Ю. Л. ЕРШОВ, Е. А. ПАЛЮТИН

МАТЕМАТИЧЕСКАЯ ЛОГИКА

Ю. Л. ЕРШОВ, Е. А. ПАЛЮТИН

МАТЕМАТИЧЕСКАЯ ЛОГИКА

ИЗДАНИЕ ВТОРОЕ,
ИСПРАВЛЕННОЕ И ДОПОЛНЕННОЕ

Допущено Министерством высшего и среднего специального образования СССР в качестве учебного пособия для студентов математических специальностей высших учебных заведений

МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1987

ББК 22.12
Е80
УДК 510.6 (075.8)

Ершов Ю. Л., Палютин Е. А. **Математическая логика:** Учеб. пособие для вузов.— 2-е изд., испр. и доп.— М.: Наука. Гл. ред. физ.-мат. лит., 1987.— 336 с.

В книге изложены основные классические исчисления математической логики: исчисление высказываний и исчисление предикатов; имеется краткое изложение основных понятий теории множеств и теории алгоритмов. Ряд разделов книги — теория моделей и теория доказательств — изложены более подробно, чем это предусмотрено программой.

Для студентов математических специальностей вузов. Может служить пособием для спецкурсов.

Рецензент
член-корреспондент АН СССР *О. Б. Лупанов*

Юрий Леонидович Ершов
Евгений Андреевич Палютин

МАТЕМАТИЧЕСКАЯ ЛОГИКА

Редактор *В. В. Донченко*
Художественный редактор *Т. Н. Кольченко*
Технический редактор *В. Н. Кондакова*
Корректоры *Г. В. Подвольская, М. Л. Медведская*

ИБ № 12972

Сдано в набор 21.05.86. Подписано к печати 16.02.87. Формат 84×108/32. Бумага тип. № 2. Гарнитура обыкновенная новая. Печать высокая. Усл. печ. л. 17,64. Усл. кр.-отт. 17,64. Уч.-изд. л. 19,38. Тираж 30 000 экз. Заказ № 218. Цена 95 коп.

Ордена Трудового Красного Знамени издательство «Наука»
Главная редакция физико-математической литературы
117071 Москва В-71, Ленинский проспект, 15

4-я типография издательства «Наука»
630077 г. Новосибирск 77, Станиславского, 25

Е $\frac{1702020000-069}{053(02)-87}$ 58-87

ОГЛАВЛЕНИЕ

Предисловие ко второму изданию 5
Предисловие к первому изданию 6
Введение 9

Глава 1. **Исчисление высказываний** 15
§ 1. Множества и слова 15
§ 2. Язык исчисления высказываний 22
§ 3. Система аксиом и правил вывода 25
§ 4. Эквивалентность формул 32
§ 5. Нормальные формы 36
§ 6. Семантика исчисления высказываний 43
§ 7. Характеризация доказуемых формул 48
§ 8. Исчисление высказываний гильбертовского типа . 52
§ 9. Консервативные расширения исчислений . . . 56

Глава 2. **Теория множеств** 65
§ 10. Предикаты и отображения 65
§ 11. Частично упорядоченные множества 70
§ 12. Фильтры булевой алгебры 78
§ 13. Мощность множества 82
§ 14. Аксиома выбора 90

Глава 3. **Истинность на алгебраических системах** . . . 96
§ 15. Алгебраические системы 96
§ 16. Формулы сигнатуры Σ 103
§ 17. Теорема компактности 111

Глава 4. **Исчисление предикатов** 119
§ 18. Аксиомы и правила вывода 119
§ 19. Эквивалентность формул 128
§ 20. Нормальные формы 132
§ 21. Теорема о существовании модели 135
§ 22. Исчисление предикатов гильбертовского типа . 142
§ 23. Чистое исчисление предикатов 147

Глава 5. **Теория моделей** 152
§ 24. Элементарная эквивалентность 152
§ 25. Аксиоматизируемые классы 161
§ 26. Скулемовские функции 169
§ 27. Механизм совместности 172
§ 28. Счетная однородность и универсальность . . . 186
§ 29. Категоричность 193

Глава 6. **Теория доказательств** 204
§ 30. Генценовская система G 204
§ 31. Обратимость правил 209
§ 32. Сравнение исчислений ИП$^{\Sigma}$ и G 214
§ 33. Теорема Эрбрана 222
§ 34. Исчисления резольвент 233

Глава 7. **Алгоритмы и рекурсивные функции** 241
§ 35. Нормальные алгорифмы и машины Тьюринга . 241
§ 36. Рекурсивные функции 251
§ 37. Рекурсивно перечислимые предикаты 268
§ 38. Неразрешимость исчисления предикатов и теорема Гёделя о неполноте 281
§ 39. Разрешимые теории 296
§ 40. Неразрешимые теории 318

Предметный указатель 335

ПРЕДИСЛОВИЕ КО ВТОРОМУ ИЗДАНИЮ

При подготовке нового издания значительной переработке подверглась глава 6, имевшая ранее серьезные погрешности. К главе 7 добавлены два новых параграфа (§ 39. Разрешимые теории и § 40. Неразрешимые теории). Незначительные изменения сделаны и по остальному тексту: исправлены замеченные опечатки и мелкие погрешности, сделаны небольшие добавления.

