так как нет никаких ограничений на объекты, которые могут быть элементами множеств, то могло бы показаться, что мы можем задать множество, если укажем для каждого объекта из универсума, будет данный объект элементом множества или нет. Однако это сразу приводит нас к парадоксу Рассела. Зададим множество A следующим образом: объект x является элементом A тогда и только тогда, когда x есть множество и x не является элементом множества x . Итак, A является элементом A тогда и только тогда, когда A не является элементом A ; приходим к противоречию.

Внимательный анализ этого парадокса показывает, что здесь в действительности нет противоречия с интуитивным понятием множества. Согласно этому понятию для образования множества A мы собираем вместе некоторые объекты, которые в своей совокупности и составляют единственный объект, являющийся множеством A . Следовательно, перед тем, как множество A образовано, мы должны иметь в распоряжении все объекты, которые являются элементами A . Отсюда следует, что множество A не является одним из возможных элементов A ; следовательно, парадокс Рассела исчезает.

Поэтому мы приходим к следующему описанию построения множеств. Мы начинаем с некоторых объектов, не являющихся множествами и не использующих множеств в своем построении. Назовем эти объекты *праэлементами*.

Затем мы образуем множества последовательно по шагам. На каждом шаге мы имеем в распоряжении праэлементы и множества, образованные на более ранних шагах, тогда мы образуем новые множества как всевозможные семейства этих объектов. Семейство считается множеством, если оно образовано на каком-то шаге этой конструкции.

Мы можем провести эту конструкцию с любым семейством праэлементов. Если мы проводим эту конструкцию без праэлементов, то получающиеся множества называются *чистыми* множествами. Оказывается, для математических целей этого достаточно; этого также достаточно для формулировки всех проблем, которые возникают в общем случае. Поэтому мы ограничиваемся лишь этим случаем и впредь под множеством или классом понимаем *чистое* множество.

В каких случаях некоторое семейство множеств образует множество? Для каждого множества x из этого семейства обозначим через S_x шаг, на котором x было образовано. Мы можем образовать множество из этого семейства тогда и только тогда, когда существует шаг S , следующий за всеми S_x . Однако такого шага может и не быть, например, тогда, когда среди шагов S_x содержатся все шаги. Поэтому нам нужен ответ на следующий вопрос: при каких условиях для данного семейства шагов существует шаг, следующий за каждым шагом из этого семейства?

Так как мы хотим допустить в качестве множеств по возможности произвольные семейства, то условимся, что такой шаг должен существовать всякий раз, когда это будет возможно, т. е. когда мы можем представить себе ситуацию, в которой все шаги этого семейства проделаны. Это несколько неясный принцип, но мы можем вывести из него некоторые точные результаты. Например, для данного шага S должен существовать шаг, следующий за S . Если семейство состоит из бесконечной последовательности шагов $S_1, S_2, \dots$, то мы можем представить себе ситуацию, когда все эти шаги проделаны; таким образом, должен существовать шаг после всех S_n .

Другой важный пример состоит в следующем. Предположим, что мы имеем множество A и мы указали шаг S_a для каждого элемента a из A . Поскольку мы можем представить семейство A как единый объект (а именно,

множество A), мы можем также представить это семейство шагов как единый объект, поэтому мы можем представить себе ситуацию, когда все эти шаги проделаны. Тогда должен существовать шаг, который следует за всеми шагами S_α . Это соглашение носит название *принципа конфинальности*.

Применим теперь эти принципы к построению теории. Эта теория называется *теорией множеств Цермело — Френкеля* и обозначается через ZF.

Единственным нелогическим символом теории ZF является бинарный предикатный символ $\in$. Понимаем, что индивидами теории ZF будут (чистые) множества и $x \in y$ будет означать, что x есть элемент y .

Первая нелогическая аксиома ZF утверждает, что если два множества имеют одни и те же элементы, то эти множества равны. Этой аксиомой, называемой *аксиомой объемности*, является

$$\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y.$$

Следующая нелогическая аксиома — *аксиома регулярности*:

$$\exists y (y \in x) \rightarrow \exists y (y \in x \wedge \neg \exists z (z \in x \wedge z \in y)).$$

Она утверждает, что если x имеет какой-то элемент, то x имеет некоторый элемент y , который не пересекается с x (т. е. x и y не имеют общих элементов). Такой элемент множества x будем называть *минимальным элементом* множества x . Чтобы увидеть, что аксиома регулярности справедлива, предположим, что x — непустое множество, и пусть y — элемент множества x , образованный на самом раннем из возможных шагов. Так как элементы множества y должны быть образованы на еще более ранних шагах, то они не являются элементами множества x . Следовательно, y есть минимальный элемент множества x .

Оставшиеся аксиомы относятся к существованию множеств. Прежде всего, имеем *аксиомы подмножеств*. Это все формулы вида

$$\exists z \forall x (x \in z \leftrightarrow x \in y \wedge A),$$

где x , y и z различны, а y и z не входят в A . Чтобы понять, что это означает, положим x , y и z равными x , y и z , и пусть A есть $\dots x \dots$. Тогда аксиома утверж-

дает, что существует множество, элементами которого являются в точности все элементы x из y такие, что $\dots x \dots$. Чтобы проверить, что это справедливо, предположим, что S есть шаг, на котором y построено. Тогда каждый элемент x из y такой, что $\dots x \dots$, должен быть построен до шага S ; значит, z может быть построено на шаге S .

Мы используем $\text{Set}_x A$ как сокращение для

$$\exists y \forall x (A \rightarrow x \in y).$$

(Переменная y должна быть отличной от x и не входить в A . В остальном выбор y произвольный ввиду теоремы о варианте.) Ясно, $\text{Set}_x \dots x \dots$ означает, что существует множество y , содержащее каждое x такое, что $\dots x \dots$.

Аксиомами замены являются все формулы вида:

$$\forall x \exists z \forall y (A \leftrightarrow y \in z) \rightarrow \text{Set}_y \exists x (x \in w \wedge A),$$

где x , y , z и w различны, z и w не входят в A . Чтобы понять, что это означает, предположим, что x , y , z и w представляют собой x , y , z и w , и пусть A будет $\dots x \dots \dots y \dots$. Посылка утверждает, что для каждого x существует множество z_x , состоящее из всех таких y , что $\dots x \dots \dots y \dots$. Заключение утверждает, что существует множество z (зависящее от w), содержащее каждое y такое, что $\dots x \dots \dots y \dots$ для подходящего x из w .

Для того чтобы проверить это, предположим, что S_x есть шаг, на котором построено z_x . По принципу конфинальности существует шаг S после всех шагов S_x для $x \in w$. Если $x \in w$ и $\dots x \dots y \dots$, то $y \in z_x$; следовательно, y построено до шага S_x и поэтому до шага S . Тогда на шаге S мы можем построить множество всех y таких, что $\dots x \dots y \dots$ для некоторого $x \in w$.

Аксиомой степени является

$$\text{Set}_y \forall z (z \in y \rightarrow z \in x).$$

Она утверждает, что для данного множества x существует множество, которое содержит каждое подмножество множества x . Предположим, что x построено на шаге S . Тогда каждый элемент из x построен до шага S ; значит, каждое подмножество множества x может быть построено на шаге S . Поэтому на любом шаге, следующем за S , мы можем построить множество, содержащее все подмножества множества x .

Нам нужна еще одна аксиома, гарантирующая существование бесконечного множества. Это будет *аксиома бесконечности*:

$$\exists x (\exists y (y \in x \ \& \ \forall z (z \notin y)) \ \& \ \forall y (y \in x \rightarrow \exists z (z \in x \ \& \ \forall w (w \in z \leftrightarrow w \in y \vee w = y)))).$$

Она утверждает, что существует множество x такое, что пустое множество $\emptyset$ есть элемент x , и такое, что если $y \in x$, то множество $S(y)$, элементами которого являются само y и все элементы из y , также будет элементом x . Ясно, что если y построено на некотором шаге, то $S(y)$ может быть построено на следующем шаге. Поэтому существуют шаги $S_0, S_1, S_2, \dots$, на которых мы можем построить $\emptyset, S(\emptyset), S(S(\emptyset)), \dots$. На шаге S , следующем за всеми шагами $S_0, S_1, S_2, \dots$, мы можем построить множество x , элементами которого являются $\emptyset, S(\emptyset), S(S(\emptyset)), \dots$. Ясно, что это множество обладает требуемыми в аксиоме бесконечности свойствами.

Этим завершается описание теории ZF. Позднее будут рассмотрены некоторые другие аксиомы, которые могут быть добавлены к ZF.

9.2. Систематическое построение теории множеств

Мы предполагаем, что читатель знаком с результатами элементарной теории множеств. Мы будем развивать теорию, в основном исходя из следующих двух соображений:

а) чтобы такие основные понятия, как *упорядоченная пара*, *функция* и *натуральное число*, могли быть определены в ZF;

б) чтобы в ZF можно было доказать существование всех множеств, использующихся в элементарной теории множеств.

Мы часто будем прибегать к расширению ZF с помощью определений. Для того чтобы не рассматривать их как расширения нашей теории, мы считаем новые нелогические символы определяемыми символами. Тогда каждая формула такого расширения будет некоторой определяемой формулой теории ZF, сокращением ее перевода в ZF. Далее, мы можем рассматривать определяющую аксиому для нового функционального или предикатного символа как определение этого символа. Конечно, в доказательствах мы рассматриваем эти определяемые функциональные или предикатные символы так же, как мы рассматривали бы обычные функциональные и предикатные символы; мы будем относиться к ним, как к функциональным и предикатным символам теории ZF.

Определения и доказательства будут даваться на русском языке; мы предполагаем, что читатель знает, как перевести их на язык теории ZF. Для большего удобства чтения мы используем все строчные латинские буквы (иногда со штрихами или индексами) в качестве переменных теории ZF. При неформальном изложении мы ограничиваем области изменения некоторых из этих переменных специальными семействами множеств.

Мы хотим избежать использования синтаксических переменных, так как их применение в русском контексте предполагало бы, что мы говорим про ZF, а не о переводе языка $L(ZF)$ на русский язык. Поэтому мы будем допускать такие утверждения, как: *если Q — предикатный символ, то...* Это будет означать, что все, что доказано про Q , выполняется для всех предикатных символов. Иногда мы будем использовать Q для специального предикатного символа, который не настолько важен, чтобы ему давать постоянное имя. В некоторых контекстах мы используем R , U и M таким же образом, как и Q . Мы используем F , G и H аналогично, за исключением того, что они должны быть функциональными символами.

Подходящее использование этих букв позволяет нам обходиться без синтаксических переменных для формул. Например, рассмотрим какую-то аксиому подмножества

$$\exists z \forall x (x \in z \leftrightarrow x \in y \ \& \ A).$$

Предположим, что x , y и z представляют собой x , y и z . Определим Q следующим образом:

$$Q(x, v_1, \dots, v_n) \leftrightarrow A,$$

где $v_1, \dots, v_n$ — все другие переменные, свободные в A . Тогда аксиома примет вид

$$\exists z \forall x (x \in z \leftrightarrow x \in y \ \& \ Q(x, v_1, \dots, v_n)).$$

Обратно, каждая формула такого вида есть некоторая аксиома подмножества. Соответствующий вид для аксиом

замены таков:

$$\forall x \exists z \forall y (Q(x, y, v_1, \dots, v_n) \leftrightarrow y \in z) \rightarrow \\ \rightarrow \text{Set}_y \exists x (x \in \omega \& Q(x, y, v_1, \dots, v_n)).$$

В обоих случаях переменные $v_1, \dots, v_n$ называются *параметрами*. Так как они обычно остаются неизменными во всем доказательстве, мы часто не будем их писать.

Предположим, что Q определен, и мы хотим определить F так, чтобы $F(v_1, \dots, v_n)$ было множеством всех таких x , что $Q(x, v_1, \dots, v_n)$. Для этого нам нужна определяющая аксиома

$$\forall x (x \in F(v_1, \dots, v_n) \leftrightarrow Q(x, v_1, \dots, v_n)). \quad (1)$$

Условие единственности для этой аксиомы легко следует из аксиомы объемности. Условием существования является

$$\exists z \forall x (x \in z \leftrightarrow Q(x, v_1, \dots, v_n)). \quad (2)$$

Покажем, что (2) может быть доказано из

$$\text{Set}_x Q(x, v_1, \dots, v_n). \quad (3)$$

Мы опускаем параметры $v_1, \dots, v_n$. Предположим (3) и выберем множество ω такое, что $Q(x) \rightarrow x \in \omega$ для всех x . В силу аксиомы подмножества существует множество z такое, что для всех x

$$x \in z \leftrightarrow x \in \omega \& Q(x).$$

Так как $Q(x) \rightarrow x \in \omega$, то это эквивалентно следующему: $x \in z \leftrightarrow Q(x)$. Это доказывает (2).

Будем называть (3) *условием существования* для (1). Когда (3) доказано, мы будем записывать определение (1) в виде

$$F(v_1, \dots, v_n) = [x | Q(x, v_1, \dots, v_n)]. \quad (4)$$

Мы можем также использовать $[x | Q(x, v_1, \dots, v_n)]$ как терм в определении или доказательстве. Это будет пониматься как сокращение для $F(v_1, \dots, v_n)$, где F определено с помощью (4). Кроме того, мы можем использовать $[x | \text{---} x \text{---}]$, где $\text{---} x \text{---}$ есть формула, в качестве термина; это будет означать сокращение для $[x | Q(x, v_1, \dots, v_n)]$, где Q определено так:

$$Q(x, v_1, \dots, v_n) \leftrightarrow \text{---} x \text{---}.$$

Конечно, $[x | \text{---} x \text{---}]$ может использоваться как сокращение только при условии, что условие существования для $\text{Set}_x \text{---} x \text{---}$ доказано. Заметим, что это всегда имеет место, если $\text{---} x \text{---}$ есть $x \in \dots$ или $x \in \dots \& \text{---} \text{---}$, где $\dots$ — некоторый терм, не содержащий x .

Определим

$$x \subset y \leftrightarrow \forall z (z \in x \rightarrow z \in y).$$

Тогда $x \subset y$ означает, что x есть подмножество множества y . Определим

$$P(x) = [y | y \subset x];$$

условие существования для этого определения есть в точности аксиома степени. Мы называем $P(x)$ *множеством степени* множества x ; это есть множество всех подмножеств множества x .

Мы используем $[F(x, v_1, \dots, v_n) | Q(x, v_1, \dots, v_n)]_x$ как сокращение для

$$[y | \exists x (Q(x, v_1, \dots, v_n) \& y = F(x, v_1, \dots, v_n))].$$

Так, например, опуская параметры, $[F(x) | Q(x)]_x$ означает множество всех $F(x)$ для x таких, что $Q(x)$. Обычно мы будем опускать индекс x . Мы часто будем писать $[\dots x \dots | \text{---} x \text{---}]$; это будет сокращением для $[F(x, v_1, \dots, v_n) | Q(x, v_1, \dots, v_n)]$, где F и Q определены следующим образом:

$$F(x, v_1, \dots, v_n) = \dots x \dots, \\ Q(x, v_1, \dots, v_n) \leftrightarrow \text{---} x \text{---}.$$

Покажем, что из $\text{Set}_x Q(x, v_1, \dots, v_n)$ следует условие существования для $[F(x, v_1, \dots, v_n) | Q(x, v_1, \dots, v_n)]$. Параметры опускаем. Имеем $F(x) \subset F(x)$; таким образом, $F(x) \in P(F(x))$; следовательно,

$$\forall y (y = F(x) \rightarrow y \in P(F(x))).$$

Из этого получаем $\forall x \text{Set}_y (y = F(x))$, что, как было показано выше, влечет

$$\forall x \exists z \forall y (y \in z \leftrightarrow y = F(x)).$$

Из этого по аксиомам замены следует

$$\text{Set}_y \exists x (x \in [x | Q(x)] \& y = F(x)),$$

которое эквивалентно

$$\text{Set}_y \exists x (Q(x) \& y = F(x)).$$

А это и есть требуемое условие существования.

Пустое множество 0 определяется следующим образом:

$$0 = [x | x \neq x].$$

Условие существования $\exists y \forall x (x \neq x \rightarrow x \in y)$ следует из аксиом тождества.

Определим *неупорядоченную пару* $\{x, y\}$, состоящую из множеств x и y , следующим образом:

$$\{x, y\} = [z | z = x \vee z = y].$$

Чтобы доказать условие существования, определим F так, чтобы $F(0) = x$ и $F(z) = y$ для $z \neq 0$. (Мы опускаем параметры x и y как аргументы F .) Пусть

$$w = [F(z) | z \in P(P(0))].$$

Достаточно будет показать, что $\forall z (z = x \vee z = y \rightarrow z \in w)$ или, что эквивалентно, $x \in w \& y \in w$. Далее $0 \in P(0)$, поэтому $0 \in P(P(0))$ и, значит, $x = F(0) \in w$. Кроме того, $P(0) \subset P(0)$, поэтому $P(0) \in P(P(0))$. Далее, $0 \in P(0)$ и $0 \notin 0$, поэтому $P(0) \neq 0$. Отсюда $y = F(P(0)) \in w$.

Определим *одноэлементное множество* $\{x\}$, состоящее из множества x , следующим образом:

$$\{x\} = \{x, x\}.$$

Определим

$$\text{Un}(x) = [y | \exists z (z \in x \& y \in z)].$$

Чтобы доказать условие существования, отметим, что $\forall z \exists v \forall y (y \in v \leftrightarrow y \in z)$, поэтому по аксиомам замены $\text{Set}_y \exists z (z \in x \& y \in z)$. Мы называем $\text{Un}(x)$ *объединением* x ; это есть объединение (в обычном смысле) всех элементов множества x .

Определим теперь операции *объединения*, *пересечения* и *разности множеств* следующим образом:

$$x \cup y = \text{Un}(\{x, y\}),$$

$$x \cap y = [z | z \in x \& z \in y],$$

$$x - y = [z | z \in x \& z \notin y].$$

Условия существования для двух последних операций доказаны, потому что они имеют вид $[z | z \in x \& \dots]$.

Определим теперь *упорядоченную пару* $\langle x, y \rangle$, состоящую из множеств x и y , следующим образом:

$$\langle x, y \rangle = \{\{x\}, \{x, y\}\}.$$

Докажем основное свойство упорядоченных пар:

$$\langle x, y \rangle = \langle x', y' \rangle \leftrightarrow x = x' \& y = y'. \quad (5)$$

Импликация справа налево тривиальна. Предположим, что $\langle x, y \rangle = \langle x', y' \rangle$. Тогда $\{x\}$ лежит в $\langle x, y \rangle$ и, следовательно, в $\langle x', y' \rangle$, поэтому $\{x\} = \{x'\}$ или $\{x\} = \{x', y'\}$. В любом случае $x' \in \{x\}$, поэтому $x = x'$. Далее, $\{x, y\}$ лежит в $\langle x, y \rangle = \langle x', y' \rangle$, поэтому $\{x, y\} = \{x'\}$ или $\{x, y\} = \{x', y'\}$. Таким образом, y лежит в $\{x'\}$ или в $\{x', y'\}$, поэтому $y = x'$ или $y = y'$. В силу симметрии $y' = x$ или $y' = y$. Если мы предположим, что $y \neq y'$, то получим $y = x' = x = y'$, поэтому мы должны иметь $y = y'$.

Если $x = \langle y, z \rangle$, то положим $\pi_1(x) = y$ и $\pi_2(x) = z$; эти операции корректно определены в силу (5). Так как функциональные символы должны быть определены для всех аргументов, то мы должны определить значения $\pi_1(x)$ и $\pi_2(x)$, когда x не является упорядоченной парой. Положим это значение равным 0 . И вообще, если мы не определяем значение некоторого функционального символа для некоторых аргументов, то будем считать, что это значение есть 0 .

Определим *декартово произведение* $x \times y$ множеств x и y следующим образом:

$$x \times y = [z | \exists a \exists b (a \in x \& b \in y \& z = \langle a, b \rangle)].$$

Чтобы доказать условие существования, заметим, что

$$a \in x \& b \in y \rightarrow \{a\} \in P(x \cup y) \& \{a, b\} \in P(x \cup y) \\ \rightarrow \langle a, b \rangle \in P(P(x \cup y)).$$

Следовательно,

$$\exists a \exists b (a \in x \& b \in y \& z = \langle a, b \rangle) \rightarrow z \in P(P(x \cup y)).$$

Определим теперь $\langle x_1, \dots, x_n \rangle$ для каждого n . Проводя индукцию по n , полагаем для $n \geq 3$

$$\langle x_1, \dots, x_n \rangle = \langle x_1, \langle x_2, \dots, x_n \rangle \rangle.$$

Чтобы включить и случай $n=1$, полагаем

$$\langle x \rangle = x.$$

Тогда мы имеем

$$\langle x_1, \dots, x_n, \langle y_1, \dots, y_k \rangle \rangle = \langle x_1, \dots, x_n, y_1, \dots, y_k \rangle, \quad (6)$$

что легко доказать индукцией по n . Применяя (5) и индукцию по n , получаем

$$\langle x_1, \dots, x_n \rangle = \langle y_1, \dots, y_n \rangle \leftrightarrow x_1 = y_1 \& \dots \& x_n = y_n. \quad (7)$$

Мы можем поэтому определить функциональные символы π_i^n ($1 \leq i \leq n$) так, чтобы

$$\pi_i^n(\langle x_1, \dots, x_n \rangle) = x_i.$$

Мы также обобщаем понятие декартова произведения на случай более чем двух сомножителей, полагая

$$x_1 \times \dots \times x_n = x_1 \times (x_2 \times \dots \times x_n).$$

Тогда $x_1 \times \dots \times x_n$ есть множество всех таких $\langle a_1, \dots, a_n \rangle$, что $a_1 \in x_1, \dots, a_n \in x_n$.

Пусть

$$[F(x_1, \dots, x_n, v_1, \dots, v_m) \mid Q(x_1, \dots, x_n, v_1, \dots, v_m)]_{x_1, \dots, x_n} \quad (8)$$

является сокращением для

$$[y \mid \exists x_1 \dots \exists x_n (Q(x_1, \dots, x_n, v_1, \dots, v_m) \& y = F(x_1, \dots, x_n, v_1, \dots, v_m))].$$

Индексы обычно будут опускаться. Опустив параметры, имеем, что

$$[F(x_1, \dots, x_n) \mid Q(x_1, \dots, x_n)]$$

есть множество $F(x_1, \dots, x_n)$ для $x_1, \dots, x_n$ таких, что $Q(x_1, \dots, x_n)$.

Используем обозначение

$$\text{Set}_{x_1, \dots, x_n} Q(x_1, \dots, x_n, v_1, \dots, v_m) \quad (9)$$

в качестве сокращения для

$$\exists w_1 \dots \exists w_n \forall x_1 \dots \forall x_n (Q(x_1, \dots, x_n, v_1, \dots, v_m) \rightarrow x_1 \in w_1 \& \dots \& x_n \in w_n).$$

Покажем, что из (9) следует условие существования для

(8). Определим функциональный символ $\langle F \rangle$ следующим образом:

$$\langle F \rangle(z) = F(\pi_1^n(z), \dots, \pi_n^n(z)).$$

Тогда

$$F(x_1, \dots, x_n) = \langle F \rangle(\langle x_1, \dots, x_n \rangle).$$

Предполагая (9), получаем, что для подходящих $w_1, \dots, w_n$

$$\exists x_1 \dots \exists x_n (Q(x_1, \dots, x_n) \& y = F(x_1, \dots, x_n)) \rightarrow y \in [\langle F \rangle(z) \mid z \in w_1 \times \dots \times w_n].$$

Это дает нам требуемое условие существования. Поэтому мы называем (9) *условием существования* для (8).

Будем отождествлять функцию с множеством упорядоченных пар $\langle a, b \rangle$, где a есть значение функции для аргумента b . Определим *область определения* $\text{Do}(x)$ и *область значений* $\text{Ra}(x)$ для x следующим образом:

$$\text{Do}(x) = [\pi_2(y) \mid y \in x].$$

$$\text{Ra}(x) = [\pi_1(y) \mid y \in x].$$

Мы будем говорить, что x есть *функция*, и записывать это $\text{Func}(x)$, если $x \subset \text{Ra}(x) \times \text{Do}(x)$ и если из $\langle a, b \rangle, \langle a', b \rangle \in x$ следует $a = a'$. Ясно, как определить *инъективную* функцию; мы пишем $\text{IFunc}(x)$, если x есть инъективная функция. Используем обозначение $x'a$ для значения функции x для аргумента a . Мы рассматриваем $'$ как бинарный функциональный символ: в соответствии с нашим соглашением $x'a = 0$, если x не является функцией или если a не находится в области определения для x . Различные понятия, связанные с отображениями, могут быть теперь определены обычным образом.

В следующем параграфе мы получим определение *натурального числа* в теории ZF. Затем мы получим все необходимое, чтобы приступить к любой из обычных конструкций действительных и комплексных чисел.

9.3. Ординалы

Для каждого шага S конструкции из § 9.1 мы выбираем некоторое множество x_S , которое впервые строится на шаге S . Можно предполагать, что x_T уже выбрано для каждого шага T , предшествующего S . Пусть x_S означает

множество всех x_T для шагов T , предшествующих шагу S . Это множество может быть впервые построено лишь на шаге S , так как S — первый шаг, на котором имеются все его элементы.

Определим в теории ZF свойство быть одним из множеств x_S . Скажем, что множество *транзитивно*, и пишем $\text{Trans}(x)$, если каждый элемент множества x есть некоторое подмножество множества x , или что эквивалентно, если $\forall y \forall z (y \in x \& z \in y \rightarrow z \in x)$. Скажем, что x есть *ординал*, и пишем $\text{Ord } x$, если множество x транзитивно и каждый элемент множества x также транзитивен. Пусть областью изменения σ, τ и ρ будут ординалы. (Эти символы будут считаться дополнительными переменными теории ZF.)

Легко видеть, что каждое множество x_S транзитивно, а из этого следует, что каждое множество x_S есть ординал. Обратное будет доказано после того, как будут получены некоторые свойства ординалов.

Имеем

$$x \in \sigma \rightarrow \text{Ord}(x). \quad (1)$$

Действительно, пусть $x \in \sigma$. Тогда множество x транзитивно. В силу транзитивности σ имеем $x \subset \sigma$, поэтому каждый элемент множества x есть элемент множества σ и, следовательно, транзитивен. Поэтому множество x есть ординал.

Определим

$$\sigma < \tau \leftrightarrow \sigma \in \tau.$$

(Заметим, что $x_S < x_T$ тогда и только тогда, когда шаг S предшествует шагу T .) Имеем

$$\sigma < \tau \& \tau < \rho \rightarrow \sigma < \rho \quad (2)$$

в силу транзитивности ρ . Далее

$$\neg(\sigma < \sigma). \quad (3)$$

Это есть частный случай такого результата:

$$x \notin x. \quad (4)$$

Чтобы доказать его, заметим, что $\{x\}$ имеет минимальный элемент, которым должен быть x . Тем самым $x \cap \{x\} = 0$, поэтому $x \notin x$. Из (2) и (3) получаем

$$\neg(\sigma < \tau \& \tau < \sigma). \quad (5)$$

Имеем

$$\begin{aligned} & \exists \sigma Q(\sigma, v_1, \dots, v_n) \rightarrow \\ & \rightarrow \exists \sigma (Q(\sigma, v_1, \dots, v_n) \& \forall \tau (\tau < \sigma \rightarrow \neg Q(\tau, v_1, \dots, v_n))). \end{aligned}$$

Параметры в доказательстве опускаем. Предположим, что $\exists \sigma Q(\sigma)$, и выберем σ так, чтобы $Q(\sigma)$. Если $\forall \tau (\tau < \sigma \rightarrow \neg Q(\tau))$, то σ — требуемый ординал. В противном случае $[x | x < \sigma \& Q(x)]$ непусто и, следовательно, имеет минимальный элемент ρ . Так как $\rho \in \sigma$, то ρ — ординал в силу (1). Ясно, что $Q(\rho)$; покажем, что $\tau < \rho \rightarrow \neg Q(\tau)$. Предположим, что $\tau < \rho$. По (2) имеем $\tau < \sigma$. По выбору ρ имеем $\tau \notin [x | x < \sigma \& Q(x)]$; таким образом, $\neg Q(\tau)$.

Ординал σ такой, что $Q(\sigma, v_1, \dots, v_n)$ и $\neg Q(\tau, v_1, \dots, v_n)$ для всех $\tau < \sigma$, называется *минимальным* ординалом σ таким, что $Q(\sigma, v_1, \dots, v_n)$. Мы можем также говорить о минимальном ординале σ таком, что $\dots \sigma \dots$; это есть минимальный ординал σ такой, что $Q(\sigma, v_1, \dots, v_n)$, где Q определяется следующим образом:

$$Q(\sigma, v_1, \dots, v_n) \leftrightarrow \dots \sigma \dots$$

Перед тем как предположить, что минимальный ординал σ такой, что $\dots \sigma \dots$, существует, мы должны доказать, что $\exists \sigma (\dots \sigma \dots)$.

Теперь докажем, что

$$\sigma < \tau \vee \sigma = \tau \vee \tau < \sigma. \quad (6)$$

Сократим эту формулу до $C(\sigma, \tau)$. Предположим, что $\exists \sigma \exists \tau \neg C(\sigma, \tau)$, и придем к противоречию. Пусть σ — минимальный ординал такой, что $\exists \tau \neg C(\sigma, \tau)$, и пусть τ — минимальный ординал такой, что $\neg C(\sigma, \tau)$. Сперва докажем, что $\tau \subset \sigma$. Пусть $\rho \in \tau$, тогда ρ — ординал в силу (1). По выбору τ имеем $C(\sigma, \rho)$, поэтому, чтобы доказать, что $\rho \in \sigma$, достаточно показать, что $\sigma = \rho \vee \sigma < \rho$ приводит к противоречию. Так как из $\rho < \tau$ и $\sigma = \rho \vee \sigma < \rho$ по (2) следует, что $\sigma < \tau$, то мы имеем противоречие с $\neg C(\sigma, \tau)$.

Так как $\tau \subset \sigma$ и $\neg C(\sigma, \tau)$, то существует ρ в $\sigma - \tau$. По (1) ρ есть ординал. По выбору σ имеем $C(\rho, \tau)$. Так как $\rho \notin \tau$, то отсюда следует, что $\tau < \rho \vee \tau = \rho$. Отсюда следует в силу (2), что $\tau < \sigma$, а это противоречит тому, что $\neg C(\sigma, \tau)$.

Теперь мы можем доказать, что каждый ординал есть некоторое множество x_S . Предположим, что σ — множество, впервые построенное на шаге S . Так как x_S также впервые строится на этом шаге, то $\sigma \notin x_S$ и $x_S \notin \sigma$. Так как оба множества σ и x_S являются ординалами, то по (6) отсюда следует, что $\sigma = x_S$.

Другим следствием формулы (6) является то, что если $\exists \sigma Q(\sigma, v_1, \dots, v_n)$, то минимальный ординал σ такой, что $Q(\sigma, v_1, \dots, v_n)$, единствен. Мы называем его *первым* ординалом σ таким, что $Q(\sigma, v_1, \dots, v_n)$, и обозначаем его через $\mu \sigma Q(\sigma, v_1, \dots, v_n)$.

Определим

$$\sigma \leq \tau \leftrightarrow \sigma < \tau \vee \sigma = \tau.$$

Обычные порядковые свойства $\leq$ могут быть выведены из свойств $<$, доказанных выше. Сверх этого имеем

$$\sigma \leq \tau \leftrightarrow \sigma \subset \tau. \quad (7)$$

Действительно, если $\sigma < \tau$, то $\sigma \subset \tau$ в силу транзитивности τ , поэтому $\sigma \leq \tau \rightarrow \sigma \subset \tau$. Теперь предположим, что $\neg(\sigma \leq \tau)$. По (6) имеем $\tau < \sigma$, но в силу (3) имеем $\neg(\tau < \tau)$. Поэтому $\tau \in \sigma - \tau$; следовательно, $\neg(\sigma \subset \tau)$.

Принцип трансфинитной индукции. Если

$$\forall \sigma (\forall \tau (\tau < \sigma \rightarrow Q(\tau, v_1, \dots, v_n)) \rightarrow Q(\sigma, v_1, \dots, v_n)),$$

то $\forall \sigma Q(\sigma, v_1, \dots, v_n)$.

Доказательство. Если заключение ложно, то существует первый ординал σ такой, что $\neg Q(\sigma, v_1, \dots, v_n)$. Но это противоречит посылке.

Принцип трансфинитной индукции утверждает, что если мы хотим доказать $Q(\sigma, v_1, \dots, v_n)$, то достаточно доказать

$$\forall \sigma (\forall \tau (\tau < \sigma \rightarrow Q(\tau, v_1, \dots, v_n)) \rightarrow Q(\sigma, v_1, \dots, v_n)).$$

Другими словами, при доказательстве $Q(\sigma, v_1, \dots, v_n)$ мы можем предположить, что $Q(\tau, v_1, \dots, v_n)$ для всех $\tau < \sigma$. Доказательство с помощью этого метода называется *доказательством трансфинитной индукцией* по σ ; предположение, что $Q(\tau, v_1, \dots, v_n)$ для всех $\tau < \sigma$, называется *индуктивным предположением*.

Можно также доказывать формулу $\dots \sigma \dots$ трансфинитной индукцией, определяя Q следующим образом:

$Q(\sigma, v_1, \dots, v_n) \leftrightarrow \dots \sigma \dots$; индуктивное предположение тогда состоит в том, что $\dots \tau \dots$ для всех $\tau < \sigma$.

Имеется также некоторый способ индуктивного подхода к доказательствам фактов про множества (вместо рассмотренных доказательств только про ординалы). Будем называть H *ординальным функциональным символом*, если $*$) $\vdash \text{Ord}(H(x_1, \dots, x_n))$. Предположим, что это имеет место. Тогда, чтобы доказать

$$Q(x_1, \dots, x_n, v_1, \dots, v_m),$$

достаточно доказать это при предположении, что

$$\forall y_1 \dots \forall y_n (H(y_1, \dots, y_n) < H(x_1, \dots, x_n) \rightarrow \rightarrow Q(y_1, \dots, y_n, v_1, \dots, v_m)).$$

Если мы доказали это при таком предположении, то мы можем доказать

$$\forall x_1 \dots \forall x_n (H(x_1, \dots, x_n) = \sigma \rightarrow Q(x_1, \dots, x_n, v_1, \dots, v_m))$$

трансфинитной индукцией по σ , а из этого мы сможем доказать

$$Q(x_1, \dots, x_n, v_1, \dots, v_m).$$

Если n — натуральное число и S — $(n+1)$ -й шаг конструкции, то множество x_S имеет в точности n элементов. Мы намерены отождествить n с этим множеством x_S . Так, например, 0 отождествляется с пустым множеством. Затем мы должны определить операцию следования и свойство быть натуральным числом.

Определим

$$S(\sigma) = \sigma \cup \{\sigma\}$$

и назовем $S(\sigma)$ *последователем* ординала σ . Имеем

$$S(\sigma) = S(\tau) \rightarrow \sigma = \tau.$$

Действительно, предположим, что $S(\sigma) = S(\tau)$ и $\sigma \neq \tau$. Тогда $\sigma \in \sigma \cup \{\sigma\} = \tau \cup \{\tau\}$, поэтому $\sigma \in \tau$. Аналогично $\tau \in \sigma$. Это невозможно по (5).

*) Заметим, что утверждение о том, что H есть ординальный функциональный символ, является утверждением о доказуемости в теории ZF, а не является утверждением теории ZF. И вообще, если мы приписываем какое-то свойство функциональному или предикатному символу, мы делаем некоторое утверждение о доказуемости в теории ZF.

Теперь покажем, что $S(\sigma)$ является некоторым ординалом. Если $y \in S(\sigma)$, то $y \in \sigma$ или $y = \sigma$, поэтому y транзитивно и $y \subset \sigma \subset S(\sigma)$. Ясно, что $\sigma < S(\sigma)$. Кроме того, $S(\sigma)$ есть первый ординал τ такой, что $\sigma < \tau$. Действительно, если $\tau < S(\sigma)$, то $\tau < \sigma \vee \tau = \sigma$ и, значит, $\neg(\sigma < \tau)$.

Пусть x — некоторое множество ординалов. Тогда $\text{Un}(x)$ — некоторый ординал. Действительно, если $y \in \text{Un}(x)$, то $y \in \sigma$ для некоторого $\sigma \in x$. Следовательно, y транзитивно и $y \subset \sigma \subset \text{Un}(x)$. Используя (7), видим, что $\text{Un}(x)$ есть первый ординал τ такой, что $\sigma \leq \tau$ для каждого $\sigma \in x$.

Если x — множество, то существует ординал, больший каждого ординала из x . Действительно, если y — множество ординалов из x , то $S(\text{Un}(y))$ — такой ординал. Из этого мы можем доказать

$$\text{Set}_x \exists \sigma (x = F(\sigma)) \rightarrow \exists \sigma \exists \tau (\tau < \sigma \& F(\tau) = F(\sigma)). \quad (8)$$

Действительно, пусть $G(x) = \mu \sigma (F(\sigma) = x)$, если $\exists \sigma (F(\sigma) = x)$, и $G(x) = 0$ в противном случае. Предположим, что $\text{Set}_x \exists \sigma (x = F(\sigma))$, и выберем ω так, чтобы $F(\sigma) \in \omega$ для всех σ . Выберем σ не принадлежащим множеству $[G(x) \mid x \in \omega]$. Тогда $G(F(\sigma)) \neq \sigma$, поэтому существует τ такое, что $\tau < \sigma$ и $F(\tau) = F(\sigma)$.

Ординал называется *предельным ординалом*, если он не 0 и не является последователем ни для какого ординала. Докажем, что предельный ординал существует. По аксиоме бесконечности существует множество x такое, что $0 \in x$ и $\forall y (y \in x \rightarrow S(y) \in x)$. Пусть z — множество ординалов из x , и пусть $\sigma = \text{Un}(z)$. Имеем $S(0) \in x$ и, следовательно, $0 < S(0) \leq \sigma$; таким образом, $\sigma \neq 0$. Предположим, что $\sigma = S(\tau)$. Тогда $\tau < \sigma = \text{Un}(z)$, следовательно, $\tau < \rho$ для некоторого $\rho \in z$. Отсюда следует, что $\sigma = S(\tau) \leq \rho < S(\rho)$. Но $S(\rho) \in z$, поэтому $S(\rho) \leq \sigma$. Это противоречие показывает, что σ — предельный ординал.

Первый предельный ординал обозначим через ω . Элементы множества ω (т. е. ординалы, меньшие ω) называются *натуральными числами*. Ординал называется *конечным* или *бесконечным* в зависимости от того, является этот ординал натуральным числом или нет. Так, например, ω — первый бесконечный ординал.

Теперь легко доказать аксиомы Пеано. Ясно, что 0 — первый ординал и, следовательно, натуральное число. Если σ — натуральное число, то $\sigma < \omega$, поэтому $S(\sigma) \leq \omega$. Так как ω не является последователем, то $S(\sigma) < \omega$; таким образом, $S(\sigma)$ — натуральное число. Ясно, что $S(\sigma) \neq 0$, а $S(\sigma) = S(\tau) \rightarrow \sigma = \tau$ уже было доказано. Пятая аксиома говорит, что если x — множество такое, что $0 \in x$ и $\forall \sigma (\sigma < \omega \& \sigma \in x \rightarrow S(\sigma) \in x)$, то x содержит каждое натуральное число. Докажем, что $\sigma < \omega \rightarrow \sigma \in x$, трансфинитной индукцией по σ . Если $\sigma = 0$, то $\sigma \in x$. В остальных случаях, так как σ меньше, чем первый предельный ординал, мы должны иметь $\sigma = S(\tau)$. Так как $\tau < \sigma$, то $\tau < \omega$ и $\tau \in x$ по индуктивному предположению. Отсюда следует, что $\sigma = S(\tau) \in x$.

Теперь мы можем определить 1, 2, ... следующим образом: $1 = S(0)$, $2 = S(1)$, ...

Теперь обратимся к определениям по трансфинитной индукции. Идея состоит в том, что мы хотим определить $F(\sigma)$ в терминах σ и значений $F(\tau)$ для ординалов $\tau < \sigma$. Добавляя параметры, мы приходим к следующей ситуации: имея определение G , мы хотим определить F так, чтобы

$$F(\sigma, v_1, \dots, v_n) = G(\sigma, [\langle F(\tau, v_1, \dots, v_n), \tau \rangle \mid \tau < \sigma], v_1, \dots, v_n). \quad (9)$$

Покажем, как это может быть сделано.

Как обычно, опускаем параметры. Пусть $G_{f, \sigma}$ есть сокращение для

$$G(\sigma, [\langle f^* \tau, \tau \rangle \mid \tau < \sigma]).$$

Пусть $Q(f, \sigma)$ означает, что f есть функция, область определения которой включает σ , и для каждого $\tau < \sigma$ имеем $f^* \tau = G_{f, \tau}$. Ясно, что

$$Q(f, \sigma) \& \tau < \sigma \rightarrow Q(f, \tau). \quad (10)$$

Докажем, что

$$Q(f, \sigma) \& Q(g, \sigma) \rightarrow G_{f, \sigma} = G_{g, \sigma}, \quad (11)$$

трансфинитной индукцией по σ . Для $\tau < \sigma$ имеем $Q(f, \tau) \& Q(g, \tau)$ по (10), поэтому $G_{f, \tau} = G_{g, \tau}$ по индуктивному предположению; следовательно, $f^* \tau = G_{f, \tau} = G_{g, \tau} = g^* \tau$. Отсюда следует, что $G_{f, \sigma} = G_{g, \sigma}$.

Определим теперь F следующим образом. Если существует функция f такая, что $Q(f, \sigma)$, то $F(\sigma) = G_{f, \sigma}$, в противном случае $F(\sigma) = 0$. Функция F корректно определена в силу (11). Кроме того,

$$\exists f Q(f, \sigma) \rightarrow F(\sigma) = G(\sigma, [\langle F(\tau), \tau \rangle \mid \tau < \sigma]). \quad (12)$$

Действительно, выберем f так, чтобы $Q(f, \sigma)$. Для каждого $\tau < \sigma$ имеем $Q(f, \tau)$ по (10), поэтому $F(\tau) = f^*\tau$. Отсюда

$$F(\sigma) = G_{f, \sigma} = G(\sigma, [\langle F(\tau), \tau \rangle \mid \tau < \sigma]).$$

В силу (12) осталось лишь доказать, что $\exists f Q(f, \sigma)$. Докажем это трансфинитной индукцией по σ . Пусть $f = [\langle F(\tau), \tau \rangle \mid \tau < \sigma]$; покажем, что $Q(f, \sigma)$. Ясно, что f — функция с областью определения σ . Если $\tau < \sigma$, то

$$F(\tau) = G(\tau, [\langle F(\rho), \rho \rangle \mid \rho < \tau])$$

в силу (12) и индуктивного предположения. Следовательно,

$$f^*\tau = F(\tau) = G(\tau, [\langle F(\rho), \rho \rangle \mid \rho < \tau]) = G_{f, \tau}.$$

Мы называем (9) определением F с помощью трансфинитной индукции по σ . На практике правая часть определения, возможно, не будет иметь точно такого вида, который имеет правая часть (9), нужно будет еще должным образом определить G , чтобы добиться этого. Так мы могли бы определить

$$F(\sigma) = H([F(\tau) \mid \tau < \sigma]).$$

Это принимает должный вид, если мы определим G следующим образом:

$$G(\sigma, f) = H(Ra(f)).$$

Теперь предположим, что H — ординальный функциональный символ такой, что

$$\text{Set}_{x_1, \dots, x_n}(H(x_1, \dots, x_n) \leq \sigma).$$

Мы можем тогда определить функциональный символ F так, что

$$\begin{aligned} F(x_1, \dots, x_n) = \\ = G(x_1, \dots, x_n, [\langle F(y_1, \dots, y_n), y_1, \dots, y_n \rangle \mid \\ H(y_1, \dots, y_n) < H(x_1, \dots, x_n)]). \end{aligned} \quad (13)$$

Чтобы получить такое F , определим

$$F(x_1, \dots, x_n) = I(H(x_1, \dots, x_n))' \langle x_1, \dots, x_n \rangle \quad (14)$$

для подходящего I . Мы хотим, чтобы $I(\sigma)$ было функцией с областью определения

$$[\langle x_1, \dots, x_n \rangle \mid H(x_1, \dots, x_n) = \sigma],$$

значением которой при $\langle x_1, \dots, x_n \rangle$ являлось бы $F(x_1, \dots, x_n)$. Поэтому мы определим с помощью трансфинитной индукции

$$\begin{aligned} I(\sigma) = [\langle G(x_1, \dots, x_n, \text{Un}([I(\tau) \mid \tau < \sigma])), \\ x_1, \dots, x_n \rangle \mid H(x_1, \dots, x_n) = \sigma]. \end{aligned}$$

Из этого определения и (14) мы можем тогда доказать (13). Определение вида (13) (или аналогичное определение с параметрами) будет называться определением с помощью индукции по $H(x_1, \dots, x_n)$.

Мы можем также определять предикаты по индукции. Для простоты рассмотрим одноместный предикат. Пусть H — ординальный функциональный символ такой, что $\vdash \text{Set}_x(H(x) \leq \sigma)$. Для данного Q мы хотим определить R так, чтобы

$$R(x) \leftrightarrow Q(x, [y \mid H(y) < H(x) \& R(y)]). \quad (15)$$

Сначала определим функцию $K_Q(x, z)$, равную 0, если $Q(x, z)$, и 1 в противном случае. Используя индукцию по $H(x)$, определим

$$K_R(x) = K_Q(x, [y \mid H(y) < H(x) \& K_R(y) = 0]).$$

Затем определим

$$R(x) \leftrightarrow K_R(x) = 0.$$

Тогда легко вывести (15). Определение такого вида также может содержать параметры.

Теперь установим соответствие между ординалами и упорядоченными парами ординалов. Вначале определим $\text{Max}(\langle \sigma, \tau \rangle) = \sigma \cup \tau$. Тогда по (7) $\text{Max}(\langle \sigma, \tau \rangle) = \tau$, если $\sigma \leq \tau$, и $\text{Max}(\langle \sigma, \tau \rangle) = \sigma$, если $\tau \leq \sigma$.

Определим теперь $\text{MP}(x)$ следующим образом. Пусть σ — первый ординал такой, что $\neg(\sigma \times \sigma \subset x)$. Такой ординал должен существовать, так как в противном случае $Ra(x)$ содержало бы все ординалы. Пусть τ — первый такой ординал, что $\langle \tau, \rho \rangle \notin x$ для некоторого $\rho \in \sigma$, и пусть

ρ — первый ординал такой, что $\langle \tau, \rho \rangle \notin x$. Положим $MP(x) = \langle \tau, \rho \rangle$.

Ясно, что $MP(x)$ — упорядоченная пара ординалов, не находящихся в x . Если σ такое, как раньше, то $Max(MP(x)) < \sigma$, поэтому по выбору σ имеем

$$Max(MP(x)) \times Max(MP(x)) \subset x. \quad (16)$$

Если σ и τ такие же, как и выше, и $\tau \neq 0$, то $\langle 0, \rho \rangle \in x$ для всех $\rho < \sigma$, поэтому и для $\rho = Max(MP(x))$. Таким образом,

$$\pi_1(MP(x)) \neq 0 \rightarrow \langle 0, Max(MP(x)) \rangle \in x. \quad (17)$$

Теперь определим K с помощью трансфинитной индукции следующим образом:

$$K(\sigma) = MP([K(\tau) \mid \tau < \sigma]).$$

Тогда $K(\sigma)$ — упорядоченная пара ординалов, не находящаяся в $[K(\tau) \mid \tau < \sigma]$; таким образом, $K(\sigma) \neq K(\tau)$ для $\tau < \sigma$. Из этого получаем

$$\sigma \neq \tau \rightarrow K(\sigma) \neq K(\tau). \quad (18)$$

В силу (16) имеем

$$Max(K(\sigma)) \times Max(K(\sigma)) \subset [K(\tau) \mid \tau < \sigma]. \quad (19)$$

Используем это, чтобы показать, что каждая упорядоченная пара ординалов x есть $K(\sigma)$ для некоторого σ . По (18) и (8) имеем $\neg \text{Set}_x \exists \sigma (x = K(\sigma))$. Следовательно, существует σ такое, что

$$K(\sigma) \notin S(Max(x)) \times S(Max(x)).$$

Из этого легко следует, что

$$x \in Max(K(\sigma)) \times Max(K(\sigma)),$$

а тогда требуемый результат следует из (19).

Имеем

$$Max(K(\tau)) < Max(K(\sigma)) \rightarrow \tau < \sigma. \quad (20)$$

Из левой части и (19) следует, что $K(\tau) \in [K(\rho) \mid \rho < \sigma]$, а из этого и (18) следует, что $\tau < \sigma$.

Далее мы докажем

$$Max(K(\sigma)) \leq \sigma \quad (21)$$

трансфинитной индукцией по σ . Предположим, что $\sigma < Max(K(\sigma))$. Выберем τ так, чтобы $K(\tau) = \langle 0, \sigma \rangle$. Тогда

$Max(K(\tau)) = \sigma < Max(K(\sigma))$; таким образом, $\tau < \sigma$ по (20). Следовательно, по трансфинитной индукции $Max(K(\tau)) \leq \tau$. Поэтому $\sigma \leq \tau < \sigma$; получили противоречие.

Наконец, докажем, что

$$\pi_1(K(\sigma)) \neq 0 \rightarrow Max(K(\sigma)) < \sigma. \quad (22)$$

Предположим, что $\pi_1(K(\sigma)) \neq 0$. По (17) существует $\tau < \sigma$ такое, что

$$K(\tau) = \langle 0, Max(K(\sigma)) \rangle.$$

Тогда $Max(K(\sigma)) = Max(K(\tau)) \leq \tau < \sigma$ по (21).

9.4. Кардиналы

Мы говорим, что x и y подобны, если существует биективное отображение из x на y ; символически

$$Sm(x, y) \leftrightarrow \exists f (IFunc(f) \& x = Do(f) \& y = Ra(f)).$$

Легко проверить, что подобие является отношением эквивалентности, т. е.

$$Sm(x, x), \quad (1)$$

$$Sm(x, y) \rightarrow Sm(y, x), \quad (2)$$

$$Sm(x, y) \& Sm(y, z) \rightarrow Sm(x, z). \quad (3)$$

Мы намерены сделать так, чтобы кардинал множества служил какой-то мерой величины этого множества; поэтому мы хотим, чтобы два множества имели один и тот же кардинал тогда и только тогда, когда эти множества подобны. Это подсказывает, что кардиналом множества x должен быть класс эквивалентности множества x по отношению подобия. Однако этот класс эквивалентности не будет множеством. Поэтому мы выбираем в качестве кардинала множества x некоторый конкретный элемент этого класса эквивалентности, а именно, первый ординал в этом классе эквивалентности. Конечно, мы должны быть уверены, что каждый класс эквивалентности содержит некоторый ординал, а это требует новой аксиомы.

Мы говорим, что f есть функция выбора на множестве x , если f — функция с областью определения $P(x) - \{0\}$ и такая, что $f'y \in y$ для каждого y в области определения

функции f . Символически,

$$CF(f, x) \leftrightarrow \text{Func}(f) \& \text{Do}(f) =$$

$$= P(x) - \{0\} \& \forall y (y \in \text{Do}(f) \rightarrow f'y \in y).$$

Аксиомой выбора называется формула

$$\forall x \exists f CF(f, x);$$

она утверждает, что для каждого множества x существует функция выбора на x .

Аксиома выбора справедлива при нашем понимании множеств. Действительно, выберем для каждого непустого подмножества y множества x элемент z_y из y , и пусть f — семейство упорядоченных пар $\langle z_y, y \rangle$. Так как каждая такая пара находится в $x \times P(x)$, то f — множество; ясно, что f — некоторая функция выбора на x .

Теория, получающаяся из теории ZF добавлением аксиомы выбора, обозначается через ZFC. Все дальнейшие результаты этого параграфа доказываются в теории ZFC.

Теорема о вполне упорядоченности (Цермело). Для каждого множества x существует биективное отображение из некоторого ординала на x .

Доказательство. Пусть g — функция выбора на x . Определим с помощью трансфинитной индукции

$$F(\sigma) = g'(x - [F(\tau) \mid \tau < \sigma])$$

(здесь опущены параметры g и x как аргументы F). Так как

$$F(\sigma) \in \text{Ra}(g) \cup \{0\},$$

то мы имеем

$$\text{Set}_z \exists \sigma (F(\sigma) = z).$$

Поэтому по (8) из § 9.3 существуют ординалы σ и τ такие, что $\tau < \sigma$ и $F(\tau) = F(\sigma)$. По определению $F(\sigma)$ и выбору g отсюда следует, что $x \subset [F(\tau) \mid \tau < \sigma]$.

Пусть σ — наименьший ординал такой, что $x \subset [F(\tau) \mid \tau < \sigma]$, и пусть

$$f = [\langle F(\tau), \tau \rangle \mid \tau < \sigma].$$

Тогда f — функция с областью определения σ и $x \subset \text{Ra}(f)$. Если $\tau < \sigma$, то отсюда следует по выбору σ , что $x - [F(\rho) \mid \rho < \tau] \neq \emptyset$; таким образом,

$$F(\tau) \in x - [F(\rho) \mid \rho < \tau].$$

Отсюда получаем, что $\text{Ra}(f) \subset x$, поэтому $\text{Ra}(f) = x$. Отсюда также следует, что

$$\rho < \tau < \sigma \rightarrow F(\rho) \neq F(\tau);$$

таким образом, f является инъективной функцией.

Замечание. Мы также показали, что если g есть функция выбора на x , то существует биективное отображение f из некоторого ординала на x такое, что для каждого $\sigma \in \text{Do}(f)$

$$x - [f'\tau \mid \tau < \sigma] \neq \emptyset \& f'\sigma = g'(x - [f'\tau \mid \tau < \sigma]).$$

Теперь докажем, что

$$x \subset \sigma \rightarrow \exists \tau (\tau \leq \sigma \& \text{Sm}(\tau, x)). \quad (4)$$

Пусть $x \subset \sigma$. Для непустого подмножества y множества x положим $g'y = \mu\tau (\tau \in y)$. Тогда g — функция выбора на x . Ввиду замечания существует биективное отображение из некоторого ординала τ на x такое, что

$$f'\rho = \mu\sigma' (\sigma' \in x - [f'\rho' \mid \rho' < \rho])$$

для $\rho < \tau$. Мы завершим доказательство, показав, что $\tau \leq \sigma$.

Предположим, что $\sigma < \tau$. Тогда $f'\sigma \in x$, откуда имеем $f'\sigma < \sigma$, так как $x \subset \sigma$. Пусть ρ — первый ординал такой, что $f'\rho < \rho$. Так как функция f инъективная, то

$$f'\rho \in x - [f'\rho' \mid \rho' < f'\rho].$$

Но $f'f'\rho$ — первый ординал в этом множестве, поэтому $f'f'\rho \leq f'\rho$. Так как $f'\rho < \rho$ и функция f инъективная, то $f'f'\rho < f'\rho$. Но это вместе с $f'\rho < \rho$ противоречит выбору ρ .

Кардиналом множества x , который будем обозначать через $\text{Card}(x)$, называется первый ординал, подобный x . Ввиду теоремы о вполне упорядоченности это определение корректно. Будем говорить, что σ есть *кардинал*, и записывать $\text{Cd}(\sigma)$, если σ есть кардинал некоторого множества.

Применяя (1) — (3), получаем

$$\text{Card}(x) = \text{Card}(y) \leftrightarrow \text{Sm}(x, y). \quad (5)$$

Из (1) имеем

$$\text{Card}(\sigma) \leq \sigma. \quad (6)$$

Более того,

$$\text{Cd}(\sigma) \leftrightarrow \text{Card}(\sigma) = \sigma. \quad (7)$$

Импликация справа налево получается немедленно. Если $\text{Cd}(\sigma)$, то $\sigma = \text{Card}(x)$ для некоторого x . Тогда $\text{Sm}(\sigma, x)$, поэтому $\text{Card}(\sigma) = \text{Card}(x) = \sigma$ по (5).

Имеем

$$x \subset y \rightarrow \text{Card}(x) \leq \text{Card}(y). \quad (8)$$

Действительно, пусть $\sigma = \text{Card}(y)$. Так как y подобно σ , то множество x подобно некоторому подмножеству ординала σ , поэтому по (4) множество x подобно некоторому ординалу $\tau \leq \sigma$. Тогда $\text{Card}(x) \leq \tau \leq \sigma$.

Имеем

$$\text{Func}(f) \rightarrow \text{Card}(\text{Ra}(f)) \leq \text{Card}(\text{Do}(f)). \quad (9)$$

Действительно, пусть g — функция выбора на $\text{Do}(f)$, и пусть h — функция с областью определения $\text{Ra}(f)$, определенная следующим образом:

$$h'z = g'[y | y \in \text{Do}(f) \& f'y = z].$$

Тогда h — биективное отображение из $\text{Ra}(f)$ на некоторое подмножество ω множества $\text{Do}(f)$, поэтому, используя (8), получаем

$$\text{Card}(\text{Ra}(f)) = \text{Card}(\omega) \leq \text{Card}(\text{Do}(f)).$$

Теперь покажем, что

$$\text{Sm}(S(\sigma), S(\tau)) \rightarrow \text{Sm}(\sigma, \tau). \quad (10)$$

Действительно, пусть f — биективное отображение из $S(\sigma) = \sigma \cup \{\sigma\}$ на $S(\tau) = \tau \cup \{\tau\}$. Изменяя, может быть, два значения f , можно предполагать, что $f'\sigma = \tau$. Тогда ограничение функции f до σ есть биективное отображение σ на τ , поэтому $\text{Sm}(\sigma, \tau)$.

Теперь докажем, что

$$\sigma \in \omega \rightarrow \neg \text{Sm}(\sigma, S(\sigma)), \quad (11)$$

индукцией (обычной) по σ . Случай $\sigma = 0$ легкий, а шаг от σ к $S(\sigma)$ следует из (10).

Теперь можно доказать

$$\sigma \in \omega \rightarrow \text{Cd}(\sigma) \quad (12)$$

индукцией по σ . Случай $\sigma = 0$ может быть выведен из (6) и (7). Теперь предположим, что $\text{Cd}(\sigma)$ для $\sigma \in \omega$. Из (7) и (8) имеем $\sigma = \text{Card}(\sigma) \leq \text{Card}(S(\sigma))$. Но $\text{Card}(S(\sigma)) \neq \text{Card}(\sigma)$ по (11), поэтому $\sigma < \text{Card}(S(\sigma))$, и отсюда $S(\sigma) \leq \text{Card}(S(\sigma))$. Используя (6) и (7), получаем $\text{Cd}(S(\sigma))$.

Таким образом, доказано, что каждое натуральное число есть кардинал. Далее, ω есть кардинал. Если бы это было не так, то было бы $\text{Card}(\omega) < \omega$ по (6) и (7). Поэтому $\text{Card}(\omega)$ есть некоторое натуральное число σ . Так как $S(\sigma) \leq \omega$, то имеем $S(\sigma) = \text{Card}(S(\sigma)) \leq \text{Card}(\omega) = \sigma$. Приходим к противоречию.