Авторы благодарны коллегам, конструктивная критика которых способствовала улучшению книги.

ПРЕДИСЛОВИЕ К ПЕРВОМУ ИЗДАНИЮ

Настоящая книга представляет собой систематическое изложение ряда разделов современной математической логики и теории алгоритмов. Написана она с целью использования ее в преподавании как в качестве учебника по математической логике для университетов, так и в качестве учебного пособия при чтении спецкурсов.

Разделы, соответствующие обязательной программе (§ 1—9 в главе 1 (без мелкого шрифта), § 10—11 в главе 2, § 15—16 в главе 3, § 18—20, 22—23 в главе 4 и § 35 в главе 7), написаны более тщательно и подробно, чем разделы, относящиеся к более специальным вопросам.

Изложение исчисления высказываний и исчисления предикатов не является традиционным и начинается с изучения секвенциальных вариантов исчислений натурального вывода (хотя традиционные исчисления также появляются здесь под названием гильбертовских). Основанием к этому являются:

1) возможность хорошего объяснения смысла всех правил вывода;

2) возможность более быстрого приобретения навыка формальных доказательств;

3) практическая возможность проделать все необходимые в курсе формальные доказательства в таких исчислениях.

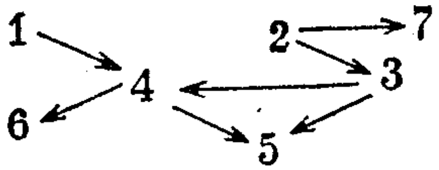
Многолетний опыт чтения старшим из авторов курса математической логики на математическом факультете НГУ, на основе которого написаны главы 1—4, показывает, что указанные выше возможности вполне реализуются. Это оправдывает использование такого способа изложения наряду с традиционными.

Более подробные сведения о содержании книги можно получить из ее оглавления.

Ввиду учебного характера книги, несмотря на названия «Теория множеств», «Теория моделей», «Теория доказательств» и «Алгоритмы и рекурсивные функции», соответствующие главы, конечно, содержат лишь малую часть содержания этих больших разделов современной математической логики. Как и принято в учебниках, большинство результатов приведено в данной книге без указания авторов.

В тексте имеется небольшое число упражнений почти после каждого параграфа книги. Однако этих упражнений явно недостаточно для учебных целей. Мы рекомендуем использовать в качестве задачника для данного курса следующий: Лавров И. А., Максимова Л. Л. Задачи по теории множеств, математической логике и теории алгоритмов.— М.: Наука, 1984.

Для облегчения пользования книгой укажем схему зависимости глав:



Сделаем несколько замечаний технического порядка. Нумерация теорем сквозная по главам, нумерация предложений и лемм своя в каждом параграфе. Выражение «предложение 12.2» («теорема 12.2», ...) означает «предложение 2 (теорема 2, ...) из § 12». При ссылке на предложения и леммы внутри одного параграфа и часто при ссылке на теоремы внутри одной главы параграф не указывается. Символ $\Rightarrow$ является сокращением для выражения «из... следует ...», символ $\Leftrightarrow$ является сокращением для выражения «... равносильно ...». Символ $\square$ указывает на окончание доказательства.

Создание этой книги не было бы возможно без коллектива кафедры алгебры и математической логики Новосибирского государственного университета. Основатель этой кафедры — выдающийся советский математик академик А. И. Мальцев (1909—1967) — оказал решающее влияние на формирование научных интересов и педагогических взглядов авторов. На разных этапах подготовки настоящей книги большую помощь и поддержку мы получали от М. И. Каргаполова, Н. В. Белякина, И. А. Лаврова, Л. Л. Максимовой и многих других. Этим коллегам и товарищам мы выражаем свою искреннюю признательность и благодарность.

При работе над данной книгой были использованы записи курсов лекций А. И. Мальцева и Ю. Л. Ершова, книги: Ершов Ю. Л., Палютин Е. А., Тайцлин М. А. Математическая логика.— Новосибирск: Изд-во НГУ, 1973; Куратовский К., Мостовский А. Теория множеств.— М.: Мир, 1970; Мальцев А. И. Алгебраические системы.— М.: Наука, 1970; Марков А. А. Теория алгорифмов.— М.: Изд-во АН СССР, 1954; Шенфилд Дж. Математическая логика.— М.: Наука, 1975, а также другие монографии и научные статьи.

Новосибирск .
Академгородок

Ю. Л. Ершов
Е. А. Палютин

ВВЕДЕНИЕ

Математическая логика как самостоятельный раздел современной математики сформировалась сравнительно недавно — на рубеже девятнадцатого — двадцатого веков. Возникновение и быстрое развитие математической логики в начале нашего века было связано с так называемым кризисом в основаниях математики. Поговорим об этом чуть подробнее.

При любой попытке систематического изложения математики (как, впрочем, и любой другой науки) возникает проблема выбора начальных (исходных) понятий и принципов, которые будут положены в основу всего изложения. Проблема выбора и обоснование этого выбора исходных данных лежит, как правило, вне самой научной дисциплины и относится к философии и методологии научного познания. Систематизация математики в конце девятнадцатого века выявила, что весьма перспективным является использование понятия множества в качестве единственного исходного понятия для всей математики. Работами Б. Больцано, Р. Дедекинда и Г. Кантора была создана новая область математики — теория множеств, которая красотой и силой своих построений и перспективами использования ее в основаниях математики привлекла внимание многих ведущих математиков того времени. Была проделана большая работа по теоретико-множественному осмыслению математических и даже логических понятий. В этой связи большой интерес представляют исследования Г. Фреге и Б. Рассела. Однако высокая степень абстрактности и «универсальность» понятия множества не могли не привести в конце концов к трудностям, хорошо и давно известным в философии при работе с «универсалиями». Проявилось это в появлении так называемых теоретико-множественных парадоксов.

Приведем один из наиболее типичных теоретико-множественных парадоксов — парадокс Рассела. Для произвольного множества является вполне осмысленным вопрос, «будет ли это множество своим собственным элементом». Примером множества, которое содержит само себя в качестве элемента, могло бы служить, например, множество всех множеств. Рассмотрим множество M_0 всех множеств, для которых ответ на этот вопрос отрицателен. Спросим теперь, является ли это множество своим элементом? К своему (наивному) удивлению обнаружим, что если ответ положительный, то имеем $M_0 \notin M_0$, т. е. ответ должен (бы) быть отрицательным. Если же ответ отрицателен, то в силу определения множества M_0 ответ должен быть положительным. Этот парадокс показывает, что если мы не хотим приходить к противоречиям, то необходимо (в частности) отказаться от приятной мысли, что любое осмысленное условие на элементы определяет некоторое множество. К счастью, такого рода парадоксы можно получить лишь с «большими» или «неестественными» множествами, без которых в математике можно вполне обойтись*).

Появление таких парадоксов в теории множеств было воспринято многими математиками очень болезненно и поэтому привлекло к вопросам оснований математики пристальное внимание практически всех ведущих математиков того времени (назовем к примеру имена Д. Гильберта, А. Пуанкаре, Г. Вейля). Было предложено несколько программ «спасения» математики от «ужаса» парадоксов, входить в детали которых мы не будем. Укажем вкратце только две наиболее действенные программы, различные модификации которых обсуждаются и в настоящее время. Отметим, что многообразие подходов к основаниям математики остается и поныне. Однако прошедшие годы и безусловные достижения математической логики, речь о которых еще впереди, сняли остроту этой проблемы настолько, что большинство математиков, работающих в других разделах математики, не уделяют особого внимания тем дискуссиям, которые ведут ныне специалисты по основаниям математики.

Одной из наиболее разработанных программ по основаниям математики является предложенная Д. Гильбертом программа финитарного обоснования математики. Суть этой программы состоит в попытке построения та-

*) Упоминаемые ниже формализации теории множеств — аксиоматические теории множеств,— сохраняя все полезное, не допускают проведения всех известных «парадоксальных» рассуждений.

кой формализации математики, что средствами этой системы можно доказать свою собственную непротиворечивость. Другим принципиальным требованием к такой формализации является условие, чтобы все простейшие, проверяемые непосредственно утверждения о натуральных числах были истинными в этой формализации. Работа над этой программой как самого Гильберта, так и его учеников и последователей оказалась весьма плодотворной для математической логики, в частности, в разработке современного аксиоматического метода. Хотя программа «финитизма» в своей исходной постановке оказалась невыполнимой, как показал в своих знаменитых работах К. Гёдель, однако возможные модификации этой программы подвергаются полезному обсуждению и до настоящего времени.

Другой подход к основаниям математики был связан с критикой ряда положений, которые использовались в математике без должного обоснования. Это относится, в частности, к неограниченному использованию закона исключенного третьего и аксиомы выбора. Программа построения математики при жестких ограничениях на использование этих принципов получила название интуиционизма; ее создание и развитие связано в первую очередь с именем Л. Э. Я. Брауэра. Развитый в Советском Союзе А. А. Марковым и его последователями конструктивистский подход к основаниям математики также связан с критическим подходом к допустимым логическим средствам в математике и систематически использует понятие алгоритма при конструктивистском воспроизведении математических результатов.

Хотя основания математики традиционно относятся к математической логике, в настоящем учебнике не место вдаваться в большие подробности этого раздела, находящегося на стыке математики и философии. Поэтому ограничим обсуждение оснований математики приведенными выше замечаниями, не претендующими на полноту и исчерпывающую точность, служащими скорее иллюстративным целям.

Основным итогом деятельности в области оснований математики можно считать становление математической логики как самостоятельного раздела математики, а принципиальным достижением математической логики — разработку *современного аксиоматического метода*, который может быть охарактеризован следующими тремя чертами:

1. Явная формулировка исходных положений (аксиом) той или иной теории.

2. Явная формулировка логических средств (правил вывода), которые допускаются для последовательного построения (развертывания) этой теории.

3. Использование искусственно построенных формальных языков для изложения всех положений (теорем) рассматриваемой теории.

Первая черта характеризует классический аксиоматический метод. Две следующие являются дальнейшими шагами в достижении максимальной точности и ясности в изложении теорий. Введение и использование подходящих обозначений было на протяжении всей истории математики весьма важной и продуктивной процедурой. Но математические символы были только элементами формальных языков. В математической же логике впервые в истории были созданы такие богатые формальные языки, которые позволяют формулировать практически все основные положения современной математики. Богатые формальные языки математической логики и успешный опыт работы с ними создали одну из объективных предпосылок для создания универсальных вычислительных машин, пользующихся в настоящее время весьма разнообразным спектром формальных языков программирования.