Множество называется *конечным* или *бесконечным* в зависимости от того, конечным или бесконечным является его кардинал. Множество называется *счетным* *), если его кардинал есть некоторое натуральное число или ω . Теперь могут быть приведены все обычные доказательства элементарных свойств конечных и счетных множеств.

Определим

$$\sigma + \tau = \text{Card}((\sigma \times \{0\}) \cup (\tau \times \{1\})),$$

$$\sigma \cdot \tau = \text{Card}(\sigma \times \tau).$$

Легко проверить, что

$$x \cap y = 0 \rightarrow \text{Card}(x \cup y) = \text{Card}(x) + \text{Card}(y), \quad (13)$$

$$\text{Card}(x \times y) = \text{Card}(x) \cdot \text{Card}(y). \quad (14)$$

Записывая $x \cup y = x \cup (y - x)$ и применяя (13) и (8), получаем

$$\text{Card}(x \cup y) \leq \text{Card}(x) + \text{Card}(y). \quad (15)$$

Кроме того, имеем

$$\begin{aligned} \text{Cd}(\sigma) \& \forall y (y \in x \rightarrow \text{Card}(y) \leq \sigma) \rightarrow \\ & \rightarrow \text{Card}(\text{Un}(x)) \leq \text{Card}(x) \cdot \sigma. \end{aligned} \quad (16)$$

Сначала заметим, что если f есть биективное отображение из $\text{Card}(y)$ на y , где $y \in x$, то $f \in P(\text{Un}(x) \times \sigma)$. Поэтому, используя функцию выбора на $P(\text{Un}(x) \times \sigma)$, получаем функцию g с областью значений x такую, что $g'y$ для $y \in x$ — биективное отображение $\text{Card}(y)$ на y . Пусть z — множество всех $\langle y, \tau \rangle$ таких, что $y \in x$ и $\tau < \text{Card}(y)$; пусть h — функция с областью определения z , определенная следующим образом: $h'\langle y, \tau \rangle = (g'y)'\tau$. Тогда h — сюръективное отображение из z на $\text{Un}(x)$. Используя (9) и (8), заключаем

$$\text{Card}(\text{Un}(x)) \leq \text{Card}(z) \leq \text{Card}(x \times \sigma) = \text{Card}(x) \cdot \sigma.$$

*) Распространено также и выражение «не более чем счетно». — Прим. ред.

Применяя (13) к $\sigma = \sigma \cup 0$ и $S(\sigma) = \sigma \cup \{\sigma\}$, получаем

$$\text{Card}(\sigma) = \text{Card}(\sigma) + 0, \quad (17)$$

$$\text{Card}(S(\sigma)) = \text{Card}(\sigma) + 1. \quad (18)$$

Из определений также имеем

$$\sigma + \sigma = \sigma \cdot 2. \quad (19)$$

Если σ и τ — натуральные числа, то

$$\sigma + 0 = \sigma,$$

$$\sigma + S(\tau) = S(\sigma + \tau),$$

$$\sigma \cdot 0 = 0,$$

$$\sigma \cdot S(\tau) = (\sigma \cdot \tau) + \sigma.$$

(Читатель легко может провести доказательства.) Из этих равенств индукцией по τ получаем

$$\sigma, \tau \in \omega \rightarrow \sigma + \tau, \sigma \cdot \tau \in \omega. \quad (20)$$

Из (8) получаем

$$\sigma \leq \tau \& \sigma' \leq \tau' \rightarrow \sigma + \sigma' \leq \tau + \tau' \& \sigma \cdot \sigma' \leq \tau \cdot \tau'. \quad (21)$$

Мы записываем $\text{Inf Cd}(\sigma)$ для обозначения того, что σ — бесконечный кардинал. Используя (21), (17) и (19), получаем

$$\text{Inf Cd}(\sigma) \rightarrow \sigma = \sigma + 0 \leq \sigma + 1 \leq \sigma + \sigma = \sigma \cdot 2 \leq \sigma \cdot \sigma. \quad (22)$$

Ввиду результатов из § 9.3 [$\langle K(\tau), \tau \rangle \mid \tau < \sigma$] — биективное отображение из σ на $[K(\tau) \mid \tau < \sigma]$. Следовательно,

$$\text{Card}(\sigma) = \text{Card}([K(\tau) \mid \tau < \sigma]).$$

Применим это к доказательству

$$\text{Inf Cd}(\sigma) \& \text{Max}(K(\sigma)) = \sigma \rightarrow \sigma \cdot \sigma = \sigma. \quad (23)$$

Ввиду (22) нам нужно лишь показать, что $\sigma \cdot \sigma \leq \sigma$. По предположению и (19) из § 9.3 получаем $\sigma \times \sigma \subset [K(\tau) \mid \tau < \sigma]$. Переходя к кардиналам и используя предыдущее равенство, получаем $\sigma \cdot \sigma \leq \sigma$.

Теперь докажем, что

$$\text{Inf Cd}(\sigma) \rightarrow \text{Max}(K(\sigma)) = \sigma, \quad (24)$$

трансфинитной индукцией по σ . Сначала покажем, что из индуктивного предположения следует

$$\rho < \sigma \rightarrow S(\rho) \cdot S(\rho) < \sigma. \quad (25)$$

Если $\rho \in \omega$, то $S(\rho) \cdot S(\rho) < \omega \leq \sigma$ по (20). Теперь предположим, что $\omega \leq \rho$. Положив $\tau = \text{Card}(\rho)$, получим $\omega = \text{Card}(\omega) \leq \tau \leq \rho < \sigma$. Из индуктивного предположения следует, что $\text{Max}(K(\tau)) = \tau$, а из этого и (23) следует, что $\tau \cdot \tau = \tau$. По (18) и (22) имеем $\text{Card}(S(\rho)) = \tau + 1 = \tau$, поэтому $S(\rho) \cdot S(\rho) = \tau \cdot \tau = \tau < \sigma$.

Возвращаясь к (24), предположим, что $\text{Max}(K(\sigma)) \neq \sigma$. Тогда

$$\rho = \text{Max}(K(\sigma)) < \sigma$$

по (21) из § 9.3. Если $\tau < \sigma$, то

$$\text{Max}(K(\tau)) \leq \text{Max}(K(\sigma)) < S(\rho)$$

по (20) из § 9.3, поэтому $K(\tau) \in S(\rho) \times S(\rho)$. Из этого и (25) видим, что

$$\sigma = \text{Card}(\sigma) \leq \text{Card}(S(\rho) \times S(\rho)) < \sigma.$$

Приходим к противоречию.

Комбинируя (23), (24) и (25), получаем

$$\text{Inf Cd}(\sigma) \rightarrow \sigma \cdot \sigma = \sigma \& \sigma + \sigma = \sigma. \quad (26)$$

Из этого мы заключаем, что

$$\text{Inf Cd}(\sigma) \& \text{Inf Cd}(\tau) \rightarrow \sigma \cdot \tau = \sigma + \tau = \text{Max}(\langle \sigma, \tau \rangle). \quad (27)$$

Действительно, пусть $\rho = \text{Max}(\langle \sigma, \tau \rangle)$. Тогда, применяя (21), находим, что

$$\begin{aligned} \rho &= \text{Max}(\langle \sigma + 0, 0 + \tau \rangle) \leq \sigma + \tau \leq \rho + \rho = \rho, \\ \rho &= \text{Max}(\langle \sigma \cdot 1, 1 \cdot \tau \rangle) \leq \sigma \cdot \tau \leq \rho \cdot \rho = \rho. \end{aligned}$$

Имеем также

$$\begin{aligned} \text{Inf Cd}(\sigma) \& \text{Card}(\omega) \leq \\ &\leq \sigma \rightarrow \text{Card}([F(x_1, \dots, x_n) \mid x_1, \dots, x_n \in \omega]) \leq \sigma. \end{aligned} \quad (28)$$

Действительно, определяя $\langle F \rangle$, как в § 9.2, имеем

$$[F(x_1, \dots, x_n) \mid x_1, \dots, x_n \in \omega] = [\langle F \rangle(a) \mid a \in \omega \times \dots \times \omega].$$

Поскольку $\text{Card}(\omega \times \dots \times \omega) \leq \sigma \cdot \dots \cdot \sigma = \sigma$, то требуемый результат следует из (9).

Будем говорить, что множество x является F -замкнутым, если для каждых $y_1, \dots, y_n \in x$ имеем $F(y_1, \dots, y_n) \in x$.

Теорема замыкания. Пусть $F_1, \dots, F_k$ — функциональные символы. Для данного множества x и бесконеч-

ного кардинала τ такого, что $\text{Card}(x) \leq \tau$, существует множество y такое, что $x \subset y$, $\text{Card}(y) \leq \tau$ и y является F_i -замкнутым для $i=1, \dots, k$.

Доказательство. Определим

$$G_i(z) = [F_i(w_1, \dots, w_n) \mid w_1, \dots, w_n \in z],$$

$$G(z) = G_1(z) \cup \dots \cup G_k(z).$$

Определим H с помощью трансфинитной индукции следующим образом: $H(0) = x$, $H(\sigma) = G(H(\rho))$, если $\sigma = S(\rho)$; $H(\sigma) = \bigcup_{\rho} ([H(\rho) \mid \rho < \sigma])$, если σ — предельный ординал. Мы утверждаем, что $y = H(\omega)$ обладает требуемыми свойствами. Очевидно, что $x \subset y$. Если $w_1, \dots, w_n \in y$, то $w_1, \dots, w_n \in H(\sigma)$ для некоторого $\sigma < \omega$; следовательно,

$$F_i(w_1, \dots, w_n) \in G(H(\sigma)) = H(S(\sigma)) \subset y.$$

Используя (28) и (15), получаем $\text{Card}(z) \leq \tau \rightarrow \text{Card}(G(z)) \leq \tau$. Используя это, мы легко доказываем индукцией, что $\sigma < \omega \rightarrow \text{Card}(H(\sigma)) \leq \tau$. Тогда по (16) имеем $\text{Card}(y) \leq \tau \cdot \omega \leq \tau \cdot \tau = \tau$.

Рассмотрим теперь операцию, которая позволит нам получать кардиналы, большие ω . Определим

$$2^\sigma = \text{Card}(P(\sigma)).$$

(Здесь 2 — функциональный символ и не связан с ранее введенной константой 2 . О причинах введения такого обозначения см. в задаче 7.) Так как $\text{Sm}(x, \sigma) \rightarrow \text{Sm}(P(x), P(\sigma))$, то мы имеем

$$\text{Card}(x) = \sigma \rightarrow \text{Card}(P(x)) = 2^\sigma. \quad (29)$$

Следующий результат известен как *теорема Кантора*:

$$\text{Cd}(\sigma) \rightarrow \sigma < 2^\sigma. \quad (30)$$

Прежде всего существует биективное отображение f из σ на подмножество из $P(\sigma)$, которое отображает τ в $\{\tau\}$. Таким образом, $\sigma \leq 2^\sigma$; поэтому достаточно доказать, что предположение $2^\sigma = \sigma$ приводит к противоречию. Предположим, что g — биективное отображение из σ на $P(\sigma)$. Пусть

$$x = [\tau \mid \tau \in \sigma \ \& \ \tau \notin g'\tau].$$

Тогда $x \in P(\sigma)$, поэтому существует τ такое, что $g'\tau = x$. По определению множества x имеем

$$\tau \in x \leftrightarrow \tau \notin g'\tau \leftrightarrow \tau \notin x;$$

получаем противоречие.

Более общо, имеем

$$\sigma < 2^\sigma. \quad (31)$$

Действительно, если $2^\sigma \leq \sigma$, то, применяя (29), получаем

$$2^{\text{Card}(\sigma)} = \text{Card}(P(\sigma)) = \text{Card}(2^\sigma) \leq \text{Card}(\sigma),$$

что противоречит теореме Кантора. Как следствие (31) мы заключаем, что для каждого ординала существует больший кардинал. Отсюда следует, что для любого множества x ординалов существует кардинал, больший каждого элемента множества x . Более того, можно предположить, что этот кардинал бесконечный, так как если бы он был конечным, то мы могли бы заменить его большим кардиналом ω .

Из только что сделанного замечания мы видим, что можно определить функциональный символ $\aleph$ с помощью трансфинитной индукции следующим образом:

$$\aleph(\sigma) = \mu\tau (\text{InfCd}(\tau) \ \& \ \tau \notin [\aleph(\rho) \mid \rho < \sigma]).$$

Мы обычно будем писать $\aleph_\sigma$ вместо $\aleph(\sigma)$. Тогда $\aleph_\sigma$ — бесконечный кардинал. Далее,

$$\sigma < \tau \rightarrow \aleph_\sigma < \aleph_\tau. \quad (32)$$

Действительно, пусть $\sigma < \tau$. Тогда $\aleph_\tau$ по определению отлично от $\aleph_\sigma$ и не лежит в $[\aleph_\rho \mid \rho < \sigma]$. Так как $\aleph_\sigma$ — наименьший бесконечный кардинал с последним свойством, то $\aleph_\sigma < \aleph_\tau$.

Покажем теперь, что каждый бесконечный кардинал есть $\aleph_\sigma$ для некоторого σ (и, следовательно, по (32) для единственного σ). Вследствие (32) и (8) из § 9.3 имеем $\bigcap \text{Set}_x \exists \sigma (x = \aleph_\sigma)$. Поэтому если τ — бесконечный кардинал, то существует σ такое, что $\aleph_\sigma \notin \tau$. Таким образом, $\tau \leq \aleph_\sigma$. Если выполняется равенство, то всё доказано. Предположим, что $\tau < \aleph_\sigma$. Так как $\aleph_\sigma$ — первый бесконечный кардинал, не лежащий в $[\aleph_\rho \mid \rho < \sigma]$, то имеем $\tau \in [\aleph_\rho \mid \rho < \sigma]$, что дает требуемый результат.

Ясно, что $\aleph_0 = \omega$ и по (32) $\aleph_{S(\sigma)}$ — первый бесконечный кардинал, больший $\aleph_\sigma$. Из этого и теоремы Кантора получаем

$$\aleph_{S(\sigma)} \leq 2^{\aleph_\sigma}. \quad (33)$$

Формула

$$\forall \sigma (2^{\aleph_\sigma} = \aleph_{S(\sigma)}),$$

которая утверждает, что в (33) всегда выполняется равенство, называется *обобщенной гипотезой континуума*. Формула

$$2^{\aleph_0} = \aleph_1,$$

выражающая один частный случай этого равенства, называется *гипотезой континуума*.

Хотя было предпринято большое число попыток решить, будут эти две формулы истинными утверждениями о множествах или нет, проблема до сих пор не решена. Логические исследования показали по крайней мере, почему эта проблема так трудна: ни одна из этих формул не может быть доказана или опровергнута в теории ZFC.

Мы посвятим доказательству этого факта несколько следующих параграфов. Вначале отметим одно затруднение. Если мы, например, докажем, что гипотеза континуума не является теоремой теории ZFC, то отсюда будет следовать непротиворечивость ZFC. Следовательно, по теореме о доказательствах непротиворечивости никакое такое доказательство не может быть проведено внутри теории ZFC. Поэтому это доказательство должно быть очень неконструктивным и, возможно, не будет признано многими математиками.

Мы обходим эту трудность, предположив заранее непротиворечивость теории ZF. Это разумный подход, так как даже если кто-то сомневается в непротиворечивости теории ZF, то он должен признать, что эта проблема непротиворечивости сильно отличается от проблемы независимости гипотезы континуума. Мы увидим, что возможно дать финитное доказательство такого утверждения: если теория ZF непротиворечива, то ни (обобщенная) гипотеза континуума, ни ее отрицание не могут быть доказаны в теории ZFC.

Мы докажем также один родственный результат: если теория ZF непротиворечива, то ни аксиома выбора, ни ее отрицание не могут быть доказаны в теории ZF. Кое-кто может спросить: почему эта проблема представляет интерес, ведь аксиома выбора, конечно, справедлива для множеств? Один из ответов состоит в том, что аксиома выбора имеет специфическую природу. Множества, существование которых утверждается в аксиомах существования теории ZF (такие, как множество подмножеств некоторого множества),

могут быть точно описаны в теории ZF; в действительности эти аксиомы имеют вид $[x | Q(x, v_1, \dots, v_n)]$. С другой стороны, нет причин предполагать, что для каждого множества v существует функция выбора на v , которая может быть описана подобным путем. Следовательно, можно представить, что при некотором понимании множества, при котором допускаются только семейства, которые могут быть описаны, аксиомы теории ZF являются истинными, в то время как аксиома выбора ложна. Конечно, это может случиться, лишь если аксиома выбора не является теоремой теории ZF.

Другим основанием для доказательства такого результата является то, что он сводит трудную проблему получения в некотором смысле приемлемого доказательства непротиворечивости теории ZFC к аналогичной и, возможно, более легкой проблеме получения такого доказательства для теории ZF.

9.5. Интерпретации теории множеств

Утверждение о том, что формула A не доказуема в теории ZF, в силу следствия к теореме редукции для непротиворечивости эквивалентно утверждению о том, что какое-то расширение ZF' теории ZF непротиворечиво. Поэтому те результаты, которые мы хотим доказывать, имеют вид: если теория ZF непротиворечива, то теория ZF' непротиворечива. По следствию к теореме об интерпретации это может быть доказано с помощью построения некоторой интерпретации теории ZF' в теории ZF. По этим причинам мы начинаем с изучения интерпретаций теории ZF и других родственных теорий.

Удобно слегка обобщить понятие интерпретации. Интерпретация языка $L(ZF)$ в теории T будет теперь содержать некоторый унарный предикатный символ U_I такой, что $\vdash \exists x U_I x$, и два бинарных предикатных символа $\in_I$ и $=_I$. Мы строим A_I и $A^{(I)}$, как и раньше, за исключением того, что мы заменяем также $=$ на $=_I$. Интерпретация языка $L(ZF)$ будет называться *интерпретацией* теории ZF, если интерпретации аксиом тождества, аксиом равенства и нелогических аксиом теории ZF являются доказуемыми. Тогда, как и раньше, мы можем доказать теорему об интерпретации и ее следствие. Если $=_I$ есть $=$, то мы получаем ранее

рассмотренный случай. При этом интерпретации аксиом тождества и аксиом равенства всегда доказуемы.

Напомним, что если Q определяется следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow D,$$

то Q_I определяется следующим образом:

$$Q_I(x_1, \dots, x_n) \leftrightarrow D_I.$$

Мы можем принять это определение даже тогда, когда I — некоторая интерпретация языка $L(ZF)$ в расширенном смысле. Тогда при образовании A_I или $A^{(I)}$ мы просто заменяем Q на Q_I .

Мы будем брать наши интерпретации в некоторой теории T , являющейся расширением теории ZF . Более того, будем предполагать, что все символы теории T , не являющиеся символами теории ZF , представляют собой константы. Это означает, что каждая из аксиом подмножества или замены для теории T есть частный случай аксиомы подмножества или замены для теории ZF и, следовательно, может быть доказана в теории T . Поэтому все результаты, доказанные для теории ZF , также выполняются для теории T . Все доказательства мы собираемся проводить в теории T , если не оговорено противное.

Так как всякая интерпретация является некоторым формальным аналогом структуры, то многие понятия, относящиеся к структурам, имеют соответствующие аналоги в теории интерпретаций. Рассмотрим аналог понятия изоморфизма.

Пусть I и J — интерпретации языка $L(ZF)$ в теории T . *Изоморфизмом между I и J* называется унарный функциональный символ F теории T такой, что

$$\vdash U_J(y) \leftrightarrow \exists x (U_I(x) \& y = F(x)), \quad (1)$$

$$\vdash U_I(x) \& U_I(y) \rightarrow (x \in_I y \leftrightarrow F(x) \in_J F(y)), \quad (2)$$

$$\vdash U_I(x) \& U_I(y) \rightarrow (x =_I y \leftrightarrow F(x) =_J F(y)). \quad (3)$$

Лемма 1. Пусть I и J — интерпретации языка $L(ZF)$ в теории T , F — некоторый изоморфизм между I и J , Q — некоторый предикатный символ теории ZF . Тогда

$$\vdash U_I x_1 \& \dots \& U_I x_n \rightarrow (Q_I(x_1, \dots, x_n) \leftrightarrow Q_J(F(x_1), \dots, F(x_n))).$$

Доказательство. Используем индукцию по длине правой части A определения Q . Если A — атомная формула,

то Q определяется следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow x_i \in x_j$$

или

$$Q(x_1, \dots, x_n) \leftrightarrow x_i = x_j,$$

и этот результат следует из (2) и (3). Если A — отрицание или дизъюнкция, то Q определяется следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow \neg R(x_1, \dots, x_n),$$

где лемма выполняется для R , или следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow R_1(x_1, \dots, x_n) \vee R_2(x_1, \dots, x_n),$$

где лемма выполняется для R_1 и R_2 . В каждом из этих случаев лемма для Q легко следует из индуктивного предположения.

Если A — подтверждение, то Q определяется так:

$$Q(x_1, \dots, x_n) \leftrightarrow \exists y R(y, x_1, \dots, x_n),$$

где по индуктивному предположению имеем

$$U_I x_1 \& \dots \& U_I x_n \& U_I y \rightarrow$$

$$\rightarrow (R_I(y, x_1, \dots, x_n) \leftrightarrow R_J(F(y), F(x_1), \dots, F(x_n))).$$

Следовательно, при предположении, что $U_I x_1 \& \dots \& U_I x_n$, имеем

$$\exists y (U_I(y) \& R_I(y, x_1, \dots, x_n)) \leftrightarrow$$

$$\leftrightarrow \exists y (U_I(y) \& R_J(F(y), F(x_1), \dots, F(x_n))).$$

Левая часть этой эквивалентности есть $Q_I(x_1, \dots, x_n)$, поэтому нам нужно лишь показать, что правая часть эквивалентна $Q_J(F(x_1), \dots, F(x_n))$. Опуская $F(x_1), \dots, F(x_n)$, в силу (1) имеем

$$\exists y (U_I(y) \& R_J(F(y))) \leftrightarrow \exists y (U_I(y) \& \exists z (z = F(y) \& R_J(z)))$$

$$\leftrightarrow \exists z (\exists y (U_I(y) \& z = F(y)) \& R_J(z))$$

$$\leftrightarrow \exists z (U_J(z) \& R_J(z)).$$

Правая часть есть $Q_J(F(x_1), \dots, F(x_n))$.

Доказательство, что все предикатные символы имеют некоторое свойство, с помощью индукции вышеприведенного типа будет называться доказательством *индукцией по предикатным символам*.

Если M — некоторый унарный предикатный символ теории T такой, что $\vdash \exists x M(x)$, то мы можем построить интер-

претацию I языка $L(ZF)$, беря M за U_I , $\in$ за $\in_I$ и $=$ за $=_I$. Мы называем эту интерпретацию $\in$ -интерпретацией M и пишем A_M и $A^{(M)}$ вместо A_I и $A^{(I)}$ соответственно. Множества x такие, что $M(x)$, будут называться M -множествами.

Пусть A — некоторая константа теории T такая, что $\vdash A \neq 0$. Определяя M следующим образом: $M(x) \leftrightarrow x \in A$, получаем $\vdash \exists x M(x)$. $\in$ -интерпретацией A будет называться $\in$ -интерпретация M ; будем писать A_A и $A^{(A)}$ вместо A_M и $A^{(M)}$. $\in$ -интерпретация M называется транзитивной, если

$$\vdash M(x) \& y \in x \rightarrow M(y).$$

Тогда, если A — константа, то $\in$ -интерпретация A транзитивна в том и только в том случае, когда $\vdash \text{Trans}(A)$.

Покажем, что всякая интерпретация, удовлетворяющая подходящим условиям, изоморфна транзитивной $\in$ -интерпретации. Предположим, что I — интерпретация языка $L(ZF)$ такая, что $=_I$ есть $=$, и такая, что интерпретация аксиомы объемности выполняется. Предположим, далее, что существует некоторый ординальный функциональный символ H такой, что

$$\vdash \text{Set}_x(H(x) \leq \sigma)$$

и

$$\vdash y \in_I x \rightarrow H(y) < H(x).$$

Определим

$$F(y) = [F(x) \mid U_I(x) \& x \in_I y]$$

индукцией по $H(y)$, а затем определим

$$M(x) \leftrightarrow \exists y (U_I(y) \& x = F(y)). \quad (4)$$

Ясно, что $\vdash \exists x M(x)$, поэтому M есть $\in$ -интерпретация. Более того, M — транзитивная интерпретация. Действительно, предположим, что $M(x) \& z \in x$. Тогда $x = F(y)$ для некоторого y , поэтому $z \in F(y)$; а тогда $z = F(w)$ для некоторого w такого, что $U_I(w)$; следовательно, $M(z)$.

Покажем, что F — изоморфизм между I и $\in$ -интерпретацией M . Мы должны доказать (1) — (3), когда J есть M . (1) есть в точности (4). Для (3) мы должны доказать

$$x = y \leftrightarrow F(x) = F(y)$$

при условии $U_I(x)$ и $U_I(y)$. Используем индукцию по $H(x)$.

Импликация слева направо получается сразу. Из интерпретации аксиомы объемности относительно I имеем

$$\forall z (U_I(z) \rightarrow (z \in_I x \leftrightarrow z \in_I y)) \rightarrow x = y,$$

поэтому достаточно показать, что если $F(x) = F(y)$ и $U_I(z)$, то $z \in_I x \leftrightarrow z \in_I y$. Предположим, что $z \in_I x$. Тогда $F(z) \in F(x) = F(y)$; следовательно, $F(z) = F(w)$ для некоторого w такого, что $U_I(w)$ и $w \in_I y$. По индуктивному предположению $z = w$; следовательно, $z \in_I y$. Импликация $z \in_I y \rightarrow z \in_I x$ доказывается аналогично.

Для (2) мы должны доказать

$$x \in_I y \leftrightarrow F(x) \in F(y)$$

при условии $U_I(x)$ и $U_I(y)$. Импликация слева направо доказывается сразу. Если $F(x) \in F(y)$, то $F(x) = F(z)$ для некоторого z такого, что $U_I(z)$ и $z \in_I y$. Как и раньше, имеем $x = z$, поэтому $x \in_I y$.

Теперь мы переходим к получению некоторых достаточных условий, при которых интерпретации аксиом теории ZF относительно некоторой транзитивной $\in$ -интерпретации были бы выводимы.

Лемма 2. Если M — транзитивная $\in$ -интерпретация языка $L(ZF)$, то интерпретации аксиомы объемности и аксиомы регулярности выполняются.

Доказательство. Интерпретацией аксиомы объемности является

$$M(x) \rightarrow M(y) \rightarrow \forall z (M(z) \rightarrow (z \in x \leftrightarrow z \in y)) \rightarrow x = y.$$

Допустим, что посылки верны. Если $z \in x$, то $M(z)$ ввиду транзитивности M , поэтому $z \in y$. Подобным образом из $z \in y$ следует $z \in x$; таким образом, $x = y$.

Интерпретацией аксиомы регулярности является

$$M(x) \rightarrow \exists y (M(y) \& y \in x) \rightarrow$$

$$\rightarrow \exists y (M(y) \& y \in x \& \neg \exists z (M(z) \& z \in x \& z \in y)).$$

Допустим, что обе посылки верны. Тогда x имеет некоторый минимальный элемент y , который является M -множеством ввиду транзитивности M . Следовательно, y удовлетворяет заключению.

Функциональный символ F теории T называется M -инвариантным, если

$$\vdash M(x_1) \& \dots \& M(x_n) \rightarrow M(F(x_1, \dots, x_n)).$$

Лемма 3. Пусть M — некоторая транзитивная $\in$ -интерпретация языка $L(ZF)$ такая, что для каждого предикатного символа Q из $L(ZF)$ функциональный символ F , определенный так:

$$F(y, v_1, \dots, v_n) = [x \mid x \in y \& Q_M(x, v_1, \dots, v_n)],$$

является M -инвариантным. Тогда выполняется интерпретация каждой аксиомы подмножества из теории ZF .

Доказательство. Всякая аксиома подмножества имеет вид

$$\exists z \forall x (x \in z \leftrightarrow x \in y \& Q(x))$$

(здесь мы опустили параметры). Ее M -интерпретацией является

$$M(y) \rightarrow \exists z (M(z) \& \forall x (M(x) \rightarrow \rightarrow (x \in z \leftrightarrow x \in y \& Q_M(x))))). \quad (5)$$

Для данного M -множества y положим $z = F(y)$, где F таков, как в лемме. Тогда z есть M -множество и для всех M -множеств x имеем $x \in z \leftrightarrow x \in y \& Q_M(x)$. Таким образом, (5) выполняется.

Лемма 4. Пусть M — некоторая транзитивная $\in$ -интерпретация языка $L(ZF)$ такая, что для каждого M -инвариантного функционального символа F

$$\vdash M(w) \& M(v_1) \& \dots \& M(v_n) \rightarrow \rightarrow \exists z (M(z) \& \forall x (x \in w \rightarrow F(x, v_1, \dots, v_n) \subset z)).$$

Тогда выполняется интерпретация каждой аксиомы замены из теории ZF .

Доказательство. Всякая аксиома замены имеет вид

$$\forall x \exists z \forall y (y \in z \leftrightarrow Q(x, y)) \rightarrow \text{Set}_y \exists x (x \in w \& Q(x, y))$$

(здесь мы опустили параметры). Ее M -интерпретация имеет посылку

$$M(w) \& \forall x (M(x) \rightarrow \exists z (M(z) \& \forall y (M(y) \rightarrow \rightarrow (y \in z \leftrightarrow Q_M(x, y)))))) \quad (6)$$

и заключение

$$\exists z (M(z) \& \forall y (M(y) \rightarrow \rightarrow \exists x (M(x) \& x \in w \& Q_M(x, y)) \rightarrow y \in z)). \quad (7)$$

Определим F следующим образом:

$$F(x) = [y \mid M(y) \& Q_M(x, y)],$$

если множество в правой части существует и является M -множеством, и $F(x) = x$ в противном случае. Тогда F является M -инвариантным. Допустим (6). Тогда для каждого M -множества x существует M -множество z такое, что

$$\forall y (M(y) \rightarrow (y \in z \leftrightarrow Q_M(x, y))).$$

Теперь $y \in z \rightarrow M(y)$ ввиду транзитивности M ; таким образом, $z = [y \mid M(y) \& Q_M(x, y)]$. Отсюда следует, что

$$M(x) \rightarrow F(x) = [y \mid M(y) \& Q_M(x, y)]. \quad (8)$$

По предположению теоремы мы можем выбрать M -множество z такое, что $\forall x (x \in w \rightarrow F(x) \subset z)$. Чтобы доказать (7), мы должны показать, что

$$M(y) \& M(x) \& x \in w \& Q_M(x, y) \rightarrow y \in z.$$

Ввиду (8) посылка влечет $y \in F(x)$; таким образом, имеем $y \in z$.

Лемма 5. Пусть M — некоторая транзитивная $\in$ -интерпретация языка $L(ZF)$ такая, что

$$\vdash M(y) \rightarrow \exists w (M(w) \& [x \mid M(x) \& x \subset y] \subset w).$$

Тогда интерпретация аксиомы степени выполняется.

Доказательство. Интерпретацией аксиомы степени является

$$M(y) \rightarrow \exists w (M(w) \& \forall x (M(x) \rightarrow \rightarrow \forall z (M(z) \rightarrow z \in x \rightarrow z \in y) \rightarrow x \in w)). \quad (9)$$

Если $M(x)$, то $z \in x \rightarrow M(z)$ ввиду транзитивности M . Поэтому в (9) мы можем опустить часть $M(z) \rightarrow$. Тогда (9) выполняется ввиду предположения леммы.

Лемма 6. Если M — транзитивная интерпретация языка $L(ZF)$ такая, что $M(\omega)$, то интерпретация аксиомы бесконечности выполняется.

Доказательство. Так как $M(\omega)$, то мы имеем $M(\sigma)$ для каждого натурального числа σ ввиду транзитивности M . Тогда легко доказать, что ω есть M -множество, удовлетворяющее условиям, требуемым для интерпретации аксиомы бесконечности.

Теперь предположим, что M — некоторая фиксированная транзитивная $\in$ -интерпретация теории ZF . Тогда мы можем образовывать F_M для каждого функционального символа F из ZF . (Это требует выбора константы в T ; мы можем

выбрать константу 0.) Пусть теперь A — формула, содержащая определимые нелогические символы, и пусть A^* — ее перевод в язык теории ZF. Тогда $\vdash A \leftrightarrow A^*$ в теории ZF; следовательно,

$$\vdash M(x_1) \& \dots \& M(x_n) \rightarrow (A_M \leftrightarrow A_M^*)$$

(где $x_1, \dots, x_n$ — переменные, свободные в A). Отсюда следует, что $\vdash A^{(M)}$ тогда и только тогда, когда $\vdash A^{*(M)}$. Это показывает, что при образовании $A^{(M)}$ нам не нужно элиминировать определимые символы, а мы можем заменять Q и F на Q_M и F_M .

Далее, формула $\exists y (y = F(x_1, \dots, x_n))$ доказуема в теории ZF. Ее M -интерпретацией является

$$M(x_1) \& \dots \& M(x_n) \rightarrow \exists y (M(y) \& y = F_M(x_1, \dots, x_n)).$$

Это показывает, что F_M есть M -инвариантный функциональный символ.

Если F определяется следующим образом:

$$F(v_1, \dots, v_n) = [x | Q(x, v_1, \dots, v_n)],$$

то

$$F_M(v_1, \dots, v_n) = [x | M(x) \& Q_M(x, v_1, \dots, v_n)] \quad (10)$$

для любых M -множеств $v_1, \dots, v_n$. Действительно, интерпретация определяющей аксиомы для F утверждает, что для таких $v_1, \dots, v_n$

$$\forall x (M(x) \rightarrow (x \in F_M(v_1, \dots, v_n) \leftrightarrow Q_M(x, v_1, \dots, v_n))).$$

Так как F_M является M -инвариантным функциональным символом, то $F_M(v_1, \dots, v_n)$ является M -множеством, поэтому имеем

$$x \in F_M(v_1, \dots, v_n) \rightarrow M(x)$$

ввиду транзитивности M . Комбинируя эти два результата, получаем (10).

Если F определяется следующим образом:

$$F(v_1, \dots, v_n) = [G(x, v_1, \dots, v_n) | Q(x, v_1, \dots, v_n)],$$

то

$$F_M(v_1, \dots, v_n) = [G_M(x, v_1, \dots, v_n) | M(x) \& Q_M(x, v_1, \dots, v_n)] \quad (11)$$

для любых M -множеств $v_1, \dots, v_n$. Действительно, в силу

(10) имеем

$$F_M(v_1, \dots, v_n) = [y | M(y) \& \exists x (M(x) \& y = G_M(x, v_1, \dots, v_n) \& Q_M(x, v_1, \dots, v_n))].$$

Используя M -инвариантность G_M , получаем (11).

Будем говорить, что предикатный символ Q теории ZF является *абсолютным* для M , если

$$\vdash M(x_1) \& \dots \& M(x_n) \rightarrow (Q(x_1, \dots, x_n) \leftrightarrow Q_M(x_1, \dots, x_n)). \quad (12)$$

Будем говорить, что функциональный символ F теории ZF является *абсолютным* для M , если

$$\vdash M(x_1) \& \dots \& M(x_n) \rightarrow F(x_1, \dots, x_n) = F_M(x_1, \dots, x_n).$$

Когда M фиксировано, мы говорим просто *абсолютно* вместо *абсолютно для M* .

Если Q абсолютно, то мы можем заменять Q_M на Q всякий раз, когда условия обеспечивают, что аргументы для Q_M являются M -множествами; аналогично для функциональных символов. Это полезно при изучении интерпретаций аксиом.

Если F — абсолютный функциональный символ, то F является M -инвариантным функциональным символом — это следует из того, что F_M является M -инвариантным функциональным символом.

Теперь рассмотрим методы для доказательства того, что нелогические символы абсолютны. Ясно, что $\in$ и $=$ абсолютны. Если Q определяется так:

$$Q(x_1, \dots, x_n) \leftrightarrow _, \quad (13)$$

где $_$ состоит из $x_1, \dots, x_n$ и абсолютных нелогических символов, то Q абсолютен. Действительно, интерпретация для (13) утверждает, что

$$Q_M(x_1, \dots, x_n) \leftrightarrow (_)_M$$

для M -множеств $x_1, \dots, x_n$. Далее, все термы в $(_)_M$ строятся из x_i и функциональных символов G_M . Так как последние M -инвариантны, то из условия, что x_i являются M -множествами, следует, что эти термы представляют M -множества. Следовательно, по сделанному выше замечанию мы можем заменить каждое G_M или R_M в $(_)_M$ на G

или R . Поэтому мы получим

$$Q_M(x_1, \dots, x_n) \leftrightarrow \text{—},$$

которое вместе с (13) дает (12).

Теперь покажем, что если F определяется следующим образом:

$$F(x_1, \dots, x_n) = y \leftrightarrow Q(y, x_1, \dots, x_n), \quad (14)$$

где Q — абсолютный символ, то F — абсолютный символ.

Допустим, что $x_1, \dots, x_n$ — M -множества. Подставив $F_M(x_1, \dots, x_n)$ вместо y в (14), получаем

$$F(x_1, \dots, x_n) = F_M(x_1, \dots, x_n) \leftrightarrow Q(F_M(x_1, \dots, x_n), x_1, \dots, x_n).$$

Таким образом, нам нужно лишь доказать правую часть этой эквивалентности. Ввиду абсолютности Q и M -инвариантности F_M это эквивалентно

$$Q_M(F_M(x_1, \dots, x_n), x_1, \dots, x_n). \quad (15)$$

Теперь по (14) $Q(F(x_1, \dots, x_n), x_1, \dots, x_n)$ доказуема в ZF. Беря ее интерпретацию, мы получаем (15).

Частный случай возникает, когда F определяется следующим образом:

$$F(x_1, \dots, x_n) = \text{—},$$

где — состоит из $x_1, \dots, x_n$ и абсолютных функциональных символов. Действительно, это определение эквивалентно (14), где Q определяется следующим образом:

$$Q(y, x_1, \dots, x_n) \leftrightarrow y = \text{—};$$

а мы видели выше, что такой символ Q абсолютен.

Если Q определяется следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow \neg R(x_1, \dots, x_n),$$

где R — абсолютный символ, или следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow R_1(x_1, \dots, x_n) \vee R_2(x_1, \dots, x_n),$$

где R_1 и R_2 — абсолютные символы, то Q — абсолютный символ; это легко доказать. Из этого мы получаем аналогичный результат для $\rightarrow$, $\&$ или $\leftrightarrow$ вместо $\vee$.

Будем говорить, что Q *полно* для M (или просто *полно*), если

$$\vdash M(y_1) \& \dots \& M(y_n) \& Q(x, y_1, \dots, y_n) \rightarrow M(x).$$

Например, ясно, что $=$ полно и $\in$ полно в силу транзитивности M . Мы иногда будем говорить, что — x — *полно* в x ; это означает, что Q , определенное следующим образом:

$$Q(x, v_1, \dots, v_n) \leftrightarrow \text{—} x \text{—},$$

является полным. Таким образом, в силу полноты $\in$ получаем, что

$$x \in y \& \text{—} x \text{—}$$

и

$$\neg(x \in y \rightarrow \text{—} x \text{—})$$

являются полными в x .

Если Q определяется следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow \exists y R(y, x_1, \dots, x_n), \quad (16)$$

где R — абсолютный и полный символ, то Q — абсолютный символ. Действительно, пусть $x_1, \dots, x_n$ — M -множества. Из интерпретации для (16) получаем

$$Q_M(x_1, \dots, x_n) \leftrightarrow \exists y (M(y) \& R_M(y, x_1, \dots, x_n)).$$

Ввиду абсолютности R мы можем заменить R_M на R , а затем в силу полноты R мы можем опустить часть $M(y) \&$. Комбинируя этот результат с (16), получаем (12). Отсюда следует, что если Q определяется следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow \forall y R(y, x_1, \dots, x_n), \quad (17)$$

где R — абсолютный символ и $\neg R$ полно, то Q — абсолютный символ.

Если F определяется следующим образом:

$$F(v_1, \dots, v_n) = [x | Q(x, v_1, \dots, v_n)],$$

где Q — абсолютный и полный символ, то F — абсолютный символ. Действительно, если $v_1, \dots, v_n$ — M -множества, то (10) выполняется. Как и раньше, мы можем вначале заменить Q_M на Q , а затем опустить часть $M(x) \&$. Из этого получаем

$$F_M(v_1, \dots, v_n) = [x | Q(x, v_1, \dots, v_n)],$$

откуда следует, что F — абсолютный символ. Подобное доказательство, использующее (11), показывает, что если F

определяется следующим образом:

$$F(v_1, \dots, v_n) = [G(x, v_1, \dots, v_n) | Q(x, v_1, \dots, v_n)],$$

где G и Q абсолютны и Q полный, то F абсолютен.

Будем использовать эти результаты, чтобы показать, что многие нелогические символы, которые мы определили, являются абсолютными. Для каждого нелогического символа мы будем давать определяющую аксиому. Мы оставляем читателю большую часть проверки того, что здесь применимы вышеприведенные результаты, указывая лишь некоторые менее очевидные шаги. Иногда определяющая аксиома, которую мы даем, несколько отличается от (но, очевидно, эквивалентна) определяющей аксиомы, которую мы использовали раньше.

$$A. x \subset y \leftrightarrow \forall z (z \in x \rightarrow z \in y).$$

Применение правил в этом случае использует то, что $\neg(z \in x \rightarrow z \in y)$ полно в z .

$$B. 0 = [x | x \neq x].$$

Ясно, что $x \neq x$ полно в x .

$$V. \{x, y\} = [z | z = x \vee z = y].$$

$$G. \{x\} = \{x, x\}.$$

$$D. Un(x) = [y | \exists z (z \in x \& y \in z)].$$

Ясно, что $z \in x \& y \in z$ полно в z . Мы должны также показать, что $\exists z (z \in x \& y \in z)$ полно в y , т. е.

$$M(x) \& \exists z (z \in x \& y \in z) \rightarrow M(y).$$

А это следует из транзитивности M .

$$E. x \cup y = Un(\{x, y\}).$$

$$Ж. x \cap y = [z | z \in x \& z \in y].$$

$$З. x - y = [z | z \in x \& z \notin y].$$

$$И. \langle x, y \rangle = \{\{x\}, \{x, y\}\}.$$

$$K. \exists y (x = \langle \pi_1(x), y \rangle) \vee (\neg \exists y \exists z (x = \langle y, z \rangle) \& \pi_1(x) = 0).$$

Необходимая полнота для этого определения следует из

$$M(\langle a, b \rangle) \rightarrow M(a) \& M(b). \quad (18)$$

А это следует из транзитивности M , так как $a, b \in \{a, b\}$ и $\{a, b\} \in \langle a, b \rangle$. С π_2 поступаем аналогичным образом.

$$Л. x \times y = [z | \exists a \exists b (a \in x \& b \in y \& z = \langle a, b \rangle)].$$

Для этого нам нужно доказать, что

$$\exists a \exists b (a \in x \& b \in y \& z = \langle a, b \rangle) \quad (19)$$

полно в z . Допустим, что (19) выполняется, когда x и y являются M -множествами. Тогда a и b являются M -множествами. Так как символ $\langle \rangle$ абсолютен, то он M -инвариантен, поэтому $z = \langle a, b \rangle$ есть M -множество.

$$M. \langle x_1, \dots, x_n \rangle = \langle x_1, \langle x_2, \dots, x_n \rangle \rangle.$$

С π_i^n поступаем подобно π_1 .

$$H. Do(x) = [\pi_2(y) | y \in x].$$

$$O. Ra(x) = [\pi_1(y) | y \in x].$$

$$П. Func(x) \leftrightarrow x \subset Ra(x) \times Do(x) \& \forall a \forall b (a \in x \& b \in x \& \pi_2(a) = \pi_2(b) \rightarrow a = b).$$

$$P. IFunc(x) \leftrightarrow Func(x) \& \forall a \forall b (a \in x \& b \in x \& \pi_1(a) = \pi_1(b) \rightarrow a = b).$$

$$C. (Func(x) \& y \in Do(x) \& \langle x'y, y \rangle \in x) \vee \vee (\neg (Func(x) \& y \in Do(x)) \& x'y = 0).$$

$$T. Trans(x) \leftrightarrow \forall y (y \in x \rightarrow y \subset x).$$

$$У. Ord(x) \leftrightarrow Trans(x) \& \forall y (y \in x \rightarrow Trans(y)).$$

$$Ф. \sigma < \tau \leftrightarrow \sigma \in \tau.$$

$$X. \sigma \leq \tau \leftrightarrow \sigma < \tau \vee \sigma = \tau.$$

Если F определяется следующим образом:

$$F(x_1, \dots, x_n) = \mu \sigma Q(\sigma, x_1, \dots, x_n),$$

где Q абсолютен, то F абсолютен. Определяющей аксиомой для F является

$$F(x_1, \dots, x_n) = y \leftrightarrow R(y, x_1, \dots, x_n),$$

где R определяется следующим образом:

$$R(y, x_1, \dots, x_n) \leftrightarrow Ord(y) \& Q(y, x_1, \dots, x_n) \& \forall z (z \in y \rightarrow \neg Q(z, x_1, \dots, x_n))$$

и, следовательно, абсолютен.

$$Ц. S(\sigma) = \sigma \cup \{\sigma\}.$$

$$Ч. \omega = \mu \sigma (\sigma \neq 0 \& \neg \exists x (Ord(x) \& \sigma = S(x))).$$

Полнота $Ord(x) \& \sigma = S(x)$ в x следует из импликации $\sigma = S(x) \rightarrow x \in \sigma$.

$$Ш. 1 = S(0), 2 = S(1), \dots$$

Теперь докажем, что если F определяется трансфинитной индукцией в терминах абсолютного функционального символа, то F абсолютен. Как обычно, параметры опускаем. Итак, пусть F определяется следующим образом:

$$F(\sigma) = G(\sigma, [\langle F(\tau), \tau \rangle \mid \tau < \sigma]),$$

где G абсолютен. Положим

$$H(\sigma) = [\langle F(\tau), \tau \rangle \mid \tau < \sigma].$$

Тогда F может быть определен следующим образом: $F(\sigma) = H(S(\sigma)) \cdot \sigma$, поэтому достаточно показать, что H абсолютен. Мы можем определить H следующим образом:

$$H(x) = y \leftrightarrow Q(y, x),$$

где Q определяется так:

$$Q(y, x) \leftrightarrow (\text{Ord}(x) \& \text{Func}(y) \& \text{Do}(y) = x \& \\ \& \forall z (z \in x \rightarrow y'z = G(z, [\langle y'w, w \rangle \mid w \in z]))) \\ \vee (\neg \text{Ord}(x) \& y = 0).$$

Тогда Q абсолютен, значит, и H абсолютен.

$$\text{Щ. } \text{Max}(x) = \pi_1(x) \cup \pi_2(x).$$

$$\text{Э. } \text{MP}(x) = \langle \pi_1(\text{MP}(x)), \pi_2(\text{MP}(x)) \rangle \& \\ \& \pi_1(\text{MP}(x)) = \mu\tau (\exists\rho (\rho \in \mu\sigma (\neg(\sigma \times \sigma \subset x)) \& \langle \tau, \rho \rangle \notin x)) \& \\ \& \pi_2(\text{MP}(x)) = \mu\rho (\langle \pi_1(\text{MP}(x)), \rho \rangle \notin x).$$

$$\text{А'. } K(\sigma) = \text{MP}(\text{Ra}([\langle K(\tau), \tau \rangle \mid \tau < \sigma])).$$

Будем говорить, что M *супертранзитивно*, если оно транзитивно и $\subset$ полно для M , т. е.

$$\vdash M(y) \& x \subset y \rightarrow M(x).$$

Теперь допустим, что M супертранзитивно, и докажем, что следующие нелогические символы абсолютны.

$$\text{Б'. } P(x) = [y \mid y \subset x].$$

$$\text{В'. } \text{Sm}(x, y) \leftrightarrow \exists f (\text{IFunc}(f) \& x = \text{Do}(f) \& y = \text{Ra}(f)).$$

Для полноты мы должны показать, что

$$M(x) \& M(y) \& \text{IFunc}(f) \& x = \text{Do}(f) \& y = \text{Ra}(f) \rightarrow M(f).$$

Так как $\times$ абсолютно, а значит, M -инвариантно, то из посылок следует, что $M(y \times x)$. Так как из них также следует, что $f \subset y \times x$, мы имеем $M(f)$ в силу супертранзитивности M .

$$\Gamma'. \text{CF}(f, x) \leftrightarrow \text{Func}(f) \& \text{Do}(f) = P(x) - \{0\} \& \\ \& \forall y (y \in \text{Do}(f) \rightarrow f'y \in y).$$

Заметим также, что CF полно. Для этого заметим, что

$$\text{CF}(f, x) \rightarrow f \subset x \times P(x),$$

и далее поступаем, как раньше.

Оставшиеся нелогические символы связаны с кардиналами. Поэтому мы будем предполагать, что M — некоторая супертранзитивная интерпретация теории ZFC.

$$\text{Д'. } \text{Card}(x) = \mu\sigma (\text{Sm}(\sigma, x)).$$

$$\text{Е'. } \text{Cd}(x) \leftrightarrow x = \text{Card}(x).$$

$$\text{Ж'. } \text{InfCd}(x) \leftrightarrow \text{Cd}(x) \& x \neq \omega.$$

$$\text{З'. } 2^\sigma = \text{Card}(P(\sigma)).$$

$$\text{И'. } \aleph(\sigma) = \mu\tau (\text{InfCd}(\tau) \& \tau \neq \text{Ra}([\langle \aleph(\rho), \rho \rangle \mid \rho < \sigma])).$$

9.6. Конструктивные множества

Мы собираемся построить транзитивную $\in$ -интерпретацию L теории ZF в теории ZF. Мы будем делать это, сопоставляя каждому ординалу некоторое множество; так построенные множества будут называться L -множествами. Элементами каждого L -множества будут более ранние L -множества (т. е. L -множества, сопоставленные меньшим ординалам); это обеспечит транзитивность интерпретации L . Отсюда, в частности, будет следовать, что выполняются интерпретации аксиомы объемности и аксиомы регулярности.

Так как остальные аксиомы являются аксиомами существования, дальнейшие проблемы будут состоять лишь в том, чтобы доказать существование достаточного числа L -множеств. В частности, мы хотим обеспечить, чтобы существовали достаточно большие L -множества. Чтобы достичь этого, мы будем определенным ординалам в качестве L -множества сопоставлять множество всех более ранних L -множеств. Более того, будут существовать произвольно большие ординалы σ , для которых это будет сделано. Отсюда будет следовать, что каждое множество L -множеств будет включаться в некоторое L -множество.

Далее, мы должны быть уверены, что существует достаточное число малых L -множеств, т. е. если a есть L -множество, то достаточное число подмножеств множества a является L -множествами. Аксиомы подмножеств требуют, чтобы для каждого Q множество всех x в a таких, что $Q_L(x)$, было L -множеством (и аналогично в случае параметров). Чтобы достичь этого, мы многократно применяем некоторые определенные операции к L -множествам, уже полученным, и множества, получающиеся в результате этого, добавляем к L -множествам. Основания для точного выбора таких операций будут выявлены в ходе доказательства, сейчас мы дадим только одну идею, откуда эти операции появляются.

Мы намерены доказать индукцией по предикатным символам, что все требуемые множества являются L -множествами. Если Q определен в терминах R , то R может иметь больше аргументов, чем Q . Следовательно, неудобно пытаться иметь дело только с унарными предикатными символами. Поэтому мы будем вынуждены доказывать, что если a есть L -множество, то множество n -ок $\langle x_1, \dots, x_n \rangle$ таких, что $x_1, \dots, x_n \in a$ и $Q_L(x_1, \dots, x_n)$, есть L -множество. По этой причине мы должны иметь возможность образовывать упорядоченные n -ки. Так как они образуются с помощью повторных построений неупорядоченных пар, то одной из наших операций будет операция образования неупорядоченных пар.

Допустим, мы рассматриваем наиболее трудный шаг в индукции, а именно, когда Q определяется так: $Q(x) \leftrightarrow \exists y R(y, x)$. (Для простоты берем здесь предикат Q унарным.) Тогда

$$Q_L(x) \leftrightarrow \exists y (L(y) \& R_L(y, x))$$

для L -множества x . Таким образом, каждое x такое, что $Q_L(x)$, есть второй элемент в упорядоченной паре $\langle y, x \rangle$ такой, что $R_L(y, x)$. Это наводит на мысль, что множество $\{x \mid x \in a \& Q_L(x)\}$ может быть получено как область определения множества $[\langle y, x \rangle \mid y, x \in b \& R_L(y, x)]$. Нет никакой трудности в выборе операций так, чтобы область определения L -множества была L -множеством; вопрос состоит только в том, как найти это множество b . Мы хотим знать, что b содержит a и что для каждого x в a , если существует L -множество y такое, что $R_L(y, x)$, то такое

L -множество y существует также и в b . Применяя аксиомы замены, мы можем легко построить множество b L -множеств с таким свойством; затем мы можем увеличить b до L -множества.

Определим бинарные функциональные символы $\mathfrak{F}_i$ для $i=1, \dots, 9$ следующим образом:

$$\begin{aligned}\mathfrak{F}_1(x, y) &= [\langle a, b \rangle \mid \langle a, b \rangle \in x \& a \in b], \\ \mathfrak{F}_2(x, y) &= [\langle a, a \rangle \mid \langle a, a \rangle \in x], \\ \mathfrak{F}_3(x, y) &= [\langle a, b \rangle \mid \langle a, b \rangle \in x \& a \in y], \\ \mathfrak{F}_4(x, y) &= [\langle a, b \rangle \mid \langle a, b \rangle \in x \& b \in y], \\ \mathfrak{F}_5(x, y) &= [\langle a, b \rangle \mid \langle a, b \rangle \in x \& \langle b, a \rangle \in y], \\ \mathfrak{F}_6(x, y) &= [\langle a, b, c \rangle \mid \langle a, b, c \rangle \in x \& \langle b, a, c \rangle \in y], \\ \mathfrak{F}_7(x, y) &= [\langle a, b, c \rangle \mid \langle a, b, c \rangle \in x \& \langle c, a, b \rangle \in y], \\ \mathfrak{F}_8(x, y) &= x - y, \\ \mathfrak{F}_9(x, y) &= x \cap \text{Do}(y).\end{aligned}$$

(Аргумент y включен в $\mathfrak{F}_1$ и $\mathfrak{F}_2$ для того, чтобы сделать все операции бинарными.) Заметим, что $\mathfrak{F}_i(x, y) \subset x$ для $i=1, \dots, 9$.

Определим также

$$\begin{aligned}J_0(\sigma) &= \pi_1(K(\sigma)), \\ J_1(\sigma) &= \pi_1(K(\pi_2(K(\sigma)))), \\ J_2(\sigma) &= \pi_2(K(\pi_2(K(\sigma)))).\end{aligned}$$

Тогда для любых σ_0, σ_1 и σ_2 существует σ такое, что $J_i(\sigma) = \sigma_i$ для $i=0, 1, 2$. По (21) и (22) из § 9.3 получаем

$$J_0(\sigma) \neq 0 \rightarrow J_1(\sigma) < \sigma \& J_2(\sigma) < \sigma. \quad (1)$$

Теперь определим функциональный символ C трансфинитной индукцией следующим образом:

$$C(\sigma) = \begin{cases} [C(\tau) \mid \tau < \sigma], & \text{если } J_0(\sigma) = 0, \\ \mathfrak{F}_i(C(J_1(\sigma)), C(J_2(\sigma))), & \text{если } J_0(\sigma) = i, i=1, \dots, 9, \\ \{C(J_1(\sigma)), C(J_2(\sigma))\}, & \text{если } 9 < J_0(\sigma). \end{cases}$$

Нам нужно условие (1), чтобы увидеть, что это действительно определение трансфинитной индукцией. Положим также

$$C^*(\sigma) = [C(\tau) \mid \tau < \sigma].$$

Определим

$$L(x) \leftrightarrow \exists \sigma (x = C(\sigma)).$$

Множество называется *конструктивным*, если оно есть L -множество. Если x конструктивно, то первый ординал σ такой, что $x = C(\sigma)$, называется *порядком* множества x и обозначается через $\text{Od}(x)$.

Докажем теперь, что конструктивные множества обладают требуемыми свойствами.

Лемма 1. Если x конструктивно и $y \in x$, то y конструктивно и $\text{Od}(y) < \text{Od}(x)$.

Доказательство. Применяем трансфинитную индукцию по $\sigma = \text{Od}(x)$. Если $J_0(\sigma) = 0$, то

$$x = C(\sigma) = C^*(\sigma).$$

Отсюда $y = C(\tau)$ для некоторого $\tau < \sigma$, поэтому $\text{Od}(y) \leq \tau < \sigma$. Если $J_0(\sigma) = i$ ($i = 1, \dots, 9$), то $x = \mathfrak{F}_i(C(J_1(\sigma)), C(J_2(\sigma))) \subset C(J_1(\sigma))$. Так как $J_1(\sigma) < \sigma$ по (1), то индуктивное предположение показывает, что y конструктивно и $\text{Od}(y) < J_1(\sigma) < \sigma$. Если $9 < J_0(\sigma)$, то $y = C(J_i(\sigma))$ для $i = 1$ или $i = 2$. В любом случае y конструктивно и $\text{Od}(y) \leq J_i(\sigma) < \sigma$.

Лемма 2. Если каждый элемент множества x конструктивен, то x содержится в некотором конструктивном множестве.

Доказательство. Пусть σ — ординал, больший каждого ординала в $[\text{Od}(y) \mid y \in x]$; выберем τ так, чтобы $K(\tau) = \langle 0, \sigma \rangle$. По (21) из § 9.3 имеем $\sigma \leq \tau$. Отсюда следует, что

$$x \subset C^*(\sigma) \subset C^*(\tau) = C(\tau).$$

Имеем

$$L(x) \& L(y) \rightarrow L(\mathfrak{F}_i(x, y)), \quad i = 1, \dots, 9. \quad (2)$$

Действительно, пусть $x = C(\sigma)$, $y = C(\tau)$; выберем ρ так, чтобы $J_0(\rho) = i$, $J_1(\rho) = \sigma$, $J_2(\rho) = \tau$. Тогда $C(\rho) = \mathfrak{F}_i(x, y)$. Аналогично

$$L(x) \& L(y) \rightarrow L(\langle x, y \rangle), \quad (3)$$

откуда следует, что

$$L(x_1) \& \dots \& L(x_n) \rightarrow L(\langle x_1, \dots, x_n \rangle). \quad (4)$$

Далее,

$$L(x) \& L(y) \rightarrow L(x \times y). \quad (5)$$

Действительно, по (4), лемме 1 и лемме 2 существует конструктивное множество z такое, что $x \times y \subset z$. Тогда

$$x \times y = \mathfrak{F}_4(\mathfrak{F}_3(z, x), y),$$

поэтому $x \times y$ конструктивно по (2).

Определим

$$x \times_1 y = [\langle a, b, c \rangle \mid b \in x \& \langle a, c \rangle \in y],$$

$$x \times_2 y = [\langle a, b, c \rangle \mid c \in x \& \langle a, b \rangle \in y].$$

Тогда

$$L(x) \& L(y) \rightarrow L(x \times_1 y) \& L(x \times_2 y). \quad (6)$$

Действительно, по (4), лемме 1 и лемме 2 существует конструктивное множество z такое, что $x \times_1 y \subset z$, тогда $x \times_1 y = \mathfrak{F}_6(z_1, x \times y)$. Доказательство для $x \times_2 y$ аналогичное, но использует $\mathfrak{F}_7$ вместо $\mathfrak{F}_6$.