Основным объектом изучения в математической логике являются различные исчисления. В понятие исчисления входят такие основные компоненты, как: а) язык (формальный) исчисления; б) аксиомы исчисления; в) правила вывода. Понятие исчисления позволяет дать строгое математическое определение понятия *доказательства* и получить точные утверждения о невозможности доказательства тех или иных предложений теории. Еще одним замечательным достижением математической логики является нахождение математического определения понятия *алгоритма*, т. е. эффективной процедуры для решения задач из того или иного (бесконечного) класса задач. Интуитивно понятие алгоритма использовалось очень давно. Выдающийся мыслитель XVII—XVIII вв. Г. Лейбниц даже мечтал о нахождении универсального алгоритма для решения всех математических проблем. Точное определение понятия алгоритма позволило довольно быстро разрушить эту красивую утопию: А. Чёрч в 1936 г. показал, что невозможен алгоритм, который по произвольному утверждению, записанному на формальном языке элементарной арифметики, отвечал бы на вопрос: будет ли это утверждение истинно на натуральных числах? Далее оказалось, что даже в системе, описывающей «чистую логику» (исчисление предикатов), проблема доказуемости алгоритмически неразрешима. В последующие годы было обнаружено большое многообразие алгоритмически неразрешимых проблем в многих разделах математики. Большой вклад в разработку теории алгоритмов и решение алгоритмических проблем внесли Э. Пост, А. Тьюринг, С. Клини и советские математики А. И. Мальцев, П. С. Новиков и А. А. Марков.

Изучение исчислений составляет *синтаксическую* часть математической логики. Наиболее глубокое изучение (синтаксического) понятия доказательства в тех или иных исчислениях составляет самостоятельный раздел математической логики, который носит название *теории доказательств*. Наряду с синтаксическим изучением исчислений проводится также *семантическое* изучение формальных языков математической логики. Основным понятием семантики является понятие истинности для выражений (формул, секвенций и т. п.) формального языка. Семантические понятия также получили точные математические определения, что дало возможность систематического и строгого изучения различных понятий истинности. Классическая семантика языка исчисления предикатов составила весьма богатый раздел математической логики — *теорию моделей*, которая активно развивается, а ее методы и результаты успешно применяются и в других областях математики (алгебре, анализе). Основателями теории моделей являются А. Тарский и А. И. Мальцев.

Исчисления позволяют формализовать многие разделы математики и других наук. Исчисление высказываний и упоминавшееся выше исчисление предикатов являются формализациями логики, древнейшей науки о законах правильного мышления. Создание и изучение этих формализаций явилось важным этапом в развитии логики как науки. Первые попытки формализации логики связаны с именами Аристотеля и Дж. Буля, но действительная (и действенная) формализация логики была осуществлена только с созданием математической логики. Итальянский математик Пеано много сделал для разработки и популяризации формальных языков логики, Для математики особенно важной оказалась возможность формализации теории множеств. Исчисления, формализующие основные конструкции «наивной» теории множеств, оказались столь богатыми, что любое теоретико-множественное рассуждение, встречающееся в реальной математической практике, можно формально воспроизвести в этих исчислениях. Естественной «расплатой» за это богатство было обнаружение К. Гёделем эффектов неполноты и даже непополнимости таких исчислений.

На пути построения семантики естественных или формальных языков нас поджидают также большие трудности. Так, простодушное убеждение, что каждой повествовательной фразе русского языка можно правдоподобным (или, по крайней мере, непротиворечивым) образом приписать значение истинности, опровергается так называемым «парадоксом лжеца». Некто говорит: «Фраза, которую я сейчас произношу, ложна». Попробуем выяснить, правду сказал этот человек или солгал. Если предположить, что он сказал правду, то из смысла фразы получается, что он солгал. Если он солгал, то из того, что фраза ложна, получаем, что он сказал правду. Этот парадокс лежит в основе ряда замечательных теорем математической логики (теорем о неполноте и о неопределимости истинности в системе).

История создания и развития математической логики является самостоятельным предметом и ей не будет уделено внимания в этой книге, за исключением приведенных выше заведомо не полных указаний некоторых имен и обстоятельств.

В заключение настоящего введения нужно отметить, что современная математическая логика представляет собой обширный и разветвленный раздел математики, источником проблем для которого наряду с внутренними ее проблемами служат как философские проблемы оснований математики и логики, так и проблемы, возникающие в других разделах математики (алгебра, анализ, математическая кибернетика, программирование и др.).

Глава 1

ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

§ 1. Множества и слова

Под *буквой* мы понимаем знак, который рассматривается как целый, т. е. знак, части которого нас не интересуют. Букву будем называть также *символом* *). Про две данные (например, написанные) буквы мы можем говорить, что они одинаковы или что они различны. Например, все строчные буквы «а» в данной книге считаем одинаковыми. Одинаковыми мы считаем также все строчные буквы «а» в некотором рукописном тексте, хотя одинаковость двух букв в этом случае установить трудней, чем в предыдущем. Будет предполагаться, что для рассматриваемых двух конкретных букв мы всегда можем установить их одинаковость или различие. Если буквы a_1 и a_2 одинаковы, то будем писать $a_1 = a_2$.