Положим

$$\text{Cv}(x) = [\langle a, b \rangle \mid \langle b, a \rangle \in x].$$

Тогда

$$L(x) \rightarrow L(\text{Cv}(x)). \quad (7)$$

Действительно, если мы выберем конструктивное множество z такое, что $\text{Cv}(x) \subset z$, то $\text{Cv}(x) = \mathfrak{F}_5(z, x)$. Из (2) получаем

$$L(x) \& L(y) \rightarrow L(x - y). \quad (8)$$

Отсюда

$$L(x) \& L(y) \rightarrow L(x \cup y) \& L(x \cap y). \quad (9)$$

Действительно, по лемме 2 мы можем выбрать конструктивное множество z такое, что $x \cup y \subset z$, и тогда

$$x \cup y = z - ((z - x) - y) \quad \text{и} \quad x \cap y = x - (x - y).$$

Имеем также

$$L(x) \rightarrow L(\text{Do}(x)). \quad (10)$$

Прежде всего заметим, что если $a \in \text{Do}(x)$, то существует b такое, что $\langle a, b \rangle \in x$. Так как $a \in \{a\}$ & $\{a\} \in \langle a, b \rangle$, то отсюда по лемме 1 следует, что $L(a)$. Следовательно, по лемме 2 существует конструктивное множество z такое, что $\text{Do}(x) \subset z$; тогда $\text{Do}(x) = \mathfrak{F}_9(z, x)$.

Лемма 3. Пусть $1 \leq i \leq n$, $1 \leq j \leq n$. Если a и b конструктивны, то существует конструктивное множество c такое, что для всех $x_1, \dots, x_n$ из a

$$\langle x_i, x_i \rangle \in b \leftrightarrow \langle x_1, \dots, x_n \rangle \in c.$$

Доказательство. Вначале предполагаем, что $i < j$, и доказываем это индукцией по n . Сначала пусть $i > 1$. По индуктивному предположению существует конструктивное множество d такое, что для $x_1, \dots, x_n$ из a

$$\langle x_i, x_j \rangle \in b \leftrightarrow \langle x_2, \dots, x_n \rangle \in d.$$

Тогда для $x_1, \dots, x_n$ из a

$$\langle x_i, x_j \rangle \in b \leftrightarrow \langle x_1, \dots, x_n \rangle \in a \times d.$$

Положим $c = a \times d$ и, применяя (5), доказываем, что c конструктивно.

Пусть теперь $i = 1$ и $j > 2$. По индуктивному предположению существует конструктивное множество d такое, что для $x_1, x_3, \dots, x_n$ из a

$$\langle x_i, x_j \rangle \in b \leftrightarrow \langle x_1, x_3, \dots, x_n \rangle \in d.$$

Тогда для $x_1, \dots, x_n$ из a

$$\langle x_i, x_j \rangle \in b \leftrightarrow \langle x_1, \dots, x_n \rangle \in a \times_1 d.$$

Берем $c = a \times_1 d$, используя (6).

Наконец, пусть $i = 1, j = 2$. Тогда для $x_1, \dots, x_n$ из a

$$\langle x_i, x_j \rangle \in b \leftrightarrow \langle x_1, \dots, x_n \rangle \in a^{n-2} \times_2 b$$

(где $a^{n-2} = a \times \dots \times a$ с $n-2$ сомножителями). Берем $c = a^{n-2} \times_2 b$, применяя (5) и (6). (Конечно, если $n = 2$, то берем $c = b$.)

Теперь предположим, что $j < i$. По (7) и доказанному выше существует конструктивное множество c такое, что для $x_1, \dots, x_n$ из a

$$\langle x_j, x_i \rangle \in C_v(b) \leftrightarrow \langle x_1, \dots, x_n \rangle \in c.$$

Тогда

$$\langle x_i, x_j \rangle \in b \leftrightarrow \langle x_1, \dots, x_n \rangle \in c.$$

И наконец, пусть $i = j$. Тогда для $x_1, \dots, x_n$ из a

$$\langle x_i, x_j \rangle \in b \leftrightarrow x_i \in \text{Do}(\mathfrak{F}_2(b, b))$$

$$\leftrightarrow \langle x_1, \dots, x_n \rangle \in a^{i-1} \times \text{Do}(\mathfrak{F}_2(b, b)) \times a^{n-i}.$$

Лемма 4. Пусть Q — предикатный символ теории ZF. Для каждого конструктивного множества a существует конструктивное множество b такое, что для $x_1, \dots, x_n$ из a

$$\langle x_1, \dots, x_n \rangle \in b \leftrightarrow Q_L(x_1, \dots, x_n).$$

Доказательство. Используем индукцию по предикатным символам. Предположим, что

$$Q(x_1, \dots, x_n) \leftrightarrow x_i \in x_j$$

или

$$Q(x_1, \dots, x_n) \leftrightarrow x_i = x_j.$$

Тогда $Q_L(x_1, \dots, x_n) \leftrightarrow Q(x_1, \dots, x_n)$. Ввиду леммы 3 достаточно будет найти конструктивные множества c и d такие, что

$$\langle x, y \rangle \in c \leftrightarrow x \in y$$

и

$$\langle x, y \rangle \in d \leftrightarrow x = y$$

для x и y из a . Возьмем $c = \mathfrak{F}_1(a \times a, a)$, $d = \mathfrak{F}_2(a \times a, a)$.

Предположим, что Q определено следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow \neg R(x_1, \dots, x_n),$$

так что

$$Q_L(x_1, \dots, x_n) \leftrightarrow \neg R_L(x_1, \dots, x_n).$$

По индуктивному предположению существует конструктивное множество c такое, что для $x_1, \dots, x_n$ из a

$$\langle x_1, \dots, x_n \rangle \in c \leftrightarrow R_L(x_1, \dots, x_n).$$

Берем $b = a^n - c$.

Если Q определен следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow R_1(x_1, \dots, x_n) \vee R_2(x_1, \dots, x_n),$$

то мы берем множества c_1 и c_2 , соответствующие R_1 и R_2 , и полагаем $b = c_1 \cup c_2$.

Теперь предположим, что Q определяется так:

$$Q(x_1, \dots, x_n) \leftrightarrow \exists y R(y, x_1, \dots, x_n),$$

так что

$$Q_L(x_1, \dots, x_n) \leftrightarrow \exists y (L(y) \& R_L(y, x_1, \dots, x_n)).$$

Определим функциональный символ F следующим образом. Если $\exists y (L(y) \& R_L(y, x_1, \dots, x_n))$, то $F(x_1, \dots, x_n)$ — конструктивное множество y наименьшего порядка такое, что

$$R_L(y, x_1, \dots, x_n);$$

в противном случае $F(x_1, \dots, x_n) = C(0)$. Пусть

$$c = [F(x_1, \dots, x_n) \mid x_1 \in a \& \dots \& x_n \in a].$$

По лемме 2 существует конструктивное множество d такое, что $a \cup c \subset d$. По индуктивному предположению существует конструктивное множество e такое, что для $y, x_1, \dots, x_n$ из d

$$\langle y, x_1, \dots, x_n \rangle \in e \leftrightarrow R_L(y, x_1, \dots, x_n).$$

Заменяя e на $e \cap d^{n+1}$, можно предположить, что $e \subset d^{n+1}$. Тогда для $x_1, \dots, x_n$ из a

$$\begin{aligned} \langle x_1, \dots, x_n \rangle \in \text{Do}(e) &\leftrightarrow \exists y (y \in d \ \& \ \langle y, x_1, \dots, x_n \rangle \in e) \\ &\leftrightarrow \exists y (y \in d \ \& \ R_L(y, x_1, \dots, x_n)) \\ &\leftrightarrow \exists y (L(y) \ \& \ R_L(y, x_1, \dots, x_n)) \\ &\leftrightarrow Q_L(x_1, \dots, x_n). \end{aligned}$$

Поэтому мы можем взять $b = \text{Do}(e)$.

Теперь мы можем доказать, что L — интерпретация теории ZF в теории ZF. Ясно, что $\exists x L(x)$. По лемме 1 L транзитивно, поэтому по лемме 2 из § 9.5 интерпретации аксиомы объемности и аксиомы регулярности выполняются.

Чтобы доказать интерпретации аксиом подмножества, достаточно по лемме 3 из § 9.5 показать, что если $y, v_1, \dots, v_n$ конструктивны, то множество

$$[x \mid x \in y \ \& \ Q_L(x, v_1, \dots, v_n)] \quad (11)$$

конструктивно. По лемме 2 существует конструктивное множество, включающее y и содержащее элементы $v_1, \dots, v_n$. Поэтому по лемме 4 существует конструктивное множество z такое, что $x \in y$

$$\langle x, v_1, \dots, v_n \rangle \in z \leftrightarrow Q_L(x, v_1, \dots, v_n).$$

Заменяя z на $z \cap (y \times \{v_1\} \times \dots \times \{v_n\})$, имеем для всех x

$$x \in \text{Ra}(z) \leftrightarrow x \in y \ \& \ Q_L(x, v_1, \dots, v_n).$$

Следовательно, множество (11) есть $\text{Ra}(z) = \text{Do}(\text{Cv}(z))$ и поэтому оно конструктивно.

Чтобы доказать интерпретации аксиом замены, достаточно по лемме 4 из § 9.5 показать, что если F является L -инвариантным и $w, v_1, \dots, v_n$ конструктивны, то существует конструктивное множество z такое, что $F(x, v_1, \dots, v_n) \subset z$ для всех $x \in w$. Пусть $u = \text{Un}([F(x, v_1, \dots, v_n) \mid x \in w])$. По лемме 1 каждое множество из u конструктивно. Поэтому по лемме 2 существует конструктивное множество z такое, что $u \subset z$. Тогда для $x \in w$

$$F(x, v_1, \dots, v_n) \subset u \subset z.$$

Чтобы доказать интерпретацию аксиомы степени, достаточно по лемме 5 из § 9.5 показать, что если y конструктивно, то существует конструктивное множество, которое содержит множество $[x \mid L(x) \ \& \ x \subset y]$. Это следует из леммы 2.

Чтобы доказать интерпретацию аксиомы бесконечности, достаточно по лемме 6 из § 9.5 показать, что ω конструктивно. В действительности мы докажем, что каждый ординал конструктивен.

Прежде всего напомним, что мы доказали в теории ZF

$$\exists x (\text{Ord}(x) \ \& \ x \not\subseteq y).$$

При доказательстве *) не использовалась аксиома бесконечности, поэтому интерпретация этой формулы

$$L(y) \rightarrow \exists x (L(x) \ \& \ \text{Ord}_L(x) \ \& \ x \not\subseteq y)$$

доказуема. Далее, Ord абсолютно для L (так как наше доказательство абсолютности не требовало интерпретации аксиомы бесконечности). Поэтому

$$L(y) \rightarrow \exists x (L(x) \ \& \ \text{Ord}(x) \ \& \ x \not\subseteq y). \quad (12)$$

Теперь мы можем доказать $L(\sigma)$ трансфинитной индукцией по σ . Индуктивное предположение показывает, что каждый элемент из σ конструктивен, поэтому по лемме 2 существует конструктивное множество y такое, что $\sigma \subset y$. По (12) существует конструктивный ординал τ такой, что $\tau \not\subseteq y$. Имеем $\sigma \leq \tau$, поэтому $\sigma = \tau$ или $\sigma \in \tau$. Так как L транзитивно, то отсюда следует, что σ — конструктивное множество.

9.7. Аксиома конструктивности

Формула $\forall x L(x)$, которая утверждает, что каждое множество конструктивно, называется *аксиомой конструктивности*. Теория, полученная из теории ZF добавлением этой аксиомы, обозначается через ZFL.

Мы вовсе не намерены принимать аксиому конструктивности в качестве аксиомы теории множеств, так как нет причин верить, что она истинна. Однако она полезна при исследованиях непротиворечивости, как показывают следующие две теоремы Гёделя.

*) Можно взять $x = S(\text{Un}[z \mid \text{Ord}(z) \ \& \ z \in y])$. — Прим. ред.

Теорема 1. Если теория ZF непротиворечива, то теория ZFL также непротиворечива.

Теорема 2. Аксиома выбора и обобщенная гипотеза континуума являются теоремами теории ZFL.

Отсюда следует, что если теория ZF непротиворечива, то ни отрицание аксиомы выбора, ни отрицание обобщенной гипотезы континуума не доказуемы в теории ZF (и даже в теории ZFC).

Чтобы доказать теорему 1, мы покажем, что L есть $\in$ -интерпретация теории ZFL в теории ZF. Так как мы уже показали, что L есть интерпретация теории ZF, то необходимо только доказать интерпретацию аксиомы конструктивности.

Вначале покажем, что C абсолютно (для всех транзитивных $\in$ -интерпретаций теории ZF). Абсолютность $\mathfrak{F}_i$ следует из результатов § 9.5. Чтобы увидеть это, лучше всего переформулировать определения, используя π_i^n . Так, например,

$$\begin{aligned}\mathfrak{F}_2(x, y) &= [z \mid z \in x \ \& \ z = \langle \pi_1(z), \pi_1(z) \rangle], \\ \mathfrak{F}_6(x, y) &= [z \mid z \in x \ \& \ z = \langle \pi_1^3(z), \pi_2^3(z), \pi_3^3(z) \rangle \ \& \\ &\quad \& \langle \pi_2^3(z), \pi_1^3(z), \pi_3^3(z) \rangle \in y].\end{aligned}$$

Абсолютность J_i получается сразу. Итак, C определяется следующим образом:

$$C(\sigma) = G(\sigma, [\langle C(\tau), \tau \rangle \mid \tau < \sigma])$$

для определенного G ; мы должны показать, что G абсолютно. Мы можем определить G так:

$$G(\sigma, f) = y \leftrightarrow R(y, \sigma, f),$$

где R определяется следующей формулой:

$$\begin{aligned}R(y, \sigma, f) &\leftrightarrow (J_0(\sigma) = 0 \ \& \ y = Ra(f)) \vee \\ &\quad \vee (J_0(\sigma) = 1 \ \& \ y = \mathfrak{F}_1(f'J_1(\sigma), f'J_2(\sigma)) \vee \dots \\ &\quad \dots \vee (9 < J_0(\sigma) \ \& \ y = \{f'J_1(\sigma), f'J_2(\sigma)\})).\end{aligned}$$

Тогда R абсолютно, поэтому и G абсолютно.

Теперь докажем, что L абсолютно для L (но не для всех транзитивных $\in$ -интерпретаций). Имеем

$$L(x) \leftrightarrow \exists y (\text{Ord}(y) \ \& \ x = C(y)).$$

Поэтому достаточно показать, что $\text{Ord}(y) \ \& \ x = C(y)$ полно

в y для L . Но это следует из того, что каждый ординал конструктивен.

L -интерпретацией аксиомы конструктивности является

$$\forall x (L(x) \rightarrow L_L(x)). \quad (1)$$

Абсолютность L для L означает, что

$$L(x) \rightarrow (L(x) \leftrightarrow L_L(x));$$

а из этого, очевидно, следует (1).

Теперь обратимся к доказательству теоремы 2. Доказательство аксиомы выбора в теории ZFL совершенно простое. Определим

$$\text{Ch}(x) = C(\mu\sigma (x \neq 0 \rightarrow C(\sigma) \in x)).$$

Аксиома конструктивности показывает, что функция Ch корректно определена и

$$x \neq 0 \rightarrow \text{Ch}(x) \in x.$$

Из этого следует, что функция выбора на x определяется следующим образом:

$$[\langle \text{Ch}(y), y \rangle \mid y \in P(x) - \{0\}].$$

Чтобы доказать обобщенную гипотезу континуума, вначале установим соотношение между кардиналами и конструктивными множествами, показав, что

$$\text{Card}(C^*(\aleph_\sigma)) = \aleph_\sigma. \quad (2)$$

Так как $[\langle C(\tau), \tau \rangle \mid \tau < \aleph_\sigma]$ является сюръективным отображением из $\aleph_\sigma$ на $C^*(\aleph_\sigma)$, то $\text{Card}(C^*(\aleph_\sigma)) \leq \text{Card}(\aleph_\sigma) = \aleph_\sigma$. Чтобы доказать обратное неравенство, достаточно определить инъективное отображение $\aleph_\sigma$ на $C^*(\aleph_\sigma)$. Пусть $F(\tau)$ будет (единственный) ординал такой, что $K(F(\tau)) = \langle 0, \tau \rangle$; пусть $f'\tau = C(F(\tau))$ для $\tau \in \aleph_\sigma$. Если $\tau < \aleph_\sigma$, то $\text{Max}(K(F(\tau))) = \tau < \aleph_\sigma = \text{Max}(K(\aleph_\sigma))$ по (24) из § 9.4, поэтому $F(\tau) < \aleph_\sigma$ по (20) из § 9.3. Таким образом, f — отображение из $\aleph_\sigma$ в $C^*(\aleph_\sigma)$. Предположим, что $\tau, \tau' \in \aleph_\sigma$ и $\tau \neq \tau'$. Тогда $F(\tau) \neq F(\tau')$. Если $F(\tau) < F(\tau')$, то

$$f'\tau = C(F(\tau)) \in C^*(F(\tau')) = C(F(\tau')) = f'\tau'.$$

Аналогично, если $F(\tau') < F(\tau)$, то $f'\tau' \in f'\tau$. В любом случае $f'\tau \neq f'\tau'$ по (4) из § 9.3. Следовательно, f инъективно.

По (29) из § 9.4 и (2)

$$\text{Card}(P(C^*(\aleph_\sigma))) = 2^{\aleph_\sigma}. \quad (3)$$

Мы докажем, что

$$P(C^*(\aleph_\sigma)) \subset C^*(\aleph_{S(\sigma)}). \quad (4)$$

Из (4), (3) и (2) имеем

$$2^{\aleph_\sigma} \leq \aleph_{S(\sigma)}.$$

Из этого и (33) из § 9.4 мы получаем обобщенную гипотезу континуума.

Доказательство (4) основано на следующей лемме, являющейся формальным аналогом теоремы о мощности.

Лемма. Пусть T — теория, полученная из теории ZFL добавлением константы B и аксиомы $\text{Trans}(B)$. Тогда в подходящем консервативном расширении T' теории T мы можем определить константу A и доказать

$$B \subset A,$$

$$\text{Trans}(A),$$

$$\text{Card}(B) \leq \aleph_\sigma \rightarrow \text{Card}(A) \leq \aleph_\sigma$$

и $A \leftrightarrow A_A$ для каждой замкнутой формулы A теории ZFL.

Доказательство. Чтобы построить T' из T , добавим константу D и аксиомы

$$B \subset D, \quad (5)$$

$$\text{Card}(B) \leq \aleph_\sigma \rightarrow \text{Card}(D) \leq \aleph_\sigma \quad (6)$$

и

$$x_1, \dots, x_n \in D \rightarrow F(x_1, \dots, x_n) \in D \quad (7)$$

для каждого функционального символа F теории ZFL. Сначала докажем, что T' является консервативным расширением теории T . Предположим, что A — формула теории T , доказуемая в теории T' . Пусть T_1 получается из теории T добавлением константы D . По теореме редукции $\vdash_{T_1} B \rightarrow A$, где B — конъюнкция замыканий аксиом (5), (6) и (7). По теореме о константах и правилу $\exists$ -введения $\vdash_T \exists x B' \rightarrow A$, где B' — результат замены D в B на новую переменную x . Но $\vdash_T \exists x B'$ по теореме замыкания; следовательно, $\vdash_T A$.

Теперь покажем, что

$$\vdash_{T'} x_1, \dots, x_n \in D \rightarrow (Q(x_1, \dots, x_n) \leftrightarrow Q_D(x_1, \dots, x_n))$$

для каждого предикатного символа Q теории ZFL. Используем индукцию по предикатным символам. Если Q определено следующим образом: $Q(x_1, \dots, x_n) \leftrightarrow x_i \in x_j$ или $Q(x_1, \dots, x_n) \leftrightarrow x_i = x_j$, то Q_D есть Q и результат очевиден. Если Q определяется как отрицание или дизъюнкция, то результат следует из индуктивного предположения. Теперь предположим, что Q определяется следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow \exists y R(y, x_1, \dots, x_n).$$

По индуктивному предположению

$$x_1, \dots, x_n, y \in D \rightarrow (R(y, x_1, \dots, x_n) \leftrightarrow R_D(y, x_1, \dots, x_n));$$

таким образом, при условии, что $x_1, \dots, x_n \in D$, имеем

$$\begin{aligned} \exists y (y \in D \& R(y, x_1, \dots, x_n) \leftrightarrow \\ \leftrightarrow \exists y (y \in D \& R_D(y, x_1, \dots, x_n)). \end{aligned}$$

Правая часть есть $Q_D(x_1, \dots, x_n)$; таким образом, нам нужно лишь доказать, что левая часть эквивалентна $Q(x_1, \dots, x_n)$. Для этого достаточно доказать (при условии, что $x_1, \dots, x_n \in D$)

$$\exists y R(y, x_1, \dots, x_n) \rightarrow \exists y (y \in D \& R(y, x_1, \dots, x_n)).$$

Определим $F(x_1, \dots, x_n)$ как множество y наименьшего порядка такое, что $R(y, x_1, \dots, x_n)$, если такое y существует, и 0 в противном случае. Если

$$\exists y R(y, x_1, \dots, x_n),$$

то

$$R(F(x_1, \dots, x_n), x_1, \dots, x_n).$$

Но $F(x_1, \dots, x_n) \in D$ по (7), следовательно, $\exists y (y \in D \& R(y, x_1, \dots, x_n))$.

Пусть теперь A — замкнутая формула теории ZFL, определим 0-местный предикатный символ Q с помощью $Q \leftrightarrow A$. Как и раньше, $\vdash Q \leftrightarrow Q_D$, поэтому $\vdash A \leftrightarrow A_D$. Из этого мы заключаем, что D есть $\in$ -интерпретация теории ZFL в T' . Действительно, пусть B — некоторая аксиома теории ZFL и A — замыкание формулы B . Тогда A_D — замыкание формулы $B^{(D)}$. Мы последовательно приходим к заключению, что B, A, A_D и $B^{(D)}$ доказуемы в теории T' .

В частности, интерпретация аксиомы объемности относительно D доказуема. Далее, $y \in x \rightarrow \text{Od}(y) < \text{Od}(x)$ по

лемме 1 из § 9.6; Od — ординальный функциональный символ такой, что $\text{Set}_x(\text{Od}(x) \leq \sigma)$, так как $\text{Od}(x) \leq \sigma \rightarrow x \in C^*(S(\sigma))$. Поэтому мы можем применить результаты из § 9.5. Определим

$$F(y) = [F(x) \mid x \in D \ \& \ x \in y]$$

и

$$A = [F(x) \mid x \in D].$$

Мы приходим к выводу, что A транзитивно и F — изоморфизм $\in$ -интерпретаций D и A . Отсюда следует, что $\text{Card}(A) = \text{Card}(D)$, поэтому в силу (6) получаем

$$\text{Card}(B) \leq \aleph_\sigma \rightarrow \text{Card}(A) \leq \aleph_\sigma.$$

Используя лемму 1 из § 9.5 (примененную к 0-местным предикатным символам), покажем, как и раньше, что $\vdash A_D \leftrightarrow \leftrightarrow A_A$ для произвольной замкнутой формулы A теории ZFL. Следовательно, $\vdash A \leftrightarrow A_A$ для такой формулы A .

Осталось доказать, что $B \subset A$. Для этого достаточно показать, что

$$x \in B \rightarrow F(x) = x.$$

Докажем это индукцией по $\text{Od}(x)$. Пусть $x \in B$. Если $y \in x$, то $\text{Od}(y) < \text{Od}(x)$ и $y \in B$ ввиду транзитивности B . Следовательно, по индуктивному предположению и включению $B \subset D$ имеем

$$F(x) = [F(y) \mid y \in D \ \& \ y \in x] = [y \mid y \in x] = x.$$

В обозначениях доказываемой леммы A есть $\in$ -интерпретация теории ZFL в теории T' ; доказательство этого факта аналогично соответствующему доказательству для D . Определение

$$\text{Od}(x) = \mu\sigma (x = C(\sigma))$$

вместе с абсолютностью C показывает, что Od абсолютно для A . (Конечно, аксиома конструктивности нужна для выполнения определяющей аксиомы для Od .) Отсюда следует, что Od будет A -инвариантным. Из этого и транзитивности A получаем

$$\begin{aligned} x \in A \rightarrow \text{Od}(x) \subset A \rightarrow \\ \rightarrow \text{Card}(\text{Od}(x)) \leq \text{Card}(A). \end{aligned}$$

Используя это вместе с $B \subset A$, $\text{Card}(B) \leq \aleph_\sigma \rightarrow \text{Card}(A) \leq \aleph_\sigma$, получаем

$$\text{Card}(B) \leq \aleph_\sigma \ \& \ x \in B \rightarrow \text{Card}(\text{Od}(x)) \leq \aleph_\sigma.$$

Из правой части следует, что $x \in C^*(\aleph_{S(\sigma)})$. Действительно, если $x \notin C^*(\aleph_{S(\sigma)})$, то $\aleph_{S(\sigma)} \leq \text{Od}(x)$, поэтому

$$\aleph_\sigma < \aleph_{S(\sigma)} = \text{Card}(\aleph_{S(\sigma)}) \leq \text{Card}(\text{Od}(x)).$$

Поэтому формула

$$\text{Card}(B) \leq \aleph_\sigma \rightarrow B \subset C^*(\aleph_{S(\sigma)})$$

доказуема в теории T' . По лемме эта формула доказуема в теории T . Следовательно, по теореме дедукции и теореме о константах получаем, что формула

$$\text{Trans}(b) \ \& \ \text{Card}(b) \leq \aleph_\sigma \rightarrow b \subset C^*(\aleph_{S(\sigma)}) \quad (8)$$

доказуема в теории ZFL.

Теперь мы можем доказать (4). Пусть $a \in P(C^*(\aleph_\sigma))$, т. е. $a \in C^*(\aleph_\sigma)$. Пусть $b = C^*(\aleph_\sigma) \cup \{a\}$. По лемме 1 из § 9.6 $C^*(\aleph_\sigma)$ транзитивно. Из этого и из того, что $a \in C^*(\aleph_\sigma)$, мы видим, что b транзитивно. Также

$$\text{Card}(b) \leq \text{Card}(C^*(\aleph_\sigma)) + \text{Card}(\{a\}) = \aleph_\sigma + 1 = \aleph_\sigma$$

по (2). Следовательно, $b \subset C^*(\aleph_{S(\sigma)})$ по (8); таким образом,

$$a \in C^*(\aleph_{S(\sigma)}).$$

Это завершает доказательство теоремы 2.

Закончим этот параграф применением доказанной леммы к выводу формального варианта теоремы Левенгейма — Скулема. Пусть ZFL_A — теория, полученная из теории ZFL добавлением константы A и аксиом

$$\begin{aligned} &\text{Trans}(A), \\ &\text{Card}(A) \leq \aleph_0 \end{aligned}$$

и $A \leftrightarrow A_A$ для каждой замкнутой формулы A теории ZFL. Докажем, что теория ZFL_A является консервативным расширением теории ZFL.

Для доказательства возьмем теории T и T' , как в лемме, и пусть T'' получается из теории T' добавлением аксиомы $B=0$. Тогда все аксиомы теории ZFL_A будут доказуемы в теории T'' , поэтому достаточно будет показать, что теория T'' является консервативным расширением теории ZFL.

Предположим, что A — некоторая формула теории ZFL, доказуемая в теории T'' . По теореме дедукции $B=0 \rightarrow A$ доказуема в теории T' и, следовательно, в теории T . По теореме дедукции и теореме о константах формула $\text{Trans}(b) \& b=0 \rightarrow A$ доказуема в теории ZFL. Подставляя 0 вместо b , видим, что A доказуема в теории ZFL.

Мы можем показать, как и раньше, что A есть $\in$ -интерпретация теории ZFL в теории ZFL_A . Таким образом, мы имеем счетную транзитивную $\in$ -интерпретацию теории ZFL в ее консервативном расширении ZFL_A .

9.8. Вынуждение

Теперь мы опишем один метод построения интерпретаций теории ZFC, которые будут применяться для доказательства независимости аксиомы выбора и гипотезы континуума *).

Мы будем строить расширение теории ZFL, в котором будет даваться эта интерпретация. Предположим, что фиксирована константа CD теории ZFL такая, что $\vdash_{\text{ZFL}} 0 \in \text{CD}$. (Фактический выбор CD будет зависеть от приложения.) Элементы множества CD называются *условиями*. Мы считаем, что областью изменения p , q и r являются условия. Если $p \subset q$, то мы говорим, что условие q есть *расширение* условия p .

Каждому условию будет соответствовать некоторое (частичное) описание интерпретации I . Кроме того, описание, соответствующее любому расширению условия p , будет содержать описание, соответствующее условию p . Однако не все эти описания будут корректными описаниями интерпретации I . Мы будем отличать некоторые условия, которые будем называть *корректными* условиями, и строить I , соединяя описания, соответствующие корректным условиям.

Чтобы обеспечить существование по крайней мере одного корректного условия, потребуем, чтобы 0 было корректным условием. Чтобы обеспечить непротиворечивость описаний, соответствующих двум корректным условиям, мы потребуем, чтобы условие $p \cup q$ было корректным, если только условия p и q корректны.

*) Приведенное здесь доказательство по существу есть первоначальное доказательство Коэна, хотя в нем используются некоторые упрощения, найденные Феферманом, Скоттом и Соловеем.

Имеется еще третье требование, которое выражает намерение обеспечить, насколько это возможно, чтобы каждое множество содержало некоторое корректное условие. Ситуация, в которой это оказывается невозможным, состоит в следующем: мы выбрали p в качестве корректного условия, но не существует условия q в множестве x такого, что $p \cup q$ является условием. Это наводит на мысль, что это требование должно состоять в следующем: для каждого множества x существует корректное условие p такое, что либо p находится в x , либо никакое расширение условия p не находится в x .

Строим теорию ZFL_{Cor} из теории ZFL, добавляя унарный предикатный символ Cor и четыре новые нелогические аксиомы:

$$\text{Cor}_1. \text{Cor}(p) \rightarrow p \in \text{CD}.$$

$$\text{Cor}_2. \text{Cor}(0).$$

$$\text{Cor}_3. \text{Cor}(p) \& \text{Cor}(q) \rightarrow \text{Cor}(p \cup q).$$

$$\text{Cor}_4. \exists p (\text{Cor}(p) \& (p \in x \vee \forall q (p \subset q \& q \in \text{CD} \rightarrow q \notin x))).$$

Заметим, что мы не добавили аксиом подмножеств и замены, содержащих новый символ Cor, поэтому мы не можем применять наши результаты об образовании множеств к формулам, содержащим этот символ.

Наша первая задача — доказать, что если теория ZF непротиворечива, то теория ZFL_{Cor} непротиворечива. Из непротиворечивости теории ZF следует непротиворечивость теории ZFL и, следовательно, ее консервативного расширения ZFL_A . Более того, A есть интерпретация теории ZFL в теории ZFL_A . Мы расширим эту интерпретацию до интерпретации языка $L(\text{ZFL}_{\text{Cor}})$, определяя Cor_A в теории ZFL_A . Затем мы докажем интерпретации всех новых аксиом, показав тем самым, что мы имеем интерпретацию теории ZFL_{Cor} в теории ZFL_A . Это даст нам требуемый результат.

Пусть область изменения p , q и r в теории ZFL_A есть CD_A . Подмножество c множества CD_A будет называться *генерическим*, если оно удовлетворяет следующим трем требованиям:

$$0 \in c,$$

$$p \in c \& q \in c \rightarrow p \cup q \in c,$$

$$\forall x (x \in A \rightarrow \exists p (p \in c \&$$

$$\& (p \in x \vee \forall q (p \subset q \& q \in \text{CD}_A \rightarrow q \notin x))).$$

Вначале докажем, что генерическое множество существует. Пусть все элементы A расположены в последовательности $x_0, x_1, \dots$. Определим индуктивно последовательность $p_0, p_1, \dots$ элементов множества CD_A . Пусть $p_0 = 0$. Теперь предположим, что p_n уже выбрано. Если существует q такое, что $p_n \subset q$ и $q \in x_n$, то пусть p_{n+1} будет таким q . (Чтобы точно указать q , мы можем считать, что это q имеет наименьший порядок.) Если такого q не существует, то пусть $p_{n+1} = p_n$. Ясно, что множество $[p_n | n \in \omega]$ генерическое.

Определим константу G с помощью аксиомы, утверждающей, что G — генерическое множество, имеющее наименьший порядок. Затем определим

$$\text{Cог}_A(p) \leftrightarrow p \in G.$$

Так как $CD_A \in A$ и A транзитивно, то каждый элемент множества CD_A находится в A . Используя это и абсолютность $0, \cup$ и $\subset$, находим, что интерпретации $\text{Cог}_1 - \text{Cог}_4$ эквивалентны формулам

$$\text{Cог}_A(p) \rightarrow p \in CD_A,$$

$$\text{Cог}_A(0),$$

$$\text{Cог}_A(p) \& \text{Cог}_A(q) \rightarrow \text{Cог}_A(p \cup q),$$

$$x \in A \rightarrow \exists p (\text{Cог}_A(p) \& \\ \& (p \in x \vee \forall q (p \subset q \& q \in CD_A \rightarrow q \notin x))).$$

А эти формулы следуют из того, что G генерическое.

Теперь возвратимся к построению нашей интерпретации теории ZFC в теории $ZFL_{\text{Cог}}$. Вначале мы должны точно определить описание I , соответствующее условию p . Мы определим, что означает для каждого предикатного символа Q теории ZFC выражение: p *вынуждает* $Q(x_1, \dots, x_n)$. Тогда описание, соответствующее условию p , будет по определению утверждением, что $Q_I(x_1, \dots, x_n)$ истинно, в случае, когда p вынуждает $Q(x_1, \dots, x_n)$.

Сначала рассмотрим случай, когда Q есть $\in$. Мы хотели бы иметь возможность строить множество y так, чтобы для каждого условия p множеством всех таких x , что p вынуждает $x \in y$, было бы заранее определенное множество z_p . Мы можем сделать это, взяв в качестве y множество всех пар $\langle x, p \rangle$ таких, что $x \in z_p$, а затем определить, что « p вынуждает $x \in y$ » означает $\langle x, p \rangle \in y$.

Это определение должно быть изменено так, чтобы описание, соответствующее любому расширению условия p , включало описание, соответствующее условию p . Поэтому мы определяем

$$x \in_p y \leftrightarrow \forall q (p \subset q \rightarrow \langle x, q \rangle \in y).$$

Ясно, что

$$x \in_p y \& p \subset q \rightarrow x \in_q y \quad (1)$$

и

$$x \in_p y \rightarrow x \in Ra(y). \quad (2)$$

Мы хотим, чтобы p вынуждало $x \in y$, как только $x \in_p y$. Естественно также считать, что p *вынуждает* $x \in y$, когда p вынуждает $x = z$ для некоторого z такого, что $z \in_p y$.

Опишем последовательный отбор корректных условий, где каждое корректное условие будет расширением всех предыдущих. Если q выбрано и $z \in_q x$, то z должно будет находиться в x . Если никакое расширение условия q не вынуждает $z \in y$, то мы не сможем никогда вынудить, чтобы z находилось в y . Поэтому x и y будут неравными. То же выполняется, если $z \in_q y$ и никакое расширение условия q не вынуждает $z \in x$. В обоих случаях мы говорим, что q *препятствует* $x = y$. Тогда мы хотим, чтобы p вынуждало $x = y$, если никакое расширение условия p не препятствует $x = y$.

Таким образом, мы приходим к следующим определениям.

А. Условие p вынуждает $x \in y$, если для некоторого z имеем $z \in_p y$, и p вынуждает $x = z$.

Б. Условие p вынуждает $x = y$, если для каждого z и каждого расширения q условия p выполняется следующее:

(i) если $z \in_q x$, то некоторое расширение условия q вынуждает $z \in y$;

(ii) если $z \in_q y$, то некоторое расширение условия q вынуждает $z \in x$.

Мы должны показать, как можно устранить порочные круги в этих определениях. Будем рассматривать А как определение множества $|x \in y|$ условий, вынуждающих $x \in y$, и Б как определение множества $|x = y|$ условий, вынуждающих $x = y$. Тогда Б определяет $|x = y|$ в терминах $|z \in x|$ и $|z \in y|$, где

$$\exists q (z \in_q x \vee z \in_q y). \quad (3)$$

Если мы заменим $|z \in x|$ и $|z \in y|$ на их определения в соответствии с А, то мы получим определение B' для $|x=y|$ в терминах $|z=w|$, где

$$\exists q (w \in_q x \vee w \in_q y). \quad (4)$$

Теперь

$$z \in Ra(x) \rightarrow Od(z) < Od(x). \quad (5)$$

Из посылки следует, что $\langle z, w \rangle \in x$ для некоторого w ; так как

$$z \in \{z\} \quad \text{и} \quad \{z\} \in \langle z, w \rangle,$$

то мы имеем $Od(z) < Od(x)$ по лемме 1 из § 9.6. Из (2), (3), (4) и (5) получаем

$$\text{Max}(\langle Od(z), Od(w) \rangle) < \text{Max}(\langle Od(x), Od(y) \rangle).$$

Поэтому мы можем рассматривать B' как определение с помощью индукции по $\text{Max}(\langle Od(x), Od(y) \rangle)$. Для этого мы должны доказать

$$\text{Set}_{x,y}(\text{Max}(\langle Od(x), Od(y) \rangle) \leq \sigma),$$

но это следует из

$$\text{Max}(\langle Od(x), Od(y) \rangle) \leq \sigma \rightarrow x, y \in C^*(S(\sigma)).$$

Поэтому мы можем принять B' в качестве определения $|x=y|$. Если мы затем примем А в качестве определения $|x \in y|$, то мы можем доказать Б из B' и А.

Теперь определим p *вынуждает* $Q(x_1, \dots, x_n)$ индукцией по предикатным символам следующим образом.

(i) Если $Q(x_1, \dots, x_n) \leftrightarrow x_i \in x_j$, то p вынуждает $Q(x_1, \dots, x_n)$, если p вынуждает $x_i \in x_j$.

(ii) Если $Q(x_1, \dots, x_n) \leftrightarrow x_i = x_j$, то p вынуждает $Q(x_1, \dots, x_n)$, если p вынуждает $x_i = x_j$.

(iii) Если $Q(x_1, \dots, x_n) \leftrightarrow \neg R(x_1, \dots, x_n)$, то p вынуждает $Q(x_1, \dots, x_n)$, если никакое расширение условия p не вынуждает $R(x_1, \dots, x_n)$.

(iv) Если

$$Q(x_1, \dots, x_n) \leftrightarrow R(x_1, \dots, x_n) \vee R'(x_1, \dots, x_n),$$

то p вынуждает $Q(x_1, \dots, x_n)$, если p вынуждает $R(x_1, \dots, x_n)$ или p вынуждает $R'(x_1, \dots, x_n)$.

(v) Если $Q(x_1, \dots, x_n) \leftrightarrow \exists y R(y, x_1, \dots, x_n)$, то p вынуждает $Q(x_1, \dots, x_n)$, если для некоторого y условие p вынуждает $R(y, x_1, \dots, x_n)$.

Если эти определения давать формально, то « p вынуждает $Q(x_1, \dots, x_n)$ » будет $(n+1)$ -местным предикатным символом от аргументов $p, x_1, \dots, x_n$. Заметим, что эти определения не используют новый символ Cог , поэтому мы можем применять наши результаты о существовании множеств к предложениям о вынуждении.

Скажем, что $Q(x_1, \dots, x_n)$ *вынужденно*, если некоторое корректное условие вынуждает $Q(x_1, \dots, x_n)$. Теперь определим нашу интерпретацию следующим образом:

$$x \in_I y \leftrightarrow x \in y \quad \text{вынужденно},$$

$$x =_I y \leftrightarrow x = y \quad \text{вынужденно},$$

$$U_I(x) \leftrightarrow x = x.$$

Мы иногда будем говорить, что p *вынуждает* $_$; это означает, что p вынуждает $Q(x_1, \dots, x_n)$, где Q определяется следующим образом:

$$Q(x_1, \dots, x_n) \leftrightarrow _.$$

Мы интерпретируем $_$ *вынужденно* аналогичным путем.

Лемма 1. Если p вынуждает $Q(x_1, \dots, x_n)$, то каждое расширение условия p вынуждает $Q(x_1, \dots, x_n)$.

Доказательство проводится индукцией по предикатным символам, используя (1), когда Q есть $\in$. Детали оставляются читателю.

Лемма 2. Если $Q(x_1, \dots, x_n)$ и $R(x_1, \dots, x_n)$ *вынужденны*, то существует корректное условие p , которое *вынуждает* $Q(x_1, \dots, x_n)$ и $R(x_1, \dots, x_n)$.

Доказательство. Выбираем корректное условие q , вынуждающее $Q(x_1, \dots, x_n)$, и корректное условие r , вынуждающее $R(x_1, \dots, x_n)$. Тогда $p = q \cup r$ корректно по Cог_3 , p вынуждает $Q(x_1, \dots, x_n)$ и $R(x_1, \dots, x_n)$ по лемме 1.

Лемма об истинности. Для каждого предикатного символа Q теории ZFC

$Q_I(x_1, \dots, x_n)$ тогда и только тогда,

когда $Q(x_1, \dots, x_n)$ *вынужденно*.

Доказательство. Используем индукцию по предикатным символам. Если $Q(x_1, \dots, x_n) \leftrightarrow x_i \in x_j$ или $Q(x_1, \dots, x_n) \leftrightarrow x_i = x_j$, то результат следует из определений $\in_I$ и $=_I$, а также пунктов (i) и (ii) определения.

Предположим, что $Q(x_1, \dots, x_n) \leftrightarrow \neg R(x_1, \dots, x_n)$. Тогда по индуктивному предположению

$$\begin{aligned} Q_I(x_1, \dots, x_n) &\leftrightarrow \neg R_I(x_1, \dots, x_n) \\ &\leftrightarrow R(x_1, \dots, x_n) \text{ не вынужденно.} \end{aligned}$$

Следовательно, нам нужно показать только, что в точности одно из $R(x_1, \dots, x_n)$ и $\neg R(x_1, \dots, x_n)$ вынужденно. По Сог₄ существует корректное условие p такое, что либо p вынуждает $R(x_1, \dots, x_n)$, либо никакое расширение условия p не вынуждает $R(x_1, \dots, x_n)^*$. Отсюда следует, что по крайней мере одно из $R(x_1, \dots, x_n)$ и $\neg R(x_1, \dots, x_n)$ вынужденно. Теперь предположим, что они оба вынуждены. По лемме 2 некоторое условие p вынуждает $R(x_1, \dots, x_n)$ и $\neg R(x_1, \dots, x_n)$. Это невозможно в силу пункта (iii) определения.

Если $Q(x_1, \dots, x_n) \leftrightarrow R(x_1, \dots, x_n) \vee R'(x_1, \dots, x_n)$, то по индуктивному предположению и пункту (iv) определения

$$\begin{aligned} Q_I(x_1, \dots, x_n) &\leftrightarrow R_I(x_1, \dots, x_n) \vee R'_I(x_1, \dots, x_n) \\ &\leftrightarrow R(x_1, \dots, x_n) \text{ вынужденно или} \\ &\quad R'(x_1, \dots, x_n) \text{ вынужденно} \\ &\leftrightarrow Q(x_1, \dots, x_n) \text{ вынужденно.} \end{aligned}$$

Если $Q(x_1, \dots, x_n) \leftrightarrow \exists y R(y, x_1, \dots, x_n)$, то по индуктивному предположению и пункту (v) определения

$$\begin{aligned} Q_I(x_1, \dots, x_n) &\leftrightarrow \exists y R_I(y, x_1, \dots, x_n) \\ &\leftrightarrow \exists y (R(y, x_1, \dots, x_n) \text{ вынужденно}) \\ &\leftrightarrow Q(x_1, \dots, x_n) \text{ вынужденно.} \end{aligned}$$

Ясно, что

$$p \text{ вынуждает } x=y \rightarrow p \text{ вынуждает } y=x. \quad (6)$$

Докажем

$$z \in_p x \rightarrow p \text{ вынуждает } z \in x \quad (7)$$

и

$$p \text{ вынуждает } x=x \quad (8)$$

индукцией по $\text{Od}(x)$. Если $z \in_p x$, то $\text{Od}(z) < \text{Od}(x)$ по (2) и (5), поэтому p вынуждает $z=z$ по индуктивному пред-

*) В качестве x в формуле Сог₄ нужно взять множество $|R(x_1, \dots, x_n)|$ всех условий, которые вынуждают $R(x_1, \dots, x_n)$. — Прим. ред.

положению; следовательно, p вынуждает $z \in x$. Теперь, если $p \subset q$ и $z \in_q x$, тогда, как только что было доказано, q вынуждает $z \in x$, поэтому p вынуждает $x=x$.

Далее мы докажем, что

$$p \text{ вынуждает } x=y \text{ и } p \text{ вынуждает } y=z \rightarrow p \text{ вынуждает } x=z, \quad (9)$$

индукцией по $\text{Od}(z)$. Ввиду симметрии достаточно показать, что если $p \subset q$ и $a \in_q x$, то некоторое расширение условия q вынуждает $a \in z$. Так как p вынуждает $x=y$, то некоторое расширение r условия q вынуждает $a \in y$. Тогда r вынуждает $a=b$, где $b \in y$. Так как p вынуждает $y=z$, то некоторое расширение r' условия r вынуждает $b \in z$. Тогда условие r' вынуждает $b=c$, где $c \in r'z$. По (2) и (5) $\text{Od}(c) < \text{Od}(z)$, а по лемме 1 условие r' вынуждает $a=b$. Следовательно, по индуктивному предположению условие r' вынуждает $a=c$. Отсюда следует, что условие r' вынуждает $a \in z$.

Теперь перейдем к доказательствам интерпретаций аксиом теории ZFC. Интерпретация аксиомы тождества есть $x=_{Ix}$. Так как 0 корректно по Сог₂ и 0 вынуждает $x=x$ по (8), то $x=_{Ix}$.

Интерпретация аксиомы равенства для $=$ есть

$$x=_{Iy} \rightarrow z=_{Iw} \rightarrow x=_{Iz} \rightarrow y=_{Iw}.$$

Это легко доказать из

$$x=_{Iy} \rightarrow y=_{Ix} \quad (10)$$

и

$$x=_{Iy} \& y=_{Iz} \rightarrow x=_{Iz}. \quad (11)$$

Но (10) следует из (6). Чтобы доказать (11), допустим $x=_{Iy}$ и $y=_{Iz}$. По лемме 2 существует корректное условие p , вынуждающее $x=y$ и $y=z$. По (9) условие p вынуждает $x=z$; следовательно, $x=_{Iz}$.

Интерпретация аксиомы равенства для $\in$ есть

$$x=_{Iy} \rightarrow z=_{Iw} \rightarrow x \in_{Iz} \rightarrow y \in_{Iw}.$$

Эта формула следует из

$$x=_{Iy} \& x \in_{Iz} \rightarrow y \in_{Iz} \quad (12)$$

и

$$x=_{Iy} \& z \in_{Ix} \rightarrow z \in_{Iy}. \quad (13)$$

Чтобы доказать (12), допустим, что $x = {}_I y$ и $x \in {}_I z$. По лемме 2 существует корректное условие p , вынуждающее $x = y$ и $x \in z$. Следовательно, для некоторого w имеем, что p вынуждает $x = w$ и $w \in {}_p z$. По (6) и (9) p вынуждает $y = w$; следовательно, p вынуждает $y \in z$; таким образом, $y \in {}_I z$.

Чтобы доказать (13), допустим, что $x = {}_I y$ и $z \in {}_I x$, и выберем корректное условие p , вынуждающее $x = y$ и $z \in x$. Тогда для некоторого w имеем, что p вынуждает $z = w$ и $w \in {}_p x$. Для каждого расширения q условия p имеем $w \in {}_q x$ и, следовательно, некоторое расширение условия q вынуждает $w \in y$. Это показывает, что условие p вынуждает $\bigcap (w \in y)$. Следовательно, $\bigcap (w \in {}_I y)$ по лемме об истинности. Таким образом, $w \in {}_I y$. Так как имеем также $z = {}_I w$, то $z \in {}_I y$ в силу (12).

Так как мы уже доказали интерпретации аксиом тождества и аксиом равенства, то мы можем сделать заключение, что интерпретация теоремы равенства выполняется. Таким образом, мы имеем

$$x = {}_I y \rightarrow (Q_I(x, v_1, \dots, v_n) \leftrightarrow Q_I(y, v_1, \dots, v_n)). \quad (14)$$

Интерпретацией аксиомы объемности является

$$\forall z (z \in {}_I x \leftrightarrow z \in {}_I y) \rightarrow x = {}_I y. \quad (15)$$

Пусть a будет множеством всех условий p таких, что

$$\exists z ((z \in {}_p x \text{ \& } p \text{ вынуждает } z \notin y) \vee (z \in {}_p y \text{ \& } p \text{ вынуждает } z \notin x)).$$

Сначала предположим, что a содержит некоторое корректное условие p . Тогда существует z такое, что, например, $z \in {}_p x$ и p вынуждает $z \notin y$. По (7) и лемме об истинности $z \in {}_I x$ и $\bigcap (z \in {}_I y)$; поэтому левая часть (15) ложна. Теперь предположим, что a не содержит корректных условий. По Сог₄ существует корректное условие p , не имеющее расширений в a . Тогда p вынуждает $x = y$; следовательно, $x = {}_I y$.

Имеем

$$x \in {}_I y \rightarrow \exists z (x = {}_I z \text{ \& } z \in \text{Ra}(y)). \quad (16)$$

Действительно, выберем корректное условие p , вынуждающее $x \in y$. Тогда p вынуждает $x = z$ и $z \in {}_p y$ для некоторого z . Следовательно, $x = {}_I z$ и $z \in \text{Ra}(y)$.

Лемма 3. Пусть p — некоторое корректное условие, вынуждающее $\exists y (y \in x)$. Тогда существует y и корректное расширение q условия p такое, что q вынуждает $y \in x$ и q вынуждает $z \notin x$ для каждого z такого, что $\text{Od}(z) < \text{Od}(y)$.

Доказательство. Пусть a — множество расширений q условия p таких, что

$$\exists y (q \text{ вынуждает } y \in x \text{ \& } \forall z (\text{Od}(z) < \text{Od}(y) \rightarrow q \text{ вынуждает } z \notin x)).$$

Мы хотим показать, что a содержит некоторое корректное условие. Предположим, что это не так. По Сог₄ существует корректное условие q , не имеющее расширений в a . По Сог₃ условие $p \cup q$ корректно и по лемме 1 $p \cup q$ вынуждает $y \in x$ для некоторого y . Таким образом, множество таких y , что

$$\exists r (p \cup q \subset r \text{ \& } r \text{ вынуждает } y \in x),$$

непусто. Пусть y — элемент этого множества, имеющий наименьший порядок, и пусть r — расширение для $p \cup q$, вынуждающее $y \in x$. Так как $r \notin a$, то существует z такое, что $\text{Od}(z) < \text{Od}(y)$ и условие r не вынуждает $z \notin x$. Поэтому некоторое расширение условия r , а значит, и условия $p \cup q$ вынуждает $z \in x$. Это невозможно по выбору y .

Интерпретацией аксиомы регулярности является

$$\exists y (y \in {}_I x) \rightarrow \exists y (y \in {}_I x \text{ \& } \bigcap \exists z (z \in {}_I x \text{ \& } z \in {}_I y)).$$

Предположим, что $\exists y (y \in {}_I x)$. По лемме об истинности существует корректное условие p , вынуждающее $\exists y (y \in x)$. Выберем y и q , как в лемме 3. Тогда $y \in {}_I x$. Предположим, что $z \in {}_I y$; мы должны показать, что $\bigcap (z \in {}_I x)$. По (16) и (14) можно предположить, что $z \in \text{Ra}(y)$, поэтому $\text{Od}(z) < \text{Od}(y)$ по (5). Таким образом, q вынуждает $z \notin x$; следовательно, $\bigcap (z \in {}_I x)$ по лемме об истинности.

Лемма 4. Если

$$z = [\langle u, p \rangle \mid u \in \text{Ra}(y) \text{ \& } p \text{ вынуждает } u \in y \text{ \& } p \text{ вынуждает } Q(u, v_1, \dots, v_n)], \text{ то для всех } x \\ x \in {}_I z \leftrightarrow x \in {}_I y \text{ \& } Q_I(x, v_1, \dots, v_n).$$

Доказательство. Параметры опускаем. По лемме 1 $u \in {}_p z \leftrightarrow \langle u, p \rangle \in z$.

Следовательно, $x \in {}_I z$ эквивалентно

$$\exists p \exists u (\text{Cог}(p) \ \& \ p \text{ вынуждает } x = u \ \& \ \langle u, p \rangle \in z),$$

а значит, и

$$\exists p \exists u (\text{Cог}(p) \ \& \ p \text{ вынуждает } x = u \ \& \ u \in \text{Ra}(y) \ \& \ p \text{ вынуждает } Q(u) \ \& \ p \text{ вынуждает } u \in y).$$

По лемме об истинности и лемме 2 это эквивалентно

$$\exists u (x = {}_I u \ \& \ u \in \text{Ra}(y) \ \& \ u \in {}_I y \ \& \ Q_I(u)).$$

По (14) это эквивалентно

$$\exists u (x = {}_I u \ \& \ u \in \text{Ra}(y) \ \& \ x \in {}_I y \ \& \ Q_I(x)).$$

Но это в силу (16) эквивалентно $x \in {}_I y \ \& \ Q_I(x)$.

Интерпретация аксиомы подмножеств имеет вид

$$\exists z \forall x (x \in {}_I z \leftrightarrow x \in {}_I y \ \& \ Q_I(x, v_1, \dots, v_n)).$$

А это следствие леммы 4.

Имеем

$$x \in {}_I (y \times \text{CD}) \leftrightarrow \exists z (z \in y \ \& \ x = {}_I z). \quad (17)$$

Импликация слева направо следует из (16). Теперь предположим, что

$$z \in y \ \& \ x = {}_I z,$$

и выберем корректное условие p , вынуждающее $x = z$. Тогда $z \in {}_p (y \times \text{CD})$, поэтому p вынуждает $x \in (y \times \text{CD})$; следовательно, $x \in {}_I (y \times \text{CD})$.

Интерпретация аксиомы замены имеет посылку

$$\forall x \exists u \forall y (y \in {}_I u \leftrightarrow Q_I(x, y)) \quad (18)$$

и заключение

$$\exists z \forall y (\exists x (x \in {}_I y \ \& \ Q_I(x, y)) \rightarrow y \in {}_I z). \quad (19)$$

(Здесь мы опустили все параметры.) Пусть $F(x, p)$ будет множеством u наименьшего порядка таким, что

$$p \text{ вынуждает } \forall y (y \in u \leftrightarrow Q(x, y)), \quad (20)$$

при условии, что такое u существует. Допустим (18). Тогда для каждого x существует u такое, что $\forall y (y \in {}_I u \leftrightarrow Q_I(x, y))$, поэтому по лемме об истинности существует корректное условие p такое, что (20) выполняется. Отсюда следует, что (20) выполняется для $u = F(x, p)$. Таким образом, используя снова лемму об истинности,

получаем

$$\forall x \exists p \forall y (y \in {}_I F(x, p) \leftrightarrow Q_I(x, y)). \quad (21)$$

Для данного ω положим

$$z = \text{Up}([\text{Ra}(F(x, p)) \mid x \in \text{Ra}(\omega)]_{x,p}) \times \text{CD}.$$

Чтобы доказать (19), мы должны показать, что

$$x \in {}_I \omega \ \& \ Q_I(x, y) \rightarrow y \in {}_I z.$$

По (16) и (14) мы можем предположить, что $x \in \text{Ra}(\omega)$. Выбирая p по (21), мы имеем $y \in {}_I F(x, p)$. По (16) $y = {}_I y'$ для некоторого y' из $\text{Ra}(F(x, p))$, поэтому $y \in {}_I z$ по (17).

Интерпретацией аксиомы степени является

$$\exists \omega \forall x (\forall z (z \in {}_I x \rightarrow z \in {}_I y) \rightarrow x \in {}_I \omega).$$

Пусть $\omega = P(\text{Ra}(y) \times \text{CD}) \times \text{CD}$. Допустим, что $\forall z (z \in {}_I x \rightarrow z \in {}_I y)$, и положим

$$v = [\langle u, p \rangle \mid u \in \text{Ra}(y) \ \& \ p \text{ вынуждает } u \in y \ \& \ p \text{ вынуждает } u \in x].$$

По лемме 4 мы имеем для всех z

$$z \in {}_I v \leftrightarrow z \in {}_I y \ \& \ z \in {}_I x \\ \leftrightarrow z \in {}_I x.$$

Ввиду интерпретированной аксиомы объемности $x = {}_I v$. Так как $v \subset \text{Ra}(y) \times \text{CD}$, то $x \in {}_I \omega$ по (17).

Пусть ZF_0 — теория, полученная из теории ZF опусканием аксиомы бесконечности.

Лемма 5. Пусть J — некоторая интерпретация теории ZF_0 в теории $\text{ZFL}_{\text{Cог}}$ и O — функциональный символ такой, что в теории $\text{ZFL}_{\text{Cог}}$

$$\vdash U_J(O(\sigma)), \quad (22)$$

$$\vdash x \in {}_J O(\sigma) \leftrightarrow \exists \tau (\tau < \sigma \ \& \ x = {}_J O(\tau)). \quad (23)$$

Тогда J — интерпретация теории ZF . Более того, интерпретацией формулы $x = \omega$ относительно J является $x = {}_J O(\omega)$.

Доказательство. Определим (в теории ZF_0)

$$\text{Zer}(x) \leftrightarrow \forall y (y \notin x),$$

$$\text{Suc}(x, y) \leftrightarrow \forall z (z \in x \leftrightarrow z \in y \vee z = y).$$

Из (23) имеем

$$\text{Zer}_J(O(0)), \quad (24)$$

$$\text{Suc}_J(O(S(\sigma)), O(\sigma)). \quad (25)$$

Используя эти формулы, а также (22) и (23), получаем

$$\exists y (U_J(y) \& y \in {}_JO(\omega) \& \text{Zer}_J(y)), \quad (26)$$

$$\forall y (U_J(y) \& y \in {}_JO(\omega) \rightarrow \exists z (U_J(z) \& z \in {}_JO(\omega) \& \text{Suc}_J(z, y))). \quad (27)$$

Аксиома бесконечности есть формула

$$\exists x (\exists y (y \in x \& \text{Zer}(y)) \& \forall y (y \in x \rightarrow \exists z (z \in x \& \text{Suc}(z, y)))).$$

Ее интерпретация легко следует из (26), (27) и (22).