Абстракция отождествления одинаковых букв дает нам понятие *абстрактной буквы*. В дальнейшем о двух одинаковых конкретных буквах a_1 и a_2 мы будем говорить как об одной и той же (абстрактной) букве a. При этом каждая из этих двух конкретных букв будет называться *представителем* абстрактной буквы a **).

Совокупность X некоторых объектов, которые будут называться элементами X, назовем *множеством* ***).

Если a — элемент множества X, то пишем $a \in X$. Если любой элемент множества X является элементом множества Y, то множество X называется *подмножеством* мно-

---

*) Иногда слово «буква» будет иметь и обычный смысл, например, «латинская буква», «строчная буква».

**) Следует при этом различать абстрактную букву, обозначаемую символом a, и сам символ a, который есть обозначение или имя упомянутой абстрактной буквы.

***) Как отмечалось во введении, такое определение, вообще говоря, может привести к противоречию. Однако это не должно пугать читателя, так как существование всех рассматриваемых в этой книге множеств можно вывести в рамках формальной системы, описанной в § 11, в которой невозможно провести ни одно известное «парадоксальное» рассуждение о множествах.

жества Y и обозначается это так: $X \subseteq Y$. Если для множеств X и Y имеем $X \subseteq Y$ и $Y \subseteq X$, то будем считать множества X и Y равными и писать $X = Y$. Таким образом, множество полностью определено своими элементами. В частности, существует только одно множество, не содержащее ни одного элемента. Такое множество будем называть *пустым* и обозначать символом $\varnothing$. Если для множества X не имеет место $a \in X$, то будем писать $a \notin X$.

Буквами i, j, k, l, m, n, p, r, s, возможно с индексами, будем обозначать натуральные числа. Множество всех натуральных чисел будем обозначать буквой ω. Если $a_1 \in X, \ldots, a_n \in X$, то будем писать $a_1, \ldots, a_n \in X$. Если X — множество, $a_1, \ldots, a_n \in X$ и любой элемент X равен одному из $a_1, \ldots, a_n$, то X называем *конечным множеством* и пишем $X = \{a_1, \ldots, a_n\}$ *). Если $\varphi(a)$ — некоторое условие на объект a, а X — множество, то через $\{a \in X \mid \varphi(a)\}$ или $\{a \mid \varphi(a), a \in X\}$ обозначаем множество, содержащее в качестве элементов те и только те элементы $a \in X$, которые удовлетворяют условию $\varphi(a)$. Например, $\{n \in \omega \mid n = 2k$ для некоторого $k \in \omega\}$ является множеством всех четных натуральных чисел.

Множество абстрактных букв называется *алфавитом*. Букву, являющуюся элементом алфавита A, будем называть *буквой алфавита A*.

Конечный ряд написанный друг за другом конкретных букв называется *конкретным словом*. В частности, каждая конкретная буква является конкретным словом. Если каждая из букв конкретного слова α является представителем некоторой буквы алфавита A, то будем говорить, что α является *словом в алфавите A*. Мы допускаем также случай, когда слово α не содержит ни одной конкретной буквы. Такое слово будем называть *пустым* и обозначать через Λ. Будем говорить, что два конкретных слова $a_1 \ldots a_n$ и $b_1 \ldots b_k$ алфавита A равны, и писать $a_1 \ldots a_n = b_1 \ldots b_k$, если $n = k$ и $a_1 = b_1, \ldots, a_n = b_n$. Все пустые слова считаем равными. Если $a_1 \ldots a_n$ — конкретное слово, состоящее из n букв $a_1, \ldots, a_n$ алфавита A, то число n называется *длиной* этого слова. Длиной пустого слова будет число 0.

---

*) Отметим, что при этом попарное различие элементов $a_1, \ldots, a_n$ не предполагается. В частности, $\{\varnothing\} = \{\varnothing, \varnothing, \varnothing\}$.

Применяя абстракцию отождествления, будем говорить о двух равных конкретных словах α_1, α_2 как об одном и том же (абстрактном) слове α. При этом эти два конкретных слова будем называть *представителями слова* α. Из определения равенства конкретных слов получаем, что абстрактное слово α можно определить как конечный ряд абстрактных букв такой, что каждый представитель слова α есть ряд представителей соответствующих абстрактных букв. Количество абстрактных букв в этом ряду будем называть *длиной абстрактного слова* α. Пустое абстрактное слово будем обозначать той же буквой Λ, что и конкретные пустые слова.

Для абстрактных слов α и β определяем абстрактное слово $\alpha\beta$ как такое абстрактное слово, все представители которого получаются приписыванием к некоторому представителю слова α некоторого представителя слова β. Абстрактное слово $\alpha\beta$ будем называть *соединением* абстрактных слов α, β; абстрактное слово α будем называть *началом* слова $\alpha\beta$. Аналогично определяется соединение $\alpha_1 \ldots \alpha_n$ абстрактных слов $\alpha_1, \ldots, \alpha_n$.

В дальнейшем под словом мы понимаем абстрактное слово. Очевидно, что для любых слов α, β имеем $\Lambda\alpha = \alpha\Lambda = \alpha$ и $\alpha\Lambda\beta = \alpha\beta$.