Теперь определим

$$\text{Np}(x) \leftrightarrow x \in \omega.$$

В теории ZF мы можем доказать

$$\exists y (y \in \omega \& \text{Zer}(y)) \& \forall y (y \in \omega \rightarrow \exists z (z \in \omega \& \text{Suc}(z, y))) \& \text{Np}(x) \rightarrow x \in \omega.$$

Если мы возьмем интерпретацию этой формулы, подставим $O(\omega)$ вместо ω и применим (26) и (27), то мы получим

$$U_J(x) \& \text{Np}_J(x) \rightarrow x \in {}_JO(\omega). \quad (28)$$

Мы можем также доказать в теории ZF формулы

$$\text{Zer}(x) \rightarrow \text{Np}(x),$$

$$\text{Np}(x) \& \text{Suc}(y, x) \rightarrow \text{Np}(y).$$

Беря их интерпретации и применяя (24) и (25), получим

$$\text{Np}_J(O(0)), \quad (29)$$

$$\text{Np}_J(O(\sigma)) \rightarrow \text{Np}_J(O(S(\sigma))). \quad (30)$$

Теперь допустим, что

$$\exists x (U_J(x) \& x \in {}_JO(\omega) \& \neg \text{Np}_J(x)). \quad (31)$$

В теории ZF в силу аксиомы регулярности мы можем доказать

$$\begin{aligned} \exists x (x \in \omega \& \neg \text{Np}(x)) \rightarrow \\ \rightarrow \exists x (x \in \omega \& \neg \text{Np}(x) \& \forall z (z \in x \& z \in \omega \rightarrow \text{Np}(z))). \end{aligned}$$

Беря интерпретацию этой формулы, подставляя $O(\omega)$ вместо ω и применяя (31), получим, что существует x такое, что

$$U_J(x) \& x \in {}_JO(\omega) \& \neg \text{Np}_J(x),$$

и такое, что для всех z

$$U_J(z) \& z \in {}_Jx \& z \in {}_JO(\omega) \rightarrow \text{Np}_J(z). \quad (32)$$

По (23) $x = {}_JO(\sigma)$ для некоторого натурального числа σ , поэтому ввиду интерпретированной теоремы равенства мы можем предположить, что x есть $O(\sigma)$. Из $\neg \text{Np}_J(O(\sigma))$, (29) и (30) получаем, что $\sigma = S(\tau)$, где $\neg \text{Np}_J(O(\tau))$. Полагая $O(\tau)$ вместо z в (32) и используя (22) и (23), получаем $\text{Np}_J(O(\tau))$. Итак, мы получили противоречие с (31). Из этого и (28) получаем

$$U_J(x) \rightarrow (\text{Np}_J(x) \leftrightarrow x \in {}_JO(\omega)). \quad (33)$$

В теории ZF формула $x = \omega$ эквивалентна $\forall y (y \in x \leftrightarrow \text{Np}(x))$. Отсюда следует, что интерпретация формулы $x = \omega$ эквивалентна

$$\forall y (U_J(y) \rightarrow (y \in {}_Jx \leftrightarrow \text{Np}_J(x))).$$

По (33) это эквивалентно

$$\forall y (U_J(y) \rightarrow (y \in {}_Jx \leftrightarrow y \in {}_JO(\omega))).$$

А это эквивалентно $x = {}_JO(\omega)$ в силу интерпретированных аксиом равенства и объемности.

Чтобы применить лемму к нашему случаю, определим трансфинитной индукцией по σ

$$O(\sigma) = [O(\tau) \mid \tau < \sigma] \times \text{CD}.$$

Тогда (22) очевидно, а (23) следует из (17).

Аксиомой мультипликативности называется следующее утверждение: если $0 \notin z$ и если каждые два различных элемента множества z не пересекаются, то существует множество y , имеющее в точности один общий элемент с каждым элементом множества z . В теории ZF из этой аксиомы следует аксиома выбора. Действительно, пусть x дано, для $a \subset x$ пусть

$$z_a = [\langle b, a \rangle \mid b \in a].$$

Пусть $z = [z_a \mid a \in P(x) - \{0\}]$ и множество y таково, как утверждается в аксиоме мультипликативности. Тогда $y \cap z$ является функцией выбора на x .

Отсюда следует, что нам нужно только доказать интерпретацию аксиомы мультипликативности. Пусть, следовательно, нам дано z такое, что

$$\omega \in {}_Jz \rightarrow \exists a (a \in {}_J\omega) \quad (34)$$

и

$$\omega \in {}_Jz \& a \in {}_J\omega \& \omega' \in {}_Jz \& a \in {}_J\omega' \rightarrow \omega = {}_J\omega'. \quad (35)$$

Мы собираемся найти y такое, что

$$\omega \in {}_I z \rightarrow \exists a (a \in {}_I \omega \& a \in {}_I y) \quad (36)$$

и

$$\omega \in {}_I z \& a \in {}_I \omega \& a \in {}_I y \& b \in {}_I \omega \& b \in {}_I y \rightarrow a = {}_I b. \quad (37)$$

Возьмем в качестве y множество всех пар $\langle a, p \rangle$ таких, что для некоторого ω условие p вынуждает $\omega \in z$ и $a \in \omega$, а также p вынуждает $b \notin \omega$ для всех b таких, что $\text{Od}(b) < \text{Od}(a)$. Тогда $a \in {}_p y \leftrightarrow \langle a, p \rangle \in y$ по лемме 1.

Вначале докажем (36). Пусть $\omega \in {}_I z$. По (34) и лемме об истинности существует корректное условие p , вынуждающее $\omega \in z$ и $\exists a (a \in \omega)$. Следовательно, по лемме 3 существует a и корректное расширение q условия p такое, что q вынуждает $a \in \omega$ и q вынуждает $b \notin \omega$ для всех b таких, что $\text{Od}(b) < \text{Od}(a)$. Тогда $\langle a, q \rangle \in y$, поэтому $a \in {}_q y$; отсюда условие q вынуждает $a \in y$. Поэтому $a \in {}_I \omega \& a \in {}_I y$.

Теперь докажем (37). Допустим, что посылка верна и выберем корректное условие p , вынуждающее $a \in y$. Тогда для некоторого c условие p вынуждает $a = c$ и $\langle c, p \rangle \in y$. Поэтому для некоторого ω' условие p вынуждает $\omega' \in z$, $c \in \omega'$ и $d \notin \omega'$ для всех d таких, что $\text{Od}(d) < \text{Od}(c)$, откуда

$$a = {}_I c \& \omega' \in {}_I z \& c \in {}_I \omega' \& \forall d (\text{Od}(d) < \text{Od}(c) \rightarrow \neg (d \in {}_I \omega')).$$

По (35) имеем $\omega = {}_I \omega'$, поэтому

$$a = {}_I c \& c \in {}_I \omega \& \forall d (\text{Od}(d) < \text{Od}(c) \rightarrow \neg (d \in {}_I \omega)).$$

Подобным образом найдем d такое, что

$$b = {}_I d \& d \in {}_I \omega \& \forall c (\text{Od}(c) < \text{Od}(d) \rightarrow \neg (c \in {}_I \omega)).$$

Из этого мы получаем $\text{Od}(c) = \text{Od}(d)$, поэтому $c = d$. Так как $a = {}_I c$ и $b = {}_I d$, то отсюда следует, что $a = {}_I b$.

9.9. Доказательства независимости

Теперь мы переходим к доказательству двух следующих теорем Коэна.

Теорема 1. Если теория ZF непротиворечива, то гипотеза континуума не является теоремой теории ZFC.

Теорема 2. Если теория ZF непротиворечива, то аксиома выбора не является теоремой теории ZF.

Для доказательства теоремы 1 мы хотим выбрать надлежащим образом константу CD, а затем показать, что выполняется интерпретация отрицания гипотезы континуума. В действительности мы докажем интерпретацию предложения, из которого следует отрицание гипотезы континуума. Определим (в теории ZFC)

$$\text{Im}(f, x, y) \leftrightarrow \langle y, x \rangle \in f,$$

$$\text{Sur}(a, b) \leftrightarrow \exists f \forall y (y \in b \rightarrow \exists x (x \in a \& \text{Im}(f, x, y) \& \forall z (\text{Im}(f, x, z) \rightarrow z = y))).$$

Тогда $\text{Sur}(a, b)$ означает, что существует сюръективное отображение из a на b . Имеем

$$b \neq 0 \& \text{Card}(b) \leq \text{Card}(a) \rightarrow \text{Sur}(a, b). \quad (1)$$

Действительно, из посылки следует, что существует биективное отображение из некоторого подмножества множества a на b ; это отображение может быть расширено до сюръективного отображения из a на b . Теперь допустим, что выполняется гипотеза континуума, и пусть

$$0 \neq a \subset b \subset P(\omega).$$

Если $\text{Card}(a) \leq \aleph_0$, то $\text{Sur}(\omega, a)$ по (1). Если $\aleph_0 < \text{Card}(a)$, то

$$\aleph_1 \leq \text{Card}(a) \leq \text{Card}(b) \leq \text{Card}(P(\omega)) = 2^{\aleph_0} = \aleph_1.$$

Следовательно, $\text{Card}(a) = \text{Card}(b)$, поэтому $\text{Sur}(a, b)$ по (1). Таким образом, из гипотезы континуума следует

$$\forall a \forall b (a \neq 0 \& a \subset b \& b \subset P(\omega) \rightarrow \text{Sur}(\omega, a) \vee \text{Sur}(a, b)).$$

Поэтому отрицание гипотезы континуума следует из

$$\exists a \exists b (a \neq 0 \& a \subset b \& b \subset P(\omega) \& \neg \text{Sur}(\omega, a) \& \neg \text{Sur}(a, b)).$$

Перепишем это так:

$$\exists a \exists b \exists c (c = \omega \& \exists x (x \in a) \& a \subset b \& \forall x (x \in b \rightarrow x \subset c) \& \neg \text{Sur}(c, a) \& \neg \text{Sur}(a, b)).$$

Беря интерпретацию этой формулы и применяя лемму 5 из § 9.8, получаем

$$\exists a \exists b \exists c (c = {}_I O_1(\omega) \& \exists x (x \in {}_I a) \& a \subset {}_I b \& \forall x (x \in {}_I b \rightarrow x \subset {}_I c) \& \neg \text{Sur}_I(c, a) \& \neg \text{Sur}_I(a, b)).$$

Используя интерпретированную теорему равенства, видим, что достаточно определить константы A и B и доказать

А. $\exists x (x \in_I A)$.

Б. $A \subset_I B$.

В. $x \in_I B \rightarrow x \subset_I O(\omega)$.

Г. $\neg \text{Sur}_I(O(\omega), A)$.

Д. $\neg \text{Sur}_I(A, B)$.

Пусть CD — множество всех отображений из конечных подмножеств из $\omega \times \aleph_2$ в $\{0, 1\}$. Пусть область изменения i и j составляют натуральные числа. Определим

$$N(\sigma) = [\langle O(i), p \rangle \mid p' \langle i, \sigma \rangle = 1],$$

$$A = [N(\sigma) \mid \sigma < \aleph_1] \times CD,$$

$$B = [N(\sigma) \mid \sigma < \aleph_2] \times CD.$$

Тогда А и Б следуют по (17) из § 9.8.

Чтобы доказать В, мы должны показать

$$x \in_I B \ \& \ y \in_I x \rightarrow y \in_I O(\omega).$$

По (17) из § 9.8 и интерпретированной теореме равенства можно предположить, что $x = N(\sigma)$. По (16) из § 9.8 $y =_I O(i)$ для некоторого i ; так как $O(i) \in_I O(\omega)$ по (17) из § 9.8, то $y \in_I O(\omega)$.

Чтобы доказать Г и Д, нам будут нужны несколько лемм.

Лемма 1. Пусть x — множество условий такое, что для всех p и q из x из $p \neq q$ следует, что $p \cup q$ не является условием. Тогда x счетно.

Доказательство. Определим индуктивно последовательность $x_0, x_1, \dots$ конечных подмножеств множества x . Пусть a_n — множество $\langle i, z \rangle$ из $\{0, 1\} \times (\omega \times \aleph_2)$ таких, что $\langle 1-i, z \rangle$ находится в некотором условии из $x_0 \cup \dots \cup x_{n-1}$. Так как каждое условие — конечное множество и $x_0 \cup \dots \cup x_{n-1}$ — конечное множество условий, то a_n конечно. Мы можем, следовательно, выбрать конечное подмножество x_n множества x такое, что для каждого $p \in x$ существует $q \in x_n$ такое, что $p \cap a_n = q \cap a_n$.

Теперь достаточно будет показать, что каждое p из x находится в некотором x_n . Так как p конечно и $a_n \subset a_{n+1}$, то можно выбрать n так, чтобы $p \cap a_n = p \cap a_{n+1}$. Выберем $q \in x_n$ так, чтобы $p \cap a_n = q \cap a_n$. Если $\langle i, z \rangle$ есть в q , то

$\langle 1-i, z \rangle$ есть в $a_{n+1} - q$. Так как

$$p \cap a_{n+1} = q \cap a_n,$$

то отсюда следует, что $\langle 1-i, z \rangle \notin p$. Из этого следует, что $p \cup q$ — некоторое условие; следовательно, по предположению $p = q$.

Лемма 2. Если p вынуждает $Q(x, v_1, \dots, v_n)$ и $\forall z (Q(z, v_1, \dots, v_n) \rightarrow z = y)$, то p вынуждает $x = y$.

Доказательство. Параметры опускаем. Пусть q — расширение условия p . Тогда q не вынуждает $\exists z \neg (Q(z) \rightarrow z = y)$ и, следовательно, не вынуждает $\neg (Q(x) \rightarrow x = y)$, поэтому некоторое расширение r условия q вынуждает $Q(x) \rightarrow x = y$. Это означает, что r вынуждает либо $\neg Q(x)$, либо $x = y$. Первое невозможно, потому что условие r , как расширение условия p , вынуждает $Q(x)$. Поэтому условие r вынуждает $x = y$.

Чтобы доказать, что условие p вынуждает $x = y$, допустим, что $p \subset q$ и, например, $z \in_q x$. Выберем условие r , как и раньше. Так как условие r вынуждает $x = y$ и $z \in_r x$, то существует некоторое расширение условия r , вынуждающее $z \in y$. Поэтому некоторое расширение условия q вынуждает $z \in y$.

Множество a называется *отделимым*, если

$$\forall p \forall x \forall y (x, y \in a \ \& \ p \text{ вынуждает } x = y \rightarrow x = y).$$

Лемма 3. Если $\text{Sur}_I(a \times CD, b \times CD)$, где $\text{Card}(a)$ бесконечен, а множество b отделимо, то $\text{Card}(b) \leq \text{Card}(a)$.

Доказательство. По предположению и (17) из § 9.8 существует f такое, что для каждого $y \in b$ существует x такое, что

$$x \in_I a \times CD \ \& \ \text{Im}_I(f, x, y) \ \& \ \forall w (\text{Im}_I(f, x, w) \rightarrow w =_I y).$$

Отсюда следует, что существует $x \in a$ такое, что

$$\text{Im}_I(f, x, y) \ \& \ \forall w (\text{Im}_I(f, x, w) \rightarrow w =_I y).$$

Тогда по лемме об истинности существует корректное условие p такое, что

$$p \text{ вынуждает } \text{Im}(f, x, y) \text{ и } \forall w (\text{Im}(f, x, w) \rightarrow w = y). \quad (2)$$

Для $x \in a$ пусть b_x — множество всех $y \in b$ таких, что (2) выполняется для некоторого условия p (не обязательно корректного). Мы показали, что $b = \text{Un}(\{b_x \mid x \in a\})$. Пока-

жем, что b_x счетно, из этого будет следовать, что $\text{Card}(b) \leq \leq \text{Card}(a) \cdot \omega = \text{Card}(a)$. Для каждого $y \in b_x$ пусть p_y будет такое p , что (2) выполняется. Предположим, что $y, z \in b_x$ и

$$p = p_y \cup p_z$$

есть условие. Тогда p вынуждает

$$\text{Im}(f, x, y) \text{ и } \forall \omega (\text{Im}(f, x, \omega) \rightarrow \omega = z).$$

По лемме 2 p вынуждает $y = z$; следовательно, $y = z$, так как множество b отделимо. Это показывает, что $p_y = p_z \rightarrow y = z$, поэтому чтобы показать, что b_x счетно, достаточно показать, что $[p_y | y \in b_x]$ счетно. Но это следует из леммы 1 и только что доказанного результата.

Докажем теперь трансфинитной индукцией по τ , что

$$\sigma < \tau \rightarrow p \text{ не вынуждает } O(\sigma) = O(\tau). \quad (3)$$

Так как $\sigma < \tau$, то $O(\sigma) \in_p O(\tau)$. Если p вынуждает $O(\sigma) = O(\tau)$, то отсюда следует, что некоторое расширение q условия p вынуждает $O(\sigma) \in O(\sigma)$. Тогда q вынуждает $O(\sigma) = O(\rho)$ для некоторого $\rho < \sigma$. Но это противоречит индуктивному предположению.

Из (3) имеем

$$p \text{ вынуждает } O(\tau) = O(\sigma) \rightarrow \tau = \sigma. \quad (4)$$

Используем это, чтобы показать, что

$$p \text{ вынуждает } N(\tau) = N(\sigma) \rightarrow \tau = \sigma. \quad (5)$$

Действительно, предположим, что $\tau \neq \sigma$. Выберем i таким большим, чтобы ни одна пара $\langle i, \rho \rangle$ не находилась в области определения условия p . Пусть q — расширение условия p такое, что $\langle i, \tau \rangle$ и $\langle i, \sigma \rangle$ находятся в области определения условия q и

$$q' \langle i, \tau \rangle = 1, \quad q' \langle i, \sigma \rangle = 0.$$

Из первого следует, что $O(i) \in_q N(\tau)$. Поэтому некоторое расширение r условия q вынуждает $O(i) \in N(\sigma)$. Отсюда следует, что для некоторого j условие r вынуждает $O(i) = O(j)$ и $O(j) \in_r N(\sigma)$. По (4) $i = j$, поэтому $r' \langle i, \sigma \rangle = 1$. Это невозможно, так как r — расширение условия q .

Из (4) и (5)

$$\tau \neq \sigma \rightarrow O(\tau) \neq O(\sigma) \& N(\tau) \neq N(\sigma).$$

Следовательно,

$$\text{Card}([O(i) | i \in \omega]) = \aleph_0,$$

$$\text{Card}([N(\sigma) | \sigma < \aleph_1]) = \aleph_1,$$

$$\text{Card}([N(\sigma) | \sigma < \aleph_2]) = \aleph_2.$$

Кроме того, множества $[N(\sigma) | \sigma < \aleph_1]$ и $[N(\sigma) | \sigma < \aleph_2]$ отделимы по (5). Вспомнив, что

$$O(\omega) = [O(i) | i \in \omega] \times \text{CD},$$

видим, что Γ и Δ следуют из леммы 3.

Заметим, что многие обобщения теоремы 1 могут быть доказаны этим же методом. Например, мы можем доказать, что теория ZFC остается непротиворечивой при добавлении аксиом $2^{\aleph_0} = \aleph_1$ и $2^{\aleph_1} = \aleph_2$.

Теперь перейдем к доказательству теоремы 2. Пусть CD — множество всех отображений из конечных подмножеств множества $\omega \times \omega$ в $\{0, 1\}$. Тогда строим I , как и раньше. Построим новую интерпретацию J теории ZF в теории ZFC_{Cor} так, чтобы выполнялась интерпретация отрицания аксиомы выбора.

Под *перестановкой* мы понимаем любое биективное отображение из ω на ω . Пусть областью изменения f и g будут перестановки. Применяем следующие обозначения: $f \cdot g$ для композиции f и g (так что $(f \cdot g)' i = f'(g'(i))$), f^* для обращения f (так что $f^{*'}(i) = j$ тогда и только тогда, когда $f'j = i$) и I для тождественной перестановки (так что $I'i = i$). Скажем, что f есть k -перестановка, если $f'i = i$ для $i \leq k$.

Положим

$$\pi_f(p) = [\langle i, j, f'k \rangle | \langle i, j, k \rangle \in p].$$

(Таким образом, π — бинарный функциональный символ, один из аргументов которого записывается в индексе.) Ясно, что $\pi_f(p)$ — условие; мы имеем $\pi_{f \cdot g}(p) = \pi_f(\pi_g(p))$ и $\pi_I(p) = p$.

Определим

$$\Pi_f(x) = [\langle \Pi_f(y), \pi_f(p) \rangle | \langle y, p \rangle \in x].$$

Это определение индукцией по $\text{Od}(x)$. Имеем $\Pi_{f \cdot g}(x) = \Pi_f(\Pi_g(x))$.

Говорим, что x *инвариантно*, и записываем $\text{Iv}(x)$, если существует такое k , что $\Pi_f(x) = x$ для каждой k -перестановки f . Отсюда, очевидно, следует, что $\Pi_I(x) = x$.

Если x инвариантно, то $\Pi_f(x)$ инвариантно. Действительно, выберем k так, чтобы $\Pi_g(x) = x$ для каждой k -перестановки g , и выберем k' так, чтобы $i \leq k \rightarrow f^*i \leq k'$. Предположим, что g есть k' -перестановка. Тогда $f^* \circ g \circ f$ есть k -перестановка, поэтому

$$\Pi_{f^*}(\Pi_g(\Pi_f(x))) = x.$$

Применяя к обеим частям Π_f , получим $\Pi_g(\Pi_f(x)) = \Pi_f(x)$.

Определим U_J индукцией по $\text{Od}(x)$ следующим образом:

$$U_J(x) \leftrightarrow \text{Iv}(x) \ \& \ \forall y (y \in \text{Ra}(x) \rightarrow U_J(y)). \quad (6)$$

Теперь завершим определение интерпретации J , взяв $\in_J$ такое же, как и $\in_I$, и $=_J$ такое же, как и $=_I$.

Для каждой открытой формулы A формула A_I такая же, как и A_J ; следовательно, если $\vdash A^{(I)}$, то $\vdash A^{(J)}$. Из этого получаем интерпретацию аксиом тождества и равенства относительно J . Тогда легко доказать

$$x =_J y \rightarrow (Q_J(x, v_1, \dots, v_n) \leftrightarrow Q_J(y, v_1, \dots, v_n)) \quad (7)$$

индукцией по предикатным символам. По (16) из § 9.8 и (6) получаем

$$U_J(y) \ \& \ x \in_J y \rightarrow \exists z (U_J(z) \ \& \ x =_J z). \quad (8)$$

Интерпретация аксиомы объемности относительно J есть

$$U_J(x) \ \& \ U_J(y) \ \& \ \forall z (U_J(z) \rightarrow (z \in_J x \leftrightarrow z \in_J y)) \rightarrow x =_J y.$$

Предположим, что посылка выполняется, а заключение ложно. Применяя интерпретацию аксиомы объемности относительно I , находим, что существует z такое, что $\neg(z \in_J x \leftrightarrow z \in_J y)$. По (8) и (7) это z может быть выбрано так, чтобы $U_J(z)$, а это противоречит посылке.

Интерпретация аксиомы регулярности относительно J есть

$$U_J(x) \ \& \ \exists y (U_J(y) \ \& \ y \in_J x) \rightarrow \rightarrow \exists y (U_J(y) \ \& \ y \in_J x \ \& \ \neg \exists z (U_J(z) \ \& \ z \in_J x \ \& \ z \in_J y)).$$

Допустим посылку. По интерпретации аксиомы регулярности относительно I существует y такое, что $y \in_J x$ и $\neg \exists z (z \in_J x \ \& \ z \in_J y)$. Но по (8) и (7) мы можем такж предположить, что $U_J(y)$.

Теперь введем понятие *J-вынуждения*. Определим p *J-вынуждает* $Q(x_1, \dots, x_n)$ точно так же, как p вынуждает

$Q(x_1, \dots, x_n)$, за исключением случая, в котором

$$Q(x_1, \dots, x_n) \leftrightarrow \exists y R(y, x_1, \dots, x_n).$$

В этом случае p *J-вынуждает* $Q(x_1, \dots, x_n)$, если для некоторого y имеем $U_J(y)$ и p *J-вынуждает* $R(y, x_1, \dots, x_n)$. Скажем, что $Q(x_1, \dots, x_n)$ является *J-вынужденным*, если некоторое корректное условие *J-вынуждает* $Q(x_1, \dots, x_n)$.

Леммы 1 и 2 последнего параграфа выполняются для *J-вынуждения*. Лемма об истинности также выполняется: $Q_J(x_1, \dots, x_n) \leftrightarrow Q(x_1, \dots, x_n)$ является *J-вынужденным*.

Докажем, что

$$U_J(x) \rightarrow U_J(\Pi_f(x)), \quad (9)$$

индукцией по $\text{Od}(x)$. Если $y \in \text{Ra}(\Pi_f(x))$, то $y = \Pi_f(z)$ для некоторого $z \in \text{Ra}(x)$. Тогда $U_J(z)$, поэтому $U_J(y)$ по индуктивному предположению. Как было доказано раньше, $\Pi_f(x)$ инвариантно, поэтому $U_J(\Pi_f(x))$.

Теперь докажем, что

$$p \text{ J-вынуждает } Q(x_1, \dots, x_n) \leftrightarrow \pi_f(p) \text{ J-вынуждает } Q(\Pi_f(x_1), \dots, \Pi_f(x_n)), \quad (10)$$

индукцией по предикатным символам. Для атомных формул мы должны доказать, что

$$p \text{ J-вынуждает } x \in y \leftrightarrow \pi_f(p) \text{ J-вынуждает } \Pi_f(x) \in \Pi_f(y), \quad (11)$$

$$p \text{ J-вынуждает } x = y \leftrightarrow \pi_f(p) \text{ J-вынуждает } \Pi_f(x) = \Pi_f(y). \quad (12)$$

Допустим, что (12) выполняется, когда $\text{Od}(x) < \sigma$ и $\text{Od}(y) < \sigma$. Покажем, что (11) выполняется, когда $\text{Od}(x) < \sigma$, $\text{Od}(y) \leq \sigma$. По определению p *J-вынуждает* $x \in y$ эквивалентно

$$\exists z (p \text{ J-вынуждает } x = z \ \& \ z \in_p y). \quad (13)$$

Имеем $z \in_p y \rightarrow \text{Od}(z) < \text{Od}(y) \leq \sigma$. Поэтому по предположению и определению $\in_p$ (13) эквивалентно

$$\exists z (\pi_f(p) \text{ J-вынуждает } \Pi_f(x) = \Pi_f(z) \ \& \ \Pi_f(z) \in \pi_f(p) \Pi_f(y)). \quad (14)$$

Теперь, если $z' \in_q \Pi_f(y)$, то $z' \in \text{Ra}(\Pi_f(y))$, и поэтому

$z' = \Pi_f(z)$ для некоторого z . Таким образом, (14) эквивалентно

$\exists z' (\pi_f(p) \text{ } J\text{-вынуждает } \Pi_f(x) = z' \text{ \& } z' \in \pi_{f(p)} \Pi_f(y)),$
а поэтому эквивалентно

$\pi_f(p) \text{ } J\text{-вынуждает } \Pi_f(x) \in \Pi_f(y).$

Теперь покажем, что при тех же предположениях, (12) выполняется для $\text{Od}(x) \leq \sigma$ и $\text{Od}(y) \leq \sigma$. Тем самым (12) будет доказано индукцией по $\text{Max}(\langle \text{Od}(x), \text{Od}(y) \rangle)$, а (11) будет следовать из ранее доказанного.

По определению $p \text{ } J\text{-вынуждает } x = y$ тогда и только тогда, когда

$$\forall q \forall z (p \subset q \text{ \& } z \in_q x \rightarrow \exists r (q \subset r \text{ \& } r \text{ } J\text{-вынуждает } z \in y)), \quad (15)$$

и такое же выражение выполняется, если x и y поменять местами. Из только что доказанного следует, что (15) эквивалентно

$$\begin{aligned} & \forall q \forall z (\pi_f(p) \subset \pi_f(q) \text{ \& } \Pi_f(z) \in \pi_{f(q)} \Pi_f(x) \rightarrow \\ & \rightarrow \exists r (\pi_f(q) \subset \pi_f(r) \text{ \& } \pi_f(r) \text{ } J\text{-вынуждает } \Pi_f(z) \in \Pi_f(y))). \end{aligned} \quad (16)$$

Теперь, если q принимает все условия в качестве значений, то $\pi_f(q)$ принимает все условия в качестве значений (так как $q = \pi_f(\pi_{f*}(q))$). Поэтому, как и раньше, (16) эквивалентно

$$\begin{aligned} & \forall q \forall z' (\pi_f(p) \subset q \text{ \& } z' \in_q \Pi_f(x) \rightarrow \\ & \rightarrow \exists r (q \subset r \text{ \& } r \text{ } J\text{-вынуждает } z' \in \Pi_f(y))). \end{aligned} \quad (17)$$

Из эквивалентности (15) и (17) и соответствующего результата, когда x и y меняются местами, получаем (12).

Теперь вернемся к (10). Случай, когда Q — отрицание или дизъюнкция, совершенно простой. Теперь предположим, что $Q(x_1, \dots, x_n) \leftrightarrow \exists y R(y, x_1, \dots, x_n)$. Тогда « $p \text{ } J\text{-вынуждает } Q(x_1, \dots, x_n)$ » эквивалентно

$$\exists y (U_J(y) \text{ \& } p \text{ } J\text{-вынуждает } R(y, x_1, \dots, x_n)),$$

которое по индуктивному предположению эквивалентно

$$\begin{aligned} & \exists y (U_J(y) \text{ \& } \pi_f(p) \\ & \text{ } J\text{-вынуждает } R(\Pi_f(y), \Pi_f(x_1), \dots, \Pi_f(x_n))). \end{aligned} \quad (18)$$

Мы хотим показать, что это эквивалентно

$$\exists y' (U_J(y') \text{ \& } \pi_f(p) \text{ } J\text{-вынуждает } R(y', \Pi_f(x_1), \dots, \Pi_f(x_n))). \quad (19)$$

Теперь по (9) из (18) следует (19). Если (19) выполняется для некоторого y' , то положим $y = \Pi_{f*}(y')$. Тогда $U_J(y)$ по (9) и $\Pi_f(y) = \Pi_f(y') = y'$, потому что y' инвариантно. Поэтому (18) выполняется.

Лемма 4. Пусть $y, v_1, \dots, v_n$ — U_J -множества, положим

$$\begin{aligned} z = [\langle u, p \rangle \mid u \in \text{Ra}(y) \text{ \& } p \text{ } J\text{-вынуждает } u \in y \text{ \& } p \\ \text{ } J\text{-вынуждает } Q(u, v_1, \dots, v_n)]. \end{aligned}$$

Тогда z есть U_J -множество и для всех x

$$x \in_J z \leftrightarrow x \in_J y \text{ \& } Q_J(x, v_1, \dots, v_n).$$

Доказательство. Доказательство эквивалентности, если использовать (7), такое же, как в лемме 4 из § 9.8. Так как $\text{Ra}(z) \subset \text{Ra}(y)$, то каждый элемент множества $\text{Ra}(z)$ есть U_J -множество. Поэтому нам нужно лишь показать, что z инвариантно.

Выберем k так, чтобы $\Pi_f(y) = y, \Pi_f(v_1) = v_1, \dots, \Pi_f(v_n) = v_n$ для каждой k -перестановки f . Тогда для k -перестановки f

$$\begin{aligned} \Pi_f(z) = [\langle \Pi_f(u), \pi_f(p) \rangle \mid u \in \text{Ra}(y) \text{ \& } p \text{ } J\text{-вынуждает } u \in y \\ \text{ \& } p \text{ } J\text{-вынуждает } Q(u, v_1, \dots, v_n)]. \end{aligned}$$

Используя (10), получаем

$$\begin{aligned} \Pi_f(z) = [\langle \Pi_f(u), \pi_f(p) \rangle \mid u \in \text{Ra}(y) \text{ \& } \pi_f(p) \text{ } J\text{-вынуждает } \\ \Pi_f(u) \in \Pi_f(y) \text{ \& } \pi_f(p) \text{ } J\text{-вынуждает } Q(\Pi_f(u), \\ \Pi_f(v_1), \dots, \Pi_f(v_n))]. \end{aligned} \quad (20)$$

Если область изменения p состоит из всех условий, то область изменения $\pi_f(p)$ состоит из всех условий. Если область изменения u состоит из всех элементов множества $\text{Ra}(y)$, то область изменения $\Pi_f(u)$ состоит из всех элементов множества

$$[\Pi_f(w) \mid w \in \text{Ra}(y)] = \text{Ra}(\Pi_f(y)) = \text{Ra}(y).$$

Поэтому (20) показывает, что $\Pi_f(z) = z$.

Интерпретация аксиомы подмножества относительно J есть

$$U_J(y) \& U_J(v_1) \& \dots \& U_J(v_n) \rightarrow \\ \rightarrow \exists z (U_J(z) \& \forall x (U_J(x) \rightarrow (x \in_J z \leftrightarrow x \in_J y \& Q_J(u, v_1, \dots, v_n))))).$$

Она следует из леммы 4.

Определим

$$\mathfrak{Z}(z) = \text{Un} [\Pi_f(z) \mid f - \text{перестановка}].$$

Тогда

$$U_J(x) \& x \in_J z \rightarrow x \in_J \mathfrak{Z}(z). \quad (21)$$

Действительно, по предположению существует корректное условие p такое, что p J -вынуждает $x \in z$. По (10)

$$\pi_I(p) \text{ } J\text{-вынуждает } \Pi_I(x) \in \Pi_I(z).$$

Так как x инвариантно, это означает, что p J -вынуждает $x \in \Pi_I(z)$. Поэтому для некоторого y условие p J -вынуждает $x=y$ и $y \in_p \Pi_I(z)$. Тогда $y \in_p \mathfrak{Z}(z)$; следовательно, p J -вынуждает $x \in \mathfrak{Z}(z)$; таким образом, $x \in_J \mathfrak{Z}(z)$.

Теперь

$$\begin{aligned} \Pi_g(\mathfrak{Z}(z)) &= [\langle \Pi_g(x), \pi_g(p) \rangle \mid \langle x, p \rangle \in \mathfrak{Z}(z)]_{x,p} \\ &= [\langle \Pi_g(x), \pi_g(p) \rangle \mid \langle x, p \rangle \in \Pi_f(z)]_{x,p,f} \\ &= [\langle \Pi_{g \circ f}(x), \pi_{g \circ f}(p) \rangle \mid \langle x, p \rangle \in z]_{x,p,f} \\ &= [\langle \Pi_f(x), \pi_f(p) \rangle \mid \langle x, p \rangle \in z]_{x,p,f} = \mathfrak{Z}(z). \end{aligned}$$

(Здесь мы использовали то, что если область изменения f состоит из всех перестановок, то область изменения $g \circ f$ состоит из всех перестановок.) Поэтому $\mathfrak{Z}(z)$ инвариантно. Из этого

$$\forall y (y \in \text{Ra}(z) \rightarrow U_J(y)) \rightarrow U_J(\mathfrak{Z}(z)). \quad (22)$$

Действительно, если $x \in \text{Ra}(\mathfrak{Z}(z))$, то $x \in \text{Ra}(\Pi_f(z))$ для некоторого f ; поэтому $x = \Pi_f(y)$ для некоторого $y \in \text{Ra}(z)$; следовательно, $U_J(x)$ по (9).

Интерпретация аксиомы замены относительно J имеет посылки $U_J(w)$ и

$$\forall x (U_J(x) \rightarrow \exists u (U_J(u) \& \forall y (U_J(y) \rightarrow (y \in_J u \leftrightarrow Q_J(x, y))))) \quad (23)$$

и заключение

$$\begin{aligned} \exists z (U_J(z) \& \forall y (U_J(y) \rightarrow \exists x (U_J(x) \& x \in_J w \& Q_J(x, y)) \rightarrow \\ \rightarrow y \in_J z)) \end{aligned} \quad (24)$$

(здесь опущены параметры). Пусть $F(x, p)$ равно элементу u наименьшего порядка такому, что $U_J(u)$ и p J -вынуждает $\forall y (y \in u \leftrightarrow Q(x, y))$, если такое u существует. Как и в предыдущем параграфе,

$$\forall x (U_J(x) \rightarrow \exists p \forall y (U_J(y) \rightarrow (y \in_J F(x, p) \leftrightarrow Q_J(x, y)))). \quad (25)$$

Положим

$$z = \mathfrak{Z}(\text{Un} ([\text{Ra}(F(x, p)) \mid x \in \text{Ra}(w)]_{x,p} \times \text{CD})).$$

Так как $U_J(F(x, p))$, то каждый элемент из $\text{Ra}(F(x, p))$ есть U_J -множество. Из этого и (22) имеем $U_J(z)$. Остается показать, что

$$U_J(y) \& U_J(x) \& x \in_J w \& Q_J(x, y) \rightarrow y \in_J z.$$

Допуская посылки, выберем условие p , как в (25). Тогда $y \in_J F(x, p)$. По (16) из § 9.8 $y =_J y'$, где $y' \in \text{Ra}(F(x, p))$. По (17) из § 9.8 и (21) $y' \in_J z$; следовательно, $y \in_J z$.

Интерпретацией аксиомы степени относительно J является

$$\begin{aligned} U_J(y) \rightarrow \exists w (U_J(w) \& \forall x (U_J(x) \rightarrow \\ \rightarrow \forall z (U_J(z) \rightarrow z \in_J x \rightarrow z \in_J y) \rightarrow x \in_J w)). \end{aligned}$$

Пусть

$$w = \mathfrak{Z}([v \mid U_J(v) \& v \subset \text{Ra}(y) \times \text{CD}] \times \text{CD}).$$

Тогда $U_J(w)$ по (22). Предположим, что $U_J(x)$ и $z \in_J x \rightarrow z \in_J y$ для каждого U_J -множества z . Пусть

$$\begin{aligned} v = [\langle u, p \rangle \mid u \in \text{Ra}(y) \& p \text{ } J\text{-вынуждает } u \in y \& p \\ J\text{-вынуждает } u \in x]. \end{aligned}$$

Имеем $U_J(v)$ по лемме 4, и для каждого U_J -множества z

$$\begin{aligned} z \in_J v \leftrightarrow z \in_J y \& z \in_J x \\ \leftrightarrow z \in_J x. \end{aligned}$$

Таким образом, $v =_J x$ ввиду интерпретированной аксиомы объемности. Так как $v \subset \text{Ra}(y) \times \text{CD}$, то $v \in_J w$ по (17) из § 9.8 и (21); поэтому $x \in_J w$.

Имеем

$$\Pi_f(O(\sigma)) = [\Pi_f(O(\tau)) \mid \tau < \sigma] \times \text{CD}.$$

Из этого легко получаем

$$\Pi_f(O(\sigma)) = O(\sigma) \quad (26)$$

трансфинитной индукцией по σ . Поэтому $O(\sigma)$ инвариантно. Используя это, докажем

$$U_J(O(\sigma)) \quad (27)$$

трансфинитной индукцией по σ . Каждый элемент из $Ra(O(\sigma))$ есть $O(\tau)$ для некоторого $\tau < \sigma$ и поэтому есть U_J -множество по индуктивному предположению. Поэтому $O(\sigma)$ есть U_J -множество. Интерпретация аксиомы бесконечности следует из (27) и леммы 5 из § 9.8.

Остается доказать интерпретацию отрицания аксиомы выбора. В действительности мы докажем интерпретацию формулы

$$\neg \exists z CF(z, P(\omega)). \quad (28)$$

(Отметим, что в противоположность этому $\exists z CF(z, \omega)$ является теоремой теории ZF. Действительно, чтобы получить функцию выбора z на ω , положим $z'x$ наименьшему натуральному числу в x для $x \in P(\omega) - \{0\}$.)

Лемма 5. Пусть p — некоторое корректное условие и $k < i$. Тогда существует k -перестановка f такая, что $f'i \neq i$ и $\pi_f(p)$ имеет корректное расширение.

Доказательство. Пусть a — множество всех расширений условий $\pi_f(p)$, где f есть k -перестановка такая, что $f'i \neq i$. Мы хотим показать, что a содержит некоторое корректное условие. Предположим, что это не так. Тогда по Сог_4 существует корректное условие q , не имеющее расширений в a . По Сог_3 $p \cup q$ есть условие. Выберем j таким большим, что $i < j$ и никакое $\langle x, j \rangle$ не находится в $\text{Do}(p) \cup \text{Do}(q)$; пусть f — перестановка, меняющая местами i и j и оставляющая на месте все другие натуральные числа. Ясно, что $\pi_f(p) \cup q$ — условие. Это противоречит выбору q , так как f есть k -перестановка и $f'i \neq i$.

Если $CF(z, P(\omega))$, то

$$a \subset P(\omega) \text{ и } a \neq 0 \rightarrow \exists x (x \in a \text{ и } \text{Im}(z, a, x) \text{ и } \forall y (\text{Im}(z, a, y) \rightarrow y = x)).$$

Поэтому (28) следует из

$$\forall z \exists a (a \subset P(\omega) \text{ и } a \neq 0 \text{ и } \neg \exists x (x \in a \text{ и } \text{Im}(z, a, x) \text{ и } \forall y (\text{Im}(z, a, y) \rightarrow y = x))).$$

Тем самым нам нужно лишь доказать интерпретацию этого предложения. Если мы строим эту интерпретацию с помощью методов, уже применявшихся в этом параграфе, то мы

видим, что для каждого U_J -множества z должны построить U_J -множество a такое, что

$$U_J(x) \text{ и } x \in_J a \rightarrow x \subset_J O(\omega), \quad (29)$$

$$\exists x (U_J(x) \text{ и } x \in_J a), \quad (30)$$

и такое, что не существует U_J -множества x , для которого $x \in_J a$ и $\text{Im}_J(z, a, x) \text{ и } \forall y (U_J(y) \rightarrow \text{Im}_J(z, a, y) \rightarrow y =_J x)$. (31)

Определим

$$N(i) = [\langle O(j), p \rangle \mid p' \langle j, i \rangle = 1].$$

Как и раньше, из того, что p J -вынуждает $N(i) = N(j)$, следует $i = j$; поэтому

$$N(i) =_J N(j) \rightarrow i = j. \quad (32)$$

Кроме того, применяя (26) и определение $\pi_{f*}(q)$, получаем

$$\begin{aligned} \Pi_f(N(i)) &= [\langle O(j), \pi_f(p) \rangle \mid p' \langle j, i \rangle = 1] \\ &= [\langle O(j), q \rangle \mid \pi_{f*}(q)' \langle j, i \rangle = 1] \\ &= [\langle O(j), q \rangle \mid q' \langle j, f'i \rangle = 1]; \end{aligned}$$

поэтому

$$\Pi_f(N(i)) = N(f'i). \quad (33)$$

Отсюда следует, что $N(i)$ инвариантно. Из этого и (27) получаем $U_J(N(i))$.

Для данного U_J -множества z выберем k так, чтобы $\Pi_f(z) = z$ для каждой k -перестановки f , и положим

$$a = [N(i) \mid k < i] \times \text{CD}.$$

Каждый элемент из $Ra(a)$ есть некоторое $N(i)$ и, следовательно, U_J -множество. Применяя (33), видим, что $\Pi_f(a) = a$ для каждой k -перестановки f , поэтому a инвариантно и, следовательно, является U_J -множеством. Доказательство (29) подобно доказательству Б. Так как $N(S(i)) \in_J a$, то мы имеем (30).

Теперь допустим, что существует U_J -множество x , удовлетворяющее (31). В силу $x \in_J a$ имеем $x =_J N(i)$ для некоторого $i > k$. С таким же успехом мы можем предположить, что x есть $N(i)$. По лемме об истинности выберем корректное условие p так, чтобы p J -вынуждало $\forall y (\text{Im}(z, a, y) \rightarrow y = N(i))$. Выберем f , как в лемме 5, и пусть q — корректное расширение для $\pi_f(p)$. Так как

$\Pi_f(z) = z$, $\Pi_f(a) = a$ и $\Pi_f(N(i)) = N(f'i)$, то по (10) имеем q вынуждает $\forall y (\text{Im}(z, a, y) \rightarrow y = N(f'i))$.

Следовательно, по лемме об истинности

$$\forall y (U_J(y) \rightarrow \text{Im}_J(z, a, y) \rightarrow y = {}_J N(f'i)).$$

Подставляя $N(i)$ вместо y и применяя (31), получаем $N(i) = {}_J N(f'i)$. Так как $i \neq f'i$, это противоречит (32).

9.10. Большие кардиналы

Так как аксиомы теории ZFC не решают гипотезу континуума и аксиому конструктивности, естественно искать аксиомы, которые делают это. И гипотеза континуума и аксиома конструктивности ограничивают число множеств. Так, недоказуемая часть гипотезы континуума утверждает, что число подмножеств множества ω не превосходит $\aleph_1$. Поэтому если мы надеемся доказать эти результаты, то мы должны найти новые аксиомы, которые ограничивают число множеств.

Аксиома объемности показывает, что индивид определяется своими элементами и поэтому может быть отождествлен с семейством, членами которого являются эти элементы. Еще одно единственное ограничение, которое мы бы хотели сделать, относится к тому, что индивиды должны быть множествами, т. е. должны встречаться на некотором шаге нашей конструкции. Но мы покажем, что это может быть в действительности доказано в теории ZFC.

Напомним, что на каждом шаге строится ровно один новый ординал. Пусть S_σ — шаг, на котором строится σ , и пусть $\text{Stg}(\sigma)$ — множество всех множеств, которые могут быть построены на шаге S_σ . Мы можем определить Stg в теории ZFC трансфинитной индукцией следующим образом:

$$\text{Stg}(\sigma) = P(\text{Un}([\text{Stg}(\tau) \mid \tau < \sigma])). \quad (1)$$

Результат, который мы хотим доказать, состоит тогда в следующем:

$$\exists \sigma (x \in \text{Stg}(\sigma)). \quad (2)$$

Сначала докажем, что существует транзитивное множество, содержащее x . Определим трансфинитной индукцией

$$F(\sigma) = \text{Un}[\text{Un}(F(\tau)) \cup \{x\} \mid \tau < \sigma].$$

Ясно, что $x \in F(\omega)$. Если $z \in F(\omega)$, то $z \in \text{Un}(F(i)) \cup \{x\}$ для некоторого i . Тогда $z \in F(S(i))$, поэтому $z \in \text{Un}(F(S(i)))$; следовательно, $z \in F(\omega)$. Это показывает, что $F(\omega)$ транзитивно.

Теперь докажем (2). Пусть a — некоторое транзитивное множество, содержащее x , и пусть b — множество элементов множества a , которые не принадлежат ни одному из $\text{Stg}(\sigma)$. Если b пусто, то доказательство закончено. В противном случае пусть y — минимальный элемент множества b . Если $w \in y$, то $w \in a$ в силу транзитивности a , но $w \notin b$ по выбору y . Следовательно, $w \in \text{Stg}(\sigma_w)$ для некоторого σ_w . Пусть σ больше, чем любой ординал в $[\sigma_w \mid w \in y]$. Из (1) следует, что $y \in \text{Stg}(\sigma)$, а это противоречит тому, что $y \in b$.

Ввиду этого, по-видимому, остается мало надежд доказать гипотезу континуума или аксиому конструктивности, не изменяя нашего понятия множества. Если же мы попытаемся опровергнуть гипотезу континуума и аксиому конструктивности, то ситуация оказывается многообещающей. Ведь для этого нам нужны аксиомы, гарантирующие существование большого количества множеств. Но аксиомы существования из теории ZFC в некоторых отношениях являются совершенно недостаточными для этого. Например, аксиомы подмножеств в действительности не гарантируют существования всех подмножеств множества x , а только тех подмножеств, которые могут быть описаны в теории ZFC (используя параметры). Если бы мы ввели символы для новых операций, которые не могут быть определены в теории ZFC, то у нас возросла бы возможность описывать множества и, следовательно, возросла бы сила аксиом подмножеств (и аксиом замены). По-видимому, это очень естественный подход, но до сих пор никто не смог предложить подходящих операций.

Более обещающим в данный момент является следующий подход — более полно использовать наш принцип существования шагов: если мы можем представить ситуацию, когда все шаги некоторого семейства выполнены, то должен существовать шаг после шагов из этого семейства. В теории ZFC мы использовали лишь некоторые специальные случаи этого принципа. Но существование дальнейших шагов эквивалентно существованию больших ординалов или, так как для любого ординала существует больший кардинал, существованию больших кардиналов. Поэтому

мы должны искать аксиомы, гарантирующие существование кардиналов, больших чем те, существование которых может быть доказано в теории ZFC. Такие аксиомы будут называться *обобщенными аксиомами бесконечности*.

Рассмотрим, как мы можем получать кардиналы в теории ZFC. Мы получаем $\aleph_0$ из аксиомы бесконечности. Получив бесконечный кардинал σ , мы можем получить больший кардинал, переходя к 2^σ . Другой метод состоит в том, чтобы взять $\text{Un}(x)$, где x — некоторое множество кардиналов. Конечно, это может рассматриваться как метод получения нового кардинала только тогда, когда $\text{Un}(x)$ больше, чем каждый элемент из x , и больше также, чем $\text{Card}(x)$. Так может случиться; например, x может быть $[\aleph_\sigma \mid \sigma \in \omega]$, так что $\text{Un}(x) = \aleph_\omega$.

Скажем, что кардинал недостижим, если он не может быть получен этими методами. Точнее кардинал σ *недостижим*, если

- (i) $\omega < \sigma$;
- (ii) $\tau < \sigma \rightarrow 2^\tau < \sigma$ для каждого кардинала τ ;
- (iii) $\text{Card}(x) < \sigma \rightarrow \text{Un}(x) < \sigma$ для каждого подмножества x из σ .

Нашей первой обобщенной аксиомой бесконечности будет *аксиома недостижимости*, утверждающая, что существует недостижимый кардинал. Сразу не ясно, что это действительно новая аксиома; может быть, мы можем доказать ее в теории ZFC, используя конструкции, отличные от рассмотренных выше. Однако мы докажем, что это не так: если теория ZFC непротиворечива, то аксиома недостижимости не является теоремой ZFC. Чтобы доказать это, строим интерпретацию теории ZFC в теории ZFC, для которой выполняется интерпретация отрицания аксиомы недостижимости.

Рангом множества x назовем первый ординал σ такой, что $x \in \text{Stg}(\sigma)$:

$$\text{rk}(x) = \mu\sigma (x \in \text{Stg}(\sigma)).$$

Тогда

$$x \in y \rightarrow \text{rk}(x) < \text{rk}(y). \quad (3)$$

Имеем $y \in \text{Stg}(\text{rk}(y))$, поэтому если $x \in y$, то по (1) $x \in \text{Stg}(\sigma)$ для некоторого $\sigma < \text{rk}(y)$. Следовательно, $\text{rk}(x) \leq \sigma < \text{rk}(y)$. Кроме того, $\text{Set}_x(\text{rk}(x) \leq \sigma)$, так как

$$\text{rk}(x) \leq \sigma \rightarrow x \in \text{Un}([\text{Stg}(\tau) \mid \tau \leq \sigma]).$$

Таким образом, мы можем давать определения индукцией по $\text{rk}(x)$.

Мы пишем $\text{Inac}(\sigma)$ для обозначения того, что σ — недостижимый кардинал. Скажем, что множество x *достижимо*, если $\text{Card}(x)$ меньше, чем каждый недостижимый кардинал:

$$\text{Ac}(x) \leftrightarrow \forall \sigma (\text{Inac}(\sigma) \rightarrow \text{Card}(x) < \sigma).$$

Затем определяем M индукцией по $\text{rk}(x)$ следующим образом:

$$M(x) \leftrightarrow \text{Ac}(x) \& \forall y (y \in x \leftrightarrow M(y)). \quad (4)$$

Ясно, что $M(0)$, поэтому $\exists x M(x)$ и, следовательно, M есть $\in$ -интерпретация. M транзитивно по (4). Так как подмножество достижимого множества достижимо, то из (4) следует, что M супертранзитивно.

Лемма 1. Если x *достижимо* и каждый элемент множества x *достижим*, то $\text{Un}(x)$ *достижимо*.

Доказательство. Пусть $\text{Inac}(\sigma)$. Тогда $\text{Card}(x) < \sigma$ и $\text{Card}(y) < \sigma$ для каждого элемента y множества x . Отсюда следует, что

$$\text{Card}(\text{Un}(x)) \leq \sigma \cdot \sigma = \sigma.$$

Поэтому мы можем предположить, что $\text{Un}(x)$ — подмножество кардинала σ . Если $y \in x$, то $y \subset \sigma$ и $\text{Card}(y) < \sigma$, поэтому $\text{Un}(y) < \sigma$. Так как $\text{Card}([\text{Un}(y) \mid y \in x]) \leq \leq \text{Card}(x) < \sigma$, то

$$\tau = \text{Un}([\text{Un}(y) \mid y \in x]) < \sigma.$$

Если $\rho \in \text{Un}(x)$, то $\rho \in y$ для некоторого $y \in x$, поэтому $\rho \leq \text{Un}(y) \leq \tau$. Отсюда следует, что $\text{Un}(x) \subset S(\tau)$; следовательно,

$$\begin{aligned} \text{Card}(\text{Un}(x)) &\leq \text{Card}(S(\tau)) = \\ &= \text{Card}(\tau) + 1 \leq \text{Max}(\langle \text{Card}(\tau), \omega \rangle) < \sigma. \end{aligned}$$

Теперь докажем интерпретации всех аксиом теории ZF посредством лемм из § 9.5. Интерпретации аксиом объемности и регулярности выполняются, потому что M транзитивно. Для аксиом подмножеств мы должны показать, что если $y, v_1, \dots, v_n$ являются M -множествами, то

$$z = [x \mid x \in y \& Q_M(x, v_1, \dots, v_n)]$$

есть M -множество. Так как $z \subset y$, то это следует из супертранзитивности M .

Для аксиом замены достаточно показать, что если F является M -инвариантным и $\omega, v_1, \dots, v_n$ являются M -множествами, то

$$z = \text{Un}([F(x, v_1, \dots, v_n) \mid x \in \omega])$$

есть M -множество. Из транзитивности M и M -инвариантности F находим, что каждый элемент множества z есть M -множество. По лемме 1 множество z достижимо. Поэтому z является M -множеством.

Для аксиомы степени мы должны показать, что если y есть M -множество, то

$$z = [x \mid M(x) \text{ и } x \subset y]$$

есть M -множество. Очевидно, что каждый элемент множества z есть M -множество, поэтому нам нужно только показать, что z достижимо. Пусть σ — недостижимый кардинал. Тогда $\text{Card}(y) < \sigma$, поэтому

$$\text{Card}(z) \leq \text{Card}(P(y)) = 2^{\text{Card}(y)} < \sigma.$$

Если σ меньше, чем каждый недостижимый кардинал, то σ есть M -множество; это легко доказывается трансфинитной индукцией. Поэтому $M(\omega)$. Это дает интерпретацию аксиомы бесконечности.

Так как CF абсолютно, то интерпретацией аксиомы выбора является

$$\forall x (M(x) \rightarrow \exists y (M(y) \text{ и } \text{CF}(y, x))).$$

Так как CF полно (для супертранзитивных интерпретаций), то эта формула эквивалентна

$$\forall x (M(x) \rightarrow \exists y \text{CF}(y, x)).$$

Но это — следствие аксиомы выбора.

Мы должны еще доказать интерпретацию отрицания аксиомы недостижимости. Определяющей аксиомой для Inac является

$$\text{Inac}(\sigma) \leftrightarrow \text{Cd}(\sigma) \text{ и } \omega < \sigma \text{ и } \forall \tau (\tau < \sigma \text{ и } \text{Cd}(\tau) \rightarrow 2^\tau < \sigma) \text{ и } \forall x (x \subset \sigma \text{ и } \text{Card}(x) < \sigma \rightarrow \text{Un}(x) < \sigma).$$

Используя результаты из § 9.5, выводим, что Inac абсолютно для супертранзитивных интерпретаций. Так как отрицание аксиомы недостижимости есть

$$\neg \exists x \text{Inac}(x),$$

то интерпретация этой формулы эквивалентна

$$\neg \exists x (M(x) \text{ и } \text{Inac}(x)).$$

Это очевидно, так как если $M(x) \text{ и } \text{Inac}(x)$, то $x = \text{Card}(x) < x$.

Аксиома недостижимости, хотя и недоказуемая в теории ZFC, удовлетворяет нашим общим принципам, так как мы можем, конечно, представить ситуацию, в которой операции, описанные выше для получения новых кардиналов, были проделаны до тех пор, пока новые кардиналы не перестанут получаться этим способом. Мы можем даже надеяться доказать непротиворечивость этой аксиомы. Точнее, мы можем надеяться доказать, что если теория ZFC непротиворечива, то такова же и теория ZFI, полученная из ZFC добавлением аксиомы недостижимости. Однако такое доказательство не может быть проведено в теории ZFC по причинам, которые мы теперь кратко обсудим.

Суть заключается в том, что непротиворечивость теории ZFC может быть доказана в теории ZFI. Пусть в теории ZFI σ означает первый недостижимый кардинал. Тогда $\text{rk}(x) < \sigma$ для каждого M -множества x , что легко доказать индукцией по $\text{rk}(x)$. Отсюда следует, что $\text{Set}_x M(x)$. Это означает, что в теории ZFI мы можем построить структуру теории ZFC, универсум которой есть $[x \mid M(x)]$ и $\in$ -отношением является обычное $\in$ -отношение. Мы можем по существу использовать только что данное доказательство, чтобы доказать, что эта структура является моделью теории ZFC. Затем мы можем доказать теорему истинности в теории ZFI и вывести, что ZFC непротиворечива.

Предположим, что утверждение *если теория ZFC непротиворечива, то теория ZFI непротиворечива* доказуемо в теории ZFC или даже в теории ZFI. Тогда непротиворечивость теории ZFI была бы доказуемой в теории ZFI; тогда отсюда по теореме о доказательствах непротиворечивости следовало бы, что теория ZFI противоречива.

Следующий и наиболее важный вопрос состоит в следующем: могут ли гипотеза континуума и аксиома конструктивности быть доказаны или опровергнуты в теории ZFI? К сожалению, ответ отрицательный. Доказательство в основном такое же, как и для теории ZFC. Новым является

лишь доказательство аксиомы недостижимости, а для этого не требуется ничего существенно нового.

Имеется много обобщенных аксиом бесконечности подобного типа. Например, мы могли бы предположить существование двух недостижимых кардиналов. Можно доказать, как и раньше, что эта аксиома недоказуема в теории ZFI. Мы могли бы предположить более сильные аксиомы; например, что кардинал множества недостижимых кардиналов сам недостижим. Однако никакая из таких аксиом не годится для решения вопроса о справедливости гипотезы континуума или аксиомы конструктивности.

Теперь мы введем одну аксиому, которая приводит к опровержению аксиомы конструктивности. Перед тем, как привести эту аксиому, нам будут нужны некоторые определения.

Под *измеримым идеалом* на множестве x мы понимаем подмножество y из $P(x)$ такое, что

(i) для каждого подмножества z множества y такого, что $\text{Card}(z) < \text{Card}(x)$, выполняется $\text{Un}(z) \in y$;

(ii) для каждого подмножества z множества x либо $z \in y$, либо $x - z \in y$;

(iii) $\text{Un}(y) = x$;

(iv) $x \notin y$.

Можно считать, что измеримый идеал на x разделяет подмножества множества x на маленькие и большие подмножества: подмножества из измеримого идеала являются маленькими, а оставшиеся подмножества являются большими.

Множество x называется *измеримым*, если оно несчетно и существует измеримый идеал на x . Ясно, что каждое множество, подобное измеримому множеству, измеримо, поэтому мы можем рассматривать только измеримые кардиналы. Аксиома измеримости утверждает, что существует измеримый кардинал.

Сразу неясно, что аксиома измеримости является обобщенной аксиомой бесконечности. Однако мы увидим, что измеримые кардиналы чрезвычайно большие, значительно больше, чем любой из кардиналов, которые мы до сих пор рассматривали. С другой стороны, исследования не выявили противоречий или даже неправдоподобных результатов, следующих из этой аксиомы. Это по крайней мере наводит на мысль, что аксиома измеримости является просто очень

сильной обобщенной аксиомой бесконечности. А если это так, то было бы разумно допустить эту новую аксиому.

Пусть ZFM — теория, полученная из ZFC добавлением аксиомы измеримости. Пусть ZFM* — теория, полученная из ZFM добавлением двух констант χ и V и аксиом, утверждающих, что χ — несчетный кардинал и V — измеримый идеал на χ . По теореме о функциональном расширении теория ZFM* является консервативным расширением теории ZFM. Докажем теперь некоторые результаты в теории ZFM*.

$$x \in V \text{ \& } y \subset x \rightarrow y \in V. \quad (5)$$

Действительно, если $y \notin V$, то $\chi - y \in V$ по (ii); поэтому $\chi = (\chi - y) \cup x \in V$ по (i), что противоречит (iv).

$$x \subset \chi \text{ \& } \text{Card}(x) < \chi \rightarrow x \in V. \quad (6)$$

Если $\sigma < \chi$, то $\{\sigma\} \in V$ по (iii) и (5). Тогда (6) получаем из (i).

$$x \subset \chi \rightarrow (x \in V \leftrightarrow \chi - x \notin V). \quad (7)$$

Ввиду (ii) нам нужно лишь вывести противоречие из $x \in V$ и $\chi - x \in V$. Но из них следует $\chi \in V$ по (i), что противоречит (iv).

$$x \subset \chi \text{ \& } y \subset \chi \rightarrow (x \cap y \in V \leftrightarrow x \in V \vee y \in V). \quad (8)$$

Если $x \in V$ или $y \in V$, то $x \cap y \in V$ по (5). Теперь предположим, что $x \cap y \in V$, $x \notin V$ и $y \notin V$. По (7) и (i) $\chi = (x \cap y) \cup (\chi - x) \cup (\chi - y) \in V$, что противоречит (iv).

Теорема Банаха — Улама. Кардинал χ недостижим.

Доказательство. Пусть σ — некоторый кардинал такой, что $\sigma < \chi$; мы должны показать, что $2^\sigma < \chi$. Предположим, что $\chi \leq 2^\sigma$. Тогда существует инъективное отображение f из χ в $P(\sigma)$. Для $\tau < \sigma$ положим

$$z_\tau = \{p \mid p < \chi \text{ \& } \tau \in f^*p\}.$$

Пусть $y_\tau = z_\tau$, если $z_\tau \in V$, и $y_\tau = \chi - z_\tau$ в противном случае. Тогда $y_\tau \in V$ по (7). Так как $\text{Card}(\sigma) \leq \sigma < \chi$, имеем $\text{Un}(\{y_\tau \mid \tau < \sigma\}) \in V$ по (i). Покажем, что самое большее один элемент из χ не находится в $\text{Un}(\{y_\tau \mid \tau < \sigma\})$. Вместе с (6) и (i) это дает $\chi \in V$, что противоречит (iv).

Предположим, что ρ не принадлежит ни одному y_τ . Тогда для каждого τ

$$\begin{aligned}\tau \in f'\rho &\leftrightarrow \rho \in z_\tau \\ &\leftrightarrow y_\tau = \chi - z_\tau \\ &\leftrightarrow z_\tau \notin V.\end{aligned}$$

Следовательно, $f'\rho = [\tau | \tau < \sigma \& z_\tau \notin V]$. Это определяет $f'\rho$ и, следовательно, ρ .

Теперь пусть $x \subset \chi$ и $\text{Card}(x) < \chi$; мы должны показать, что $\text{Un}(x) < \chi$. Каждый элемент из χ есть некоторый ординал, меньший χ , и поэтому является подмножеством из χ , кардинал которого меньше χ . По (6) каждый элемент из χ лежит в V ; следовательно, $\text{Un}(x) \in V$ по (i). Тогда $\text{Un}(x) \neq \chi$ по (iv). Так как ясно, что $\text{Un}(x) \leq \chi$, то мы имеем $\text{Un}(x) < \chi$.

Теперь обратимся к определению интерпретации теории ZFM в теории ZFM*. Интерпретация I определяется так:

$$\begin{aligned}x \in_I y &\leftrightarrow [\sigma | \sigma < \chi \& x'\sigma \notin y'\sigma] \in V, \\ x =_I y &\leftrightarrow [\sigma | \sigma < \chi \& x'\sigma \neq y'\sigma] \in V, \\ U_I(x) &\leftrightarrow x = x.\end{aligned}$$

Вначале докажем, что для каждого предикатного символа Q теории ZFM

$$Q_I(x_1, \dots, x_n) \leftrightarrow [\sigma | \sigma < \chi \& \bigwedge Q(x'_1\sigma, \dots, x'_n\sigma)] \in V. \quad (9)$$

Используем индукцию по предикатным символам. Если

$$Q(x_1, \dots, x_n) \leftrightarrow x_i \in x_j$$

или

$$Q(x_1, \dots, x_n) \leftrightarrow x_i = x_j,$$

то результат следует из определений $\in_I$ и $=_I$. Предположим, что

$$Q(x_1, \dots, x_n) \leftrightarrow \neg R(x_1, \dots, x_n).$$

Тогда по индуктивному предположению и (7)

$$\begin{aligned}Q_I(x_1, \dots, x_n) &\leftrightarrow \neg R_I(x_1, \dots, x_n) \\ &\leftrightarrow [\sigma | \sigma < \chi \& \neg R(x'_1\sigma, \dots, x'_n\sigma)] \notin V \\ &\leftrightarrow [\sigma | \sigma < \chi \& \neg Q(x'_1\sigma, \dots, x'_n\sigma)] \in V.\end{aligned}$$

Если Q — дизъюнкция, то доказательство аналогично, только используется (8) вместо (7). Теперь предположим, что

$$Q(x_1, \dots, x_n) \leftrightarrow \exists y R(y, x_1, \dots, x_n).$$

Тогда

$$\begin{aligned}Q_I(x_1, \dots, x_n) &\leftrightarrow \exists y R_I(y, x_1, \dots, x_n) \\ &\leftrightarrow \exists y ([\sigma | \sigma < \chi \& \bigwedge R(y'\sigma, x'_1\sigma, \dots, x'_n\sigma)] \in V).\end{aligned}$$

Положим

$$\begin{aligned}a_y &= [\sigma | \sigma < \chi \& \bigwedge R(y'\sigma, x'_1\sigma, \dots, x'_n\sigma)], \\ a &= [\sigma | \sigma < \chi \& \bigwedge \exists z R(z, x'_1\sigma, \dots, x'_n\sigma)].\end{aligned}$$

Мы должны показать, что $\exists y (a_y \in V)$ тогда и только тогда, когда $a \in V$. Так как $a \subset a_y$ для всех y , то

$$\exists y (a_y \in V) \rightarrow a \in V$$

по (5). Теперь предположим, что $a \in V$. Если $\sigma < \chi$ и $\sigma \notin a$, то существует z_σ такое, что $R(z_\sigma, x'_1\sigma, \dots, x'_n\sigma)$. Пусть y таково, что $y'\sigma = z_\sigma$ для $\sigma < \chi$ и $\sigma \notin a$. Тогда $a_y \subset a$, поэтому $a_y \in V$ по (5).

Из (9) следует, что

$$Q_I(\{x_1\} \times \chi, \dots, \{x_n\} \times \chi) \leftrightarrow [\sigma | \sigma < \chi \& \bigwedge Q(x_1, \dots, x_n)] \in V.$$

Теперь $[\sigma | \sigma < \chi \& \bigwedge Q(x_1, \dots, x_n)]$ есть 0 или χ в соответствии с тем, выполняется ли $Q(x_1, \dots, x_n)$ или $\neg Q(x_1, \dots, x_n)$. Так как $0 \in V$ и $\chi \notin V$ по (iv) и (7), то

$$Q_I(\{x_1\} \times \chi, \dots, \{x_n\} \times \chi) \leftrightarrow Q(x_1, \dots, x_n). \quad (10)$$

В частности, отсюда следует, что $Q_I \leftrightarrow Q$ для 0-местного Q . Как мы видели в § 9.7, отсюда следует, что I — интерпретация теории ZFM.

Теперь мы собираемся показать, что I изоморфна транзитивной $\in$ -интерпретации. Ввиду результатов из § 9.5 достаточно показать, что I изоморфна интерпретации J , где $=_J$ есть $=$ и существует ординальный функциональный символ H такой, что $\text{Set}_x(H(x) \leq \sigma)$ и $x \in_J y \rightarrow \neg H(x) < H(y)$.

Имеем

$$x =_I x, \quad (11)$$

$$x =_I y \rightarrow y =_I x, \quad (12)$$

$$x =_I y \& y =_I z \rightarrow x =_I z. \quad (13)$$

Действительно, эти формулы являются интерпретациями теорем теории ZF. Хотя $=_I$ имеет свойства отношения эквивалентности, мы не можем использовать классы эквивалентности в их обычном смысле, так как они не являются множествами. Поэтому мы определяем класс эквивалент-

ности $EC(x)$ как множество всех $y \in Stg(\sigma)$ таких, что $x =_I y$, где σ — первый ординал такой, что $\exists y (y \in Stg(\sigma) \& x =_I y)$. (Такой ординал существует в силу (11).) Используя (11)–(13), легко доказать основное свойство классов эквивалентности:

$$EC(x) = EC(y) \leftrightarrow x =_I y. \quad (14)$$

Теперь определим интерпретацию J так:

$$x \in_J y \leftrightarrow \exists x' \exists y' (x = EC(x') \& y = EC(y') \& x' \in_I y'),$$

$$x =_J y \leftrightarrow x = y,$$

$$U_J(x) \leftrightarrow \exists x' (x = EC(x')).$$

Мы утверждаем, что EC — изоморфизм между I и J . Ввиду (14) и определения U_J для этого необходимо лишь доказать

$$x \in_I y \leftrightarrow EC(x) \in_J EC(y). \quad (15)$$

Импликация слева направо очевидна. Предположим, что $EC(x) \in_J EC(y)$. Тогда $EC(x) = EC(x')$, $EC(y) = EC(y')$ и $x' \in_I y'$. По (14) $x =_I x'$ и $y =_I y'$. Поэтому нам нужно доказать только

$$x =_I x' \& y =_I y' \& x' \in_I y' \rightarrow x \in_I y.$$

Но это интерпретация теоремы теории ZF.

Мы должны еще определить H . Сначала определим трансфинитной индукцией

$$Z(\sigma) = [x \mid x \in Stg(\sigma) \& \forall y (y \in_J x \rightarrow \exists \tau (\tau < \sigma \& y \in Z(\tau)))].$$

Мы покажем, что каждое множество принадлежит некоторому $Z(\sigma)$. Тогда определим

$$H(x) = \mu \sigma (x \in Z(\sigma)). \quad (16)$$

Тогда $Set_x(H(x) \leq \sigma)$, потому что

$$H(x) \leq \sigma \rightarrow x \in Un([Z(\tau) \mid \tau < S(\sigma)]);$$

и $x \in_J y \rightarrow H(x) < H(y)$ следует из определения Z .

Допустим, что x не находится ни в одном из $Z(\sigma)$, и приходим к противоречию. Если $\neg U_J(x)$, то $\forall y (y \notin_J x)$ и поэтому $x \in Z(rk(x))$. Таким образом, $U_J(x)$; следовательно, $x = EC(y)$ для некоторого y . Выбираем σ большим каждого кардинала в $[rk(z) \mid z \in Ra(y)]$. Тогда если $z \in Ra(y)$, то $z \in Stg(rk(z)) \subset Stg(\sigma)$. Поэтому, если $y' =$

$= y \cap (Stg(\sigma) \times \chi)$, то мы имеем $y' =_I y$ и, следовательно, $x = EC(y')$. Это показывает, что множество

$$a = [EC(u) \mid u \subset Stg(\sigma) \times \chi]$$

содержит элемент, не находящийся ни в одном из $Z(\sigma)$.

Далее мы заметим, что если $y \in a$ и $z \in_J y$, то $z \in a$. Действительно, мы имеем $y = EC(u)$, где $u \subset Stg(\sigma) \times \chi$. По (15) $z = EC(v)$, где $v \in_J u$. Пусть $v' = \langle v', \tau, \tau \rangle$, где $\tau < \chi$ и $v' \tau \in u' \tau$. Ясно, что $v' =_I v$, поэтому $z = EC(v')$. По (3) $v' \subset Stg(\sigma) \times \chi$; следовательно, $z \in a$.

Если $y \in a$ и y не находится ни в одном из $Z(\tau)$, то существует $z \in a$ такое, что $z \in_J y$ и z не находится ни в одном из $Z(\tau)$. Действительно, предположим, что это не так. Тогда для каждого $z \in_J y$ имеем $z \in a$, и поэтому $z \in Z(\tau_z)$ для некоторого τ_z . Выберем τ большим каждого ординала в $[\tau_z \mid z \in_J y \& z \in a]$ и большим $rk(y)$. Тогда $y \in Z(\tau)$, что противоречит предположению.

Применяя доказанные результаты и аксиому выбора, найдем последовательность $y'_0, y'_1, \dots$ элементов из a таких, что y'_i не находится ни в одном из $Z(\tau)$ и $y_{S(i)} \in_J y'_i$. Тогда, если $y'_i = EC(y_i)$, то по (15)

$$y_{S(i)} \in_I y'_i$$

и

$$[\rho \mid \rho < \chi \& y'_{S(i)} \rho \notin y'_i \rho] \in V$$

для всех i . Так как $\omega < \chi$, то объединение этих множеств находится в V и, следовательно, не равно χ . Поэтому существует $\rho < \chi$ такое, что $y'_{S(i)} \rho \in y'_i \rho$ для всех i . Это означает, что множество $[y'_i \rho \mid i \in \omega]$ не имеет минимального элемента. Таким образом, мы добились требуемого противоречия.

Мы делаем вывод, что существует транзитивная $\in$ -интерпретация M и изоморфизм G между I и M . Определим

$$F(x) = G(\{x\} \times \chi).$$

Тогда из (10) и того, что G — изоморфизм, имеем

$$Q_M(F(x_1), \dots, F(x_n)) \leftrightarrow Q(x_1, \dots, x_n). \quad (17)$$

$F(x_1), \dots, F(x_n)$ являются M -множествами, поэтому, когда Q абсолютно для M , мы можем опускать индекс M . В частности,

$$F(x) \in F(y) \leftrightarrow x \in y, \quad (18)$$

$$Ord(F(x)) \leftrightarrow Ord(y). \quad (19)$$

Имеем

$$G(y) \in F(x) \& \text{Card}(x) < \chi \rightarrow \exists z (z \in x \& G(y) = F(z)). \quad (20)$$

В самом деле, допустим посылку. Так как G — изоморфизм, то

$$y \in {}_I\{x\} \times \chi,$$

поэтому

$$[\sigma \mid \sigma < \chi \& y' \sigma \in x] \notin V$$

по (7). Но

$$[\sigma \mid \sigma < \chi \& y' \sigma \in x] = \text{Un}[a_z \mid z \in x],$$

где

$$a_z = [\sigma \mid \sigma < \chi \& y' \sigma = z].$$

Так как $\text{Card}(x) < \chi$, то из (i) следует, что для некоторого $z \in x$ имеем $a_z \notin V$. Из этого и (7) имеем $y = {}_I\{z\} \times \chi$. Применяя изоморфизм G , имеем $G(y) = F(z)$.

Используем это, чтобы доказать

$$\text{Card}(x) < \chi \& \forall z (z \in x \rightarrow F(z) = z) \rightarrow F(x) = x. \quad (21)$$

Допустим, что посылка верна. Если $z \in x$, то $F(z) = z$ по предположению и $F(z) \in F(x)$ по (18); следовательно, $z \in F(x)$. Это доказывает, что $x \subset F(x)$. Теперь пусть $u \in F(x)$. Так как имеет место $M(F(x))$ и M транзитивно, то u есть M -множество, поэтому $u = G(y)$ для некоторого y . По (20) $u = F(z)$ для некоторого $z \in x$. Но $F(z) = z$ по предположению, поэтому $u \in x$. Следовательно, $F(x) \subset x$.

Из (21) мы легко доказываем трансфинитной индукцией, что

$$\sigma < \chi \rightarrow F(\sigma) = \sigma. \quad (22)$$

С другой стороны, мы докажем, что

$$\chi < F(\chi). \quad (23)$$

Действительно, пусть $i = [\langle \sigma, \sigma \rangle \mid \sigma < \chi]$. Тогда ясно, что $i \in {}_I\{\chi\} \times \chi$. Применяя G , получим $G(i) \in F(\chi)$. Так как $F(\chi)$ — ординал по (19), то $G(i)$ — ординал и

$$G(i) < F(\chi). \quad (24)$$

Теперь предположим, что $\sigma < \chi$. Тогда

$$[\tau \mid \tau < \chi \& \sigma \notin i' \tau] = \sigma \cup \{\sigma\}$$

и $\sigma \cup \{\sigma\} \in V$ по (6) и (i). Следовательно, $\{\sigma\} \times \chi \in {}_I i$. Применяя G , получим $F(\sigma) \in G(i)$. Используя (22), получаем

$\sigma < G(i)$. Таким образом, $\sigma < \chi \rightarrow \sigma < G(i)$. Подставляя $G(i)$ вместо σ , видим, что $\chi \leq G(i)$. Из этого и (24) получаем (23).

Лемма 2. Пусть M — транзитивная интерпретация теории ZFC. Тогда

$$M(\sigma) \& \text{Inac}(\sigma) \rightarrow \text{Inac}_M(\sigma).$$

Доказательство. Взяв интерпретацию определяющей аксиомы для Sm и используя наши результаты об абсолютности, получаем

$$\text{Sm}_M(x, y) \leftrightarrow \exists z (M(z) \& \text{IFunc}(z) \& \text{Do}(z) = x \& \text{Ra}(z) = y)$$

для M -множеств x и y . Поэтому

$$M(x) \& M(y) \& \text{Sm}_M(x, y) \rightarrow \text{Sm}(x, y). \quad (25)$$

Взяв интерпретацию теоремы

$$\text{Ord}(\text{Card}(x)) \& \text{Sm}(\text{Card}(x), x)$$

и используя (25), получаем

$$M(x) \rightarrow \text{Ord}(\text{Card}_M(x)) \& \text{Sm}(\text{Card}_M(x), x),$$

поэтому

$$M(x) \rightarrow \text{Ord}(\text{Card}_M(x)) \& \text{Card}(x) \leq \text{Card}_M(x). \quad (26)$$

Интерпретация теоремы $\sigma \leq \text{Card}(\sigma) \rightarrow \text{Cd}(\sigma)$ дает

$$\sigma \leq \text{Card}_M(\sigma) \rightarrow \text{Cd}_M(\sigma)$$

для M -множества σ . Если $\text{Cd}(\sigma)$, то

$$\sigma = \text{Card}(\sigma) \leq \text{Card}_M(\sigma)$$

по (26); следовательно,

$$M(\sigma) \& \text{Cd}(\sigma) \rightarrow \text{Cd}_M(\sigma). \quad (27)$$

По (10) из § 9.5 и абсолютности $\subset$ имеем

$$P_M(x) = [y \mid M(y) \& y \subset x]$$

для M -множества x ; следовательно,

$$M(x) \rightarrow P_M(x) \subset P(x). \quad (28)$$

Интерпретация определяющей аксиомы для Inac утверждает, что для M -множества σ

$$\text{Inac}_M(\sigma) \leftrightarrow \text{Cd}_M(\sigma) \& \omega < \sigma$$

$$\& \forall \tau (\text{Cd}_M(\tau) \& \tau < \sigma \rightarrow \text{Card}_M(P_M(\tau)) < \sigma)$$

$$\& \forall x (M(x) \& x \subset \sigma \& \text{Card}_M(x) < \sigma \rightarrow \text{Un}(x) < \sigma).$$

Мы должны показать, что если σ недостижимо, то правая часть выполняется. По (27) $\text{Cd}_M(\sigma)$ и ясно, что $\omega < \sigma$. Предположим, что $\text{Cd}_M(\tau)$ и $\tau < \sigma$. Тогда $\text{Card}(\tau) < \sigma$, поэтому

$$\text{Card}(P(\tau)) = 2^{\text{Card}(\tau)} < \sigma.$$

Следовательно, по (28) $\text{Card}(P_M(\tau)) < \sigma$. Из этого и (25) следует, что

$$\neg \exists y (M(y) \& y \subset P_M(\tau) \& \text{Sm}_M(\sigma, y)).$$

Если мы возьмем интерпретацию теоремы

$$\neg \exists y (y \subset P(\tau) \& \text{Sm}(\sigma, y) \& \text{Cd}(\sigma) \rightarrow \text{Card}(P(\tau)) < \sigma,$$

то мы получим, что $\text{Card}_M(P_M(\tau)) < \sigma$.

Наконец, предположим, что $M(x)$, $x \subset \sigma$ и $\text{Card}_M(x) < \sigma$. По (26) $\text{Card}(x) < \sigma$; следовательно, $\text{Up}(x) < \sigma$.

Теорема Ханфа—Тарского. Кардинал множества всех недостижимых чисел, меньших χ , есть χ .

Доказательство. Определим Q так:

$$Q(\tau, a) \leftrightarrow \forall \sigma (\text{Inac}(\sigma) \& \sigma < \tau \rightarrow \sigma \in a).$$

Из (17) имеем

$$Q_M(F(\chi), F(a)) \leftrightarrow Q(\chi, a),$$

т. е.

$$\begin{aligned} \forall \sigma (M(\sigma) \& \text{Inac}_M(\sigma) \& \sigma < F(\chi) \rightarrow \sigma \in F(a)) \leftrightarrow \\ \leftrightarrow \forall \sigma (\text{Inac}(\sigma) \& \sigma < \chi \rightarrow \sigma \in a). \end{aligned}$$

Взяв в качестве a множество всех недостижимых кардиналов, меньших χ , находим, что правая часть, конечно, выполняется, поэтому левая часть также выполняется. Подставляя χ вместо σ , получаем

$$M(\chi) \& \text{Inac}_M(\chi) \& \chi < F(\chi) \rightarrow \chi \in F(a).$$

Теперь по (23) имеем $\chi < F(\chi)$. Так как $M(F(\chi))$ и M транзитивно, то из этого следует $M(\chi)$. Также $\text{Inac}_M(\chi)$ по лемме 2 и теореме Банаха—Улама. Таким образом, мы имеем $\chi \in F(a)$. Но $\chi \notin a$; следовательно, $F(a) \neq a$. Если $x \in a$, то x — кардинал, меньший χ ; следовательно, $F(x) = x$ по (22). Из этих фактов и (21) заключаем, что $\chi \leq \text{Card}(a)$. Так как $a \subset \chi$, то мы имеем $\text{Card}(a) = \chi$.

Вышеприведенная теорема является обещанным результатом, показывающим, как велики должны быть измеримые кардиналы. В действительности, теми же методами были

доказаны еще более сильные результаты в этом же направлении.

Теорема Скотта. Отрицание аксиомы конструктивности является теоремой теории ZFM.

Доказательство. Добавим к теории ZFM* аксиому, утверждающую, что χ — первый измеримый кардинал. Это будет всё еще консервативным расширением теории ZFM, поэтому вышеприведенные результаты остаются справедливыми.

По (19) $\text{Ord}(F(\sigma))$ для всех σ . Кроме того, $\sigma \leq F(\sigma)$ для всех σ . Так как иначе существовал бы первый ординал σ такой, что $F(\sigma) < \sigma$. По (18) $F(F(\sigma)) < F(\sigma)$. Это и $F(\sigma) < \sigma$ противоречат выбору σ . Из $\sigma \leq F(\sigma)$ и транзитивности M выводим, что $M(\sigma)$ для всех σ . Далее, C является абсолютным и, следовательно, M -инвариантным, поэтому $M(C(\sigma))$ для всех σ . Это показывает, что каждое конструктивное множество является M -множеством.

Поэтому достаточно будет получить противоречие из предположения $\forall x M(x)$. Из этого предположения следует, что $Q_M(x) \leftrightarrow Q(x)$ для всех Q и x . Следовательно, по (17) имеем $Q(F(x)) \leftrightarrow Q(x)$ для всех Q и x . Если $Q(x)$ будет означать, что x — первый измеримый ординал, то $Q(F(x)) \leftrightarrow Q(x)$ для всех x ; следовательно, $Q(F(\chi)) \leftrightarrow Q(\chi)$. Но $Q(\chi)$ истинно, хотя $Q(F(\chi))$ ложно по (23). Это и есть требуемое противоречие.

Так как измеримые кардиналы являются очень большими, можно было бы предположить, что неконструктивные множества, полученные с помощью аксиомы измеримости, должны были бы очень далеко отстоять от множеств, обычно используемых в математике. Однако Рубиноттом доказано в теории ZFM, что существуют неконструктивные множества натуральных чисел; в действительности доказано, что существует только счетное число конструктивных множеств натуральных чисел. Известно несколько дальнейших обобщений теоремы Скотта в этих направлениях.

Теперь можно было бы надеяться получить решение гипотезы континуума с помощью аксиомы измеримости. Однако Леви и Соловей показали, что гипотеза континуума и ее отрицание недоказуемы в теории ZFM (при условии, что теория ZFM непротиворечива).

Имеется несколько других известных обобщений аксиом бесконечности и для некоторых из них доказаны резуль-

таты, подобные вышеприведенным. Однако ни одна из них не решает гипотезу континуума.

В настоящее время ситуация в этой области может быть описана следующим образом. Мы имеем некоторые аксиомы, из которых следует отрицание аксиомы конструктивности. Имеются некоторые основания, что эти аксиомы истинны, хотя это еще открытый вопрос. Но мы не имеем разумных аксиом, которые решали бы гипотезу континуума.

Хотя эти результаты могут показаться несколько ограниченными, ситуация, в действительности, весьма многообещающая, в особенности при сравнении ее с ситуацией, имевшейся несколько лет назад. Мы знаем, что гипотеза континуума не может быть решена на основе имеющихся сейчас аксиом, но мы имеем некоторую идею, какого сорта новые аксиомы нужно искать. Оптимист хотел бы надеяться, что гипотеза континуума, которая не поддается математикам почти в течение века, будет доказана в течение нескольких ближайших лет.

Задачи

1. (а) Пусть теория ZF_1 получается из теории ZF опусканием аксиом подмножеств и замены и добавлением аксиомы

$$\text{Set}_x \exists z (x \in z \ \& \ z \in y)$$

и всевозможных аксиом

$$\forall x \exists z \forall y (A \rightarrow y = z) \rightarrow \exists v \forall y (y \in v \leftrightarrow \exists x (x \in w \ \& \ A)),$$

где x, y, z, v и w различны и z, v и w не встречаются в A . Показать, что теория ZF_1 эквивалентна теории ZF .

(б) Пусть теория ZF_2 получается из теории ZF опусканием аксиомы бесконечности и добавлением аксиомы

$$\exists x (\exists y (y \in x) \ \& \ \forall y (y \in x \rightarrow \exists z (z \in x \ \& \ y \subset z \ \& \ y \neq z))).$$

Показать, что теория ZF_2 эквивалентна теории ZF . [В теории ZF_2 определить натуральное число как ординал, который меньше, чем каждое предельное число. Доказать трансфинитной индукцией, что никакое натуральное число не подобно меньшему натуральному числу. Пусть x таково, как в последней аксиоме. Доказать, что множество всех натуральных чисел, подобных подмножествам элементов множества x , существует, и это множество содержит все натуральные числа.]

2. Пусть теория ZF' получается из теории ZF опусканием аксиомы регулярности. Множество a называется *регулярным*, если каждое непустое подмножество множества a имеет минимальный элемент.

(а) Определим x как ординал, если x транзитивно и регулярно и каждый элемент из x транзитивен. Показать, что все результаты из § 9.3 могут быть доказаны в теории ZF' .

(б) Показать, что если теория ZF' непротиворечива, то теория ZF непротиворечива. [Пусть $M(x) \leftrightarrow \exists \sigma (x \in \text{Stg}(\sigma))$. Показать, что M — интерпретация теории ZF в теории ZF' .]

3. Пусть E — некоторый бинарный предикат теории ZF такой, что

$$\vdash x \neq 0 \rightarrow \exists y (y \in x \ \& \ \neg \exists z (z \in x \ \& \ z E y))$$

и

$$\vdash \text{Set}_x (x E y).$$

Показать, что существует ординальный функциональный символ H такой, что $\vdash \text{Set}_x (H(x) \leq \sigma)$ и $\vdash x E y \rightarrow H(x) < H(y)$. [Аналогично методу, который используется в § 9.10 для $\in_I$.]

4. Множество a называется *цепью*, если $\forall x \forall y (x, y \in a \rightarrow x \subset y \vee y \subset x)$. Множество a называется *индуктивным*, если $\text{Un}(b) \in a$ для каждой непустой цепи b , содержащейся в a . *Максимальным элементом* множества a называется элемент множества a , не входящий ни в один элемент из a . *Лемма Цорна* утверждает, что если a — непустое индуктивное множество, то a имеет максимальный элемент.

(а) Доказать лемму Цорна в теории ZFC . [Предположим, что a — непустое индуктивное множество, не имеющее максимального элемента. Показать, что a не является цепью. Затем показать, что существует функция выбора g на a такая, что если $b \subset a$ и b — цепь, то $\text{Un}(b) \subset g'(a - b)$. Пусть f таково, как в замечании после теоремы о вполне упорядоченности. Показать, что $\sigma < \tau \rightarrow f'\sigma \subset f'\tau$ для $\sigma, \tau \in \text{Do}(f)$, и прийти к противоречию.]

(б) Доказать в теории ZFC лемму Тейхмюллера — Тьюки. [Применить (а).]

(в) Показать, что в теории ZF аксиома выбора следует из леммы Тейхмюллера — Тьюки. [Для данного множества x пусть z — множество функций f , где $\text{Do}(f) \subset P(x)$ и $f'y \in y$ для $y \in \text{Do}(f)$. Выбрать максимальный элемент из z .]

5. Пусть y — некоторое подмножество из $x \times x$, будем писать $a <_y b$ вместо $\langle a, b \rangle \in y$. Если $z \subset x$, то y -*первым элементом* из z называется элемент a из z такой, что $a <_y b$ для всех $b \in z - \{a\}$. Скажем, что y *вполне упорядочивает* x , если $\neg (a <_y a)$ для всех a и каждое непустое подмножество из x имеет y -первый элемент.

(а) Пусть y вполне упорядочивает x . Показать, что если $a, b \in x$, то выполняется в точности одно из $a <_y b$, $a = b$ и $b <_y a$. Показать, что если $a <_y b$ и $b <_y c$, то $a <_y c$. Показать, что каждое непустое подмножество из x имеет единственный y -первый элемент.

(б) Пусть f — отображение из σ в σ' такое, что $\tau < \rho < \sigma \rightarrow f'\tau < f'\rho$. Показать, что $\tau \leq f'\tau$ для $\tau < \sigma$. [Использовать трансфинитную индукцию.] Доказать, что $\sigma \leq \sigma'$.

(в) Пусть y вполне упорядочивает x . Показать, что существует единственное биективное отображение f ординала σ на x такое, что $\tau < \rho < \sigma \rightarrow f'\tau <_y f'\rho$. [Использовать замечание, данное после теоремы о вполне упорядоченности, и (б).]

(г) *Убывающей y -последовательностью* в x называется последовательность $a_0, a_1, \dots$ элементов x такая, что $a_{S(i)} <_y a_i$ для всех i .

Доказать в теории ZFC, что подмножество y из $x \times x$ вполне упорядочивает x тогда и только тогда, когда y является линейным порядком x и не существует убывающей y -последовательности в x .

6. (а) Показать, что Card' можно определить в теории ZF так, чтобы $\text{Card}'(x) = \text{Card}'(y) \leftrightarrow \text{Sm}(x, y)$. [Подобно определению ЕС из § 9.10.]

б) Определим $x \leq' y \leftrightarrow \exists a \exists b (x = \text{Card}'(a) \& y = \text{Card}'(b) \& a \subset b)$. Доказать (в теории ZF), что

$$\begin{aligned} \exists a (x = \text{Card}'(a)) &\rightarrow x \leq' x, \\ x \leq' y \& y \leq' z &\rightarrow x \leq' z. \end{aligned}$$

(в) Доказать в теории ZF, что если существует инъективное отображение f из a в b и инъективное отображение g из b в a , то a подобно b . [Пусть

$$d = [c \mid c \subset a \& \forall x (x \in b \& g'x \in c \rightarrow \exists y (y \in c \& x = f'y))].$$

Пусть $a_1 = \text{Un}(d)$, $a_2 = a - a_1$, $b_1 = [f'x \mid x \in a_1]$, $b_2 = b - b_1$. Показать, что $a_1 \in d$, и вывести, что g отображает b_2 в a_2 . Пусть e — множество элементов из a , не представимых в виде $g'x$, где $x \in b_2$. Показать, что $e \in d$, и вывести, что g отображает b_2 на a_2 .] Вывести, что $x \leq' y \& y \leq' x \rightarrow x = y$.

(г) Показать, что для каждого множества x существует множество ординалов, подобных подмножествам множества x . [Заметить, что существует множество множеств, вполне упорядочивающих подмножества множества x , и применить 5 (в).]

(д) Показать, что формула

$$\forall x \forall y (\exists a (x = \text{Card}'(a)) \& \exists b (y = \text{Card}'(b)) \rightarrow x \leq' y \vee y \leq' x)$$

эквивалентна аксиоме выбора. [Допустив эту формулу, применить (г), чтобы доказать теорему о вполне упорядоченности, и вывести аксиому выбора.]

7. В теории ZFC определим σ^τ как кардинал множества отображений из τ в σ .

(а) Доказать, что 2^σ при этом определении имеет такое значение, как и при старом определении.

(б) Для кардиналов σ , τ и ρ показать, что

$$\begin{aligned} \sigma^{\tau+\rho} &= \sigma^\tau \cdot \sigma^\rho, \\ \sigma^{\tau \cdot \rho} &= (\sigma^\tau)^\rho, \\ (\sigma \cdot \tau)^\rho &= \sigma^\rho \cdot \tau^\rho. \end{aligned}$$

(в) Показать, что

$$\sigma \leq \sigma' \& \tau \leq \tau' \rightarrow \sigma^\tau \leq \sigma'^{\tau'}.$$

(г) Показать, что

$$\sigma \leq \tau \rightarrow \aleph_\sigma^{\aleph_\tau} = 2^{\aleph_\tau}.$$

[Использовать (б) и (в).]

8. Для кардинала σ пусть $\text{cf}(\sigma)$ — первый кардинал τ такой, что

$$\exists x (x \subset \sigma \& \text{Un}(x) = \sigma \& \text{Card}(x) = \tau).$$

Кардинал σ называется *регулярным*, если $\text{cf}(\sigma) = \sigma$, и *сингулярным*, если $\text{cf}(\sigma) < \sigma$. Кардинал $\aleph_\sigma$ называется *слабо недостижимым*, если он регулярный, и σ — предельное число.

(а) Показать, что $\text{cf}(\sigma) \leq \sigma$.

(б) Показать, что $\aleph_{\text{cf}(\sigma)}$ — регулярный кардинал.

(в) Показать, что каждый недостижимый кардинал является слабо недостижимым. Показать, что из обобщенной гипотезы континуума следует, что каждый слабо недостижимый кардинал является недостижимым.

(г) Показать, что если теория ZF непротиворечива, то утверждение о том, что слабо недостижимый кардинал существует, не может быть доказано в теории ZFC. [В теории ZFL определим M , как в (4) из § 9.10, только недостижимость заменим на слабую недостижимость. Использовать (4) из § 9.7, чтобы доказать интерпретацию аксиомы степени.]

(д) Показать, что

$$\text{cf}(\aleph_\sigma) \leq \tau \rightarrow \aleph_\sigma < \aleph_\sigma^\tau.$$

[Допустим, что $\tau = \text{cf}(\sigma)$ и $\aleph_\sigma = \aleph_\sigma^\tau$. Пусть

$$x \subset \aleph_\sigma, \text{Card}(x) = \tau, \text{Un}(x) = \aleph_\sigma,$$

и пусть $\rho \rightarrow f_\rho$ — биективное отображение из $\aleph_\sigma$ на множество отображений из x в $\aleph_\sigma$. Для каждого $v \in x$ выберем f'_v в $\aleph_\sigma - [f'_\rho v \mid \rho < v]$. Показать, что f не является f_ρ .]

(е) Показать, что

$$\text{cf}(\aleph_\sigma) \leq \aleph_\tau \rightarrow 2^{\aleph_\tau} \neq \aleph_\sigma.$$

[Использовать (д).] Вывести, что $2^{\aleph_0} \neq \aleph_\omega$.

9. (а) Доказать в теории ZFL

$$\omega \leq \rho \& a \subset C^*(\rho) \& \rho < \text{Card}(\tau) \rightarrow a \in C^*(\tau).$$

[Пусть $\text{Card}(\rho) = \aleph_\sigma$; применить (8) из § 9.7 к $b = C^*(\rho) \cup \{a\}$.]

(б) Доказать в теории ZFC

$$L(a) \& a \subset C^*(\aleph_{\text{cf}(\sigma)}) \& \text{Card}(a) \leq \aleph_\sigma \rightarrow a \in C^*(\aleph_{\text{cf}(\sigma)}).$$

[Взять интерпретацию теоремы из (а) относительно L и применить (26) из § 9.10 и 8 (б).]

(в) Доказать в теории ZFC, что каждое конструктивное подмножество из ω и каждое конструктивное отображение из ω на ω имеет счетный порядок. [Применить (б).] Вывести, что из формулы $\forall x (x \subset \omega \rightarrow L(x))$ следует гипотеза континуума.

10. (а) Показать, что существует арифметический предикат P такой, что для любого дерева A

$$P(K_A, i, j) \leftrightarrow A(i) \& \|A_{[i]}\| = j.$$

(б) Показать, что существует арифметический предикат P такой, что если A — дерево, то $P(K_A, \alpha)$ неявно определяет $\langle K_{R_A} \rangle$, где

$$R_A(i, j, k) \leftrightarrow A(i) \& A(j) \& A(k) \& K(\|A_{[i]}\|) = \langle \|A_{[j]}\|, \|A_{[k]}\| \rangle.$$

Вывести, что существует гиперарифметическое отношение Q такое, что для любого дерева A

$$Q(K_A, i, j, k) \leftrightarrow R_A(i, j, k).$$

(в) Показать, что существуют арифметические отношения $P_1 - P_4$ такие, что если A есть дерево и C_A определяется следующим образом:

$$C_A(i, j) \leftrightarrow A(i) \& A(j) \& C(\|A_{[i]}\|) \in C(\|A_{[j]}\|),$$

то

$$P_1(K_A, \langle K_{C_A} \rangle, i, j) \leftrightarrow A(i) \& A(j) \& C(\|A_{[i]}\|) = C(\|A_{[j]}\|),$$

$$P_2(K_A, \langle K_{C_A} \rangle, i, j, k) \leftrightarrow A(i) \& A(j) \& A(k) \& C(\|A_{[i]}\|) = \\ = \{C(\|A_{[j]}\|), C(\|A_{[k]}\|)\},$$

$$P_3(K_A, \langle K_{C_A} \rangle, i, j, k) \leftrightarrow A(i) \& A(j) \& A(k) \& C(\|A_{[i]}\|) = \\ = \langle C(\|A_{[j]}\|), C(\|A_{[k]}\|) \rangle,$$

$$P_4(K_A, \langle K_{C_A} \rangle, i, j, k, m) \leftrightarrow \\ \leftrightarrow A(i) \& A(j) \& A(k) \& A(m) \& C(\|A_{[i]}\|) = \\ = \langle C(\|A_{[j]}\|), C(\|A_{[k]}\|), C(\|A_{[m]}\|) \rangle.$$

(г) Показать, что существует гиперарифметическое отношение P такое, что для дерева A и C_A , как в (в), $P(K_A, \alpha)$ неявно определяет $\langle K_{C_A} \rangle$. [Применить (а), (б) и (в).]

(д) Показать, что существует арифметическое отношение P такое, что если A есть дерево, то для C_A , как в (в),

$$P(K_A, \langle K_{C_A} \rangle, i, j) \leftrightarrow A(i) \& C(\|A_{[i]}\|) = j.$$

(е) Показать, что существует гиперарифметическое отношение P такое, что для дерева A

$$P(K_A, \alpha, i) \leftrightarrow A(i) \& C(\|A_{[i]}\|) = \alpha.$$

[Применить (г) и (д).]

(ж) Показать, что класс конструктивных множеств натуральных чисел является множеством рода Σ_2^1 . [Применить (е) и 9 (в).]

(з) Показать, что если α и β конструктивны, то либо α имеет род Δ_2^1 в β , либо β имеет род Δ_2^1 в α . [Предположим, что $\text{Od}(\alpha) < \text{Od}(\beta)$. Пусть P таково, как в (е). Применить 9 (в) и теорему униформизации, чтобы найти γ такое, что $\text{Tr}(\gamma) \& \exists i P(\gamma, \beta, i)$ и γ имеет род Δ_2^1 в β . Показать, что α гиперарифметическое в γ .]

11. Допустим аксиому конструктивности. Пусть $\alpha <_L \beta$ означает, что $\text{Od}(\alpha) < \text{Od}(\beta)$.

(а) Доказать, что $<_L - (2, 0)$ -местное отношение рода Δ_2^1 . [Применить 10 (е) и 9 (в).]

(б) Доказать, что для $n \geq 2$ класс функций рода Δ_{n+1}^1 является базисом для семейства функциональных классов рода Π_n^1 . [Если P имеет род Π_n^1 и непусто, то пусть α — элемент из P наименьшего порядка; применить (а).]

(в) Доказать, что для $n \geq 3$ семейство подмножеств рода Σ_n^1 из $N_{m,k}$ удовлетворяет принципу редукции. [Подобно задаче 25 (б) из главы 7, применяя (а).]

12. (а) Пусть M — транзитивная $\in$ -интерпретация теории ZF; Q и Q' — предикатные символы, абсолютные для M ; R — предикатный символ такой, что

$$\vdash_{ZF} R(x_1, \dots, x_n) \leftrightarrow \exists y Q(y, x_1, \dots, x_n),$$

$$\vdash_{ZF} R(x_1, \dots, x_n) \leftrightarrow \forall y Q'(y, x_1, \dots, x_n).$$

Показать, что R абсолютно для M . [Взять интерпретации этих двух теорем.]

(б) Пусть $We(y, x)$ означает, что y вполне упорядочивает x . Показать, что We абсолютно для всех транзитивных $\in$ -интерпретаций теории ZF. [Применить (а) и 5 (в).]

(в) Показать, что существует интерпретация J теории P в теории ZF такая, что для каждого определимого предикатного символа Q из P для всех транзитивных $\in$ -интерпретаций теории ZF Q_J абсолютно. Вывести, что каждый рекурсивный предикат может быть представлен в теории ZF предикатным символом, абсолютным для всех транзитивных $\in$ -интерпретаций теории ZF. Обобщить этот результат на арифметические отношения. [Использовать метод из задачи 11 (а) главы 8.]

(г) Показать, что любое $(2, 1)$ -местное отношение рода Π_1^1 может быть представлено в теории ZF предикатным символом Q , определенным следующим образом:

$$Q(\alpha, \beta, i) \leftrightarrow We(F(\alpha, \beta, i), G(\alpha, \beta, i)),$$

где F и G абсолютны. [Применить задачу 19 (е) главы 7.] Вывести, что Q абсолютно. [Применить (б).]

(д) Показать, что если Q такое же, как в (г), и R определяется следующим образом:

$$R(\alpha, i) \leftrightarrow \exists \beta Q(\alpha, \beta, i),$$

то R абсолютно для L . [Применяя 5 (в), получим

$$R(\alpha, i) \leftrightarrow \exists \beta \exists f \exists \sigma (\text{Func}(f) \& \text{Do}(f) = \omega \& \text{Ra}(f) \subset \sigma \& \\ \& \forall j \forall k (j, k \in G(\alpha, \beta, i) \rightarrow (\langle j, k \rangle \in F(\alpha, \beta, i) \rightarrow f'j < f'k))).$$

Пусть $f \upharpoonright j$ — ограничение f на j ; перепишем эту формулу так:

$$R(\alpha, i) \leftrightarrow \exists f \exists \sigma (\text{Func}(f) \& \text{Do}(f) = \\ = \omega \& \text{Ra}(f) \subset \sigma \times \omega \& \forall j R'(f \upharpoonright j, \sigma, \alpha, i)),$$

где R' абсолютно. Используя идею из доказательства (г) и вполне упорядоченность $\sigma \times \omega$, доставляемую K , перепишем эту формулу так:

$$R(\alpha, i) \leftrightarrow \exists \sigma \neg We(H_1(\sigma, \alpha, i), H_2(\sigma, \alpha, i)),$$

где H_1 и H_2 абсолютны, и применим (б), не забывая, что $\forall \sigma L(\sigma)$.

(е) Показать, что каждый предикат рода Σ_2^1 или Π_2^1 конструктивен. [Определить R , как в (д), опуская α ; использовать абсолютность R .]

(ж) Ординал σ называется ординалом рода Δ_2^1 , если он конечен или существует биективное отображение f из ω на σ такое, что $f'i < f'j$ — предикат рода Δ_2^1 . Показать, что порядок всякого предиката

ката рода Δ_2^1 представляет собой ординал рода Δ_2^1 . [Применить следствие к теореме униформизации.]

13. Пусть теория ZF^Y получается из теории ZF добавлением константы Y и аксиом $Y \subset \omega$ и $\neg L(Y)$. Определим C^Y подобно C , за исключением того, что добавляется новая операция $\delta_{10}^Y(x, y) = x \cap y$; определим C^{*Y} и L^Y аналогично. Пусть теория ZFL^Y получается из теории ZF^Y добавлением аксиомы $\forall x L^Y(x)$.

(а) Показать, что если теория ZF непротиворечива, то теория ZF^Y непротиворечива. [Применить теорему 1 из § 9.9 и 9(в).]

(б) Показать, что L^Y — интерпретация теории ZF в теории ZF^Y и имеет место $\forall \sigma L^Y(\sigma)$.

(в) Показать, что L абсолютно для L^Y и $L(x) \leftrightarrow L^Y(x)$. [Заметить, что C абсолютно для L^Y и, следовательно, L^Y -инвариантно, и применить (б).] Вывести, что $L^Y(Y)$ имеет место. [Применить аналог леммы 2 из § 9.6.]

(г) Если M есть $\in$ -интерпретация теории ZF в теории ZF^Y такая, что имеет место $M(Y)$, то мы расширяем M до интерпретации языка $L(ZF^Y)$, беря Y_M вместо Y . Показать, что M — интерпретация теории ZF^Y . Определим абсолютность для M нелогических символов теории ZF^Y , как раньше. Показать, что Y абсолютно и что если M транзитивно, то C^Y абсолютно.

(д) Показать, что L^Y абсолютно для L^Y . Вывести, что L^Y — интерпретация теории ZFL^Y в теории ZF^Y .

(е) Доказать аксиому выбора в теории ZFL^Y .

(ж) Доказать в теории ZFL^Y

$$Y \in b \ \& \ \text{Trans}(b) \ \& \ \text{Card}(b) \leq \aleph_\sigma \rightarrow b \subset C^{*Y}(\aleph_{S(\sigma)}).$$

[Подобно (8) из § 9.7. В доказательстве леммы заметить, что $F(y) = y$.]

(з) Доказать обобщенную гипотезу континуума в теории ZFL^Y . [Подобно теореме 2 из § 9.7. В доказательстве аналога для (4) из § 9.7 взять $b = C^*(\aleph_\sigma) \cup \{a\} \cup \{Y\} \cup \omega$.]

(и) Пусть теория ZFC' получается из теории ZFC добавлением обобщенной гипотезы континуума. Показать, что если теория ZF непротиворечива, то $\forall x (x \subset \omega \rightarrow L(x))$ не является теоремой теории ZFC' . [Применить (а), (д), (е) и (з).]

14. δ -идеалом на множестве x называется подмножество y из $P(x)$, удовлетворяющее условиям (ii), (iii) и (iv) определения измеримого идеала и дополнительному условию: (i') $\text{Un}(z) \subseteq y$ для каждого счетного подмножества z множества y . Предположим, что χ есть кардинал, y есть δ -идеал на χ и не существует никакого δ -идеала на любом кардинале, меньшем χ . Показать, что y — измеримый идеал. [Допустим, что это не так. Пусть σ — первый кардинал такой, что $\text{Card}(z) = \sigma$ для некоторого подмножества z множества y и $\text{Un}(z) \not\subseteq y$. Показать, что это z может быть выбрано таким, что $\text{Un}(z) = \chi$. Пусть f — биективное отображение из σ на z и ω — множество всех подмножеств v из σ таких, что $\text{Un}(\{f^* \tau \mid \tau \in v\}) \not\subseteq y$. Показать, что ω есть δ -идеал на σ .]

ПРОБЛЕМА ТОЖДЕСТВА СЛОВ

Мы собираемся рассмотреть одну проблему разрешимости, возникшую в теории групп. Мы будем предполагать, что читатель знаком с группами, заданными образующими и соотношениями, и со свободными произведениями. Напомним нужные нам понятия.

Единичный элемент любой группы обозначается через e . Мы называем $\{e\}$ *единичной* подгруппой и называем элемент *неединичным*, если он отличен от e . Через $\{A\}$ мы обозначаем подгруппу, порождаемую множеством A . Если φ — отображение, то $\varphi|A$ означает ограничение отображения φ на множество A . Если G — группа, то G_1 будет обозначать изоморфную копию группы G при изоморфизме, отображающем g в g_1 ; образ множества A при этом изоморфизме будет обозначаться через A_1 .

Свободная группа $[A]$ над множеством A есть группа, содержащая множество A и обладающая следующим свойством: каждый элемент из $[A]$ может быть единственным способом записан в виде

$$a_1^{\pm 1} a_2^{\pm 1} \dots a_n^{\pm 1},$$

где a_i принадлежат A и никакое a не является смежным с a^{-1} . (Мы допускаем случай $n=0$; это дает выражение для e .) Такие выражения называются *словами* в A . Мы можем рассматривать их как элементы группы $[A]$. Два слова мы умножаем, выписывая их последовательно, а затем вычеркивая выражения вида aa^{-1} и $a^{-1}a$ до тех пор, пока не получим слово; этот процесс вычеркивания называется *сокращением*. Справедливо $[A] = \{A\}$. Более общо, если $B \subset A$, то $\{B\}$ состоит из слов в B и может быть отождествлена с $[B]$.

Если φ является отображением из A в группу G , то существует и единственно продолжение φ' отображения φ до гомоморфизма $[A]$ в G , и φ' сюръективно тогда и только тогда, когда $\varphi(A)$ порождает G . В частности, если A — порождающее множество группы G , то существует един-

ственный гомоморфизм $[A]$ в G , тождественный на A , и этот гомоморфизм является сюръективным. Таким образом, G естественно изоморфна некоторой фактор-группе группы $[A]$. Отсюда следует, что каждая конечно порожденная группа изоморфна некоторой фактор-группе свободной группы над конечным множеством.

Подмножество A группы G свободно, если гомоморфизм $[A]$ в G , тождественный на A , инъективен. В этом случае мы можем отождествить подгруппу $\{A\}$ группы G с $[A]$.

Пример. Если $z \notin A$, то множество всех XzX^{-1} из $[A, z]$, где X — слово в A , свободно.

Соотношением на A называется выражение $X=Y$, где X и Y — слова в A . Это соотношение истинно в фактор-группе $[A]/K$, если X и Y находятся в одном и том же смежном классе по K , или, что эквивалентно, если $XY^{-1} \in K$.

Пусть R — некоторое множество соотношений на A . Соотношение на A называется следствием множества R , если оно истинно в каждой фактор-группе группы $[A]$, в которой истинны все соотношения из R . Множество следствий множества R обозначается через $C(R)$. Существует лишь одна фактор-группа $[A]/K_R$ группы $[A]$, в которой все истинные соотношения являются следствиями множества R ; K_R является нормальной подгруппой, порожденной XY^{-1} для $X=Y$ из R . Мы называем $[A]/K_R$ группой с множеством образующих A и множеством определяющих соотношений R и обозначаем ее через $[A; R]$.

Обобщим обозначение $[A; R]$, допуская несколько образующих или множеств образующих перед точкой с запятой и несколько соотношений или множеств соотношений после точки с запятой. Так, $[A, t; R, X=Y]$ имеет множество образующих $A \cup \{t\}$ и множество определяющих соотношений $R \cup \{X=Y\}$. При этом подразумевается, что ни одна из образующих не повторяется; таким образом в приведенном выше примере должно быть $t \notin A$. Если A находится перед точкой с запятой, а a — после точки с запятой, то подразумевается, что областью изменения для служит A ; аналогично для других букв. Например, в $[A, t; at=ta]$ определяющими соотношениями являются все $at=ta$ для a из A .

Так как $[A]$ является подгруппой группы $[A, B]$, а K_R является подгруппой группы $K_{R \cup S}$, то существует

естественный гомоморфизм из $[A; R]$ в $[A, B; R, S]$, отображающий смежный класс *) из $[A; R]$, содержащий некоторое слово в A , в смежный класс из $[A, B; R, S]$, содержащий это же слово. Если этот гомоморфизм биективен, то мы отождествляем эти две группы. Это наверняка произойдет в следующем случае: S состоит из соотношений вида $b=X$, где X — слово в A , по одному для каждого b из B .

Напомним, что каждая группа G естественным образом отождествляется с фактор-группой группы $[G]$ и, следовательно, с группой $[G; R_G]$, где R_G — множество всех соотношений на G , истинных в этой фактор-группе. Если G находится перед точкой с запятой, то подразумевается, что соотношения из R_G принадлежат множеству определяющих соотношений, даже если они не появляются в явном виде после точки с запятой.

Пример. Группа $[G, H; gh=hg]$ является прямым произведением групп G и H . (Мы предполагаем, что G и H не пересекаются, в противном случае их вначале следует заменить на изоморфные группы.)

Пусть G и G' — группы, и пусть φ — изоморфизм подгруппы H группы G и подгруппы H' группы G' . Рассмотрим группу

$$G *_{\varphi} G' = [G, G'; h = \varphi(h)].$$

Естественные отображения групп G и G' в $G *_{\varphi} G'$ инъективны, поэтому мы отождествляем G и G' с их образами при этих отображениях. Тогда H и H' отождествляются посредством изоморфизма φ . Мы имеем $G *_{\varphi} G' = \{G, G'\}$ и $G \cap G' = H = H'$. Группа $G *_{\varphi} G'$ называется свободным произведением групп G и G' с объединенной подгруппой $G \cap G'$.

Пусть T содержит по одному элементу из каждого правого смежного класса в G по H , отличного от самой H , и пусть T' сформировано аналогично при помощи H' и G' . Слово в $G \cup G'$ находится в нормальной форме, если оно имеет вид $ht_1t_2 \dots t_n$, где $h \in H$, $t_1, t_2, \dots, t_n \in T \cup T'$ и $t_i \in T$ тогда и только тогда, когда $t_{i+1} \in T'$ при $1 \leq i \leq n$. Тогда теорема Шрайера утверждает, что каждый смежный

*) Здесь и ниже, говоря о смежном классе, автор подразумевает представление группы в виде фактор-группы свободной группы и называет ее элементы смежными классами (без указания подгруппы). — Прим. ред.

класс из $G *_\varphi G'$ содержит в точности одно слово, находящееся в нормальной форме.

Пусть K и K' — такие подгруппы групп G и G' соответственно, что

$$\varphi(H \cap K) = \varphi(H) \cap K.$$

(Это означает, что в $G *_\varphi G'$ подгруппы K и K' имеют одно и то же пересечение с объединенной подгруппой.) Тогда ограничение $\psi = \varphi|_{(H \cap K)}$ является изоморфизмом между $H \cap K$ и $\varphi(H) \cap K$. Таким образом, мы можем образовать группу $K *_\psi K'$, причем существует естественное отображение χ группы $K *_\psi K'$ в $G *_\varphi G'$, при котором образом является $\{K, K'\}$. Мы покажем, что χ инъективно. Так как элементы из разных смежных классов по $H \cap K$ в K находятся в разных смежных классах по H в G , то мы можем предполагать, что T содержит по одному элементу из каждого смежного класса по $H \cap K$ в K , отличного от $H \cap K$. Также можно предполагать, что T' выбрано аналогично. Тогда слова в $K \cup K'$, находящиеся в нормальной форме, содержатся в множестве слов в $G \cup G'$, находящихся в нормальной форме. Так как χ отображает смежный класс, содержащий некоторое слово, в смежный класс, содержащий то же самое слово, то по теореме Шрайера χ инъективно.

Таким образом, мы можем отождествить $K *_\psi K'$ с $\{K, K'\} \subset G *_\varphi G'$. Тогда

$$G \cap \{K, K'\} = K. \quad (1)$$

Для доказательства достаточно показать, что левая часть содержится в правой. Нормальной формой элемента g из G является h или ht , где $t \in T$. Если это является также нормальной формой элемента из $\{K, K'\}$, то $h \in H \cap K$ и $t \in K$, поэтому $g \in K$.

Если φ является изоморфизмом единичных подгрупп, то вместо $G *_\varphi G'$ мы пишем $G * G'$ и называем $G * G'$ *свободным произведением* групп G и G' . Таким образом, $G * G' = [G, G']$. Нормальные формы становятся произведениями неединичных элементов, выбранных поочередно в G и в G' (если мы опустим начальное e). Тогда описанные ранее K и K' могут быть любыми подгруппами групп G и G' .

Пусть G и G' — подгруппы группы L . Пусть $H = G \cap G'$ и φ — тождественное отображение из H на H . Тогда существ-

ует единственный гомоморфизм группы $G *_\varphi G'$ в L , тождественный на G и G' ; при этом образом является $\{G, G'\}$. Если этот гомоморфизм инъективен, то мы отождествляем $G *_\varphi G'$ и $\{G, G'\}$ и говорим, что $\{G, G'\}$ является свободным произведением групп G и G' с объединенной подгруппой H (не упоминая об H , если H — единичная подгруппа).

Пример. Если h — неединичный элемент из H , то в группе $G * H$ подгруппа $\{G, hGh^{-1}\}$ является свободным произведением групп G и hGh^{-1} ; это легко следует из теоремы Шрайера.

Группа называется *конечно определенной*, если она изоморфна группе $[A; R]$, где A и R конечны. Прямое произведение двух конечно определенных групп является конечно определенной группой, так как

$$[A; R] \times [B; S] = [A, B; R, S, ab = ba].$$

Свободное произведение двух конечно определенных групп с конечно порожденной объединенной подгруппой является конечно определенной группой. Действительно, пусть произведением будет $[A; R] *_\varphi [B; S]$, причем область определения отображения φ содержит конечное число образующих $h_1, \dots, h_n$. Пусть X_i — слово в A из смежного класса, содержащего h_i , и пусть Y_i — слово в B из смежного класса, содержащего $\varphi(h_i)$. Тогда

$$[A; R] *_\varphi [B; S] = [A, B; R, S, X_1 = Y_1, \dots, X_n = Y_n].$$

Пусть R — некоторое множество соотношений на конечном множестве A . *Проблемой тождества слов* для R называется проблема разрешимости для $C(R)$. Так как $C(R)$ является множеством соотношений, истинных на $[A; R]$, то эту проблему мы называем также *проблемой тождества слов для $[A; R]$* .