Слово β алфавита A называется *подсловом* слова α алфавита A, если $\alpha = \gamma\beta\delta$ для некоторых слов γ, δ. В частности, любое начало слова α будет подсловом α. Может оказаться, что $\alpha = \gamma\beta\delta = \gamma_1\beta\delta_1$ и $\gamma \neq \gamma_1$. В этом случае говорим о различных *вхождениях* подслова β в α. Таким образом, вхождением подслова β в слово α называется слово β вместе с местом его расположения в слове α. Вхождение подслова β в слово α можно изображать так: $\gamma * \beta * \delta$, где $*$ — символ, не принадлежащий алфавиту A. В частности, если $\alpha = \gamma\beta\delta = \gamma_1\beta\delta_1$ и $\gamma \neq \gamma_1$, то мы имеем два различных вхождения $\gamma * \beta * \delta$ и $\gamma_1 * \beta * \delta_1$ подслова β в слово α. Если для вхождения $\gamma_0 * \beta * \delta_0$ подслова β в α слово γ_0 (слово δ_0) имеет наименьшую длину среди всех слов γ (слов δ), для которых $\alpha = \gamma\beta\delta$, то $\gamma_0 * \beta * \delta_0$ называется *первым* (*последним*) *вхождением* β в α.

Вхождением буквы a в слово α называется вхождением в α слова, состоящего из одной буквы a. Если существует вхождение буквы a в слово α, то говорим, что *буква a входит в* α. Пусть $\gamma * \beta * \delta$ — вхождение слова β в α. Если $\alpha' = \gamma\beta'\delta$ для некоторого слова β', то будем говорить, что слово α' получается из α *заменой вхождения* $\gamma * \beta * \delta$ *подслова* β *на слово* β'.

Ряд $X_1, \ldots, X_n$ некоторых объектов X_i, $i \in \{1, \ldots, n\}$, будем называть *последовательностью* или *кортежем*, а число n — *длиной* этой последовательности. Объекты X_i, $i \in \{1, \ldots, n\}$, будут называться *членами* или *элементами* последовательности $X_1, \ldots, X_n$. Мы предполагаем, что по записи последовательности ее члены и их порядок восстанавливаются однозначно. Для этого нам необходимо разделять члены последовательности, например, с помощью запятой. Если $n = 0$, то ряд $X_1, \ldots, X_n$ будем считать пустой последовательностью и обозначать его тем же символом $\varnothing$, что и пустое множество. Иногда последовательность $X_1, \ldots, X_n$ будем обозначать через $\langle X_1, \ldots, X_n \rangle$. Если $X_1, \ldots, X_n$ — множества, то множество всех кортежей $\langle a_1, \ldots, a_n \rangle$, где $a_1 \in X_1, \ldots, a_n \in X_n$, будем обозначать через $X_1 \times \ldots \times X_n$. Если $X_1 = X_2 = \ldots = X_n$, то множество $X_1 \times X_2 \times \ldots \times X_n$ будем обозначать также через X_n^1. Последовательность из двух (трех и т. д.) членов будем называть *парой* (*тройкой* и т. д.). Последовательность из n элементов будем называть *n-кой.*

Отображением f множества X в множество Y называется соответствие, сопоставляющее каждому элементу $a \in X$ элемент $f(a) \in Y$, называемый *значением* отображения f на элементе a. Ясно, что отображение f множества X в множество Y однозначно определяется множеством $\{\langle a, f(a) \rangle \in X \times Y \mid a \in X\}$. Это множество (называемое иногда *графиком* f) мы будем отождествлять с отображением f. Если f — отображение X в Y, то пишем $f\colon X \to Y$. Если X — множество, то всякое отображение $f\colon X^n \to X$ будем называть *n-местной операцией* на X, а n — *местностью* операции f. Если $f\colon Y \to X$ и $Y \subseteq X^n$, то f будет называться *частичной n-местной операцией на* X с областью определения Y.

Пусть X — множество, $X_0 \subseteq X$ и $f_1, \ldots, f_k$ — операции на X, местности которых равны $n_1, \ldots, n_k$ соответственно. Определим множество $W \subseteq X$ следующим образом: $a \in W$ тогда и только тогда, когда существует последовательность $a_0, \ldots, a_m$ элементов множества X, обладающая следующим свойством: $a_m = a$ и для любого $i \leqslant m$ либо $a_i \in X_0$, либо $a_i = f_j\left(a_{i_1}, \ldots, a_{i_{n_j}}\right)$ для некоторого $j \in \{1, \ldots, k\}$ и некоторых $i_1, \ldots, i_{n_j} < i$. В этом случае будем говорить, что множество W *определено по индукции с помощью следующего определения*:

1) *если* $a \in X_0$, *то* $a \in W$;

2) *если* $i \in \{1, \ldots, k\}$ *и* $a_1, \ldots, a_{n_i} \in W$, *то* $f_i(a_1, \ldots, a_{n_i}) \in W$.

Будем говорить, что задано *исчисление* I, если заданы следующие четыре множества:

а) алфавит $A(I)$;

б) множество $E(I)$ слов алфавита $A(I)$, называемое *множеством выражений исчисления* I;

в) множество $\mathrm{Ax}(I)$ выражений исчисления I, называемое множеством *аксиом исчисления* I;

г) множество $\{f_1, \ldots, f_n\}$ частичных операций на множестве $E(I)$, называемых *правилами вывода исчисления* I.

Выражения рассматриваемых в этой книге исчислений будут называться *секвенциями* и *формулами*, а правила вывода $f\colon Y \to E(I)$ записываться так:

$$\frac{\Phi_0, \ldots, \Phi_n}{f(\Phi_0, \ldots, \Phi_n)}.$$

При этом указывается область определения f, если она не совпадает с $(E(I))^n$. Выражения $\Phi_0, \ldots, \Phi_n$ в предыдущей записи будут называться *посылками*, а выражение $f(\Phi_0, \ldots, \Phi_n)$ — *заключением правила* f. n-местное правило f исчисления I будем называть также *n-посылочным* правилом. Пару $\langle A(I), E(I)\rangle$, состоящую из алфавита $A(I)$ и множества выражений $E(I)$ исчисления I, будем называть *языком* исчисления I и обозначать через $L(I)$. Пусть даны два исчисления I_1 и I_2. Если $A(I_1) \subseteq A(I_2)$ и $E(I_1) \subseteq E(I_2)$, то будем говорить, что язык $L(I_2)$ исчисления I_2 является *расширением* языка $L(I_1)$ исчисления I_1, и обозначать это так: $L(I_2) \subseteq L(I_1)$ *).

Если дано исчисление I, то множество $T(I) \subseteq E(I)$ *доказуемых выражений* или *теорем исчисления* I определяется с помощью следующего индуктивного определения:

1) если S — аксиома I, то S — теорема I;

2) если $S_1, \ldots, S_n$ — теоремы I, f — n-посылочное правило исчисления I и кортеж $\langle S_1, \ldots, S_n\rangle$ принадлежит области определения f, то $f(S_1, \ldots, S_n)$ — теорема I.

---

*) Это обозначение не совсем согласуется с уже введенным обозначением включения для множеств, однако оно удобно и путаницы не вызывает.

Для того чтобы задать множество X, достаточно указать, для каких объектов a истинно отношение $a \in X$. Поэтому следующие выражения будут однозначно определять по двум множествам X и Y новые множества $X \cap Y$, $X \cup Y$ и $X \setminus Y$, называемые соответственно *пересечением*, *объединением* и *разностью* множеств X и Y:

а) $a \in X \cap Y \Leftrightarrow (a \in X$ и $a \in Y)$;

б) $a \in X \cup Y \Leftrightarrow (a \in X$ или $a \in Y)$;

в) $a \in X \setminus Y \Leftrightarrow (a \in X$ и $a \notin Y)$.

Предложение 1. *Операции пересечения и объединения удовлетворяют следующим равенствам для любых множеств X, Y и Z:*

$$\left.\begin{array}{ll} \text{1а.} & X \cap Y = Y \cap X, \\ \text{1б.} & X \cup Y = Y \cup X \end{array}\right\} \text{— \textit{коммутативность};}$$

$$\left.\begin{array}{ll} \text{2а.} & X \cap X = X, \\ \text{2б.} & X \cup X = X \end{array}\right\} \text{— \textit{идемпотентность};}$$

$$\left.\begin{array}{ll} \text{3а.} & (X \cap Y) \cap Z = X \cap (Y \cap Z), \\ \text{3б.} & (X \cup Y) \cup Z = X \cup (Y \cup Z) \end{array}\right\} \text{— \textit{ассоциативность};}$$

$$\left.\begin{array}{ll} \text{4а.} & X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z), \\ \text{4б.} & X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) \end{array}\right\} \text{— \textit{дистрибутивность}.}$$

Проверка этих равенств не представляет труда. Докажем, например, 4б. Пусть a принадлежит левой части равенства. Тогда $a \in X$ или $a \in Y \cap Z$, поэтому $a \in X \cup Y$ и $a \in X \cup Z$, т. е. a принадлежит правой части. Если $a \in X \cup Y$ и $a \in X \cup Z$, то $a \in X$ или $a \in Y \cap Z$. Следовательно, a принадлежит левой части равенства 4б. □

Если X — множество, то множество всех его подмножеств будем называть *множеством-степенью* X и обозначать через $P(X)$.

Пусть J — непустое множество и X_i для $i \in J$ — некоторые множества. *Объединением* $\bigcup\limits_{i \in J} X_i$ *и пересечением* $\bigcap\limits_{i \in J} X_i$ множеств X_i, $i \in J$, будем называть множества, определенные следующим образом:

$$a \in \bigcup_{i \in J} X_i \Leftrightarrow (a \in X_i \text{ для некоторого } i \in J),$$

$$a \in \bigcap_{i \in J} X_i \Leftrightarrow (a \in X_i \text{ для всех } i \in J).$$

Если $X_0, \ldots, X_n, Y$ — множества, то запись $X_0, \ldots, X_n \to Y$ будет обозначать, что $\bigcap_{i \leqslant n} X_i \subseteq Y$, а $X_0, \ldots, X_n \to$ будет обозначать, что $\bigcap_{i \leqslant n} X_i = \varnothing$. Если $\Phi_0, \ldots, \Phi_n, \Psi$ — какие-то утверждения, то запись

$$\frac{\Phi_0, \ldots, \Phi_n}{\Psi}$$

будет обозначать, что либо одно из утверждений $\Phi_0, \ldots, \Phi_n$ ложно, либо Ψ истинно.