Чтобы перевести эту проблему на язык теории рекурсии, мы отождествим символы a и a^{-1} ($a \in A$) и символ $=$ с натуральными числами. Тогда каждое слово в A и каждое соотношение на A становятся конечными последовательностями натуральных чисел, и потому имеют некоторый номер (последовательности). Множество P слов или соотношений называется *рекурсивным* (или *рекурсивно перечислимым*), если множество номеров элементов множества P рекурсивно (или рекурсивно перечислимо). Легко проверить, что это определение не зависит от выбора чисел, с кото-

рыми были отождествлены символы, поэтому проблема тождества слов для R разрешима тогда и только тогда, когда $C(R)$ рекурсивно.

Соотношение $X=Y$ принадлежит множеству $C(R)$ тогда и только тогда, когда XY^{-1} принадлежит K_R , а X принадлежит K_R тогда и только тогда, когда $X=e$ принадлежит множеству $C(R)$. Отсюда следует, что подгруппа K_R рекурсивна (рекурсивно перечислима) тогда и только тогда, когда множество $C(R)$ рекурсивно (рекурсивно перечислимо). Кроме того, если R рекурсивно перечислимо, то $C(R)$ рекурсивно перечислимо. Действительно, множество J таких XY^{-1} , что соотношение $X=Y$ принадлежит R , рекурсивно перечислимо. Мы получим все слова из K_R , сокращая выражения $X_1 Y_1^{\pm 1} X_1^{-1} \dots X_n Y_n^{\pm 1} X_n^{-1}$, где Y_i принадлежит J . Отсюда следует, что подгруппа K_R рекурсивно перечислима, и потому множество $C(R)$ рекурсивно перечислимо.

Группа называется *рекурсивно определенной*, если она изоморфна группе $[A; R]$, где A конечно, а R рекурсивно перечислимо. Очевидно, каждая конечно определенная группа является рекурсивно определенной. (Как известно, обратное неверно.)

Предположим, что $[A; R]$ вложена в $[B; S]$ (где A и B конечны). Выберем для каждого a из A такое слово Y_a в B , что смежные классы, содержащие a и Y_a , соответствуют друг другу при этом изоморфизме. Для каждого слова X в A пусть X' будет словом в B , полученным из X заменой a на Y_a и a^{-1} на Y_a^{-1} и последующим сокращением. Тогда при упомянутом изоморфизме смежные классы, содержащие X и X' , соответствуют друг другу, поэтому $X=Y$ истинно в $[A; R]$ тогда и только тогда, когда $X'=Y'$ истинно в $[B; S]$. Первым следствием этого является то, что если проблема тождества слов разрешима для $[B; S]$, то проблема тождества слов разрешима и для $[A; R]$. Вторым следствием является то, что если $C(S)$ рекурсивно перечислимо, то и $C(R)$ рекурсивно перечислимо. Так как $[A; R]=[A; C(R)]$, то отсюда следует, что каждая подгруппа рекурсивно определенной группы будет рекурсивно определенной.

Если G — конечно порожденная группа, то G изоморфна группе $[A; R]$, где A конечно. Мы говорим, что проблем тождества слов для G *разрешима* или *неразрешима*, в зависимости от того, будет ли разрешимой или неразрешимой

мой проблема тождества слов для $[A; R]$. Согласно только что доказанному утверждению это не зависит от выбора представления $[A; R]$.

Нашей основной целью является доказательство следующего утверждения.

Теорема Новикова. *Существует конечно определенная группа, для которой проблема тождества слов неразрешима.*

Мы получим рекурсивно определенную группу с неразрешимой проблемой тождества слов следующим образом. Пусть A — рекурсивно перечислимое множество, а H — подгруппа группы $G=[a, b]$, порожденная элементами $a^n b a^{-n}$, где $n \in A$. Пусть φ — тождественное отображение из H на H . Тогда $G *_{\varphi} G$ есть

$$[a, b, a_1, b_1; a^n b a^{-n} = a_1^n b_1 a_1^{-n} \text{ для } n \in A],$$

и потому она является рекурсивно определенной. Далее, соотношение $a^n b a^{-n} = a_1^n b_1 a_1^{-n}$ истинно в $G *_{\varphi} G$ тогда и только тогда, когда $n \in A$. Действительно, если это соотношение истинно, то $a^n b a^{-n}$ принадлежит объединенной подгруппе H ; так как множество $\{a^m b a^{-m}\}$ свободно, то отсюда следует, что $n \in A$. Таким образом, проблема разрешимости для A сводима к проблеме тождества слов для $G *_{\varphi} G$. Если мы выберем множество A нерекурсивным, то отсюда будет следовать, что $G *_{\varphi} G$ имеет неразрешимую проблему тождества слов.

Для того чтобы доказать теорему Новикова, достаточно вложить группу $G *_{\varphi} G$ в какую-нибудь конечно определенную группу. Мы сделаем это с помощью следующей теоремы.

Теорема Хигмена. *Конечно порожденная группа вложима в конечно определенную группу тогда и только тогда, когда она является рекурсивно определенной.*

У теоремы Хигмена имеется одна замечательная черта. Назовем группу *группой Хигмена*, если она является конечно порожденной и вложима в некоторую конечно определенную группу. Это является чисто алгебраическим понятием. По теореме Хигмена оно совпадает с понятием рекурсивно определенной группы, которое определено с помощью теории рекурсии.

Утверждение «только тогда» в теореме Хигмена тривиально. Каждая группа Хигмена изоморфна некоторой

подгруппе конечно определенной, а потому и рекурсивно определенной группы, поэтому она рекурсивно определенная. Оставшаяся часть этого приложения посвящена доказательству обратного утверждения.

Лемма 1. Если G и H — группы Хигмена, то $G \times H$ — группа Хигмена.

Доказательство. Очевидно, $G \times H = \{G, H\}$ является конечно порожденной группой. Если G и H вложимы в конечно определенные группы L и M , то $G \times H$ вложима в $L \times M$, которая является конечно определенной группой.

Лемма 2. Если G и G' — группы Хигмена, а φ — изоморфизм некоторой конечно порожденной подгруппы группы G в G' , то $G *_{\varphi} G'$ — группа Хигмена.

Доказательство. Очевидно, группа $G *_{\varphi} G' = \{G, G'\}$ является конечно порожденной. Если G и G' вложимы в конечно определенные группы K и K' , то $G *_{\varphi} G'$ вложима в $K *_{\varphi} K'$, которая является конечно определенной группой.

Изоморфизмом в группе G называется изоморфизм некоторой подгруппы H группы G в G . Пусть φ — такой изоморфизм, положим

$$G_{\varphi} = [G, t; tht^{-1} = \varphi(h)].$$

Чтобы изучить G_{φ} , мы вложим ее в большую группу. В группе $[G, r] = G * [r]$ подгруппа $\{G, rHr^{-1}\}$ является свободным произведением групп G и rHr^{-1} . Аналогично, в группе $[G_1, s]$ подгруппа $\{G_1, s\varphi(H)_1 s^{-1}\}$ является свободным произведением групп G_1 и $s\varphi(H)_1 s^{-1}$. Следовательно, существует изоморфизм ψ между $\{G, rHr^{-1}\}$ и $\{G_1, s\varphi(H)_1 s^{-1}\}$, определенный следующим образом: $\psi(g) = g_1$, $\psi(rhr^{-1}) = s\varphi(h)_1 s^{-1}$. Тогда

$$\begin{aligned} [G, r] *_{\varphi} [G_1, s] &= [G, G_1, r, s; g = g_1, rhr^{-1} = s\varphi(h)_1 s^{-1}] \\ &= [G, r, s; rhr^{-1} = s\varphi(h)_1 s^{-1}] \\ &= [G, r, s, t; rhr^{-1} = s\varphi(h)_1 s^{-1}, t = s^{-1}r] \\ &= [G, t, s, r; tht^{-1} = \varphi(h), r = st] \\ &= [G, t, s; tht^{-1} = \varphi(h)] = G_{\varphi} * [s]. \end{aligned}$$

Таким образом, существует изоморфизм из группы G_{φ} в $[G, r] *_{\varphi} [G_1, s]$, отображающий смежный класс, содержащий g , в g , и отображающий t в $s^{-1}r$.

Отсюда следует, что различные элементы из G лежат в различных смежных классах в G_{φ} , так что естественное

отображение из G в G_{φ} инъективно. Поэтому мы отождествляем G с некоторой подгруппой группы G_{φ} . Мы также отождествляем t с содержащим его смежным классом из G_{φ} и называем t φ -элементом. Тогда G_{φ} порождается G и t , и $tht^{-1} = \varphi(h)$ для $h \in H$.

Так как $\{G, rGr^{-1}\}$ является свободным произведением групп G и rGr^{-1} , то вследствие (1) мы имеем

$$\{G, rHr^{-1}\} \cap rGr^{-1} = rHr^{-1}.$$

Аналогично,

$$\{G_1, s\varphi(H)_1 s^{-1}\} \cap sG_1 s^{-1} = s\varphi(H)_1 s^{-1}.$$

Отсюда следует, что подгруппа $\{rGr^{-1}, sG_1 s^{-1}\} = \{rGr^{-1}, sGs^{-1}\}$ является свободным произведением групп rGr^{-1} и sGs^{-1} с объединенной подгруппой rHr^{-1} . Применяя внутренний автоморфизм, определенный элементом r^{-1} , и вспоминая, что $r^{-1}s = t$, мы видим, что $\{G, t^{-1}Gt\}$ является свободным произведением групп G и $t^{-1}Gt$ с объединенной подгруппой H . Отсюда

$$G \cap t^{-1}Gt = H. \quad (2)$$

Пусть G , φ и H такие же, как и ранее. Подгруппа K группы G инвариантна относительно φ , если $\varphi(H \cap K) = \varphi(H) \cap K$. (Это означает, что $h \in K \leftrightarrow \varphi(h) \in K$ для $h \in H$.) Если K инвариантна относительно φ , то $\varphi' = \varphi|_{(H \cap K)}$ является изоморфизмом в K . Покажем, что естественное отображение из $K_{\varphi'}$ в G_{φ} является вложением. Для этого достаточно показать, что естественное отображение из $[K, r] *_{\varphi'} [K_1, s]$ в $[G, r] *_{\varphi} [G_1, s]$ является вложением (здесь φ' определено так же, как и φ). Это отображение является вложением $[K, r]$ в $[G, r]$ как $\{K, r\}$, а $[K_1, s]$ в $[G_1, s]$ как $\{K_1, s\}$. Следовательно, мы должны проверить, что $\{K, r\}$ и $\{K_1, s\}$ имеют одно и то же пересечение с объединенной подгруппой. Однако

$$\{K, r\} \cap \{G, rHr^{-1}\} = \{K, r(H \cap K)r^{-1}\}. \quad (3)$$

Чтобы доказать это, заметим, что нормальная форма любого элемента из свободного произведения $\{G, rHr^{-1}\}$ имеет вид $\dots g_1 r h_1 r^{-1} g_2 r h_2 r^{-1} \dots$. Это является также нормальной формой в свободном произведении $[G, r]$, и этот элемент принадлежит $\{K, r\} = [K, r]$ тогда и только тогда, когда все g_i и h_i принадлежат K . Отсюда следует (3). Аналогично,

$$\{K_1, s\} \cap \{G_1, s\varphi(H)_1 s^{-1}\} = \{K_1, s(\varphi(H)_1 \cap K_1) s^{-1}\}. \quad (4)$$

Так как $\varphi(H \cap K) = \varphi(H) \cap K$, то правые части в (3) и (4) соответствуют друг другу при отображении ψ , как и требовалось.

Таким образом, мы можем отождествить K_φ с подгруппой $\{K, t\}$ группы G_φ . Из (1) также следует, что

$$\{K, r, s\} \cap \{G, r\} = \{K, r\}. \quad (5)$$

Применяя (1) к $\{K, r\} = K * [r]$, рассматриваемой в качестве подгруппы группы $G * [r]$, мы получаем, что

$$\{K, r\} \cap G = K.$$

Отсюда и из (5) следует, что $\{K, r, s\} \cap G \subset K$, и потому в G_φ

$$\{K, t\} \cap G = K. \quad (6)$$

Предположим, что мы задали множество $\varphi, \psi, \dots$ изоморфизмов в G . Тогда

$$G_{\varphi, \psi, \dots} = [G, t_\varphi, t_\psi, \dots; t_\varphi h t_\varphi^{-1} = \varphi(h), \dots].$$

Существует естественное вложение G в $G_{\varphi, \psi, \dots}$. Действительно, если это не так, то найдется некоторое соотношение $g = g'$, истинное в $G_{\varphi, \psi, \dots}$, но ложное в G , причем оно должно быть следствием конечного числа определяющих соотношений. Таким образом, нам надо рассмотреть лишь случай, когда существует только конечное число изоморфизмов. Этот случай легко доказывается индукцией, потому что

$$G_{\varphi_1, \dots, \varphi_n, \varphi_{n+1}} = (G_{\varphi_1, \dots, \varphi_n})_{\varphi_{n+1}}.$$

Если K является подгруппой группы G , инвариантной относительно всех $\varphi, \psi, \dots$, то

$$\{K, t_\varphi, t_\psi, \dots\} \cap G = K. \quad (7)$$

Правая часть содержится в левой. Так как любой элемент из $\{K, t_\varphi, t_\psi, \dots\}$ порождается подгруппой K и конечным числом элементов вида t , то нам надо доказать лишь обратное включение для конечного числа изоморфизмов. Мы сделаем это индукцией по числу изоморфизмов n . Случаем $n=1$ является (6). Если $n > 1$, то по индуктивному предположению

$$\{K, t_1, \dots, t_{n-1}\} \cap G = K.$$

Отсюда следует, что $\{K, t_1, \dots, t_{n-1}\}$ инвариантна относительно φ_n , поэтому вследствие (6)

$$\{K, t_1, \dots, t_n\} \cap G_{\varphi_1, \dots, \varphi_{n-1}} = \{K, t_1, \dots, t_{n-1}\}.$$

Рассматривая пересечение обеих частей с G и снова пользуясь индуктивным предположением, получаем

$$\{K, t_1, \dots, t_n\} \cap G \subset K.$$

Если φ является тождественным отображением из H в H , то вместо G_φ мы пишем G_H . Тогда любая подгруппа K группы G инвариантна относительно φ и $K_{H \cap K}$ вложена в G_H .

Пусть G — группа Хигмена. Изоморфизм φ в G называется *мягким*, если G_φ — группа Хигмена. Подгруппа H группы G называется *мягкой*, если G_H — группа Хигмена, т. е. если тождественное отображение из H в H является мягким. Заметим, что G_φ и G_H — обязательно конечно порожденные группы (потому что такова G).

Лемма 3. Если G — группа Хигмена, а φ — изоморфизм некоторой конечно порожденной подгруппы H группы G в G , то φ является мягким в G .

Доказательство. Группы $[G, r]$ и $[G_1, s]$ являются группами Хигмена по лемме 2. Так как группа $[G, r H r^{-1}]$ конечно порожденная, то $[G, r] *_\varphi [G_1, s]$ — группа Хигмена по лемме 2, и потому ее конечно порожденная подгруппа G_φ является группой Хигмена.

Следствие. Каждая конечно порожденная подгруппа группы Хигмена G является мягкой в G .

Лемма 4. Пусть K — группа Хигмена, а G — подгруппа Хигмена группы K . Тогда изоморфизм φ в G является мягким в G тогда и только тогда, когда он мягкий в K , поэтому подгруппа группы G является мягкой в K тогда и только тогда, когда она является мягкой в K .

Доказательство. Предположим, что K_φ — группа Хигмена. Тогда G_φ вложена в K_φ и потому является группой Хигмена. Теперь предположим, что G_φ — группа Хигмена. Если $\psi(g) = g_1$, то $G_\varphi *_\psi K_1$ — группа Хигмена по лемме 2. Далее, если H — область определения изоморфизма φ , то

$$\begin{aligned} G_\varphi *_\psi K_1 &= [G, t, K_1; t h t^{-1} = \varphi(h), g = g_1] \\ &= [G, t, K_1; t h_1 t^{-1} = \varphi(h)_1, g = g_1] \\ &= [K_1, t; t h_1 t^{-1} = \varphi(h_1)] \simeq K_\varphi. \end{aligned}$$

Мы будем часто неявно использовать лемму 4, не оговаривая особо, в какой именно группе Хигмена изоморфизм или подгруппа являются мягкими.

Лемма 5. Если H и K — мягкие подгруппы группы Хигмена G , то $H \cap K$ и $\{H, K\}$ являются мягкими в G .

Доказательство. Предположим вначале, что одна из подгрупп, например K , является конечно порожденной и, следовательно, группой Хигмена. Тогда $K_{H \cap K}$ вложима в G_H и потому является группой Хигмена, поэтому подгруппа $H \cap K$ мягкая. В G_H подгруппа $\{G, t^{-1}Gt\}$ является свободным произведением групп G и $t^{-1}Gt$ с объединенной подгруппой $H = t^{-1}Ht$. Так как $\{H, K\}$ и $t^{-1}Gt$ включают объединенную подгруппу, то вследствие (1) мы имеем

$$\{H, K, t^{-1}Gt\} \cap G = \{H, K\},$$

откуда следует, что

$$\{K, t^{-1}Gt\} \cap G = \{H, K\}. \quad (8)$$

Обе группы слева конечно порожденные, поэтому их пересечение $\{H, K\}$ мягкое.

В общем случае имеем $G \cap t^{-1}Gt = H$ в G_H , поэтому

$$H \cap K = G \cap (t^{-1}Gt \cap K).$$

Так как G и $t^{-1}Gt$ — конечно порожденные и потому мягкие группы (согласно следствию из леммы 3), то два рассмотренных частных случая показывают, что $H \cap K$ — мягкая группа. Равенство (8) все еще выполняется. Согласно рассмотренному частному случаю $\{K, t^{-1}Gt\}$ — мягкая группа. Таким образом, $\{H, K\}$ является пересечением двух мягких подгрупп и, следовательно, сама мягкая.

Лемма 6. Пусть φ — гомоморфизм группы Хигмена G в группу Хигмена H . Если L — мягкая подгруппа группы G , то $\varphi(L)$ — мягкая подгруппа группы H . Если M — мягкая подгруппа группы H , то $\varphi^{-1}(M)$ — мягкая подгруппа группы G .

Доказательство. По лемме 1 $G \times H$ — группа Хигмена. Пусть Q — подгруппа группы $G \times H$, состоящая из всех $(g, \varphi(g))$. Тогда Q изоморфна G (при отображении $(g, \varphi(g)) \rightarrow g$). Таким образом, группы G , H и Q конечно порожденные и, следовательно, мягкие в $G \times H$. Так как

$$\begin{aligned} \varphi(L) &= \{L, H\} \cap Q, G \cap H, \\ \varphi^{-1}(M) &= \{M, G\} \cap Q, H \cap G, \end{aligned}$$

то утверждение леммы следует из леммы 5.

Лемма 7. Если φ — изоморфизм группы Хигмена G в G и H — мягкая подгруппа группы G , то $\varphi|_H$ мягкий в G .

Доказательство. По лемме 3 φ является мягким в G , поэтому G_φ — группа Хигмена. Отсюда следует, что H — мягкая группа в G_φ и потому $(G_\varphi)_H$ — группа Хигмена. Однако

$$\begin{aligned} (G_\varphi)_H &= [G, s, t; sgs^{-1} = \varphi(g), tht^{-1} = h] \\ &= [G, s, t, r; sgs^{-1} = \varphi(g), stht^{-1}s^{-1} = \varphi(h), r = st] \\ &= [G, r, s, t; rhr^{-1} = \varphi(h), sgs^{-1} = \varphi(g), t = s^{-1}r] \\ &= [G, r, s; rhr^{-1} = \varphi(h), sgs^{-1} = \varphi(g)] = (G_\varphi|_H)_\varphi. \end{aligned}$$

Таким образом, $G_\varphi|_H$ вложима в группу Хигмена и, следовательно, сама является группой Хигмена.

Множество $\varphi, \psi, \dots$ изоморфизмов в группе Хигмена G называется мягким, если $G_{\varphi, \psi, \dots}$ может быть так вложена в некоторую группу Хигмена H , что $\{t_\varphi, t_\psi, \dots\}$ является мягкой подгруппой группы H . Любое конечное множество мягких изоморфизмов в G является мягким, так как мы можем ввести $H = G_{\varphi, \psi, \dots}$ и воспользоваться следствием из леммы 3.

Лемма 8. Пусть G — группа Хигмена, H — мягкая подгруппа группы G , $\varphi, \psi, \dots$ — мягкое множество изоморфизмов в G , K — наименьшая подгруппа группы G , содержащая H и инвариантная относительно $\varphi, \psi, \dots$. Тогда K является мягкой.

Доказательство. Вложим $G_{\varphi, \psi, \dots}$ в группу Хигмена L так, что $\{t_\varphi, t_\psi, \dots\}$ является мягкой. Покажем, что

$$K = G \cap \{H, t_\varphi, t_\psi, \dots\}.$$

Тогда лемма будет следовать из леммы 5. Очевидно, правая часть инвариантна относительно $\varphi, \psi, \dots$ и потому включает K . Вследствие (7)

$$G \cap \{H, t_\varphi, t_\psi, \dots\} \subset G \cap \{K, t_\varphi, t_\psi, \dots\} = K.$$

Пусть A — конечное множество, выберем элемент z , не принадлежащий A . Если P — множество слов в A , то через E_P обозначим подгруппу группы $[A, z]$, порожденную словами XzX^{-1} , где X принадлежит P . Так как слова XzX^{-1} , где X — слово в A , образуют свободное множество, то $XzX^{-1} \in E_P$ тогда и только тогда, когда $X \in P$.

Подмножество P группы $[A]$ называется *мягким* в $[A]$, если E_P является мягкой в $[A, z]$. Отсюда получается два определения *мягкости*, если P является подгруппой группы $[A]$; мы должны показать, что они совпадают. Предположим, что множество P мягкое как подгруппа, тогда по лемме 5 $\{P, z\}$ является мягкой в $[A, z]$. Далее, $E_{[A]}$ является наименьшей подгруппой группы $[A, z]$, содержащей z и инвариантной относительно внутренних автоморфизмов, определенных элементами из A . Вследствие лемм 3 и 8 $E_{[A]}$ является мягкой. Покажем, что $E_P = \{P, z\} \cap E_{[A]}$, тогда из леммы 5 будет следовать, что E_P мягкая. Очевидно, $E_P \subset \{P, z\} \cap E_{[A]}$. Далее, E_P содержит z и инвариантна относительно внутренних автоморфизмов, определенных элементами из P , поэтому она является нормальной подгруппой группы $\{P, z\}$. Так как $z \in E_P$, то естественное отображение из P в $\{P, z\}/E_P$ сюръективно. Следовательно, если $x \in \{P, z\}$, то $x = py$, где $p \in P$, $y \in E_P$. Гомоморфизм φ группы $[A, z]$ в $[A]$, определенный равенствами $\varphi(a) = a$, $\varphi(z) = e$, отображает $E_{[A]}$ в единичную подгруппу. Поэтому если $x = py$ принадлежит $E_{[A]}$, то $e = \varphi(x) = \varphi(p)\varphi(y) = \varphi(p) = p$. Отсюда $x = y$, поэтому $x \in E_P$.

Теперь предположим, что E_P мягкая; мы должны доказать, что P — мягкая подгруппа. Пусть c и d — новые элементы и для каждого слова X в A пусть φ_X — изоморфизм между $\{c\}$ и $\{dX\}$, определенный следующим образом: $\varphi_X(c) = dX$. Мы хотим показать, что множество всех φ_X , где X принадлежит P , является мягким. Если это так, то наименьшая подгруппа содержащая c и d и инвариантная относительно φ_X , где X принадлежит P , является мягкой. Этой подгруппой является $\{P, c, d\}$. Так как

$$P = \{P, c, d\} \cap G,$$

то P является мягкой по лемме 5.

Пусть $H = [A, c, d]_{\varphi_X, \varphi_Y, \dots}$ (здесь использованы все слова в A). Тогда

$$H = [A, c, d, t_X, t_Y, \dots; t_X c t_X^{-1} = dX, \dots].$$

Для доказательства достаточно вложить H в такую группу Хигмена, в которой подгруппа, порожденная элементами t_X , где X принадлежит P , является мягкой. Предположим, что $A = \{a_1, \dots, a_n\}$. Определим автоморфизм ψ_i группы

$[A, c, d, t_X, t_Y, \dots]$ следующим образом: $\psi_i(a) = a$, $\psi_i(c) = c$, $\psi_i(d) = da_i$, $\psi_i(t_X) = t_{a_i X}$. Применяя ψ_i к соотношению $t_X c t_X^{-1} = dX$, получаем $t_{a_i X} c t_{a_i X}^{-1} = da_i X$. Таким образом, ψ_i переставляет определяющие соотношения группы H и потому индуцирует некоторый автоморфизм группы H . Следовательно, мы можем вложить H в группу K с образующими A, c, d , всеми t_X и $a'_1, \dots, a'_n$ и с определяющими соотношениями

$$t_X c t_X^{-1} = dX, \quad (9)$$

$$a'_i a a_i^{-1} = a, \quad (10)$$

$$a'_i c a_i^{-1} = c, \quad (11)$$

$$a'_i d a_i^{-1} = da_i, \quad (12)$$

$$a'_i t_X a_i^{-1} = t_{a_i X}. \quad (13)$$

Пусть $t = t_e$, и пусть для слова X в A слово X' является словом, полученным из X заменой каждого a_i на a'_i . Вследствие (13) $X' t X'^{-1} = t_X$. Из леммы 6 и из предположения, что E_P мягкая, мы видим, что подгруппа K , порожденная $X' t X'^{-1} = t_X$ для $X \in P$, является мягкой. Равенство $X' t X'^{-1} = t_X$ показывает, что мы можем исключить образующие t_X , отличные от t , заменяя (9) на

$$(X' t X'^{-1}) c (X' t X'^{-1})^{-1} = dX \quad (9')$$

и опуская (13). Мы хотим показать, что (9') является следствием из (10), (11), (12) и $t c t^{-1} = d$; отсюда будет следовать, что K — конечно определенная группа и потому является группой Хигмена. Из (10), (11) и (12) мы получаем $X' c X'^{-1} = c$, $X' d X'^{-1} = dX$. Поэтому, применяя внутренний автоморфизм, определенный X' , к $t c t^{-1} = d$, мы получаем (9').

Основная лемма. Если A конечно, а P — рекурсивно перечислимое множество слов в A , то P мягкое.

Сначала посмотрим, каким образом основная лемма позволяет нам завершить доказательство теоремы Хигмена. Рекурсивно определенную группу можно записать как G/K , где G — свободная группа над конечным множеством, а K — рекурсивно перечислимая нормальная подгруппа группы G . По основной лемме подгруппа K мягкая, поэтому мы можем вложить G_K в конечно определенную группу H . В G_K подгруппа $\{G, t^{-1} G t\}$ является свободным произведением

групп G и $t^{-1}Gt$ с объединенной подгруппой $K = t^{-1}Kt$. Естественное отображение из G в G/K и отображение из $t^{-1}Gt$ в единичную подгруппу группы G/K согласовано с объединенной подгруппой, поэтому мы имеем гомоморфизм φ подгруппы $\{G, t^{-1}Gt\}$ в G/K такой, что $\varphi(g) = gK$, $\varphi(t^{-1}gt) = eK$. Определим гомоморфизм ψ подгруппы $\{G, t^{-1}Gt\}$ в $H \times G/K$, полагая $\psi(x) = (x, \varphi(x))$. Тогда ψ является изоморфизмом в $H \times G/K$. Так как G/K вложима в $(H \times G/K)_\psi$, то для доказательства достаточно показать, что последняя группа является конечно определенной.

Группа H имеет конечное число образующих и определяющих соотношений. Добавляя, если это необходимо, новые образующие, мы можем предполагать, что это множество образующих включает t и множество образующих группы G . Чтобы получить образующие для $(H \times G/K)_\psi$, мы присоединим к нему конечное число образующих группы G_1 и какой-нибудь ψ -элемент s . Кроме определяющих соотношений группы H , нам нужны в качестве определяющих соотношений группы $(H \times G/K)_\psi$ соотношения, утверждающие, что элементы из K_1 равны e , соотношения, утверждающие, что образующие группы H перестановочны с образующими группы G_1 , и соотношения, которые дают значения shs^{-1} , где h — образующая группы $\{G, t^{-1}Gt\}$. Мы покажем, что соотношения, утверждающие, что элементы из K_1 равны e , излишни; тогда мы будем иметь дело с конечным числом определяющих соотношений.

Пусть X_1 — слово в множестве образующих группы G_1 , представляющее некоторый элемент из K_1 . Равенства для значений shs^{-1} дают $sX_1s^{-1} = X \cdot X_1$ и $st^{-1}X_1ts^{-1} = X$. Так как X принадлежит K , то соотношения в H влекут $t^{-1}Xt = X$. Из этих трех равенств мы получаем, что $X_1 = e$.

Теперь мы докажем несколько лемм о мягких множествах слов. При этом предполагается, что A и B конечны.

Лемма 9. Каждое конечное подмножество элементов из $[A]$ является мягким в $[A]$.

Доказательство получается из следствия к лемме 3.

Лемма 10. Если $A \subset B$ и P — множество слов в A , то P является мягким в $[A]$ тогда и только тогда, когда P является мягким в $[B]$.

Доказательство по лемме 4.

Лемма 11. Если P и Q — мягкие подмножества элементов из $[A]$, то $P \cap Q$ и $P \cup Q$ мягкие.

Доказательство. Так как XzX^{-1} свободны, то $E_{P \cap Q} = E_P \cap E_Q$ и $E_{P \cup Q} = \{E_P, E_Q\}$. Теперь воспользуемся леммой 5.

Спутником отображения φ группы $[A]$ в $[B]$ называется такой гомоморфизм ψ группы $[A, z]$ в $[B, z]$, что $\psi(XzX^{-1}) = \psi(X)z\psi(X)^{-1}$, где X — слово в A . Если φ — гомоморфизм, то он имеет спутника. Действительно, мы можем продолжить φ до гомоморфизма ψ группы $[A, z]$ в $[B, z]$, полагая $\psi(z) = z$, и тогда ψ является спутником гомоморфизма φ .

Биективное отображение группы $[A]$ в $[A]$ называется *точным*, если оно имеет спутника, являющегося автоморфизмом группы $[A, z]$. Очевидно, композиция двух точных отображений является точным отображением. Всякий автоморфизм φ группы $[A]$ является точным; действительно, φ можно продолжить до автоморфизма ψ группы $[A, z]$, если положить $\psi(z) = z$, и ψ является спутником отображения φ .

Для каждого слова Y в A мы определяем отображения L_Y и R_Y группы $[A]$ в $[A]$ следующим образом: $L_Y(X) = Y \cdot X$, $R_Y(X) = X \cdot Y$. Эти отображения являются точными. Действительно, определенный Y внутренний автоморфизм является спутником отображения L_Y , а спутник φ отображения R_Y определен следующим образом: $\varphi(a) = a$, $\varphi(z) = YzY^{-1}$.

Лемма 12. Пусть φ — отображение группы $[A]$ в $[B]$, имеющее спутника. Если P — мягкое подмножество элементов из $[A]$, то $\varphi(P)$ — мягкое подмножество элементов из $[B]$.

Доказательство. Если ψ — спутник отображения φ , то $E_{\varphi(P)} = \psi(E_P)$. Теперь воспользуемся леммой 6.

Пусть P и Q — подмножества элементов из $[A]$, и пусть φ — отображение группы $[A]$ в $[A]$. Мы говорим, что P является (φ, Q) -инвариантным, если для каждого X из Q имеем $X \in P$ тогда и только тогда, когда $\varphi(X) \in P$. Если $Q = [A]$, то вместо (φ, Q) -инвариантно мы говорим инвариантно относительно φ .

Лемма 13. Пусть $P, Q_1, \dots, Q_n$ — мягкие подмножества элементов из $[A]$, $\varphi_1, \dots, \varphi_n$ — точные отображения группы $[A]$ в $[A]$, R — наименьшее подмножество элементов из A , включающее P и являющееся (φ_i, Q_i) -инвариантным при $i = 1, \dots, n$. Тогда R мягкое.

Доказательство. Пусть ψ_i — автоморфизм группы $[A, z]$, являющийся спутником отображения φ_i . По лемме 7 отображение $\psi_i|E_{Q_i}$ мягкое. Следовательно, по лемме 8 наименьшая подгруппа, включающая E_R и инвариантная относительно $\psi_i|E_{Q_i}$, является мягкой. Мы покажем, что этой подгруппой является E_R . Элемент g из E_{Q_i} является произведением слов $Xz^{\pm 1}X^{-1}$, где X принадлежит Q_i . Чтобы получить $\psi_i(g)$, заменим каждое X на $\varphi_i(X)$. Тогда $g \in E_R$ тогда и только тогда, когда $\psi_i(g) \in E_R$. Таким образом, E_R инвариантно относительно $\psi_i|E_{Q_i}$. Далее, всякий элемент из R получается из элемента из P многократным применением φ_i и φ_i^{-1} с соблюдением условия, что φ_i применяется только к словам из Q_i , а φ_i^{-1} применяется только к словам из $\varphi_i(Q_i)$. Отсюда следует, что если $X \in R$, то XzX^{-1} принадлежит каждой подгруппе, включающей E_R и инвариантной относительно $\psi_i|E_{Q_i}$. Отсюда следует нужное утверждение.

Так как $[A]$ является мягкой в качестве подгруппы, а следовательно, и в качестве подмножества, то в лемме 13 мы можем заменить (φ_i, Q_i) -инвариантно на инвариантно относительно φ_i .

Лемма 14. Пусть $b_i = b^i a b^{-i}$, и пусть P — множество всех таких слов $b_{i_1} b_{i_2} \dots b_{i_n}$, что $0 \leq i_1 < i_2 < \dots < i_n$. Тогда P — мягкое подмножество элементов из $[a, b]$.

Доказательство. Пусть H, H^+ и H' — подгруппы, порожденные соответственно всеми b_i , всеми b_i , для которых $i > 0$, и всеми b_i , для которых $i \geq 0$. Покажем, что эти подгруппы мягкие. Так как H является наименьшей подгруппой, содержащей a и инвариантной относительно внутреннего автоморфизма, определенного b , то по лемме 8 она мягкая. Далее, $H' = \{H^+, a\}$, поэтому вследствие леммы 5 достаточно рассмотреть H^+ .

Определим гомоморфизмы φ и χ группы $[a, b]$ в $[a, b]$ следующим образом:

$$\varphi(a) = a, \quad \chi(a) = bab^{-1}, \quad \varphi(b) = \chi(b) = b^2.$$

Легко заметить, что φ и χ инъективны, поэтому по лемме 7 $\varphi|H$ и $\chi|H$ мягкие. Следовательно, по лемме 8 достаточно показать, что H^+ — наименьшая подгруппа, содержащая b_1 и инвариантная относительно $\varphi|H$ и $\chi|H$. Имеем $\varphi(b_i) = b_{2i}$, $\chi(b_i) = b_{2i+1}$. Индукцией по i легко проверить, что

любая подгруппа, содержащая b_1 и инвариантная относительно $\varphi|H$ и $\chi|H$, должна содержать b_i , где $i > 0$. Любой элемент x из H равен произведению элементов b_i и обратных к ним, и $x \in H^+$ тогда и только тогда, когда для всех использующихся b_i имеем $i > 0$. Отсюда мы видим, что $x \in H^+ \Leftrightarrow \varphi(x) \in H^+ \Leftrightarrow \chi(x) \in H^+$. Это доказывает, что H^+ инвариантна относительно $\varphi|H$ и $\chi|H$.

Пусть теперь ψ — автоморфизм группы $[a, b]$, определенный следующим образом:

$$\psi(a) = bab^{-1}, \quad \psi(b) = b.$$

Тогда $\psi(b_i) = b_{i+1}$. Принимая во внимание лемму 13, достаточно показать, что P — наименьшее подмножество, которое содержит e и является (L_a, H^+) -инвариантным и (ψ, H') -инвариантным. Покажем, например, что P является (L_a, H^+) -инвариантным. Элемент h из H^+ есть $b_{i_1}^{\pm 1} \dots b_{i_n}^{\pm 1}$, где i_i положительны. Тогда $L_a(h)$ есть $b_0 b_{i_1}^{\pm 1} \dots b_{i_n}^{\pm 1}$. Вспоминая, что b_i свободны, мы видим, что они оба принадлежат P , если все показатели равны $+1$ и $i_1 < \dots < i_n$, и оба не принадлежат P в противном случае.

Слово в A позитивно, если оно не содержит a^{-1} ни для какого a из A .

Лемма 15. Множество всех позитивных слов в A является мягким.

Доказательство. Пусть $A = \{a_1, \dots, a_n\}$. Определим автоморфизм φ группы $[A, z]$ следующим образом:

$$\varphi(a_i) = a_{i+1} \text{ для } i < n, \quad \varphi(a_n) = a_1, \quad \varphi(z) = z.$$

Тогда по лемме 3 $[A, z]_\varphi$ — группа Хигмена. Пусть t — φ -элемент, а ψ — гомоморфизм из $[a, b, z]$ в $[A, z]_\varphi$, определенный следующим образом:

$$\psi(a) = a_1, \quad \psi(b) = t, \quad \psi(z) = z.$$

Если P то же, что и в лемме 14, то легко заметить, что $\psi(P)$ совпадает с множеством Q позитивных слов в A . Тогда $\psi(E_P) = E_Q$, и потому E_Q мягкая вследствие лемм 14 и 6.

Отождествим каждую k -ку натуральных чисел с позитивным словом в $\{a, b\}$, отождествляя $x_1, \dots, x_k$ с $a^{x_1} b a^{x_2} b \dots b a^{x_k}$. Тогда можно говорить о том, что k -местный предикат мягкий. Мы изучим некоторые свойства мягких

предикатов. Обозначим через W множество позитивных слов, а через W_b множество слов из W , начинающихся с b . Из лемм 15 и 12 следует, что эти множества мягкие (потому что $W_b = L_b(W)$). Везде далее предполагается, что число i целое, а числа m и n натуральные.

А. Предикаты $=$, $\mathfrak{G}_+$ и $\mathfrak{G}$ мягкие.

Доказательство. Наименьшим множеством, содержащим b и инвариантным относительно $L_a R_a$, является множество всех $a^i b a^i$. Его пересечение с W является множеством всех $a^n b a^n$, а это множество есть предикат $=$. Наименьшим множеством, содержащим $L_b(=)$ и инвариантным относительно $L_a R_a$, является множество всех $a^i b a^n b a^{i+n}$; пересечение этого множества с W есть $\mathfrak{G}_+$.

Наименьшим множеством слов в $\{a, b, c\}$, содержащим b и инвариантным относительно $L_a R_c$, является множество всех $a^i b c^i$. Если мы возьмем пересечение этого множества с W и рассмотрим его образ при L_{cb} , то получим множество Q всех $c b a^n b c^n$. Пусть φ — автоморфизм группы $[a, b, c]$, определенный следующим образом:

$$\varphi(a) = a, \quad \varphi(b) = b, \quad \varphi(c) = ca.$$

Если мы возьмем пересечение наименьшего множества, включающего Q и инвариантного относительно φ , с W , то получим множество P всех $ca^m b a^n b (ca^m)^n$. Если ψ — гомоморфизм группы $[a, b, c]$ в $[a, b]$, определенный следующим образом: $\psi(a) = a$, $\psi(b) = b$, $\psi(c) = e$, то $\psi(P) = \mathfrak{G}$.

Б. Если предикат P мягкий, а предикат Q определен следующим образом: $Q(a, x) \leftrightarrow P(x, a)$, то предикат Q мягкий.

Доказательство. Мы можем предполагать, что a непуста, так как в противном случае Q совпадает с P . Наименьшим множеством, включающим $R_b(P)$ и инвариантным относительно $L_a^{-1} R_a$, является множество всех $a^n b X b a^i$, где $a^n b X$ принадлежит P . Если мы возьмем пересечение этого множества с W_b и рассмотрим его образ при $L_{b^{-1}}$, то получим Q .

В. Если предикат P мягкий, а предикат Q определен следующим образом: $Q(x, a) \leftrightarrow P(a)$, то Q мягкий.

Доказательство. Взять пересечение наименьшего множества, включающего $L_b(P)$ и инвариантного относительно L_a , с W .

Г. Если предикат P мягкий, а предикат Q определен следующим образом: $Q(a) \leftrightarrow \exists x P(x, a)$, то предикат Q мягкий.

Доказательство. Взять пересечение наименьшего множества, включающего P и инвариантного относительно L_a , с W_b и рассмотреть его образ при $L_{b^{-1}}$.

Д. Если предикат P мягкий, а предикат Q определен следующим образом:

$$Q(x, a) \leftrightarrow \forall y_{y < x} P(y, a),$$

то Q мягкий.

Доказательство. Множество всех a мягкое; это доказывается индукцией по числу переменных в a , используя В. Применяя L_b , мы получим, что предикат R , определенный следующим образом: $R(x, a) \leftrightarrow x = 0$, является мягким. Тогда Q — наименьшее множество, которое включает R и является (L_a, P) -инвариантным.

Теперь мы покажем, что некоторые явные определения предикатов дают мягкие предикаты. Предположим сначала, что в определении используются только переменные и символы мягких предикатов. Тогда оно имеет вид

$$P(x_1, \dots, x_k) \leftrightarrow Q(x_{j_1}, \dots, x_{j_p}),$$

где Q мягкий. Мы можем переписать его следующим образом: $P(x_1, \dots, x_k) \leftrightarrow$

$$\leftrightarrow \exists y_1 \dots \exists y_p (y_1 = x_{j_1} \& \dots \& y_p = x_{j_p} \& Q(y_1, \dots, y_p)).$$

Чтобы показать, что P мягкий, достаточно доказать, ввиду леммы 11 и Г, что $y_r = x_{j_r}$ и $Q(y_1, \dots, y_p)$ являются мягкими предикатами от $y_1, \dots, y_p, x_1, \dots, x_k$. Однако это легко следует из Б и В, так как $=$ и Q мягкие.

Вследствие леммы 11, Г и Д в явных определениях мягких предикатов мы можем применять $\vee$, $\&$, кванторы существования и ограниченные кванторы всеобщности. Мы можем также применять константы. Например, мы можем заменить $\dots 0 \dots$ на $\exists x (x = 0 \& \dots x \dots)$, а затем отметить, что по лемме 9 $x = 0$ — мягкий предикат.

Лемма 16. Если F — рекурсивная функция, то $\mathfrak{G}_F$ мягкий.

Доказательство. Воспользуемся индукцией по рекурсивным функциям. Если F есть I_i^n , то утверждение следует из А, Б и В. Если F есть $+$ или $\cdot$, то оно сле-

дует из А. Далее, предикат $x \neq 0$ мягкий, потому что он является образом предиката $x = x$ при L_a . Отсюда и из явных определений

$$\begin{aligned} x \leq y &\leftrightarrow \exists z \mathfrak{G}_+(x, z, y), \\ x < y &\leftrightarrow \exists z (z \neq 0 \& \mathfrak{G}_+(x, y, z)) \end{aligned}$$

мы видим, что $\leq$ и $<$ мягкие. Следовательно, если F есть $K_<$, то мы имеем явное определение

$$\mathfrak{G}_F(x, y, z) \leftrightarrow (x < y \& z = 0) \vee (y \leq x \& z = 1).$$

Предположим, что F определена следующим образом:

$$F(a) = G(H_1(a), \dots, H_k(a)),$$

где $G, H_1, \dots, H_k$ мягкие. Тогда $\mathfrak{G}_F$ имеет явное определение

$$\begin{aligned} \mathfrak{G}_F(a, x) &\leftrightarrow \\ &\leftrightarrow \exists y_1 \dots \exists y_k (\mathfrak{G}_{H_1}(a, y_1) \& \dots \& \mathfrak{G}_{H_k}(a, y_k) \& \mathfrak{G}_G(y_1, \dots, y_k, x)). \end{aligned}$$

Предположим, что F определена следующим образом:

$$F(a) = \mu x (G(a, x) = 0),$$

где G мягкая. Тогда $\mathfrak{G}_F$ имеет явное определение

$$\mathfrak{G}_F(a, x) \leftrightarrow \mathfrak{G}_G(a, x, 0) \& \forall y_{y < x} \exists z (z \neq 0 \& \mathfrak{G}_G(a, x, z)).$$

Лемма 17. *Каждый рекурсивно перечислимый предикат мягкий.*

Доказательство. Вследствие Г достаточно рассмотреть рекурсивный предикат P . Так как $P(a) \leftrightarrow \mathfrak{G}_{K_P}(a, 0)$, то P мягкий по лемме 16.

Лемма 18. *Если Q — рекурсивно перечислимое множество позитивных слов в A , то Q мягкое.*

Доказательство. Пусть P такое же, как в лемме 14, а ψ такой же, как в доказательстве леммы 15. Так как $\psi(P)$ является множеством позитивных слов в A , то

$$\psi(\psi^{-1}(Q) \cap P) = Q$$

и потому

$$\psi(E_{\psi^{-1}(Q) \cap P}) = E_Q.$$

Поэтому достаточно показать, что $\psi^{-1}(Q) \cap P$ мягкое. Так как очевидно, что $\psi^{-1}(Q) \cap P$ рекурсивно перечисливо, то достаточно доказать, что каждое рекурсивно перечислимое подмножество R множества P мягкое.

Пусть φ — гомоморфизм группы $[a, z]$ в $[a, z]$, определенный следующим образом: $\varphi(a) = a^2$, $\varphi(z) = z$. Тогда отображение φ инъективно. По лемме 3 $[a, z]_\varphi$ — группа Хигмена. Пусть b является φ -элементом, а χ является естественным отображением группы $[a, b, z]$ в $[a, z]_\varphi$. В обозначениях леммы 14 имеем $\chi(b_i) = a^{2^i}$ при $i \geq 0$. Следовательно, если $X = b_{i_1} \dots b_{i_n}$ является словом в P , то $\chi(X) = a^x$, где $x = 2^{i_1} + \dots + 2^{i_n}$, поэтому $\chi(XzX^{-1}) = a^x z a^{-x}$. Теперь число x может быть записано в виде $2^{i_1} + \dots + 2^{i_n}$, где $0 \leq i_1 < \dots < i_n$, только одним способом. Вследствие этого χ инъективно на E_P , поэтому $E_R = E_P \cap \chi^{-1}(\chi(E_R))$. Таким образом, достаточно показать, что $\chi(E_R)$ мягкое. Далее, $\chi(E_R) = E_{\chi(R)}$, где $\chi(R)$ является множеством позитивных слов в $\{a\}$. Так как R рекурсивно перечисливо, то $\chi(R)$ рекурсивно перечисливо. Это означает, что $\chi(R)$ является рекурсивно перечислимым унарным предикатом. Следовательно, по лемме 17 $\chi(R)$ мягкое.

Теперь мы можем доказать основную лемму. Пусть P — рекурсивно перечислимое множество слов в A . Пусть A' состоит из элементов a' для каждого элемента a из A , и пусть φ — гомоморфизм группы $[A, A']$ в $[A]$, определенный следующим образом: $\varphi(a) = a$, $\varphi(a') = a^{-1}$. Пусть, наконец, P' — такое множество позитивных слов X в $A \cup A'$, что $\varphi(X) \in P$. Тогда множество P' рекурсивно перечислимое и в силу леммы 18 мягкое. Так как $P = \varphi(P')$, то P мягкое по лемме 12.

НЕРАЗВЕТВЛЕННОЕ ВЫНУЖДЕНИЕ *)

1. Введение

Метод вынуждения был придуман Коэном для решения некоторых классических проблем независимости. Как только стало ясно, что сам метод применим в гораздо более общих случаях, специалисты по теории множеств упростили и обобщили этот метод. Одним из результатов таких попыток являются булевозначные модели, исследуемые в статье Скотта и Соловея **).

Характерная черта булевозначного подхода состоит в том, что использование разветвленной иерархии конструктивных множеств становится ненужным. Так как модели вынуждения могут быть получены из булевозначных моделей, то очевидно, что эта иерархия не нужна также и для моделей вынуждения.

Одна из целей настоящей статьи — дать прямую конструкцию моделей вынуждения, не использующую разветвленную иерархию. В дополнение к этому я попытался дать сводку некоторых упрощений и обобщений теории вынуждения, упомянутой выше. Многие из этих результатов в настоящее время содержатся лишь в малодоступных источниках.

Было бы невозможно перечислить всех лиц, добившихся каких-либо продвижений в этой проблематике. Наши исторические справки будут по крайней мере указывать, кем были получены основные результаты. Общая картина заимствована из заметок Скотта и Сильвера **) и лекций Роуботтома в Калифорнийском университете, прочитанных осенью 1967 г. Беседы с Чжаном и Роуботтомом были также очень полезны.

*) J. R. Shoenfield, Unramified forcing, Proc. Symp. Pure Math. 13, № 1 (1971), 357—380.

**) Статьи Скотта и Соловея, Скотта и Сильвера публикуются в Proc. Symp. Pure Math. 13, №1, №2.

2. Предварительные сведения

Здесь мы перечислим основные результаты теории множеств, которые нам нужны.

Обозначим через ZF аксиоматическую систему Цермело — Френкеля (аксиомы объемности, регулярности, бесконечности, объединения, замены и степени), а через ZFC систему ZF с аксиомой выбора. При рассмотрении функций как некоторых множеств упорядоченных пар мы считаем, что значение функции есть первая, а аргумент функции — вторая компонента упорядоченной пары. Таким образом, областью значений (областью определения) f является множество первых (вторых) элементов упорядоченных пар из f . Обозначения: $U(x)$ — объединение всех множеств из x , $S(x)$ — множество степени множества x , $\langle x, y \rangle$ — упорядоченная пара, $Ra(x)$ — область значений множества x , $Do(x)$ — область определения множества x , ${}^x y$ — множество всех отображений из множества x в y .

Мы отождествляем ординал с множеством предшествующих ординалов, а кардинал с наименьшим ординалом, имеющим заданную мощность (таким образом, $\aleph_\alpha = \omega_\alpha$). Греческие буквы используются для обозначения ординалов, а готические — для обозначения бесконечных кардиналов (или бесконечных мощностей моделей). Через $|x|$ будем обозначать мощность (кардинал) множества x и через m^+ — следующий за m кардинал. Напомним, что $cf(\alpha)$ означает наименьшее β такое, что существует отображение β на конфинальное подмножество из α . Бесконечный кардинал m называется *регулярным*, если $cf(m) = m$, и *сингулярным*, если $cf(m) < m$. В любом случае $cf(\alpha)$ всегда равно 1 или является регулярным кардиналом. Если m — регулярный кардинал, то объединение $< m$ множеств, мощность каждого из которых $< m$, имеет мощность $< m$. Через $S_m(x)$ обозначаем $\{y \mid y \subset x \text{ и } |y| < m\}$.

$V(\alpha)$ (иногда используется обозначение $R(\alpha)$) определяется трансфинитной индукцией следующим образом:

$$V(\alpha) = \bigcup_{\beta < \alpha} S(V(\beta)).$$

Рангом множества x , обозначаемым через $rk(x)$, называется наименьшее α такое, что $x \in V(\alpha + 1)$. Это понятие всюду

определено и из $x \in y$ следует $\text{rk}(x) < \text{rk}(y)$. Более того, $\text{rk}(\alpha) = \alpha$.

Мы предполагаем известными некоторые факты элементарной арифметики кардиналов. Напомним, что

$$|xy| = |y|^{|x|}, \quad |S(x)| = 2^{|x|}.$$

Теорема Кёнига утверждает, что $\text{cf}(2^m) > m$. Обозначим через GCH обобщенную гипотезу континуума: $\forall n (2^n = n^+)$. Слабые степени определяются следующим образом:

$$m^n = \sum_{p < n} m^p.$$

(Здесь мы допускаем случай, когда p конечны, но эти члены могут быть опущены, если $n > \aleph_0$.) Тогда $m^{n^+} = m^n$. Так как каждое подмножество множества x мощности p является областью значений некоторого элемента из ${}^p x$, то мы имеем $|S_n(x)| \leq |x|^n$.

Имеем

$$n < \text{cf}(m) \text{ \& } \forall p < m (2^p \leq m) \rightarrow m^n = m. \quad (2.1)$$

Действительно, из $n < \text{cf}(m)$ следует $m^n = \bigcup_{\alpha < m} m^\alpha$. Однако

$|m^\alpha| = |\alpha|^n \leq 2^{|\alpha| \cdot n} \leq m$ по предположению, поэтому $m^n \leq m \cdot m = m$. Если GCH выполняется, то утверждение (2.1) сводится к $n < \text{cf}(m) \rightarrow m^n = m$. Из (2.1) следует, что

$$m \text{ регулярное \& } \forall p < m (2^p \leq m) \rightarrow m^m = m.$$

Так, например, если m есть $\aleph_0$, то $m^m = m$ является сильно недостижимым, и если GCH выполняется, то $m^m = m$ для всех регулярных m .

Обратимся теперь к моделям теории множеств. Модель называется *транзитивной*, если ее универсум является транзитивным множеством и ее предикат принадлежности является обычным предикатом принадлежности, ограниченным до ее универсума. Метод сжатия Мостовского [8] показывает, что каждая вполне фундированная модель аксиомы объемности изоморфна транзитивной модели. В дальнейшем под моделью мы будем понимать транзитивную модель и будем отождествлять модель с ее универсумом.

Пусть M — некоторая модель. Чтобы отметить, что какой-то объект рассматривается в модели M , мы будем до-

бавлять фразу «в M » или верхний индекс M . Так, если Φ — предложение (возможно, содержащее имена элементов из M), то будем сокращать фразу « Φ истинно при интерпретации в M » до « Φ выполняется в M » или просто до Φ^M .

Кардиналом в M называется элемент a из M такой, что « a есть кардинал» выполняется в M . Через ω_1^M мы обозначаем элемент a из M такой, что $\Phi(a)^M$, где $\Phi(x)$ — предложение теории множеств, утверждающее, что x есть ω_1 . Подобным же образом интерпретируются и другие меры.

Классом в M называется множество $[a | a \in M \& \Phi(a)^M]$, где $\Phi(x)$ содержит только символы языка теории ZFC и символы для множеств из M . Каждое множество из M есть класс в M . Если M — модель теории ZFC, то каждый класс в M , который включается в некоторое множество из M , сам является множеством из M . *Функционалом в M* называется функция F такая, что для некоторой формулы $\Phi(x, y)$ описанного выше типа $F(a) = b$ тогда и только тогда, когда $a, b \in M$ и $\Phi(a, b)^M$. Если M — модель теории ZFC, то образ множества из M относительно функционала в M есть множество из M .

Лемма 2.1. Каждое транзитивное множество M , удовлетворяющее следующим четырем условиям, является моделью теории ZF.

(а) $\omega \in M$.

(б) Каждый класс в M , который включается в некоторое множество из M , сам является множеством из M .

(в) Для каждого функционала F в M и каждого множества a из M , включенного в область определения функционала F , множество $U(\{F(b) | b \in a\})$ включено в некоторое множество из M .

(г) Для каждого множества a из M множество $S(a) \cap M$ включается в некоторое множество из M .

Предикатный символ P , определяемый в теории ZFC, называется *абсолютным*, если для каждой модели M теории ZFC предикат P^M совпадает с P на аргументах из M . Подобное определение вводится для функциональных символов (в том числе и для констант как функциональных символов с нулевым числом аргументов). Большинство символов, введенных при изучении ординалов, абсолютны, за исключением S . Детали смотри в [9] или в данной

книге. Если F абсолютный, то F принимает значения из M (так как F^M таков). Из абсолютного предиката «... есть ординал» следует, что ординалы в M являются настоящими ординалами, принадлежащими M .

Аксиома конструктивности (см. [5]) утверждает, что каждое множество конструктивно. Отсюда следует, что существует определяемое вполне упорядочение универсума и что выполняется GCH. Если M — модель теории ZFC, то конструктивные множества в M образуют модель теории ZFC с аксиомой конструктивности. Каноническая функция, отображающая ординалы на конструктивные множества, абсолютна, поэтому конструктивные множества в некоторой модели M теории ZFC являются образами ординалов в M относительно этой функции. Таким образом, если M и N имеют одинаковые ординалы, то они имеют и одинаковые конструктивные множества.

3. Понятия вынуждения

Предположим, что M — модель теории ZFC и $a, b \in M$. Мы хотим расширить M до модели N , в которой существует отображение F множества a на b . Чтобы избежать очевидных трудностей, допустим, что a бесконечно и $b \neq 0$.

Пусть C — множество всех отображений всевозможных конечных подмножеств множества a в b . Тогда $C \in M$ в силу абсолютности. Множество G всех конечных подмножеств множества F будет подмножеством множества C , но оно не обязательно будет в M . Наша идея состоит в том, чтобы, во-первых, подобрать G , а затем, используя G , построить N .

Каждое $p \in C$ дает некоторое условие, которому должно удовлетворять F , чтобы p было в G , а именно, мы должны иметь $p \subset F$. Если $p \subset q$, то условие q дает больше информации, чем условие p . Тогда мы говорим, что q есть расширение p , и пишем $q \leq p$. (Такое обозначение должно намекать на то, что q допускает меньше моделей N , чем p .) Тогда C является частично упорядоченным множеством с наибольшим элементом 0.

Имеются три очевидных условия, которым должно удовлетворять G : (а) $0 \in G$; (б) если $p \in G$ и $p \leq q$, то $q \in G$; (в) любые два элемента из G имеют общее расширение в G . Если G удовлетворяет этим условиям, то $F = U(G)$ будет

отображением некоторого подмножества множества a на некоторое подмножество множества b .

Для того чтобы получить $\text{Do}(F) = a$ и $\text{Ra}(F) = b$, множество G должно, кроме того, пересекаться с некоторыми множествами, а именно, с каждым множеством $[p \mid x \in \text{Do}(p)]$ для $x \in a$ и с каждым множеством $[p \mid y \in \text{Ra}(p)]$ для $y \in b$. Эти множества являются множествами в M и имеют следующее свойство: каждое условие из C имеет расширение в каждом таком множестве. Поэтому мы будем требовать, чтобы G пересекалось с каждым множеством в M , имеющим это свойство.

Теперь обобщим эти понятия. *Понятие вынуждения* есть частично упорядоченное множество C , имеющее наибольший элемент. Мы обозначим этот порядок через $\leq_C$ или $\leq$, а наибольший элемент через 1_C или 1 . Элементы множества C называются *условиями*. Обычно условия будут обозначаться через p, q и r . Если $p \leq q$, то мы скажем, что p есть *расширение* q . Подмножество D множества C назовем *C-плотным* (или просто *плотным*), если каждое условие из C имеет расширение в D .

Пусть C — некоторое понятие вынуждения, а M — некоторое множество. Подмножество G множества C называется *C-генерическим* над M (или просто *генерическим*), если справедливы следующие утверждения:

- (G1) $1 \in G$;
- (G2) для любых $p \in G$ и $q \geq p$ имеем $q \in G$;
- (G3) для любых $p, q \in G$ условия p и q имеют общее расширение в G ;
- (G4) для каждого плотного множества D в M имеем $G \cap D \neq \emptyset$.

Теорема существования. Пусть C — некоторое понятие вынуждения, M — счетное множество, $p \in C$. Тогда существует *C-генерическое* над M множество G , содержащее p .

Доказательство. Пусть $a_0, a_1, \dots$ — элементы M . Выбираем p_n индуктивно следующим образом: $p_0 = p$, p_{n+1} — некоторое расширение условия p_n из a_n , если такое расширение существует, и $p_{n+1} = p_n$ в противном случае. Тогда множество $G = [q \mid \exists n (p_n \leq q)]$ имеет требуемые свойства.

Замечание. Это единственное место, где мы прямо используем счетность M . Очевидно, достаточно было бы предположить, что $M \cap S(C)$ счетно.

Пусть $H_m(A; B)$ — множество всех отображений p всевозможных элементов множества $S_m(A)$ в B . Если $p, q \in H_m(A; B)$, то мы пишем $p \leq q$ вместо $q \subset p$. Тогда $H_m(A; B)$ есть понятие вынуждения с наибольшим элементом 0. Мы пишем $H(A; B)$ вместо $H_{\aleph_0}(A; B)$. Заметим, что $H(A; B)$ абсолютно.

Теперь предположим, что M — модель теории ZFC, $a, b \in M$, $b \neq 0$, m — бесконечный кардинал в M такой, что $m \leq |a|$ в M , $C = H_m^M(a; b)$, G — C -генерическое над M множество и $F = U(G)$. Тогда замечания в начале параграфа показывают, что F — отображение из a на b . (Нам нужно $m \leq |a|$ в M для того, чтобы гарантировать, что для каждого $y \in b$ множество $\{p \mid y \in \text{Ra}(p)\}$ плотно.) Таким образом, если мы можем построить расширение N модели M , содержащее G , то мы получим расширение, в котором существует отображение из a на b .

З а м е ч а н и е. Это показывает, что если a счетно и бесконечно и b несчетно, то не существует C -генерического множества над M . Поэтому требование счетности в теореме существования не может быть опущено.

Историческая справка. Основные идеи этого параграфа принадлежат Коэну [1], [2]. Понятие плотного множества принадлежит Соловею.

4. Построение модели

Теперь предположим, что C — понятие вынуждения*) в некоторой счетной модели M теории ZFC и G — C -генерическое множество над M . Мы собираемся построить расширение модели M , содержащее G .

Вначале определим структуру, универсумом которой является M , а отношение принадлежности $\in_G$ определяется следующим образом: $a \in_G b \leftrightarrow \exists p \in G (\langle a, p \rangle \in b)$ (здесь и в дальнейшем a, b, c и d обозначают элементы множества M). Теперь мы применим метод сжатия, чтобы переделать $\langle M, \in_G \rangle$ в транзитивную модель. Сначала заметим, что

$$a \in_G b \rightarrow a \in \text{Ra}(b) \quad (4.1)$$

*) Понятие вынуждения C лежит в некоторой модели M , если множество C и отношение $\leq$ лежат в M .

и, следовательно,

$$a \in_G b \rightarrow \text{rk}(a) < \text{rk}(b). \quad (4.2)$$

Затем мы определяем

$$K_G(b) = [K_G(a) \mid a \in_G b].$$

По (4.2) это есть правильное определение индукцией по $\text{rk}(b)$. Наконец, определим

$$M[G] = [K_G(a) \mid a \in M].$$

Главная теорема. Пусть M — счетная модель теории ZFC, C — некоторое понятие вынуждения в M , G — некоторое C -генерическое над M множество. Тогда $M[G]$ — счетная модель теории ZFC, расширяющая M и содержащая G , и это есть наименьшая такая модель.

Доказательство этой фундаментальной теоремы будет дано здесь и в следующих двух параграфах. Мы предполагаем, что всюду дальше в этой статье M , C и G удовлетворяют условиям основной теоремы, за исключением специально оговоренных случаев. Мы будем писать $\hat{a}$ вместо $K_G(a)$.

Начнем с некоторых простых замечаний. Из определения $M[G]$ и счетности M видно, что $M[G]$ счетно и транзитивно. Теперь определим

$$\hat{b} = [\langle \hat{a}, 1 \rangle \mid a \in b]$$

индукцией по $\text{rk}(b)$. Это определение может быть дано в M , поэтому отображение, переводящее a в $\hat{a}$, есть функционал в M . В частности, $\hat{a} \in M$. Простая индукция (используя (G1)) показывает, что $K_G(\hat{b}) = b$; таким образом, $M \subset M[G]$. Теперь положим (обозначая несколько неправильно)

$$\hat{G} = [\langle \hat{p}, p \rangle \mid p \in C].$$

Тогда $\hat{G} \in M$ и $K_G(\hat{G}) = G$. Следовательно, $G \in M[G]$. Итак, $M[G]$ — счетное транзитивное множество, расширяющее M и содержащее G . Проверка того, что это есть модель теории ZFC, требует одного нового понятия, к которому мы сейчас и переходим.

5. Вынуждение

Введем язык, называемый *языком вынуждения*, подходящий для исследования $M[G]$. Символами языка вынуждения являются символы теории ZFC и все элементы*) множества M . Каждый элемент a множества M считается константой, которая отмечает элемент $\bar{a}$ из $M[G]$; мы называем a *именем* элемента $\bar{a}$. Если Φ — предложение языка вынуждения, то $\vdash_G \Phi$ означает, что Φ истинно в $M[G]$.

Пусть $p \in C$ и Φ — предложение языка вынуждения. Скажем, что p *вынуждает* Φ , и записываем это $p \Vdash \Phi$, если $\vdash_G \Phi$ для каждого множества G , являющегося C -генерическим над M и содержащего p .

Наша первоочередная задача — доказать три леммы о вынуждении.

Лемма определимости. Если $\Phi(x_1, \dots, x_n)$ — формула теории ZFC, содержащая только указанные свободные переменные, то

$$[\langle p, a_1, \dots, a_n \rangle \mid p \Vdash \Phi(a_1, \dots, a_n)]$$

является классом в M .

Лемма о расширении. Если $p \Vdash \Phi$ и $q \leq p$, то $q \Vdash \Phi$.

Лемма об истинности. Если G генерическое, то $\vdash_G \Phi$ тогда и только тогда, когда $\exists p \in G (p \Vdash \Phi)$.

Наш метод состоит в следующем. Мы определим видоизмененное понятие вынуждения, обозначаемое через $p \Vdash^* \Phi$. Затем докажем, что эти три леммы выполняются при замене $\Vdash$ на $\Vdash^*$. Далее мы покажем, что

$$p \Vdash \Phi \leftrightarrow p \Vdash^* \neg \neg \Phi. \quad (5.1)$$

Затем, беря эти три леммы для $\Vdash^*$ и заменяя Φ на $\neg \neg \Phi$, получим леммы для $\Vdash$.

Вначале укажем неопределяемые символы языка вынуждения. Считаем, что $\neg$ и $\vee$ — неопределяемые пропозициональные связки и $\exists$ — неопределяемый квантор. В качестве неопределяемых символов отношений мы берем $\in$ и $\neq$.

*) Те, кому не нравится использование множеств в качестве символов, могут ввести некоторое новое множество символов, которое находится во взаимно однозначном соответствии с M .

Конечно, $x \neq y$ определяется как $\neg(x \in y)$, $x = y$ определяется как $\neg(x \neq y)$.

Теперь определяем $p \Vdash^* \Phi$ с помощью следующих пяти пунктов.

- (а) $p \Vdash^* a \in b$, если $\exists c \exists q \geq p (\langle c, q \rangle \in b \ \& \ p \Vdash^* a = c)$.
- (б) $p \Vdash^* a \neq b$, если $\exists c \exists q \geq p (\langle c, q \rangle \in a \ \& \ p \Vdash^* c \notin b)$ или $\exists c \exists q \geq p (\langle c, q \rangle \in b \ \& \ p \Vdash^* c \notin a)$.
- (в) $p \Vdash^* \neg \Phi$, если $\forall q \leq p \neg(q \Vdash^* \Phi)$.
- (г) $p \Vdash^* \Phi \vee \Psi$, если $p \Vdash^* \Phi$ или $p \Vdash^* \Psi$.
- (д) $p \Vdash^* \exists x \Phi(x)$, если $\exists b (p \Vdash^* \Phi(b))$.

Сначала мы должны убедиться, что в этом определении нет порочных кругов. Если мы проанализируем определение $p \Vdash^* a \neq b$, то найдем, что оно определяется в терминах $p' \Vdash^* a' \neq b'$ и $p' \Vdash^* b' \neq a'$, где $\text{rk}(a') < \text{rk}(a)$ и $\text{rk}(b') < \text{rk}(b)$. Тем самым мы можем определить $p \Vdash^* a \neq b$ индукцией по $\max(\text{rk}(a), \text{rk}(b))$. Затем мы применяем (в) для определения $p \Vdash^* a = b$, (а) для определения $p \Vdash^* a \in b$ и (в) для определения $p \Vdash^* a \notin b$. Тогда мы можем получить (б). Это определяет $p \Vdash^* \Phi$ для атомных формул Φ . Затем применяем (в), (г) и (д) для определения $p \Vdash^* \Phi$ для всех Φ индукций по длине Φ .

* Лемма определимости для $\Vdash^*$ тривиально доказывается индукцией по длине $\Phi(x_1, \dots, x_n)$ (замечая, что область действия кванторов в (а)–(д) есть M или множество C в M). Конечно, определение класса $[\langle p, a, b \rangle \mid p \Vdash^* a \neq b]$ должно быть проведено трансфинитной индукцией в M так, как описано выше.

Мы докажем другие две леммы, доказывая их для предложений в левых частях (а)–(д) при предположении, что эти леммы являются истинными для предложений в правых частях; как мы видели выше, это правильный метод доказательства. Лемма о расширении совсем тривиальна, поэтому мы рассмотрим лишь лемму об истинности.

Вначале покажем, что если лемма об истинности выполняется для Φ , то

$$a \in_G b \ \& \ \vdash_G \Phi \leftrightarrow$$

$$\leftrightarrow \exists p \in G \exists q \geq p (\langle a, q \rangle \in b \ \& \ p \Vdash^* \Phi). \quad (5.2)$$

Если левая часть выполняется, то существуют $q, r \in G$ такие, что $\langle a, q \rangle \in b$ и $r \Vdash^* \Phi$. Выбирая общее расширение

ние p для q и r в G по (G3), получаем $p \Vdash^* \Phi$ ввиду леммы о расширении. Обратно, пусть правая часть (5.2) выполняется для p и q . Тогда $\vdash_G \Phi$ ввиду леммы об истинности. Также $q \in G$ ввиду (G2), следовательно, $a \in_G b$.

Теперь обратимся к пяти случаям леммы об истинности.

(а) $\vdash_G a \in b$ эквивалентно $\exists c (c \in_G b \ \& \ \vdash_G a = c)$ по определению b . По предположению и (5.2) это эквивалентно

$$\exists c \exists p \in G \exists q \geq p (\langle c, q \rangle \in b \ \& \ p \Vdash^* a = c)$$

и, следовательно, эквивалентно $\exists p \in G (p \Vdash^* a \in b)$.

(б) Ясно, что $\vdash_G a \neq b$ тогда и только тогда, когда или $\exists c (c \in_G a \ \& \ \vdash_G c \notin b)$, или $\exists c (c \in_G b \ \& \ \vdash_G c \notin a)$. По предположению и (5.2) это эквивалентно

$$\begin{aligned} \exists c \exists p \in G \exists q \geq p (\langle c, q \rangle \in a \ \& \ p \Vdash^* c \notin b) \vee \\ \vee \exists c \exists p \in G \exists q \geq p (\langle c, q \rangle \in b \ \& \ p \Vdash^* c \notin a) \end{aligned}$$

и, следовательно, эквивалентно $\exists p \in G (p \Vdash^* a \neq b)$.

(в) По предположению $\vdash_G \neg \Phi$ тогда и только тогда, когда $\neg \exists p \in G (p \Vdash^* \Phi)$. Поэтому мы должны доказать, что выполняется в точности одно из двух: $\exists p \in G (p \Vdash^* \Phi)$ или $\exists p \in G (p \Vdash^* \neg \Phi)$. Чтобы доказать, что по крайней мере одна из формул выполняется, по (G4) достаточно показать, что $D = [p \mid p \Vdash^* \Phi \text{ или } p \Vdash^* \neg \Phi]$ является плотным множеством в M . По лемме определимости множество D является множеством в M , поэтому мы должны лишь показать, что каждое p имеет расширение в D . Но либо p имеет расширение q такое, что $q \Vdash^* \Phi$ и, следовательно, $q \in D$, либо $p \Vdash^* \neg \Phi$ и, следовательно, p само находится в D .

Теперь предположим, что существуют $p, q \in G$ такие, что $p \Vdash^* \Phi$ и $q \Vdash^* \neg \Phi$. По (G2) p и q имеют общее расширение r , а по лемме о расширении $r \Vdash^* \Phi$. Это противоречит тому, что $q \Vdash^* \neg \Phi$.

Легкие доказательства (г) и (д) оставляем читателю.

Теперь докажем (5.1). Предположим, что $p \Vdash^* \neg \neg \Phi$. Если множество G генерическое и $p \in G$, то по лемме об истинности $\vdash_G \neg \neg \Phi$, поэтому $\vdash_G \Phi$. Таким образом, $p \Vdash \Phi$. Теперь предположим, что $\neg (p \Vdash^* \neg \neg \Phi)$. Тогда $q \Vdash^* \neg \neg \Phi$ для некоторого $q \leq p$. Выберем такое генерическое множество G , что $q \in G$. Ввиду леммы об истинности $\vdash_G \neg \neg \Phi$, а по (G2) $p \in G$. Следовательно, $\neg (p \Vdash \Phi)$.

Таким образом, мы показали все наши леммы. Подставляя $\neg \neg \Phi$ вместо Φ в (в), получаем

$$p \Vdash \neg \Phi \text{ тогда и только тогда, когда } \forall q \leq p (q \Vdash \Phi). \quad (5.3)$$

Заменяя Φ на $\neg \Phi$ и замечая, что $p \Vdash \neg \neg \Phi$ эквивалентно $p \Vdash \Phi$, получаем

$$p \Vdash \Phi \text{ тогда и только тогда, когда } \forall q \leq p (q \Vdash \neg \Phi). \quad (5.4)$$

Историческая справка. По существу понятие вынуждения Коэна есть наше $\Vdash^*$. Часть (в) определения, которая упрощает определение Коэна, введена Скоттом. Наше понятие вынуждения введено Феферманом [4], который назвал его *слабым вынуждением*. Все три фундаментальные леммы доказаны Коэном.

6. Завершение доказательства

Покажем, что $M[G]$ — модель теории ZF, доказав, что $M[G]$ удовлетворяет всем условиям леммы 2.1. Так как $\omega \in M \subset M[G]$, то условие (а) выполняется.

Лемма 6.1. Пусть A — класс в $M[G]$ такой, что $A \subset \bar{a}$. Тогда $A \in M[G]$ и A имеет имя c такое, что $c \subset Ra(a) \times C$.

Доказательство. Существует формула $\Phi(x)$ языка вынуждения такая, что

$$\bar{b} \in A \leftrightarrow \vdash_G \Phi(b) \quad (6.1)$$

для всех b . Положим

$$c = [\langle b, p \rangle \mid b \in Ra(a) \ \& \ p \Vdash \Phi(b)].$$

Ввиду леммы определимости c есть класс в M . А так как $c \subset Ra(a) \times C$, то $c \in M$.

Мы должны показать, что

$$\bar{b} \in c \leftrightarrow \bar{b} \in A.$$

Если $\bar{b} \in c$, то мы можем предположить, изменив b , но не изменяя $\bar{b}$, что $b \in_G c$. Тогда для некоторого $p \in G$ имеем $\langle b, p \rangle \in c$ и, следовательно, $p \Vdash \Phi(b)$. Таким образом, $\vdash_G \Phi(b)$, поэтому $\bar{b} \in A$ в силу (6.1). Пусть теперь $\bar{b} \in A$. Тогда $\bar{b} \in \bar{a}$, поэтому мы можем предположить, что $b \in_G a$. Ввиду (4.1) $b \in Ra(a)$. Ввиду

(6.1) $\vdash_G \Phi(b)$, поэтому по лемме об истинности некоторое $p \in G$ вынуждает $\Phi(b)$. Тогда $\langle b, p \rangle \in c$, поэтому $b \in_G c$, таким образом, $\bar{b} \in \bar{c}$.

Из леммы 6.1 следует, что утверждение (б) леммы 2.1 выполняется.

Лемма 6.2. Если $x \subset M[G]$ и каждый элемент из x имеет имя в a , то x включается в некоторое множество в $M[G]$.

Доказательство. Пусть $b = a \times \{1\}$. Любой элемент из x есть $\bar{c}$ для некоторого $c \in a$. Но $c \in_G b$ в силу (G1), следовательно, $\bar{c} \in \bar{b}$. Таким образом, $x \subset \bar{b}$.

Теперь докажем, что утверждение (в) леммы 2.1 выполняется. Пусть F — функционал в $M[G]$ и $\bar{a}$ — множество в $M[G]$, входящее в область определения для F . Существует формула $\Phi(x, y)$ языка вынуждения такая, что для всех b, c имеем

$$F(\bar{b}) = \bar{c} \leftrightarrow \vdash_G \Phi(b, c).$$

Выберем множество d в M со следующим свойством: для каждого $p \in C$ и каждого $b \in \text{Ra}(a)$, если существует c такое, что $p \vdash \Phi(b, c)$, то существует такое же множество в d . Заменяя d его транзитивным замыканием, мы можем предполагать, что d транзитивно.

Теперь покажем, что каждый элемент x из $U(\{F(\bar{b}) \mid \bar{b} \in \bar{a}\})$ имеет имя в d ; ввиду леммы 6.2 на этом наше доказательство будет закончено. Имеем $x \in F(\bar{b})$, где $\bar{b} \in \bar{a}$. Мы можем предположить, что $b \in_G a$. Пусть c будет именем $F(\bar{b})$. Имеем $\vdash_G \Phi(b, c)$, поэтому некоторое $p \in G$ вынуждает $\Phi(b, c)$. Следовательно, для некоторого $c' \in d$ имеем $p \vdash \Phi(b, c')$. Тогда $\vdash_G \Phi(b, c')$, поэтому $F(\bar{b}) = \bar{c}'$. Следовательно, $x \in \bar{c}'$, откуда $x = \bar{a}'$ для $a' \in_G c'$, а поэтому $a' \in \text{Ra}(c')$. Так как $c' \in d$ и d транзитивно, то $a' \in d$, что и требовалось.

Наконец, докажем, что утверждение (г) леммы 2.1 выполняется. Пусть $\bar{a} \in M[G]$, и пусть $\bar{b} \in S(\bar{a}) \cap M[G]$. Ввиду леммы 6.1 $\bar{b}$ имеет имя c такое, что $c \subset \text{Ra}(a) \times C$ и, значит, $c \in S^M(\text{Ra}(a) \times C)$. Требуемый результат теперь следует из леммы 6.2. Тем самым $M[G]$ является моделью теории ZF.

Лемма 6.3. Если N — модель теории ZF, расширяющая M и содержащая G , то существует функционал в N ограничением которого на M является K_G .

Доказательство. Определим (в N)

$$x \in^* y \leftrightarrow \exists p \in G (\langle x, p \rangle \in y), \\ K^*(y) = [K^*(x) \mid x \in^* y]$$

(индукцией по $\text{rk}(y)$). Легко видеть (используя транзитивность M), что $\in^*$ и K^* совпадают соответственно с $\in_G$ и K_G для аргументов из M .

Из леммы следует, что $K_G(a) \in N$ для всех $a \in M$, так что $M[G] \subset N$. Поэтому $M[G]$ является даже наименьшей моделью теории ZF, расширяющей M и содержащей G . Далее, можно применить лемму 6.3 к $M[G]$. Мы получим функцию K в $M[G]$, ограничение которой на M есть K_G .

Пусть теперь $\bar{a} \in M[G]$. Тогда в M и, значит, в $M[G]$ существует отображение некоторого ординала на $\text{Ra}(a)$. Комбинируя K с этим отображением, получим в $M[G]$ отображение некоторого ординала на

$$[K(x) \mid x \in \text{Ra}(a)] = [\bar{b} \mid b \in \text{Ra}(a)].$$

Но ввиду (4.1) это множество включает $\bar{a}$. Поэтому в $M[G]$ выполняется следующее: для каждого x существует отображение некоторого ординала на некоторое множество, содержащее x . Из этого следует, что аксиома выбора выполняется в $M[G]$. Итак, мы завершили доказательство главной теоремы.

Историческая справка. Большинство идей этого параграфа принадлежит Козну. Доказательство того, что аксиома степени выполняется в $M[G]$, по существу принадлежит Соловею; оно проще, чем доказательство Козна.

7. Аксиома конструктивности

Для наилучшего применения фундаментальной теоремы нам нужна информация про отношение между M и $M[G]$. Следующий простой результат часто бывает полезен.

Лемма 7.1. M и $M[G]$ имеют одинаковые ординалы.

Доказательство. Так как $M \subset M[G]$, то нам нужно лишь показать, что каждый ординал α из $M[G]$ есть в M . Простая индукция показывает, что $\text{rk}(\bar{a}) \leq \text{rk}(a)$ для всех a . Пусть a будет именем α , тогда $\alpha = \text{rk}(\alpha) \leq \text{rk}(a)$. Так как rk абсолютно, то $\text{rk}(a) \in M$, поэтому $\alpha \in M$ в силу транзитивности M .

Следствие. M и $M[G]$ имеют одинаковые конструктивные множества.

Пусть теперь M — счетная модель теории ZFC, и пусть $C = H(\omega; 2)$. В силу абсолютности, C лежит в M . Возьмем G генерическим над M и положим $F = U(G)$. Как мы видели в § 3, F — отображение из ω на 2. Очевидно, $F \in M[G]$; мы утверждаем, что $F \notin M$. Чтобы показать это, допустим, что f — произвольное отображение из ω на 2, лежащее в M . Тогда $\{p \mid \exists n \in \omega (n \in \text{Do}(p) \& p(n) \neq f(n))\}$ — множество в M , которое является, как легко видеть, плотным. Поэтому оно содержит некоторое $p \in G$, а отсюда следует, что $F \neq f$.

Поэтому множество A , характеристическая функция которого есть F , лежит в $M[G] - M$. По следствию A не является конструктивным в $M[G]$. Поэтому $M[G]$ — это модель теории ZFC', где теория ZFC' — теория ZFC с дополнительной аксиомой: существует неконструктивное подмножество множества ω .

Мы показали, как построить модель теории ZFC' из счетной модели M теории ZFC. Существование M может быть показано следующим образом. Мы начинаем с любой модели N теории ZFC. Применяя теорему Левенгейма — Скулема для того, чтобы получить счетную подмодель, и применяя технику сжатия, мы получим счетную модель M теории ZFC.

К несчастью, существование (транзитивной) модели N теории ZFC не может быть доказано в теории ZFC даже в предположении, что теория ZFC непротиворечива. Поэтому, если мы хотим иметь финитное доказательство относительной непротиворечивости теории ZFC' по отношению к теории ZFC, то мы должны сделать небольшие изменения. Добавим к теории ZFC константу N и аксиомы, которые утверждают, что N транзитивно и непусто и каждая аксиома теории ZFC выполняется в N . Принцип отражения (см. [6]) показывает, что это будет консервативным расширением теории ZFC. Затем определим M и $M[G]$, как раньше. Наше доказательство будет тогда показывать, что каждая аксиома теории ZFC' выполняется в $M[G]$. Немного другой метод изложен в данной книге.

Мы можем получить более сильный результат с помощью «сжатия» кардинала в M . Допустим, что M удовлетворяет аксиоме конструктивности. (Мы можем получить такую

модель из любой счетной модели N теории ZFC, взяв множества, конструктивные в N .) Возьмем $C = H(\aleph_0; \aleph_1^M)$. Тогда в $M[G]$ существует отображение из $\aleph_0$ на $\aleph_1^M$; таким образом, $\aleph_1^M$ счетно в $M[G]$. Существует одно-однозначное соответствие между $S^M(\omega)$ и $\aleph_1^M$, которое лежит в M , и, следовательно, в $M[G]$, поэтому $S^M(\omega)$ счетно в $M[G]$. Но в силу следствия каждое подмножество множества ω , которое конструктивно в $M[G]$, есть в M и, следовательно, в $S^M(\omega)$. Таким образом, в $M[G]$ существует только счетное число конструктивных подмножеств множества ω .

Историческая справка. Независимость аксиомы конструктивности была доказана Коэном. Кардинальное сжатие введено Леви.

8. Произведения

Пусть C_1 и C_2 — некоторые понятия вынуждения в M . Мы будем снабжать индексами 1 или 2 все ранее введенные понятия, чтобы отличать, что относится к C_1 , а что к C_2 ; например, p_1 — некоторый элемент из C_1 , G_2 — некоторое C_2 -генерическое множество. Будем писать $M[G_1, G_2]$ вместо $(M[G_1])[G_2]$.

Определим частичный порядок на $C_1 \times C_2$ следующим образом:

$$\langle p_1, p_2 \rangle \leq \langle q_1, q_2 \rangle \leftrightarrow p_1 \leq q_1 \& p_2 \leq q_2.$$

Ясно, что $C_1 \times C_2$ является понятием вынуждения в M с наибольшим элементом $\langle 1_1, 1_2 \rangle$.

Теорема о произведении. Пусть C_1 и C_2 — произвольные понятия вынуждения в M . Если G_1 является C_1 -генерическим над M , а G_2 — C_2 -генерическим над $M[G_1]$, то $G_1 \times G_2$ является $(C_1 \times C_2)$ -генерическим над M , и $M[G_1 \times G_2] = M[G_1, G_2]$. Каждое множество, являющееся $(C_1 \times C_2)$ -генерическим над M , получается таким путем.

Доказательство. Легко проверить (G_1) , (G_2) и (G_3) для $G_1 \times G_2$. Пусть D — произвольное $(C_1 \times C_2)$ -плотное множество в M . Мы должны показать, что $(G_1 \times G_2) \cap D \neq \emptyset$, т. е. что $G_2 \cap D_2 \neq \emptyset$, где

$$D_2 = \{p_2 \mid \exists p_1 \in G_1 (\langle p_1, p_2 \rangle \in D)\}.$$

Так как $D_2 \in M[G_1]$, то достаточно показать, что D_2 является C_2 -плотным.

Пусть $q_2 \in C_2$; мы должны найти $p_2 \leq q_2$ и $p_1 \in G$ такие, что $\langle p_1, p_2 \rangle \in D$. Другими словами, мы должны показать, что $G_1 \cap D_1 \neq 0$, где

$$D_1 = [p_1 \mid \exists p_2 \leq q_2 (\langle p_1, p_2 \rangle \in D)].$$

Так как $D_1 \in M$, то достаточно показать, что D_1 является C_1 -плотным. Пусть $q_1 \in C_1$, и выберем $\langle p_1, p_2 \rangle \leq \langle q_1, q_2 \rangle$ так, чтобы $\langle p_1, p_2 \rangle \in D$. Тогда $p_1 \leq q_1$ и $p_1 \in D_1$.

Равенство $M[G_1 \times G_2] = M[G_1, G_2]$ выполняется, потому что оба множества являются наименьшими моделями теории ZFC, расширяющими M и содержащими G_1 и G_2 .

Пусть теперь G будет $(C_1 \times C_2)$ -генерическим над M , а G_1 и G_2 — проекции G на C_1 и C_2 соответственно. Ясно, что $G \subset G_1 \times G_2$. Чтобы доказать, что $G = G_1 \times G_2$, допустим, что $\langle p_1, p_2 \rangle \in G_1 \times G_2$. Для некоторых q_1 и q_2 имеем $\langle p_1, q_2 \rangle, \langle q_1, p_2 \rangle \in G$. Поэтому они имеют общее расширение $\langle r_1, r_2 \rangle$ в G . А так как $\langle r_1, r_2 \rangle \leq \langle p_1, p_2 \rangle$, то получаем $\langle p_1, p_2 \rangle \in G$.

Проверка (G1), (G2) и (G3) для G_1 и G_2 совсем легкая. Чтобы проверить (G4) для G_1 , допустим, что D_1 является C_1 -плотным множеством в M . Тогда $D_1 \times C_2$ является $(C_1 \times C_2)$ -плотным множеством в M . Поэтому $G \cap (D_1 \times C_2) \neq 0$; таким образом, $G_1 \cap D_1 \neq 0$.

Чтобы проверить (G4) для G_2 , допустим, что D_2 — C_2 -плотное множество в $M[G_1]$. Пусть a — имя D_2 , и пусть Φ — предложение языка вынуждения, утверждающее, что $\bar{a}$ является C_2 -плотным.

Покажем, что

$$D = [\langle p_1, p_2 \rangle \mid p_1 \Vdash \Phi \rightarrow \hat{p}_2 \in a]$$

плотно. Пусть дано $\langle q_1, q_2 \rangle$. Выберем G'_1 C_1 -генерическое над M так, чтобы $q_1 \in G'_1$. Если $K_{G'_1}(a)$ является C_2 -плотным, то выберем $p_2 \leq q_2$ так, чтобы $p_2 \in K_{G'_1}(a)$, в противном случае положим $p_2 = q_2$. В любом случае имеем $\vdash_{G'_1} \Phi \rightarrow \hat{p}_2 \in a$. Поэтому некоторое $p_1 \in G'_1$ вынуждает $\Phi \rightarrow \hat{p}_2 \in a$, а по (G3) и лемме о расширении мы можем предположить, что $p_1 \leq q_1$. Тогда $\langle p_1, p_2 \rangle \leq \langle q_1, q_2 \rangle$ и $\langle p_1, p_2 \rangle \in D$.

Так как $D \in M$, то отсюда следует, что $G \cap D \neq 0$. Пусть $\langle p_1, p_2 \rangle \in G \cap D$. Поскольку $p_1 \in G_1$ и $p_1 \Vdash \Phi \rightarrow$

$\rightarrow \hat{p}_2 \in a$, то мы имеем $\vdash_{G_1} \Phi \rightarrow \hat{p}_2 \in a$. Но $\vdash_{G_1} \Phi$, поэтому $p_2 \in \bar{a} = D_2$. Но $p_2 \in G_2$, следовательно, $G_2 \cap D_2 \neq 0$.

Следствие. Пусть C_1 и C_2 — произвольные понятия вынуждения в M . Пусть G_1 — C_1 -генерическое множество над M , а G_2 — C_2 -генерическое множество над $M[G_1]$. Тогда G_1 является C_1 -генерическим над $M[G_2]$ и $M[G_2, G_1] = M[G_1, G_2]$.

Доказательство. По предыдущей теореме $G_1 \times G_2$ является $(C_1 \times C_2)$ -генерическим над M . Применяя очевидный изоморфизм между $C_1 \times C_2$ и $C_2 \times C_1$, получаем, что $G_2 \times G_1$ является $(C_2 \times C_1)$ -генерическим над M . Снова применяя теорему, получаем, что G_1 является C_1 -генерическим над $M[G_2]$. Имеем

$$M[G_2, G_1] = M[G_1, G_2],$$

так как оба эти множества являются наименьшими моделями теории ZFC, расширяющими M и содержащими G_1 и G_2 .

Рассмотрим только один пример бесконечных произведений, так называемую *слабую степень*. Если C — понятие вынуждения, а I — произвольное множество, то C^I — множество всех отображений p множества I в C таких, что множество $[i \mid i \in I \text{ и } p(i) \neq 1]$ конечно. Пусть $p \leq q$ означает $\forall i \in I (p(i) \leq q(i))$. Ясно, что C^I — понятие вынуждения, наибольший элемент которого — функция, тождественно равная 1_C . Если C и I принадлежат модели M теории ZFC, то и C^I принадлежит модели M ; именно для этого мы ограничиваемся конечностью.

Если J и K — не пересекающиеся подмножества множества I такие, что $J \cup K = I$, то C^I изоморфно $C^J \times C^K$ естественным образом. В частности, если $i \in I$ и $J = I - \{i\}$, то C^I естественно изоморфно $C^J \times C$. В обоих случаях мы можем применять теорему о произведении.

9. Аксиома выбора

Под *автоморфизмом* понятия вынуждения C мы понимаем автоморфизм частично упорядоченного множества C .

Лемма 9.1. Пусть π — некоторый автоморфизм понятия вынуждения C , который находится в M . Тогда $\pi(G)$ является C -генерическим над M и $M[G] = M[\pi(G)]$.

Доказательство. Так как π отображает множества из M в множества из M , то первое утверждение тривиально.

Поскольку $M[G]$ содержит G и π , оно также содержит и $\pi[G]$, поэтому в силу фундаментальной теоремы $M[\pi(G)] \subset M[G]$. Подставляя $\pi(G)$ вместо G и π^{-1} вместо π , получаем $M[G] \subset M[\pi(G)]$. Таким образом, $M[G] = M[\pi(G)]$.

Пусть $\mathcal{A}$ — некоторое множество автоморфизмов S такое, что $\mathcal{A} \in M$. Элемент a множества M называется $\mathcal{A}$ -инвариантным, если $K_G(a) = K_{\pi(G)}(a)$, для каждого $\pi \in \mathcal{A}$. Например, каждое $\hat{a}$ инвариантно, так как $K_G(\hat{a}) = K_{\pi(G)}(\hat{a}) = a$. Предложение Φ языка вынуждения называется $\mathcal{A}$ -инвариантным, если каждая константа в Φ является $\mathcal{A}$ -инвариантной.

Пусть $\mathcal{A}$ — некоторое множество автоморфизмов S . Скажем, что S является $\mathcal{A}$ -однородным, если для любых $p, q \in S$ существует $\pi \in \mathcal{A}$ такое, что $\pi^{-1}(p)$ и q имеют общее расширение. Если $\mathcal{A}$ — множество всех автоморфизмов S , то мы говорим об однородности вместо $\mathcal{A}$ -однородности.

Если A — бесконечное множество, то $H(A; B)$ однородно. Для данных $p, q \in H(A; B)$ мы выбираем перестановку σ множества A такую, что $\sigma(\text{Do}(p)) \cap \text{Do}(q) = \emptyset$, и определим автоморфизм π так: $\pi(r) = r \cdot \sigma$. Тогда $\pi^{-1}(p) \cup q$ — общее расширение для $\pi^{-1}(p)$ и q .

Лемма 9.2. Пусть $\mathcal{A}$ — некоторое множество автоморфизмов S такое, что $\mathcal{A} \in M$ и S является $\mathcal{A}$ -однородным. Пусть Φ — некоторое предложение языка вынуждения, являющееся $\mathcal{A}$ -инвариантным. Тогда $\vdash_G \Phi$ тогда и только тогда, когда $1 \Vdash \Phi$.

Доказательство. Так как $1 \in G$, то из $1 \Vdash \Phi$ следует $\vdash_G \Phi$. Теперь предположим, что $\vdash_G \Phi$, но $\neg(1 \Vdash \Phi)$. В силу первого некоторое p вынуждает Φ , а в силу последнего и (5.4) некоторое q вынуждает $\neg \Phi$. Выберем $\pi \in \mathcal{A}$ так, чтобы $\pi^{-1}(p)$ и q имели общее расширение. Ввиду теоремы существования и (G2) существует генерическое множество G' , содержащее $\pi^{-1}(p)$ и q . По лемме 9.1 $\pi(G')$ генерическое. Так как $p \in \pi(G')$ и $q \in G'$, получаем $\vdash_{\pi(G')} \Phi$ и $\vdash_{G'} \neg \Phi$. Но $M[\pi(G')] = M[G']$ по лемме 9.1, а константы в Φ представляют одинаковые множества в этих двух моделях. Поэтому $\vdash_{\pi(G')} \Phi$ тогда и только тогда, когда $\vdash_{G'} \Phi$; получили противоречие.

Мы предполагаем, что читатель знаком с OD (ординально определимыми) и HOD (наследственно ординально

определимыми множествами *)). Мы нуждаемся в небольшом обобщении этих понятий.

Скажем, что u OD через $v_1, \dots, v_k$, если существует α такой, что $v_1, \dots, v_k \in V(\alpha)$ и u определимо в $\langle V(\alpha), \in, v_1, \dots, v_k \rangle$. Скажем, что u OD над w , если u OD через $v_1, \dots, v_k$, w для некоторых $v_1, \dots, v_k \in w$. Скажем, что u HOD над w , если u OD над w и каждый элемент из u HOD над w . Это определение индукцией по $\text{rk}(u)$.

Основные результаты про OD и HOD множества переносятся на эту ситуацию. Так, например, каждый ординал OD через любые $v_1, \dots, v_k$ и, следовательно, OD над любым w . Если $u_1, \dots, u_m$ OD над $v_1, \dots, v_k$ (или над w), то $\mu(u_1, \dots, u_m)$ такое же (где μ — терм, определимый в теории ZFC). Класс всех множеств HOD над w является моделью теории ZF (но не обязательно аксиомы выбора). Также ясно, что каждый элемент из w OD над w .

Лемма 9.3. Пусть $\mathcal{A}$ — некоторое множество автоморфизмов S такое, что $\mathcal{A} \in M$, и предположим, что S является $\mathcal{A}$ -однородным. Пусть u OD через $v_1, \dots, v_k$ в $M[G]$ и $v_1, \dots, v_k$ имеют $\mathcal{A}$ -инвариантные имена. Тогда $u \cap M \in M$.

Доказательство. Существует формула $\Phi(x)$ языка вынуждения, содержащая только имена для $v_1, \dots, v_k$ и некоторое $\alpha \in M[G]$ такое, что

$$\bar{a} \in u \leftrightarrow \vdash_G \Phi(a) \quad (9.1)$$

для всех a . Так как $\alpha \in M$ по лемме 7.1, то $\hat{\alpha}$ является $\mathcal{A}$ -инвариантным; поэтому мы можем предположить, что каждое имя в $\Phi(x)$ является $\mathcal{A}$ -инвариантным. Тогда, полагая $\hat{a}$ вместо a в (9.1) и применяя лемму 9.2, получим

$$a \in u \leftrightarrow \vdash_G \Phi(\hat{a}) \leftrightarrow 1 \Vdash \Phi(\hat{a}).$$

Таким образом, $u \cap M = [a \mid 1 \Vdash \Phi(\hat{a})]$ — класс в M . Но если $\beta = \text{rk}(u)$, то $u \cap M \subset V(\beta) \cap M = V^M(\beta)$; следовательно, $u \cap M$ — множество в M .

Теорема 9.1. Пусть S — однородно в M . Если u OD в $M[G]$, то $u \cap M \in M$; если u HOD в $M[G]$, то $u \in M$.

*) J. Myhill, D. Scott, Ordinal definability, Proc. Symp. Pure Math. 13, № 1 (1971), 271—278.

Доказательство. Первое утверждение есть специальный случай леммы 9.3. Второе легко следует из первого индукцией по $\text{rk}(u)$.

Пусть теперь M удовлетворяет аксиоме конструктивности, и пусть $C = H(\omega; 2)$. Применяя теорему 9.1, следствие леммы 7.1 и тот факт, что каждое конструктивное множество HOD , мы видим, что в $M[G]$ конструктивные множества совпадают с HOD множествами. Как мы видели в § 7, существует подмножество множества ω , не являющееся конструктивным в $M[G]$. Так как каждый элемент из $\omega \cap \text{HOD}$, то отсюда следует, что такое множество не OD в $M[G]$. Из этого следует, что в $M[G]$ не существует OD отображения какого-либо ординала на $S(\omega)$, ибо если бы F было OD , то таким же было бы каждое $F(\alpha)$.

Теперь предположим, что $C = H(\omega; 2)^\omega$. Пусть G_i — множество i -х координат элементов из G , и пусть $H = [G_i \mid i \in \omega]$. Пусть N — множество всех множеств, являющихся HOD над H в $M[G]$. Тогда N — модель теории ZF. Сейчас мы покажем, что N не является моделью аксиомы выбора; в действительности мы покажем, что в N не существует отображения какого-либо ординала на $S(\omega)$.

Предположим, что такое отображение F существует. Тогда F OD через $G_0, G_1, \dots, G_{n-1}, H$ для некоторого n (в $M[G]$). Каждый элемент из $S(\omega) \cap N$ есть $F(\alpha)$ для некоторого α в $M[G]$ и, следовательно, OD через $G_0, G_1, \dots, G_{n-1}, H$.

Рассмотрим C как произведение $C' \times C''$, где $C' = H(\omega; 2)^n$ и $C'' = H(\omega; 2)^{\omega-n}$. Пусть G' и G'' — проекции G на C' и C'' соответственно. По теореме о произведении G' является C' -генерическим над M , G'' является C'' -генерическим над $M' = M[G']$ и $M'[G''] = M[G]$. Снова применяя теорему о произведении, получаем, что G_n будет $H(\omega; 2)$ -генерическим над M' . Поэтому множество A , имеющее $U(G_n)$ своей характеристической функцией, является подмножеством множества ω , не лежащим в M' . Так как $A \subset \omega \subset M'$, то $A \cap M' = A$; следовательно, $A \cap M'$ не лежит в M' .

Завершим доказательство, применив лемму 9.3, чтобы показать, что $A \cap M' \in M'$. Для каждой перестановки π множества $\omega - n$ определим автоморфизм π^* множества C'' следующим образом: $(\pi^*(p))_i = p_{\pi(i)}$. Пусть $\mathcal{A}$ — множество всех π^* для π из M . Ясно, что $\mathcal{A} \in M'$. Заметив, что каждая перестановка множества $\omega - n$, которая передвигает

только конечное число элементов, содержится в M' , мы видим, что C'' будет $\mathcal{A}$ -однородным. Теперь $A \cap \text{OD}$ через G_n и, следовательно, лежит в N . Таким образом, $A \cap \text{OD}$ через $G_0, G_1, \dots, G_{n-1}, H$ в $M[G] = M'[G'']$. Поэтому нам нужно лишь показать, что $G_0, G_1, \dots, G_{n-1}, H$ имеют $\mathcal{A}$ -инвариантные имена в M' .

Так как $G_0, G_1, \dots, G_{n-1}$ лежат в M' , то они имеют $\mathcal{A}$ -инвариантные имена $\hat{G}_0, \hat{G}_1, \dots, \hat{G}_{n-1}$. Положим

$$\begin{aligned} a_i &= \hat{G}_i, & \text{если } i < n, \\ a_i &= [\langle \hat{p}_i, p \rangle \mid p \in C''], & \text{если } i \geq n, \\ a &= [a_i \mid i \in \omega] \times \{1\}. \end{aligned}$$

Легко видеть, что a_i — имя G_i , а a — имя H . В $M'[\pi^*(G'')]$ a_i есть имя G_i , если $i < n$, и имя $\pi^*(G'')_i = G_{\pi^{-1}(i)}$, если $i \geq n$; таким образом, a — имя H . Это показывает, что a будет $\mathcal{A}$ -инвариантным.

Историческая справка. Независимость аксиомы выбора доказана Коэном. Модели теории ZFC, в которых нет OD отображений никакого ординала на $S(\omega)$, были впервые построены Феферманом [4]. Теорема 9.1 принадлежит Леви [7].

10. Сохранимость кардиналов

Теперь обратимся к исследованию отношения между кардиналами в M и кардиналами в $M[G]$.

Лемма 10.1. *Каждый кардинал в $M[G]$ является кардиналом в M .*

Доказательство. Пусть m — некоторый кардинал в $M[G]$. По лемме 7.1 m — ординал в M . Если m не является кардиналом в M , то существует отображение некоторого ординала, меньшего m , на m , которое лежит в M и, следовательно, в $M[G]$. Но это невозможно.

Так как $0, 1, \dots, \omega$ абсолютны, то они являются кардиналами как в M , так и в $M[G]$. С другой стороны, несчетные кардиналы в M не обязаны быть кардиналами в $M[G]$, как мы видели в предыдущем параграфе.

Если α — ординал в M , то, так как $M \subset M[G]$, имеем

$$\text{cf}^{M[G]}(\alpha) \leq \text{cf}^M(\alpha). \quad (10.1)$$

Равенство выполняется, когда $\text{cf}^M(\alpha) \leq \omega$, так как свойства «быть предельным ординалом» абсолютно. И опять-таки предыдущий параграф показывает, что равенство может нарушаться, когда $\text{cf}(\alpha)$ несчетно в M .

Теперь мы получим некоторые достаточные условия для того, чтобы достигалось равенство.

Пусть C — понятие вынуждения и $p, q \in C$. Будем говорить, что p и q совместны, если они имеют общее расширение; в противном случае называем p и q несовместными. Будем говорить, что C удовлетворяет условию m -цепи, если каждое множество попарно несовместных элементов в C имеет кардинал $< m$.

Лемма 10.2. Пусть m — регулярный кардинал в M такой, что C удовлетворяет условию m -цепи в M . Тогда

(а) если $\alpha \in M$ и $m \leq \text{cf}^M(\alpha)$, то $\text{cf}^M(\alpha) = \text{cf}^{M[G]}(\alpha)$;

(б) каждый кардинал в M , который $\geq m$, есть кардинал в $M[G]$.

Доказательство. Пусть $x(y) = z$ — формула теории множеств, которая утверждает, что x — функция, значение которой для аргумента y равно z . Будем говорить, что γ есть возможное значение a в β , если некоторое p вынуждает $a(\hat{\beta}) = \hat{\gamma}$. Мы утверждаем, что множество возможных значений a в β имеет кардинал $< m$. Для каждого такого возможного значения γ пусть p_γ вынуждает $a(\hat{\beta}) = \hat{\gamma}$. Ясно, что достаточно показать, что если $\gamma \neq \delta$, то p_γ и p_δ несовместны. Предположим, что они имеют общее расширение q . Выберем генерическое G' такое, что $q \in G'$. По лемме о расширении q вынуждает $a(\hat{\beta}) = \hat{\gamma}$ и $a(\hat{\beta}) = \hat{\delta}$; тогда по лемме об истинности $\vdash_{G'} a(\hat{\beta}) = \hat{\gamma}$ и $\vdash_{G'} a(\hat{\beta}) = \hat{\delta}$. Следовательно, $\gamma = \bar{a}(\beta) = \delta$.

Теперь пусть α таково, как утверждается в (а). Пусть $n = \text{cf}^{M[G]}(\alpha)$. Тогда n — некоторый кардинал в $M[G]$ и, следовательно, в M . Пусть $\bar{a}$ — отображение из n на конфинальное подмножество множества α . Пусть b — множество возможных значений a среди ординалов $< n$. Ясно, что $b \in M$. Если $\sigma < n$ и $\bar{a}(\sigma) = \tau$, то некоторое $p \in G$ вынуждает $a(\hat{\sigma}) = \hat{\tau}$; таким образом, τ — возможное значение a в σ . Поэтому $Ra(\bar{a}) \subset b$; таким образом, b конфинально в α . Следовательно, $\text{cf}(\alpha) \leq |b|$ в M .

В силу вышеприведенного результата, b — объединение n множеств в M , кардинал каждого из которых $< m$.

Если $n < m$, то $|b| < m$ в M (так как m регулярен в M). Это невозможно, так как $m \leq \text{cf}(\alpha) \leq |b|$ в M . Таким образом, $m \leq n$, поэтому $|b| \leq m \cdot n = n$ в M . Следовательно, $\text{cf}(\alpha) \leq |b| \leq n$ в M , т. е. $\text{cf}^M(\alpha) \leq \text{cf}^{M[G]}(\alpha)$. Применяя (10.1), получаем равенство.

Пусть теперь n — кардинал в M такой, что $m \leq n$. Покажем индукцией по n , что n — кардинал в $M[G]$. Если n — регулярный в M , то $\text{cf}^M(n) = n \geq m$, тогда $\text{cf}^{M[G]}(n) = \text{cf}^M(n) = n$ по (а); следовательно, n — кардинал в $M[G]$. Если n сингулярный в M , то n — точная верхняя грань множества кардиналов p в M таких, что $m \leq p < n$. Так как все они являются кардиналами в $M[G]$, а точная верхняя грань множества кардиналов является кардиналом, то n — кардинал в $M[G]$.

Следствие. Если C удовлетворяет условию $\aleph_1$ -цепи в M , то $\text{cf}^M = \text{cf}^{M[G]}$, а M и $M[G]$ имеют одинаковые кардиналы.

Мы хотим применить эти результаты к $H_m(A; B)$. Сначала заметим, что для каждого $p < m$ (включая конечные p) существует самое большее $|A|^p$ подмножеств D множества A таких, что $|D| = p$, и для каждого такого D существует $|B|^p$ отображений из D в B . Поэтому

$$|H_m(A; B)| \leq \sum_{p < m} |A|^p |B|^p;$$

таким образом,

$$|H_m(A; B)| \leq (|A| \cdot |B|)^m. \quad (10.2)$$

Лемма 10.3. Если $m^m = m$ и $|B| \leq m$, то $H_m(A; B)$ удовлетворяет условию m^+ -цепи.

Доказательство. Пусть I — множество попарно несовместных элементов из $H_m(A; B)$. Индуктивно определим подмножество A_α множества A для каждого α . Пусть $A_0 = \emptyset$; для предельного числа α положим $A_\alpha = \bigcup_{\beta < \alpha} A_\beta$. Пусть те-

перь A_α выбрано. Для каждого $p \in H_m(A_\alpha; B)$ выберем $q \in I$, ограничение которого до A_α есть p , при условии, что такое q существует. Пусть $A_{\alpha+1}$ будет объединением A_α и областей определения всех таких q .

Докажем индукцией, что $|A_\alpha| \leq m$ для $\alpha \leq m$. Случай тривиален, когда $\alpha = 0$ или α — предельный ординал.

Предположим, что $|A_\alpha| \leq m$. По (10.2)

$$|H_m(A_\alpha; B)| \leq (m \cdot |B|)^m = m^m = m. \quad (10.3)$$

Теперь ясно, что

$$|A_{\alpha+1}| \leq |A_\alpha| + |H_m(A_\alpha; B)| \cdot m \leq m + m \cdot m = m.$$

В частности, $|A_m| \leq m$; таким образом, $|H_m(A_m; B)| \leq m$ по (10.3).

Завершим доказательство, показав, что $I \subset H_m(A_m; B)$. Пусть $p \in I$. Так как $|\text{Do}(p)| < m$, то существует $\alpha < m$ такое, что $\text{Do}(p) \cap A_\alpha = \text{Do}(p) \cap A_{\alpha+1}$. Выберем $q \in I$ так, чтобы p и q имели одинаковое ограничение до A_α и $\text{Do}(q) \subset A_{\alpha+1}$. Если $x \in \text{Do}(p) \cap \text{Do}(q)$, то $x \in A_{\alpha+1}$; тогда $x \in \text{Do}(p) \cap A_{\alpha+1} \subset A_\alpha$, поэтому $p(x) = q(x)$. Отсюда следует, что p и q совместны. Так как $p, q \in I$, то $p = q$. Поэтому $\text{Do}(p) \subset A_{\alpha+1} \subset A_m$ и, следовательно, $p \in H_m(A_m; B)$.

Условия, при которых выполняется $m^m = m$, см. в § 2.

Подмножество D множества S называется *сечением*, если каждое расширение условия из D лежит в D .

Лемма 10.4. Пусть D — сечение в M . Если $D \cap G' \neq \emptyset$ для каждого G' , являющимся S -генерическим над M , то D плотно.

Доказательство. Для данного p выберем G' генерическим так, что $p \in G'$. Выберем $q \in D \cap G'$, и пусть r — общее расширение p и q . Тогда $r \leq p$ и $r \in D$.

Понятие вынуждения S называется *m-замкнутым*, если для каждого $\alpha < m$ и для каждой убывающей последовательности $\{p_\beta\}_{\beta < \alpha}$ условий в S существует $p \in S$ такое, что $p \leq p_\beta$ для всех $\beta < \alpha$. Например, если m регулярно, то $H_m(A; B)$ будет m -замкнутым; действительно, мы можем взять $p = \bigcup_{\beta < \alpha} p_\beta$.

Лемма 10.5. Если S является m -замкнутым в M , $\alpha < m$ и $\{D_\beta\}_{\beta < \alpha}$ — последовательность плотных сечений в M , то $\bigcap_{\beta < \alpha} D_\beta$ плотно.

Доказательство. Для данного p мы можем определить индуктивно в M убывающую последовательность $\{p_\beta\}_{\beta < \alpha}$ такую, что $p_\beta \in D_\beta$ и $p_\beta \leq p$. (Мы должны использовать предположение о том, что S является m -замкнутым

в случае, когда β — предельный ординал.) Выбирая q так, чтобы $q \leq p_\beta$ для всех $\beta < \alpha$, получаем $q \leq p$ и $q \in \bigcap_{\beta < \alpha} D_\beta$.

Лемма 10.6. Пусть S является m -замкнутым в M и $\alpha < m$. Тогда $(^a a)^M = (^a a)^{M[G]}$ для каждого $a \in M$, а также $S^M(\alpha) = S^{M[G]}(\alpha)$.

Доказательство. Ясно, что $(^a a)^M \subset (^a a)^{M[G]}$. Пусть теперь $\bar{b} \in (^a a)^{M[G]}$. Пусть $\Phi(x, y)$ будет

$$\exists z (z \in \hat{a} \ \& \ \langle z, y \rangle \in b) \rightarrow \langle x, y \rangle \in b,$$

и для каждого $\beta < \alpha$ положим

$$D_\beta = [p \mid \exists c (p \Vdash \Phi(\hat{c}, \hat{\beta}))].$$

Тогда D_β — сечение в M . Применим лемму 10.4, чтобы доказать, что оно плотно. Пусть G' генерическое. Тогда для некоторого $c \in a$ имеем $\vdash_{G'} \Phi(\hat{c}, \hat{\beta})$; таким образом, по лемме об истинности $D_\beta \cap G' \neq \emptyset$.

По лемме 10.5 множество $D = \bigcap_{\beta < \alpha} D_\beta$ плотно. Поэтому существует $q \in G \cap D$. Если $q \Vdash \Phi(\hat{c}, \hat{\beta})$, то $c = \bar{b}(\beta)$.

Следовательно, $\bar{b}(\beta)$ — единственное c такое, что $q \Vdash \Phi(\hat{c}, \hat{\beta})$. Отсюда легко следует, что $\bar{b} \in M$.

Последнее утверждение доказывается, если взять $a = 2$ и использовать соответствие между множеством и его характеристической функцией.

Следствие. Пусть S является m -замкнутым в M . Тогда

- (а) если $\alpha \in M$ и $\text{cf}^M(\alpha) \leq m$, то $\text{cf}^M(\alpha) = \text{cf}^{M[G]}(\alpha)$,
- (б) каждый кардинал κ в M , который $\leq m$, есть кардинал в $M[G]$.

Доказательство. (а) Если утверждение ложно, то $\text{cf}^{M[G]}(\alpha) < \text{cf}^M(\alpha) \leq m$. Пусть f — отображение из $\text{cf}^{M[G]}(\alpha)$ на конфинальное подмножество α в $M[G]$. По лемме $f \in M$; таким образом, $\text{cf}^{M[G]}(\alpha) \geq \text{cf}^M(\alpha)$, и мы получили противоречие. (б) Если утверждение ложно, то существует отображение f ординала $< \kappa$ на κ в $M[G]$. По лемме $f \in M$, а это невозможно.

Отметим, что во всех утверждениях этого параграфа, если мы доказали, что M и $M[G]$ имеют одинаковые кардиналы, то всегда оказывалось, что $\text{cf}^M = \text{cf}^{M[G]}$. В связи с этим возникает одна проблема: можно ли выбрать S так,

чтобы M и $M[G]$ имели одинаковые кардиналы, но $\text{cf}^M \neq \text{cf}^{M[G]}$? Прикри показал, что это возможно, если существует измеримый кардинал в M .

Историческая справка. Результаты о m -замкнутых понятиях принадлежат Соловею, а остальные результаты принадлежат Коэну.

11. Гипотеза континуума

Вначале исследуем величину множества степени в $M[G]$.

Лемма 11.1. Пусть C удовлетворяет условию m -цепи в M . Тогда для каждого бесконечного кардинала n в M

$$|S(n)|^{M[G]} \leq ((|C|^m)^n)^M.$$

Доказательство. Для $a \in M$ и $\alpha < n$ пусть $\varphi_a(\alpha) = [p \mid p \vdash \hat{\alpha} \in a]$. Тогда

$$\bar{a} \subset n \text{ \& } \bar{b} \subset n \text{ \& } \varphi_a = \varphi_b \rightarrow \bar{a} = \bar{b}.$$

Ввиду симметрии достаточно показать, что $\bar{a} \subset \bar{b}$. Пусть $\alpha \in \bar{a}$. Тогда некоторое $p \in G$ есть в $\varphi_a(\alpha)$ и, следовательно, в $\varphi_b(\alpha)$; таким образом, $\vdash_{\alpha} \hat{\alpha} \in b$, а поэтому $\alpha \in \bar{b}$.

Отсюда следует, что

$$|S(n)|^{M[G]} \leq |\{\varphi_a \mid a \in M\}|^M.$$

Далее, φ_a — отображение из n в Q , где Q — множество всех множеств $[p \mid p \vdash \Phi]$. Поэтому достаточно будет доказать, что $|Q| \leq |C|^m$ в M .

Пусть $a \in Q$. Применяя лемму Цорна, выберем максимальное подмножество b множества a , состоящее из попарно несовместных элементов. Тогда a может быть восстановлена из b с помощью следующей эквивалентности:

$$p \in a \leftrightarrow \forall q \leq p \exists r \in b \quad (q \text{ и } r \text{ совместны}).$$

Импликация слева направо выполняется в силу леммы о расширении и максимальной b . Предположим $p \notin a$. Если $a = [p \mid p \vdash \Phi]$, то по (5.4) существует $q \leq p$ такое, что $q \vdash \neg \Phi$. По (5.3) и лемме о расширении элемент r , совместный с q , не может вынуждать Φ , поэтому такого r не может быть в b .

Отсюда следует, что $|Q|$ равно самое большее числу подмножеств b из C , состоящих из попарно несовместных

элементов. Так как $|b| < m$ для каждого такого b , то

$$|Q| \leq |S_m(C)| \leq |C|^m.$$

Пусть теперь m и n — кардиналы в M . Можно ли выбрать C так, чтобы M и $M[G]$ имели одинаковые кардиналы и $2^m = n$ в $M[G]$? Если это можно сделать, то

$$n^m = (2^m)^m = 2^m = n$$

в $M[G]$. Так как $(^m n)^M \subset (^m n)^{M[G]}$, а M и $M[G]$ имеют одинаковые кардиналы, то мы имеем $(n^m)^M \leq (n^m)^{M[G]}$. Следовательно, $n^m = n$ в M .

Поэтому предположим, что $n^m = n$ в M . Для того чтобы получить $2^m = n$, нам необходимо ввести n подмножеств m . Фактически мы введем отображение F из $n \times m$ в 2 и возьмем $[\beta \mid F(\alpha, \beta) = 0]$ в качестве α -го подмножества из m . Пусть $C = H(n \times m; 2)$. Положив $F = \bigcup_{p \in G} p$, видим, что F — отображение в $M[G]$ из $n \times m$ в 2 . Для $\alpha < n$ положим $A_\alpha = [\beta \mid \beta < m \text{ \& } F(\alpha, \beta) = 0]$. Тогда A_α — подмножество m в $M[G]$. Кроме того, $\alpha \neq \alpha' \rightarrow A_\alpha \neq A_{\alpha'}$; это следует из того, что

$$[p \mid \exists \beta (p(\alpha, \beta) \text{ \& } p(\alpha', \beta) \text{ определены и не равны})]$$

— плотное множество в M .

По лемме 10.3 и следствию к лемме 10.2 $\text{cf}^M = \text{cf}^{M[G]}$ и, кроме того, M и $M[G]$ имеют одинаковые кардиналы. В частности, m и n являются кардиналами в $M[G]$. Так как мы указали n различных подмножеств m в $M[G]$, то $2^m \geq n$ в $M[G]$. По лемме 11.1

$$(2^m)^{M[G]} \leq ((|C|^{\aleph_0})^m)^M.$$

Подсчитывая в M , имеем по (10.2)

$$|C| \leq (m \cdot n)^{\aleph_0} = n$$

(так как из $n^m = n$ следует $m < n$); поэтому

$$(|C|^{\aleph_0})^m = |C|^m \leq n^m = n.$$

Отсюда $2^m = n$ в $M[G]$. Это доказывает следующую теорему.

Теорема 11.1. Пусть m и n — бесконечные кардиналы в M такие, что $n^m = n$ в M . При подходящем выборе C

имеем $\text{cf}^M = \text{cf}^{M[G]}$; M и $M[G]$ имеют одинаковые кардиналы и $2^m = n$ в $M[G]$.

Теперь предположим, что мы определили константу Γ в теории ZFC и доказали в теории ZFC, что Γ — кардинал. Мы хотели бы показать, что $2^{\aleph_0} = \Gamma$ совместно с теорией ZFC. В силу теоремы Кёнига мы требуем, чтобы $\text{cf}(\Gamma) > \omega$ было доказуемым в теории ZFC. Допустим это и возьмем M удовлетворяющим аксиоме конструктивности, а значит, и GCH. Из GCH и $\text{cf}(\Gamma) > \omega$ мы можем доказать $\Gamma^{\aleph_0} = \Gamma$, поэтому $(\Gamma^{\aleph_0})^M = \Gamma^M$. Выбирая C , как в теореме 11.1, имеем $2^{\aleph_0} = \Gamma^M$ в $M[G]$. Затем мы получим требуемый результат, если докажем, что $\Gamma^M = \Gamma^{M[G]}$. Вспоминая, что M и $M[G]$ имеют одинаковые кардиналы и одинаковые функции cf , мы видим, что равенство выполняется, если Γ , скажем, $\aleph_2$ или $\aleph_{\omega_1}$ или первый слабо недостижимый кардинал (при условии, что существует слабо недостижимый кардинал в M).

Предположим теперь, что GCH выполняется в M . Если $2^m = n$ в $M[G]$, то $2^p \geq n$ для $p \geq m$, поэтому GCH может быть ложной в $M[G]$ выше m . Покажем, что можно сохранить GCH ниже m , если m регулярно в M .

Теорема 11.2. Пусть GCH выполняется в M . Пусть m и n — бесконечные кардиналы из M такие, что m регулярно в M и $\text{cf}(n) > m$ в M . При подходящем выборе C имеем $\text{cf}^M = \text{cf}^{M[G]}$, M и $M[G]$ имеют одинаковые кардиналы, $2^m = n$ в $M[G]$ и $\forall p (p < m \rightarrow 2^p = p^+)$ выполняется в $M[G]$.

Доказательство. Возьмем $C = H_m^M(m \times n; 2)$. Условия теоремы показывают, что $m^m = m$ в M . Поэтому леммы 10.2 и 10.3 и следствие к лемме 10.6 показывают, что $\text{cf}^M = \text{cf}^{M[G]}$, а M и $M[G]$ имеют одинаковые кардиналы. Доказательство того, что $2^m = n$ в $M[G]$, по существу такое же, как раньше (отметим, что из $\text{cf}(n) > m$ и GCH следует, что $n^m = n$). Если $p < m$, то $S^M(p) = S^{M[G]}(p)$ по лемме 10.6. Так как M и $M[G]$ имеют одинаковые кардиналы и $2^p = p^+$ в M , то мы видим, что $2^p = p^+$ в $M[G]$.

Неизвестно, выполняется ли теорема 11.2, когда m сингулярна в M . Простейшей нерешенной проблемой является

следующая: будет ли совместным с теорией ZFC предположение, что $\forall n (n < \omega \rightarrow 2^{\aleph_n} = \aleph_{n+1})$ и $2^{\aleph_\omega} \neq \aleph_{\omega+1}$?

Историческая справка. Теорема 11.1 принадлежит Козну, теорема 11.2 принадлежит Соловею.

12. Вынуждение с классами

До сих пор мы предполагали, что C — множество в M . Но иногда мы можем строить модели вынуждения и тогда, когда C — просто класс в M . Так как общая ситуация еще не исследована полностью, рассмотрим лишь одну частную проблему.

Эта проблема является обобщением результатов предыдущего параграфа. Предположим, что H — отображение множества бесконечных кардиналов из M в себя, которое является функционалом в M . Мы хотим выбрать C так, чтобы M и $M[G]$ имели одинаковые кардиналы и чтобы для каждого бесконечного кардинала m в M было $2^m = H(m)$ в $M[G]$.

Очевидно, мы должны иметь

$$m \leq n \rightarrow H(m) \leq H(n). \quad (12.1)$$

Кроме того,

$$m < \text{cf}(H(m)) \quad (12.2)$$

должно выполняться в M . Действительно, это выполняется в $M[G]$ по теореме Кёнига, а потому и в M по (10.1). Будем предполагать дополнительно, что M удовлетворяет аксиоме конструктивности*). В этом случае мы покажем, что M и $M[G]$ для подходящего C имеют одинаковые кардиналы, $\text{cf}^M = \text{cf}^{M[G]}$ и $2^m = H(m)$ в $M[G]$ для каждого регулярного кардинала m в M .

Замечание. Снова не очень много известно про сингулярные кардиналы. Ясно, что на H должны быть наложены дополнительные условия, если бы мы хотели включить в рассмотрение и этот случай. Например,

$$\forall n \in \omega (2^{\aleph_n} = \aleph_{\omega+1}) \rightarrow 2^{\aleph_\omega} = \aleph_{\omega+1}.$$

Действительно,

$$2^{\aleph_\omega} = 2^{\sum \aleph_n} = \prod 2^{\aleph_n} = \prod \aleph_{\omega+1} = (\aleph_{\omega+1})^{\aleph_\omega} = 2^{\aleph_\omega} = \aleph_{\omega+1}.$$

*) Используется только GCH и вполне упорядоченность универсума, а можно обойтись и без последнего. Однако это не существенно для вопросов непротиворечивости.

Теперь опишем C . Пусть областью изменения m и n будут *регулярные* кардиналы из M . Положим

$$Q_m = [\langle n, \alpha, \beta \rangle \mid n \leq m \text{ и } \alpha < H(n) \text{ и } \beta < n].$$

Пусть C — множество всех функций p в M таких, что $Ra(p) \subset 2$, $Do(p) \subset \bigcup_m Q_m$ и $|Do(p) \cap Q_m| < m$ в M для каждого m .

Для $p, q \in C$ пусть $p \leq q$ означает $q \subset p$. Очевидно, что C — понятие вынуждения, которое является классом в M .

Естественно потребовать, чтобы генерическое множество пересекалось со всеми плотными классами в M . Поэтому мы выбираем G C -генерическим над M' , где M' — множество всех классов в M . Так как M' счетно, то это может быть сделано по теореме существования.

Теперь определим $M[G]$, как раньше. Точно так же, как и раньше, мы доказываем, что $M[G]$ счетно и транзитивно и $M \subset M[G]$. При попытке обобщить результаты § 5 возникают трудности: индуктивное определение $p \Vdash^* a \neq b$ уже не может быть дано в M . Поэтому мы будем действовать по-другому.

Пусть

$$C_m = [p \mid p \in C \text{ и } Do(p) \subset Q_m],$$

$$C^m = [p \mid p \in C \text{ и } Do(p) \cap Q_m = \emptyset].$$

Как C_m , так и C^m содержат 1 и, следовательно, являются понятиями вынуждения. Кроме того, C_m является множеством в M ; функция, которая переводит m в C_m , — функционал в M , а C^m — класс в M .

Для $p \in C$ пусть p_m будет ограничением p до Q_m и пусть $p^m = p - p_m$. Легко проверить, что $p \rightarrow \langle p_m, p^m \rangle$ — изоморфизм между C и $C_m \times C^m$, обращение которого переводит $\langle q, r \rangle$ в $q \cup r$. Пусть $G_m = [p_m \mid p \in G]$, $G^m = [p^m \mid p \in G]$. Тогда по теореме о произведении *) G_m является C_m -генерическим над M , а G^m — C^m -генерическим над $M[G_m]$.

*) Строго говоря, теорема о произведении здесь неприменима, но нужная часть доказательства переносится без затруднений.

Кроме того, G соответствует $G_m \times G^m$ при этом изоморфизме, т. е.

$$G = [p \cup q \mid p \in G_m \text{ и } q \in G^m]. \quad (12.3)$$

Отсюда следует, что

$$G \cap C_m = G_m. \quad (12.4)$$

Заметим, что C — объединение всех C_m , тогда мы можем определить $\Delta(b)$ в M индукцией по $rk(b)$ следующим образом: $\Delta(b)$ есть наименьшее m такое, что $\Delta(a) \leq m$ для каждого $a \in Ra(b)$ и $p \in C_m$ для каждого $p \in Do(b)$. Докажем индукцией по $rk(b)$, что

$$\Delta(b) \leq m \rightarrow K_G(b) = K_{G_m}(b). \quad (12.5)$$

Если $\langle a, p \rangle \in b$, то $\Delta(a) \leq \Delta(b) \leq m$, $rk(a) < rk(b)$, поэтому $K_G(a) = K_{G_m}(a)$ по индуктивному предположению.

Кроме того, $p \in C_m$, поэтому $p \in G \leftrightarrow p \in G_m$ по (12.4). Отсюда $K_G(b) = K_{G_m}(b)$.

Теперь определим

$$a^{(m)} = [\langle b^{(m)}, p \rangle \mid \langle b, p \rangle \in a \text{ и } p \in C_m].$$

Опять это есть функционал в M . Докажем

$$K_G(a^{(m)}) = K_{G_m}(a) \quad (12.6)$$

индукцией по $rk(a)$. По индуктивному предположению и (12.4)

$$\begin{aligned} K_G(a^{(m)}) &= [K_G(b^{(m)}) \mid \exists p \in G (\langle b, p \rangle \in a \text{ и } p \in C_m)] = \\ &= [K_{G_m}(b) \mid \exists p \in G_m (\langle b, p \rangle \in a)] = \\ &= K_{G_m}(a). \end{aligned}$$

Простая индукция показывает, что

$$\Delta(a^{(m)}) \leq m. \quad (12.7)$$

Из (12.5) и (12.6) получаем

$$M[G] = \bigcup_m M[G_m]. \quad (12.8)$$

Кроме того,

$$m \leq n \rightarrow M[G_m] \subset M[G_n]. \quad (12.9)$$

Действительно,

$$K_{G_m}(a) = K_G(a^{(m)}) = K_{G_n}(a^{(m)})$$

по (12.6), (12.7) и (12.5).

Все C_m имеют такой же язык вынуждения, как и C . Определим $p \Vdash_m^* \Phi$ для C_m , как раньше. Затем положим $\Delta(a, b) = \max(\Delta(a), \Delta(b))$ и определим

$$\begin{aligned} p \Vdash^* a \in b, & \text{ если } p_{\Delta(a, b)} \Vdash_{\Delta(a, b)}^* a \in b, \\ p \Vdash^* a \neq b, & \text{ если } p_{\Delta(a, b)} \Vdash_{\Delta(a, b)}^* a \neq b. \end{aligned}$$

Лемма определимости и лемма о расширении тривиальны. Чтобы доказать лемму об истинности, скажем для $a \in b$, мы имеем для $m = \Delta(a, b)$:

$$\begin{aligned} \vdash_G a \in b &\leftrightarrow \vdash_{G_m} a \in b \text{ по (12.5)} \\ &\leftrightarrow \exists p \in G_m (p \Vdash_m^* a \in b) \\ &\leftrightarrow \exists p \in G (p \Vdash_m^* a \in b) \\ &\leftrightarrow \exists p \in G (p \Vdash^* a \in b). \end{aligned}$$

Теперь можно определить $p \Vdash^* \Phi$ для неатомных Φ и доказать все три леммы о вынуждении, как раньше.

Далее мы заметим, что C_m удовлетворяет условию m^+ -цепи (в M). Действительно, по лемме 10.3 $H_m(Q_m; 2)$ удовлетворяет условию m^+ -цепи. Но $C_m \subset H_m(Q_m; 2)$ и элементы (из C_m), совместные в $H_m(Q_m; 2)$, являются совместными и в C_m , так как их объединение лежит в C_m . Это дает требуемый результат. Также отметим, что C^m будет m^+ -замкнутым в M .

Будем говорить, что $\{D_\beta\}_{\beta < m}$ есть последовательность классов в M , если множество пар $\langle p, \beta \rangle$ таких, что $p \in D_\beta$, является классом в M . Отметим, что лемма 10.4 обобщается на классы в M , а лемма 10.5 обобщается на последовательности классов в M .

Лемма 12.1. Пусть $\{D_\beta\}_{\beta < m}$ — последовательность классов в M такая, что каждое D_β — плотное сечение в C . Тогда существует $q \in G^m$ такое, что

$$\forall \alpha < m \exists p \in G_m (p \cup q \in D_\alpha).$$

Доказательство. Для $q \in C^m$ положим

$$D_\alpha^q = [p \mid p \in C_m \text{ и } p \cup q \in D_\alpha].$$

Достаточно выбрать $q \in G^m$ так, чтобы D_α^q было C_m -плотным для каждого $\alpha < m$. Поэтому, полагая

$$D'_\alpha = [q \mid q \in C^m \text{ и } D_\alpha^q \text{ является } C_m\text{-плотным}],$$

достаточно будет показать, что $\bigcap_{\alpha < m} D'_\alpha$ плотно. Ввиду вышеприведенных замечаний нам нужно лишь показать, что D'_α плотно.

Пусть $q' \in C^m$. Выберем r_β индуктивно в M так, чтобы $r_\beta \leq q'$, $r_\beta \in D_\alpha$ и для всех $\gamma < \beta$ имело место неравенство $(r_\beta)^m \leq (r_\gamma)^m$ и $(r_\beta)_m$ и $(r_\gamma)_m$ были несовместны.

Если существует много таких r_β , то используем определенное вполне упорядочение на D_α , имеющееся вследствие аксиомы конструктивности, для того чтобы выбрать одно такое r_β ; если такого r_β не существует, то r_β не определено.

Так как C_m удовлетворяет условию m^+ -цепи в M , то мы видим, что наименьшее β такое, что r_β не определено, существует и удовлетворяет $|\beta| \leq m$ в M . Поэтому существует $q \in C^m$ такое, что $q \leq (r_\gamma)^m$ для всех $\gamma < \beta$ и $q \leq q'$. Мы должны показать, что $q \in D'_\alpha$, т. е. что D_α^q плотно.

Пусть $p \in C_m$. Тогда $p \cup q$ имеет расширение r в D_α . Так как r не является возможным значением для r_β , то r_m совместно с некоторым $(r_\gamma)_m$. Пусть p' — общее расширение для r_m и $(r_\gamma)_m$. Тогда $p' \leq r_m \leq p$ и $p' \cup q \leq (r_\gamma)_m \cup (r_\gamma)^m = r_\gamma$, поэтому $p' \cup q \in D_\alpha$ и, следовательно, $p' \in D_\alpha^q$.

Лемма 12.2. Пусть F — функционал в $M[G]$ такой, что m содержится в области определения F . Тогда ограничение f функционала F до m находится в $M[G]$. Если $[F(\alpha) \mid \alpha < m]$ содержится в некотором множестве из $M[G_m]$, то f находится в $M[G_m]$.

Доказательство. Пусть $\Phi(x, y)$ — формула языка вынуждения такая, что

$$F(a) = b \leftrightarrow \vdash_G \Phi(a, b). \quad (12.10)$$

Для каждого $\alpha < m$ положим

$$D_\alpha = [p \mid \exists b (p \Vdash \exists x \Phi(\hat{\alpha}, x) \rightarrow \Phi(\hat{\alpha}, b))].$$

Тогда $\{D_\alpha\}$ — последовательность классов в M . Применяя лемму 10.4, мы видим, что D_α — плотное сечение. Поэтому по лемме 12.1 существует $q \in G_m$ такое, что

$$\forall \alpha < m \exists p \in G_m (p \cup q \in D_\alpha). \quad (12.11)$$

Для $\alpha < m$ и $p \in G_m$ пусть $A_{\alpha,p}$ — множество всех таких b , что

$$p \cup q \Vdash \exists x \Phi(\hat{\alpha}, x) \rightarrow \Phi(\hat{\alpha}, b). \quad (12.12)$$

Пусть g — функция в M , область определения которой представляет собой множество пар $\langle \alpha, p \rangle$ из $m \times C_m$ таких, что $A_{\alpha,p} \neq \emptyset$ и $g(\langle \alpha, p \rangle) \in A_{\alpha,p}$ для каждой такой пары $\langle \alpha, p \rangle$.

Покажем, что

$$f = [\langle K_G(b), \alpha \rangle \mid \exists p \in G_m (b = g(\langle \alpha, p \rangle))]. \quad (12.13)$$

По (12.11) для каждого $\alpha < m$ существует такое $p \in G_m$, что $A_{\alpha,p} \neq \emptyset$, и, следовательно, такое, что $q(\langle \alpha, p \rangle)$ определено. Поэтому мы должны показать, что если $p \in G_m$ и $b = g(\langle \alpha, p \rangle)$, то $K_G(b) = f(\alpha)$. Так как (12.12) выполняется и $p \cup q \in G$ по (12.3), то $\vdash_G \exists x \Phi(\hat{\alpha}, x) \rightarrow \Phi(\hat{\alpha}, b)$. Отсюда и из (12.10) $F(\alpha) = K_G(b)$, поэтому $f(\alpha) = K_G(b)$.

Выберем n так, чтобы $m \leq n$ и $\Delta(b) \leq n$ для $b \in \text{Ra}(g)$. По (12.4) и (12.5) мы можем записать (12.13) следующим образом:

$$f = [\langle K_{G_n}(b), \alpha \rangle \mid \exists p \in G_n (b = g(\langle \alpha, p \rangle))].$$

Так как $G_n \in M[G_n]$ и существует функционал в $M[G_n]$, совпадающий с K_{G_n} на аргументах в M , то отсюда следует, что $f \in M[G_n]$. Следовательно, $f \in M[G]$.

Теперь предположим, что $[F(\alpha) \mid \alpha < m] \subset K_{G_m}(a)$; мы хотим показать, что можно взять $n = m$. Переделаем D_α на множество таких p , что

$$\exists b \in \text{Ra}(a^{(m)}) [p \Vdash \exists x (x \in a^{(m)} \& \Phi(\hat{\alpha}, x)) \rightarrow \Phi(\hat{\alpha}, b)].$$

Для доказательства того, что оно плотно, мы должны отметить, что каждый элемент из $K_G(a^{(m)})$ имеет имя в $\text{Ra}(a^{(m)})$ по (4.1).

Из того, что

$$\vdash_G \exists x (x \in a^{(m)} \& \Phi(\alpha, x)) \rightarrow \Phi(\alpha, b),$$

получаем

$$F(\alpha) = K_G(b).$$

Далее используется (12.6).

Мы можем теперь предположить, что каждое b в $\text{Ra}(g)$ содержится в $\text{Ra}(a^{(m)})$ и поэтому имеет вид $b'^{(m)}$. Но $\Delta(b'^{(m)}) \leq m$; таким образом, действительно можно взять $n = m$.

Лемма 12.3. Если $\bar{a} \in M[G]$ и $\bar{a} \neq 0$, то существует m такое, что $\bar{a} \in M[G_m]$, и отображение f из m на $\bar{a}$, которое содержится в $M[G_m]$.

Доказательство. Выберем n по (12.8) так, чтобы $\bar{a} \in M[G_n]$. Выберем m так, чтобы $n \leq m$ и $|\bar{a}| \leq m$ в $M[G_n]$. Тогда существует f в $M[G_n]$, отображающая m на $\bar{a}$, и $\bar{a}, f \in M[G_m]$ по (12.9).

Теперь проверим, что $M[G]$ удовлетворяет условиям леммы 2.1. Так как $\omega \in M \subset M[G]$, то (а) выполняется. Пусть теперь $\bar{a} \in M[G]$, $\bar{a} \neq 0$ и выберем m и f , как в лемме 12.3. Предположим, что A — класс в $M[G]$ такой, что $A \subset \bar{a}$ и $A \neq \emptyset$. Так как $f \in M[G]$, то легко определить функционал F в $M[G]$ с областью определения m и областью значений A . По лемме 12.2 $F \in M[G_m]$; таким образом $A \in M[G_m] \subset M[G]$. Это доказывает (б). Это также показывает, что каждое подмножество из $\bar{a}$ в $M[G]$ содержится в $M[G_m]$ и, следовательно, в множестве степени для $\bar{a}$ в $M[G_m]$. Это доказывает (г).

Пусть теперь F — функционал в $M[G]$, и пусть $\bar{a}$ — непустое подмножество области определения F . Снова пусть m и f таковы, как в лемме 12.3, и F_1 — функционал, определенный следующим образом: $F_1(\alpha) = F(f(\alpha))$. Тогда $F_1 \in M[G]$ по лемме 12.2. Поэтому для некоторого n имеем $F_1 \in M[G_n]$, а также $U(\text{Ra}(F_1)) \in M[G_n] \subset M[G]$. Но $U(\text{Ra}(F_1)) = U([F(x) \mid x \in \bar{a}])$. Итак, мы доказали (в).

По лемме 2.1 $M[G]$ — модель теории ZF. Используя лемму 12.3, получаем, что $M[G]$ — модель теории ZFC.

Теперь покажем, что $\text{cf}^M = \text{cf}^{M[G]}$. Если это не так, то мы имели бы $\aleph_0 \leq \text{cf}^{M[G]}(\alpha) < \text{cf}^M(\alpha)$ для некоторого α . Положим $m = \text{cf}^{M[G]}(\alpha)$. Это есть бесконечный кардинал в M , а так как $m = \text{cf}^{M[G]}(m) \leq \text{cf}^M(m) \leq m$, то он регулярен в M . Пусть f — отображение из m на конфинальное подмножество из α такое, что $f \in M[G]$. По лемме 12.2 $f \in M[G_m]$. Следовательно, $\text{cf}^{M[G_m]}(\alpha) \leq m$. С другой стороны, из $m < \text{cf}^M(\alpha)$ следует $m^+ \leq \text{cf}^M(\alpha)$, поэтому $\text{cf}^M(\alpha) = \text{cf}^{M[G_m]}(\alpha)$ по лемме 10.2. Таким образом, $m < \text{cf}^M(\alpha) = \text{cf}^{M[G_m]}(\alpha) \leq m$; получаем противоречие.

Из $\text{cf}^M = \text{cf}^{M[G]}$ следует, что M и $M[G]$ имеют одинаковые кардиналы; доказательство этого подобно доказательству леммы 10.2 (б).

Каждое непустое подмножество из m в $M[G]$ есть образ m относительно некоторого функционала в $M[G]$ и поэтому по лемме 12.2 содержится в $M[G_m]$. Тем самым $S^{M[G]}(m) = S^{M[G_m]}(m)$, поэтому, чтобы доказать $2^m = H(m)$ в $M[G]$, достаточно доказать это в $M[G_m]$. Полагая $F = U(G_m)$ и

$$A_\alpha = [\beta \mid \beta < m \text{ \& } F(m, \alpha, \beta) = 0]$$

для $\alpha < H(m)$, мы доказываем, как и раньше, что все A_α дают $H(m)$ различных подмножеств m . Используя (12.1), имеем в M

$$|Q_m| \leq m \cdot H(m) \cdot m = H(m)$$

(так как (12.2) дает $m < H(m)$). Так как $C_m \subset H_m(Q_m; 2)$, получаем

$$|C_m| \leq H(m)^m = H(m)$$

по (10.2) и (12.2)*. Тогда по лемме 11.1

$$|S(m)|^{M[G_m]} \leq (H(m)^{m \cdot m})^M = H(m).$$

Таким образом, $2^m = H(m)$ в $M[G_m]$.

Историческая справка. Все результаты этого параграфа принадлежат Истону [3].

*) И по (2.1), так как это можно вычислять в M , а в M полна GCH. — Прим. ред.

ЛИТЕРАТУРА К ПРИЛОЖЕНИЮ II

- [1] P. J. Cohen, The independence of the continuum hypothesis, Parts I, II, Proc. Nat. Acad. Sci. U. S. A. 50 (1963), 1143—1148; 51 (1964), 105—110.
- [2] P. J. Cohen, Set theory and the continuum hypothesis, Benjamin, New York, 1966. (Русский перевод: П. Дж. Коэн, Теория множеств и континуум-гипотеза, «Мир», 1969.)
- [3] W. Easton, Powers of regular cardinals, Thesis, Princeton University, 1964.
- [4] S. Feferman, Some applications of the notion of forcing and generic sets, Fundam. Math. 56 (1965), 325—345.
- [5] K. Gödel, The consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory, Ann. of Math. Studies, No. 3, Princeton University Press, Princeton, N. J., 1940. (Русский перевод: К. Гёдель, Совместимость аксиомы выбора и обобщенной континуум-гипотезы с аксиомами теории множеств, УМН 3, № 1 (1948), 96—149.)
- [6] A. Lévy, Axiom schemata of strong infinity in axiomatic set theory, Pacific J. Math. 10 (1960), 223—238.
- [7] A. Lévy, Definability in axiomatic set theory. I. (Proc. 1964 Internat. Congr.) Logic, Methodology and Philosophy of Science, North-Holland, Amsterdam, 1966.
- [8] A. Mostowski, An undecidable arithmetical statement, Fundam. Math. 36 (1949), 143—164.
- [9] J. C. Shepherdson, Inner models for set theory, Part I, J. Symbolic Logic 16 (1951), 161—190.

Автоморфизм (*automorphism*) 499
 Аксиома (*axiom*) 11, 16
 — бесконечности (*axiom of infinity*) 352
 — — обобщенная (*generalized axiom of infinity*) 438
 — выбора (*axiom of choice*) 370
 — выделения (*comprehension axiom*) 335
 — замены (*replacement axiom*) 351
 — измеримости (*axiom of measurability*) 442
 — индукции (*induction axiom*) 300, 335
 — конструктивности (*axiom of constructibility*) 401, 486
 — логическая (*logical axiom*) 40, 41
 — мультипликативности (*multiplicative axiom*) 421
 — недостижимости (*axiom of inaccessibility*) 438
 — нелогическая (*nonlogical axiom*) 40, 42
 — объемности (*extensionality axiom*) 335, 350
 — определяющая (*defining axiom*) 93, 95, 97
 — подмножеств (*subset axiom*) 350
 — подстановки (*substitution axiom*) 41, 316
 — пропозициональная (*propositional axiom*) 41
 — равенства (*equality axiom*) 41
 — регулярности (*regularity axiom*) 350
 — специальная (*special axiom*) 75
 — — равенства (*special equality axiom*) 85
 — степени (*power set axiom*) 351
 — тождества (*identity axiom*) 41
 Аналитичность в (*analytical in*) 261
 Арифметика второго порядка (*second-order arithmetic*) 334
 — Пеано (*Peano arithmetic*) 301
 Арифметичность в (*arithmetical in*) 245

База (*base*) 210
 Базис (*basis*) 277

Вариант (*variant*) 59
 Вид квантора (*kind of a quantifier*) 239, 258

Вложение (*embedding*) 113
 Вхождение выражения (*occurrence of an expression*) 15
 — свободное (*free*) 29, 34
 — связанное (*bound*) 29, 34
 — символа (*occurrence of a symbol*) 15
 Выводимость по правилу 16
 Вынуждение (*forcing*) 410, 412, 413, 490
 — слабое (*weak forcing*) 493
 Выражение (*expression*) 15
 —, свободное от переменных (*variable-free*) 37
 Выражения сравнимые (*compatible expressions*) 33
 Высота (*height*) 32
 Вычислимость (*calculability*) 165, 181, 182, 215

Гиперскачок (*hyperjump*) 294
 Гиперстепень (*hyperdegree*) 294
 Гипотеза континуума (*continuum hypothesis*) 378
 — обобщенная (*generalized continuum hypothesis*) 378
 — четырех красок (*four-color conjecture*) 149
 Гомоморфизм (*homomorphism*) 146
 — негативный (*negative*) 146
 — позитивный (*positive*) 146
 График (*graph*) 219, 225
 Группа (*group*) 43
 — конечно определенная (*finitely presented*) 464
 — полная (*divisible*) 145
 — рекурсивно определенная (*recursively presented*) 464
 — свободная (*free*) 459
 — Хигмена (*Higman's group*) 465

Дерево (*tree*) 268
 Дизъюнкт (*disjunct*) 104
 Дизъюнкция (*disjunction*) 36
 Длина выражения (*length of an expression*) 15
 Доказательство (*proof*) 18
 — индукцией (*by induction*) 17, 18, 53, 168, 381
 — обозримое (*visualize*) 14
 — трансфинитной индукцией (*by transfinite induction*) 362
 — конечное (*finitary*) 13
 — формулы 18

Заклучение правила (*conclusion of a rule*) 16
 Замыкание (*closure*) 56
 Значение возможное (*possible value*) 504
 — истинностное (*truth*) 26
 — отображения (*value of a mapping*) 24

Идеал измеримый (*measure ideal*) 442
 Иерархия аналитическая (*analytical hierarchy*) 259
 — арифметическая (*arithmetical*) 240
 Изоморфизм (*isomorphism*) 111, 151
 — интерпретаций (*of interpretations*) 380
 — мягкий (*benign*) 469
 Импликация (*implication*) 36
 Имя выражения (*name of an expression*) 20
 — индивида (*of an individual*) 37
 — элемента (*of an element*) 490
 Индекс (*index*) 32, 235
 — по (*from*) 249
 — функциональный (*functional*) 250
 Индивид (*individual*) 24, 37
 Индукция по объектам (*induction on objects*) 18
 — предикатным символам (*on predicate symbols*) 381
 — теоремам (*on theorems*) 17
 Интерпретация опровержением контр-примера (*no counterexample interpretation*) 328
 — простая (*simple*) 203
 — теории в теории (*of a theory in a theory*) 99
 — точная (*faithful*) 201
 — транзитивная (*transitive*) 382
 — формулы (*of a formula*) 99
 — языка в теории (*of a language in a theory*) 99
 — — языке (*in a language*) 98

Кардинал (*cardinal*) 371
 — в M (*in M*) 485
 — недостижимый (*inaccessible*) 438
 — регулярный (*regular*) 454, 483
 — сингулярный (*singular*) 454, 483
 — слабо недостижимый (*weakly inaccessible*) 454
 Категоричность (*categoricity*) 138
 Квизитавтология (*quasi-tautology*) 80
 Квантор (*quantifier*) 36
 — всеобщности (*universal*) 36
 — для бесконечно многих (*for infinitely many*) 286
 — неограниченный (*unbounded*) 172
 — ограниченный (*bounded*) 172
 — существования (*existential*) 36
 Класс (*class*) 24, 348
 — аксиоматизируемый 144
 — в M (*in M*) 485
 — замкнутый (*closed*) 148
 — обобщенно элементарный (*generalized elementary*) 144
 — центрированный (*satisfies the finite intersection property*) 159
 — элементарный (*elementary*) 144

Константа (*constant*) 31, 318
 — специальная (*special*) 75
 Конъюнкция (*conjunction*) 36

Лемма бесконечности (*infinity lemma*) 279
 — диагональная (*diagonal lemma*) 196
 — интерполяционная Крейга (*Craig interpolation lemma*) 126
 — об истинности (*truth lemma*) 413, 490
 — о диаграмме (*diagram lemma*) 116
 — — замене (*replacement lemma*) 246
 — — конечности (*finiteness lemma*) 246
 — определимости (*definability lemma*) 490
 — о проекции (*projection lemma*) 251
 — — расширении (*extension lemma*) 490
 — транзитивности (*transitivity lemma*) 245
 — Тарского (*Tarski's lemma*) 120
 — Тейхмюллера — Тьюки (*Teichmüller — Tukey lemma*) 77
 — Цорна (*Zorn's lemma*) 453

Матрица (*matrix*) 62
 Метод (*method*) 164
 — механический (*mechanical*) 164
 — разрешающий (*decision method*) 162, 163, 215, 216, 221, 224
 — сжатия (*collapsing technique*) 484
 Множества много-односводимые (*many-one reducible sets*) 285
 — одно-односводимые (*one-one reducible*) 285
 — подобные (*similar*) 369
 — рекурсивно изоморфные (*recursively isomorphic*) 283
 — — неотделимые (*recursively inseparable*) 210
 — таблично сводимые (*truth-table reducible*) 287
 — эффективно рекурсивно неотделимые (*effectively recursively inseparable*) 286
 Множество (*set*) 24, 348
 — автоморфизмов $\mathcal{A}$ -однородное (*$\mathcal{A}$ -homogeneous set of automorphisms*) 500
 — бесконечное (*infinite*) 373
 — вполне упорядоченное (*well-ordered*) 293
 — — упорядочивающее (*well-ordering*) 453
 — — фундированное (*well-founded*) 293
 — вычислимое (*calculable*) 165
 — гиперпростое (*hypersimple*) 288
 — достижимое (*accessible*) 439
 — измеримое (*measurable*) 442
 — изоморфизмов мягкое (*benign set of isomorphisms*) 471

- Множество инвариантное (*invariant*) 427
- индуктивное (*inductive*) 453
 - конечное (*finite*) 373
 - конструктивное (*constructible*) 396
 - креативное (*creative*) 284
 - наследственно ординально определимое (*hereditarily ordinal-definable*) 500
 - одноэлементное (*unit set*) 356
 - ординально определимое (*ordinal-definable*) 500
 - отделимое (*separated*) 425
 - отделяющее (*separating*) 210
 - полное (*complete*) 287
 - простое (*simple*) 284
 - пустое (*empty*) 356
 - регулярное (*regular*) 452
 - реляционное (*relational*) 293
 - гиперарифметическое (*hyperarithmetical relational*) 294
 - рекурсивное (*recursive relational*) 294
 - слов рекурсивное (*recursive set of words*) 463
 - рекурсивно перечислимое (*recursively enumerable*) 463
 - степени (*power set*) 355
 - счетное (*countable*) 373
 - транзитивное (*transitive*) 360
 - чистое (*pure*) 349
 - формул главное (*principal set of formulas*) 141
 - инвариантное (*invariant*) 146
 - регулярное (*regular*) 116
 - тавтологически непротиворечивое (*tautologically consistent*) 103
 - — полное (*tautologically complete*) 104
 - — противоречивое (*tautologically inconsistent*) 103
 - F-замкнутое (*F-closed*) 375
 - Q-замкнутое (*Q-closed*) 295
- Модель простая (*prime model*) 15
- регулярная (*regular*) 339
 - стандартная (*standard*) 43, 307, 336
 - теории (*model of a theory*) 43
 - тотальная (*total*) 340
 - транзитивная (*transitive*) 484
 - элементарно простая (*elementarily prime*) 159
- Мощность структуры (*cardinal of a structure*) 122
- Мягкость (*benign*) 469, 471
- Номер (*number*) 185
- выражения (*expression number*) 185
 - последовательности (*sequence number*) 177
 - символа (*symbol number*) 185

- Обеднение (*restriction*) 71, 149
- Область значений (*range*) 359
- изменения переменной (*a variable varies through*) 20
 - определения (*domain*) 215, 216, 359

- Обобщение (*generalization*) 36
- Обогащение (*expansion*) 71
- несущественное (*inessential*) 212
 - с помощью определений (*expansion by definitions*) 202
- Образ гомоморфный (*homomorphic image*) 147
- Образующая (*generator*) 142
- Образующие группы (*generators*) 460
- Объединение (*union*) 356
- теорий (*of theories*) 124
 - цепи (*of a chain*) 119
- Однородность (*homogeneous*) 500
- Операция пренексная (*prenex operation*) 62
- эффективная (*effective*) 288
- Определение истинности (*truth definition*) 208
- неявное (*implicit*) 237, 280
 - обобщенное индуктивное (*generalized inductive*) 17
 - разбором случаев (*by cases*) 173
 - символа (*of symbol*) 19
 - с помощью индукции (*by induction*) 367
 - трансфинитной индукцией (*by transfinite induction*) 356
 - явное (*explicit*) 168
- Оракул (*oracle*) 222
- Ординал (*ordinal*) 360
- бесконечный (*infinite*) 364
 - дерева (*of a tree*) 270
 - конечный (*finite*) 364
 - минимальный (*minimal*) 361
 - первый (*first*) 362
 - предельный (*limit*) 364
 - рекурсивный (*recursive*) 272
 - рода Δ_1^1 (Δ_1^1 ordinal) 457
- Отношение (*relation*) 233
- аналитическое (*analytical*) 258
 - арифметическое (*arithmetical*) 239
 - борелевское (*Borel*) 267
 - всюду определенное (*total*) 223
 - вычислимое (*calculable*) 224
 - гиперарифметическое (*hyperarithmetical*) 263
 - — в (*in*) 266, 267
 - отделяющее (*separating*) 275
 - перечисляющее (*enumerating*) 236
 - позитивно вычислимое (*positively calculable*) 224
 - проективное (*projective*) 261
 - рекурсивное (*recursive*) 225
 - — частичное (*recursive partial*) 225
 - — в (*in*) 245
 - рекурсивно перечислимое (*recursively enumerable*) 225
 - — в (*in*) 244
 - рода 239, 259, 261
 - функционально арифметическое (*functionally arithmetical relation*) 250
 - — перечисляющее (*enumerating*) 251
 - рекурсивное (*recursive*) 250
 - — в (*in*) 245
 - рекурсивно перечислимое (*recursively enumerable*) 250

- Отношение частичное (*partial*) 223
- Π_1 -равномерное (Π_1 uniformly) 296
- Отношения непересекающиеся (*disjoint relations*) 274
- Отображение (*mapping*) 24
- биективное (*bijective*) 111
 - взаимно однозначное 111
 - всюду определенное (*total*) 215
 - вычислимое (*calculable*) 165, 205, 215
 - инъективное (*injective*) 111
 - монотонное (*monoton*) 271
 - на (*onto*) 111
 - сюръективное (*surjective*) 111
 - точное (*nice*) 475
 - частичное (*partial*) 215
 - 1—1 (*one — one*) 111
- Отрицание (*negation*) 36
- Оценка истинностная (*truth valuation*) 47
- Пара неупорядоченная (*unordered pair*) 356
- упорядоченная (*ordered*) 357
- Парадокс Рассела (*Russel paradox*) 348
- Параметр (*parameter*) 354
- Перевод (*translation*) 93
- Переменная (*variable*) 20, 28, 31, 318
- индивидуальная (*individual*) 28
 - свободная (*free*) 34
 - связанная (*bound*) 34
 - синтаксическая (*syntactical*) 21
 - функциональная (*function*) 223
 - числовая (*number*) 223
- Пересечение (*intersection*) 356
- Перестановка (*permutation*) 427
- Подгруппа единичная (*zero subgroup*) 459
- инвариантная (*invariant*) 467
 - мягкая (*benign*) 469
 - объединенная (*amalgam*) 461
- Подкласс вполне рекурсивно перечислимый (*completely recursively enumerable subclass*) 283
- рекурсивный (*completely recursive*) 288
 - тотально рекурсивно перечислимый (*totally recursively enumerable*) 289
 - рекурсивный (*totally recursive*) 289
- Подмножество всюду определенное (*total subset*) 216
- вычислимое (*calculable*) 216
 - генерическое (*generic*) 409, 487
 - инвариантное (*invariant*) 475
 - мягкое (*benign*) 472
 - плотное (*dense*) 487
 - свободное (*free*) 460
 - частичное (*partial*) 216
 - C-генерическое (*C-generic*) 487
 - C-плотное (*C-dense*) 487
- Подмодель (*submodel*) 113
- Подструктура (*substructure*) 113
- порожденная множеством (*generated by set*) 145
 - элементарная (*elementary*) 115
- Подтверждение (*instantiation*) 36

- Поле алгебраически замкнутое (*algebraically closed field*) 134
- вещественно замкнутое (*real closed*) 136
- Понятие вынуждения (*notion of a forcing*) 487
- — m-замкнутое (*m-closed notion of a forcing*) 506
 - логическое (*logical concept*) 23
 - нелогическое (*nonlogical concept*) 23
 - основное (*basic concept*) 12
 - производное (*derived concept*) 12
- Порядок алфавитный (*alphabetical order*) 31
- множества (*order of a set*) 396
- Последователь (*successor*) 17, 363
- Последовательность классов (*sequence of classes*) 514
- специальная (*special*) 80
 - убывающая (*descending*) 268, 293
- Посылка правила (*hypothesis of the rule*) 16
- Правило ассоциативности (*associative rule*) 41
- вывода (*rule of the inference*) 16
 - — конечное (*finite rule*) 18
 - дистрибутивности (*distribution*) 55
 - индукции (*induction*) 316, 336
 - логическое (*logical*) 40
 - нелогическое (*nonlogical*) 40
 - обобщения (*generalization*) 54
 - отделения (*detachment*) 49
 - подстановки (*substitution*) 54
 - расширения (*expansion*) 41
 - сечения (*cut*) 41
 - — слабое (*weak cut*) 105
 - сокращения (*contraction*) 41
 - $\forall$ -введения ($\forall$ -introduction) 54, 316
 - $\exists$ -введения ($\exists$ -introduction) 41
- Праэлемент (*urelement*) 348
- Предикат (*predicate*) 24
- бинарный (*binary*) 24
 - всюду определенный (*total*) 217
 - дизъюнктивно определенный (*disjunctively definable*) 152
 - индивидуальный (*individual*) 25
 - определимый (*definable*) 203
 - позитивно вычислимый (*positively calculable*) 184
 - представимый (*representable*) 191
 - примитивно рекурсивный (*primitive recursive*) 206
 - равенства (*equality*) 25
 - рекурсивно перечислимый (*recursively enumerable*) 184
 - рекурсивный (*recursive*) 168
 - — в (*in*) 244
 - — частичный (*recursive partial*) 220
 - слабо представимый (*weakly representable*) 208
 - унарный (*unary*) 24
 - частичный (*partial*) 217
- Предикаты эквивалентные (*equivalent predicates*) 252
- H-эквивалентные (*H-equivalent*) 294
- Предложение $\mathfrak{A}$ -инвариантное ($\mathfrak{A}$ -invariant sentence) 500

- Предположение индуктивное (*induction hypothesis*) 17, 18, 362
 Препятствует (*prevents*) 411
 Принцип кофинальности (*principle of cofinality*) 350
 — наименьшего числа (*least number*) 302
 — отделмости (*separation principle*) 297
 — полной индукции (*principle of complete induction*) 301
 — редукции (*reduction principle*) 297
 — трансфинитной индукции (*principle of transfinite induction*) 362
 Приставка (*prefix*) 62
 — нормализованная (*normalized*) 259
 Проблема Гильберта (*Hilbert's problem*) 163
 — разрешимости (*decision*) 162, 163
 — тождества слов (*word*) 463
 — — неразрешимая (*unsolvable*) 464
 — — разрешимая (*solvable*) 464
 — характеристики (*characterization*) 67
 Программа Гильберта (*Hilbert's program*) 14
 Произведение декартово (*Cartesian product*) 357
 — свободное групп (*free product of groups*) 462
 — — с объединенной группой (*with the amalgamation*) 461
 — прямое (*direct product*) 147
 Равенство определяющее (*defining equation*) 318
 Разность множеств (*set difference*) 356
 Ранг (*rank*) 80
 — множества (*of a set*) 438, 483
 Расширение конечное (*finite extension*) 201
 — консервативное (*conservative*) 68
 — номера (*of a number*) 268
 — простое (*simple*) 77
 — рекурсивное (*recursive*) 303
 — с помощью определений (*by definitions*) 97
 — структуры (*of a structure*) 113
 — теории (*of a theory*) 68
 — условия (*of a condition*) 408, 487
 — элементарное (*elementary*) 115
 — языка (*of a language*) 68
 Рекурсивность (*recursive*) 220
 Род 261
 Сандвич (*sandwich*) 150
 Свертка (*contraction*) 178, 246
 Свертывание кванторов (*contraction of quantifiers*) 227
 Селектор (*selector*) 284
 Семантический (*semantical*) 14
 Сечение (*section*) 506
 Символ (*symbol*) 15
 — абсолютный (*absolute*) 387, 485

- Символ доминирует (*dominates*) 345
 — логический (*logical*) 31
 — нелогический (*nonlogical*) 31
 — определяемый (*defined*) 19
 — — в терминах (*definable in terms of*) 126
 — ординальный функциональный (*ordinal function*) 363
 — полный (*complete*) 388
 — предикатный (*predicate*) 31
 — равенства (*equality*) 31
 — типовой (*type*) 317
 — функциональный (*function*) 31
 — — *M*-инвариантный (*M-invariant*) 383
 Синтаксический (*syntactical*) 14
 Система аксиоматическая (*axiom system*) 12
 — — классическая (*classical*) 12
 — — современная (*modern*) 12
 — формальная (*formal*) 14
 Скачок (*jump*) 254
 Следствие (*consequence*) 40, 460
 — логическое (*logical*) 40
 — тавтологическое (*tautological*) 47
 Слово (*word*) 459
 — позитивное (*positive*) 477
 Случай частный (*instance*) 38, 54
 — — численный (*numerical*) 309
 Сокращение (*reduction*) 459
 Соотношение (*relation*) 460
 — истинное (*hold*) 460
 — определяющее (*defining*) 460
 Сочетание скобок правое (*association to the right*) 36
 Спутник отображения (*associate of a mapping*) 475
 Степень (*degree*) 252
 — рекурсивной неразрешимости (*of recursive unsolvability*) 252
 — рекурсивно перечислимая (*recursively enumerable*) 253
 — — в (*in*) 253
 — слабая (*weak power*) 484, 499
 Структура (*structure*) 37
 — каноническая (*canonical*) 72
 — конечно порожденная (*finitely generates*) 145
 — насыщенная (*saturated*) 157
 — неразрешимая (*undecidable*) 209
 — однородная (*homogeneous*) 157
 — определимая (*definable*) 204
 — слабо насыщенная (*weakly saturated*) 157
 — строго неразрешимая (*strongly undecidable*) 202
 — универсальная (*universal*) 157
 Структуры изоморфные (*isomorphic structures*) 111
 — элементарно эквивалентные (*elementarily equivalent*) 113
 Тавтология (*tautology*) 47
 Тезис Чёрча (*Church thesis*) 181
 Теорема (*theorem*) 11, 16
 — Артина — Шрайера — (*Artin — Schreier theorem*) 155

- Банаха — Улама (*Banach — Ulam theorem*) 443
 — Генкина — Оре (*Henkin — Orey theorem*) 341
 — Гёделя (*theorem of Gödel*) 402
 — Гильберта о корнях (*Hilbert's Nullstellensatz*) 154
 — главная (*principal theorem*) 489
 — дедукции (*deduction theorem*) 56
 — замыкания (*closure theorem*) 56, 375
 — истинности (*validity theorem*) 44
 — Кантора (*Cantor's theorem*) 376
 — Кёнига (*König's theorem*) 484
 — Клини о базисе (*Kleene basis theorem*) 278
 — компактности (*compactness theorem*) 108
 — Крайзеля о базисе (*Kreisel basis theorem*) 280
 — Лёвенгейма — Скулема (*Löwenheim — Skolem theorem*) 123
 — Линденбаума (*Lindenbaum's theorem*) 77
 — Лося — Воота (*Łoś — Vaught theorem*) 139
 — Лося — Тарского (*Łoś — Tarski theorem*) 119
 — Морли (*theorem of Morley*) 141
 — непротиворечивости (*consistency theorem*) 80
 — Новикова 465
 — о варианте (*variant theorem*) 59
 — — вполне упорядоченности (*well-ordering theorem*) 370
 — — вхождении (*occurrence theorem*) 33
 — — дереве (*tree theorem*) 268
 — — доказательствах непротиворечивости (*theorem on consistency proofs*) 314
 — — константах (*theorem on constants*) 57
 — — мощности (*cardinality theorem*) 123
 — — неполноте (*incompleteness theorem*) 199
 — — нормальной форме (*normal form theorem*) 235
 — — перечислении (*enumeration theorem*) 236
 — — подстановке (*substitution theorem*) 232
 — — представимости (*representability theorem*) 193
 — — произведении (*product theorem*) 497
 — — расширении модели (*model extension theorem*) 116
 — — рекурсии (*recursion theorem*) 237
 — — совместной непротиворечивости (*joint consistency theorem*) 124
 — — функциональном расширении (*theorem on functional extension*) 90
 — — об аналитической иерархии (*analytical hierarchy theorem*) 261
 — — аналитическом перечислении (*analytical enumeration theorem*) 261
 — — арифметической иерархии (*arithmetical hierarchy theorem*) 243
 Теорема об арифметическом перечислении (*arithmetical enumeration theorem*) 242
 — — интерпретации (*interpretation theorem*) 100
 — — отрицании (*negation theorem*) 197, 244
 — — элиминации кванторов (*quantifiers elimination theorem*) 133
 — — ограниченности (*boundedness theorem*) 274
 — — определимости (*definability theorem*) 127
 — — отделмости (*separation theorem*) 275
 — — подстановки (*substitution theorem*) 55
 — — полноты (*completeness theorem*) 70
 — Поста (*Post's theorem*) 249
 — построения (*formation theorem*) 33
 — равенства (*equality theorem*) 60
 — редукции (*reduction theorem*) 68
 — — для непротиворечивости (*reduction theorem for consistency*) 70
 — Россера (*Rosser's theorem*) 342
 — Рыль-Нардзевского (*Ryll-Nardzewski's theorem*) 142
 — симметрии (*symmetry theorem*) 60
 — системы (*theorem of the system*) 18
 — Скотта (*Scott's theorem*) 451
 — Скулема (*Skolem's theorem*) 92
 — существования (*existence theorem*) 487
 — тавтологии (*tautology theorem*) 49
 — униформизации (*uniformization theorem*) 280
 — Фридберга — Мучника (*Fridberg — Muchnik theorem*) 254
 — Ханфа — Тарского (*Hanf — Tarski theorem*) 450
 — характеристики (*characterization theorem*) 275
 — Хигмена (*Higman's theorem*) 465
 — Чёрча (*Church's theorem*) 197
 — Чжана — Лося — Сушко (*Chang-Łoś — Suszko theorem*) 120
 — Шрайера (*Schreier's theorem*) 461
 — эквивалентности (*equivalence theorem*) 59
 — Эрбрана (*Herbrand theorem*) 87
 — Эренфойхта (*Ehrenfeucht's theorem*) 141
 Теории слабо эквивалентные (*weakly equivalent theories*) 106
 — совместимые (*compatible*) 209
 — эквивалентные (*equivalent*) 68
 Теория (*theory*) 42
 — Генкина (*Henkin theory*) 73
 — групп элементарная (*elementary theory of groups*) 43
 —, допускающая элиминацию кванторов (*admits elimination of quantifiers*) 129
 — интерпретируемая (*interpretable*) 103
 — категоричная (*categorical*) 140
 — в мощности (*categorical in power*) 138
 — *m*-категоричная (*m-categorical*) 138

- Теория конечно аксиоматизируемая (*finitely axiomatized*) 108
- множеств Цермело — Френкеля (*Zermelo — Fraenkel set theory*) 350
 - модельно полная (*model-complete*) 153
 - наследственно неразрешимая (*hereditarily undecidable*) 211
 - непротиворечивая (*consistent*) 69
 - неразрешимая (*undecidable*) 186
 - открытая (*open*) 79
 - первого порядка (*first-order*) 42
 - полей элементарная (*elementary theory of fields*) 109
 - полная (*complete*) 74
 - противоречивая (*inconsistent*) 69
 - разрешимая (*decidable*) 186
 - рекурсивно аксиоматизированная (*axiomatized*) 189
 - аксиоматизируемая (*axiomatizable*) 207
 - структуры (*of a structure*) 128
 - совместимая (*compatible*) 209
 - строго неразрешимая (*strongly undecidable*) 209
 - существенно неразрешимая (*essentially undecidable*) 209
 - счетная (*countable*) 122
 - , удовлетворяющая подмодельному условию (*satisfies submodel condition*) 131
 - , — условию изоморфизма (*satisfies isomorphism condition*) 131
 - упорядоченных полей элементарная (*elementary theory of ordered fields*) 136
 - численная (*numerical theory*) 208
- Терм (*term*) 31, 318
- допустимый для подстановки (*substitutable*) 35
 - представляет (*represents*) 191
 - сводимый (*reducible*) 332
- Тип кванторов (*type of quantifiers*) 258
- *n*-ки (*type of a n-tuple*) 139
- Указатель (*designator*) 32
- Ультрапроизведение (*ultraproduct*) 160
- Ультрарасепень (*ultrapower*) 160
- Ультрафильтр (*ultrafilter*) 159
- Универсум (*universe*) 24, 37, 98
- интерпретации (*of an interpretation*) 98
- Уровень специальной константы (*level of a special constant*) 75
- Условие (*condition*) 408, 487
- единственности (*uniqueness condition*) 95
 - изоморфизма (*isomorphism*) 131
 - корректное (*correct*) 408
 - подмодельное (*submodel*) 131
 - существования (*existence*) 95, 303, 354, 359
 - Π -цепи (Π -chain) 504
- Условия совместные (*compatible conditions*) 504
- Форма дизъюнктивная (*disjunctive form*) 65
- конъюнктивная (*conjunctive*) 65
 - пренексная (*prenex form*) 62, 64
 - скулемовская (*Skolem form*) 107
- Формула (*formula*) 15, 32, 319
- атомная (*atomic*) 32, 319
 - верная (*valid*) 323
 - выполнимая (*satisfiable*) 107
 - замкнутая (*closed*) 38
 - истинная (*true*) 38, 43, 307, 319
 - логически истинная (*logically valid*) 40
 - Маккинси (*McKinsey*) 147
 - негативная (*negative*) 146
 - неразрешимая (*undecidable*) 74
 - обобщенная (*generalized*) 321
 - определяемая (*defined*) 19
 - открытая (*open*) 62
 - , относящаяся к специальной константе (*belong to special constant*) 79
 - позитивная (*positive*) 146
 - представляет (*represents*) 191
 - простая экзистенциальная (*simply existential*) 130
 - разрешимая (*decidable*) 74
 - свертывания (*contraction*) 178
 - секущая (*cut*) 105
 - слабо представляет (*weakly represents*) 208
 - универсальная (*universal*) 91
 - Хорна (*Horn*) 147
 - экзистенциальная (*existential*) 85
 - элементарная (*elementary*) 47
- Формулы эквивалентные (*equivalent formulas*) 129
- Функции эквивалентные (*equivalent functions*) 252
- Функционал (*functional*) 223, 317
- в M (*in M*) 485
 - всюду определенный (*total*) 223
 - вычислимый (*calculable*) 224
 - представляющий частичный (*representing partial*) 224
 - рекурсивного типа (*type recursive*) 328
 - рекурсивный частичный (*recursive partial*) 225
 - — в (*recursive in*) 224
 - типа r (*of type r*) 317
 - функционально рекурсивный (*functionally recursive*) 250
 - частичный (*partial*) 223
- Функция (*function*) 24, 359
- всюду определенная (*total*) 217
 - выбора (*choice*) 369
 - гиперарифметическая (*hyperarithmetical*) 276
 - , имеющая свойство (*having property*) 168
 - индивидуальная (*individual*) 25
 - инъективная (*injective*) 359
 - истинности (*truth*) 26
 - креативная (*creating*) 284
 - определяемая (*definable*) 44, 203
 - , перечисляющая множество (*enumerates a set*) 207
 - представимая (*representable*) 191
 - представляющая (*representing*) 166
 - — частичная (*representing partial*) 218
 - примитивно рекурсивная (*primitive recursive*) 206
 - рекурсивная (*recursive*) 167

- — в (*recursive in*) 244
- Функция рекурсивная частичная (*recursive partial*) 220
- сингулярная (*singular*) 45
 - частичная (*partial*) 217
- Характер конечный (*finite character*) 76
- Цепь (*chain*) 119, 453
- элементарная (*elementary*) 120
- Цифра (*numeral*) 191
- Часть теории (*part of a theory*) 108
- Число действительное рекурсивное (*recursive real number*) 206
- натуральное (*natural*) 17, 359, 364
- Эквивалентность (*equivalence*) 36
- Элемент бесконечный (*infinite element*) 346
- максимальный (*maximal*) 77, 272, 453
 - минимальный (*minimal*) 350
 - неединичный (*nonzero*) 459
 - y -первый (*y-first*) 453
- Элиминация кванторов (*elimination of quantifiers*) 130
- Язык (*language*) 14
- вынуждения (*forcing*) 490
 - первого порядка (*first-order*) 31, 32
 - счетный (*countable*) 122
- H -индекс (H -index) 263
- по (H -index from) 266
- J -вынуждение (J -forcing) 428
- k -перестановка (k -permutation) 427
- M -множество (M -set) 382
- n -ка (n -tuple) 24
- n -сэндвич (n -sandwich) 150
- n -тип (n -type) 140
- R -символ (R -symbol) 343
- R -формула (R -formula) 307
- RE -индекс (RE -index) 236, 251
- по (RE -index from) 250
- u -изоморфизм (u -isomorphism) 126
- y -последовательность (y -sequence) 453
- Π -теория (Π -theory) 122
- Π -язык (Π -language) 122
- Γ -диаграмма (Γ -diagram) 116
- Γ -морфизм (Γ -morphism) 145
- Γ -подструктура (Γ -substructure) 115
- Γ -расширение (Γ -extension) 115
- δ -идеал (δ -ideal) 458
- μ -оператор (μ -operator) 167
- неограниченный (*unbounded*) 171
 - ограниченный (*bounded*) 171
- φ -элемент (φ -element) 467
- ω -модель (ω -model) 340
- $\models$ -интерпретация ($\models$ -interpretation) 382
- транзитивная (*transitive*) 382
- $\neg$ -правило ($\neg$ -rule) 105
- $\neg V$ -правило ($\neg V$ -rule) 105
- $\neg \exists$ -правило ($\neg \exists$ -rule) 105
- V -правило (V -rule) 109
- $\exists$ -правило ($\exists$ -rule) 105

Джозеф Шенфилд

МАТЕМАТИЧЕСКАЯ ЛОГИКА

(Серия: «Математическая логика
и основания математики»)

М., 1975 г., 528 стр.

Редактор *В. В. Донченко*

Техн. редактор *С. Я. Шкляр*

Корректор *Е. Я. Строева*

Сдано в набор 27/XII 1974 г. Подписано к печати
31/VII 1975 г. Бумага $84 \times 108 \frac{1}{32}$. Физ. печ. л. 16,5.
Условн. печ. л. 27,72. Уч.-изд. л. 27,48. Тираж
25 000 экз. Цена книги 2 р. 16 к. Заказ № 1815

Издательство «Наука»

Главная редакция физико-математической
литературы

117071, Москва, В-71, Ленинский проспект, 15

Ордена Трудового Красного Знамени Ленинград-
ское производственно-техническое объединение
«Печатный Двор» имени А. М. Горького Союз-
полиграфпрома при Государственном комитете
Совета Министров СССР по делам издательств,
полиграфии и книжной торговли. 197136, Ленин-
град, П-136, Гатчинская ул., 26.