Предложение 2. *Пусть $X_0, \ldots, X_n, Y_1, Y_2, Z$ — множества. Тогда*

1) $$\frac{X_0, \ldots, X_n \to Y_1;\ X_0, \ldots, X_n \to Y_2}{X_0, \ldots, X_n \to Y_1 \cap Y_2};$$

2) $$\frac{X_0, \ldots, X_n, Y_1 \to Z;\ X_0, \ldots, X_n, Y_2 \to Z;\ X_0, \ldots, X_n \to Y_1 \cup Y_2}{X_0, \ldots, X_n \to Z}.$$

Доказательство. Пусть $a \in \bigcap_{i \leqslant n} X_i$. Из истинности утверждений в 1) над чертой имеем $a \in Y_1$ и $a \in Y_2$, т. е. $a \in Y_1 \cap Y_2$. Теперь предположим, что утверждения в 2) над чертой истинны и $a \in \bigcap_{i \leqslant n} X_i$. Из истинности третьего утверждения над чертой следует, что $a \in Y_1 \cup Y_2$, т. е. $a \in Y_1$ или $a \in Y_2$. В обоих случаях из истинности первых двух утверждений над чертой получаем $a \in Z$. □

Упражнения

1. Сколько различных вхождений имеет пустое слово Λ в слово длины n?

2. Показать, что число различных подслов слова α длины n не превышает $\frac{n(n+1)}{2} + 1$.

3. Для каких слов α длины n число различных подслов α равно $\frac{n(n+1)}{2} + 1$?

4. Пусть множества $X_0, \ldots, X_{n+1}$ являются подмножествами некоторого множества Y. Обозначим через $\overline{X}_i$ множество $Y \setminus X_i$. Показать, что

а) $\overline{\bigcup_{i<n} X_i} = \bigcap_{i<n} \overline{X}_i$; б) $\overline{\bigcap_{i<n} X_i} = \bigcup_{i<n} \overline{X}_i$; в) $\dfrac{X_0, \ldots, X_n, \overline{X}_{n+1} \to}{X_0, \ldots, X_n \to X_{n+1}}$;

г) $\dfrac{X_0, \ldots, X_n \to X_{n+1}}{X_0, \ldots, X_n, \overline{X}_{n+1} \to}$; д) $X_0 \cap X_1 = X_0 \setminus (X_0 \setminus X_1)$.

§ 2. Язык исчисления высказываний

Высказыванием в русском языке мы называем повествовательное предложение, про которое можно утверждать, что оно истинно или ложно. Например, высказывание «вода — продукт горения водорода» истинно, а высказывание «все нечетные натуральные числа простые» ложно. Из высказываний A, B в русском языке мы можем образовывать более сложные высказывания такие, как «A и B», «A или B», «неверно, что A», «если A, то B». Если мы знаем, истинно или ложно каждое из высказываний A, B, то мы можем определить, истинны или ложны выписанные выше сложные высказывания. Например, если A истинно, а B ложно, то высказывание «если A, то B» ложно. Однако иногда мы можем утверждать об истинности сложного высказывания, не зная, истинны или ложны высказывания, из которых оно составлено. Например, каковы бы ни были высказывания A и B, высказывание «неверно, что A, или если B, то A» всегда истинно. В этом случае говорим, что схема «неверно, что A, или если B, то A» тождественно истинна. Одной из основных задач исчисления высказываний, к изучению которого мы приступаем, является описание тождественно истинных схем. Для этого придется заменить русский язык формальным языком, который не допускает двусмысленностей.

Алфавит исчисления высказываний, которое будем обозначать через ИВ, состоит из трех групп символов.

1. Пропозициональные переменные: $Q_0, Q_1, \ldots, Q_n, \ldots$, где n — натуральное число.

2. Логические символы или связки: импликация $\rightarrow$, конъюнкция $\wedge$, дизъюнкция $\vee$, отрицание $\neg$, символ следования $\vdash$.

3. Вспомогательные символы: левая скобка (, правая скобка), запятая ,.

Определение. *Формулой* ИВ назовем слово алфавита ИВ, удовлетворяющее следующему индуктивному определению.

1. Пропозициональная переменная является формулой (будем называть ее *элементарной* или *атомарной*).

2. Если Φ и Ψ — формулы, то $(\Phi\wedge\Psi)$, $(\Phi\vee\Psi)$, $(\Phi\rightarrow\Psi)$ и $\neg\Phi$ — формулы.

Из определения следует, что $(Q_0\wedge Q_1)\vee Q_0$ — не формула (нет внешних скобок). Однако в целях сокращения записи мы часто будем опускать внешние скобки. Таким образом, $(Q_0 \wedge Q_1) \vee Q_0$ будет сокращенной записью формулы $((Q_0 \wedge Q_1) \vee Q_0)$.

В дальнейшем формулы исчисления высказываний будут обозначаться буквами Φ, Ψ, X, а пропозициональные переменные — буквами P, R, причем Φ, Ψ, X, P, R могут иметь индексы.

Подформулой Ψ формулы Φ ИВ будем называть подслово Φ, являющееся формулой ИВ.

Докажем теперь утверждение об однозначности разложения формулы ИВ.

Предложение 1. *Всякая неатомарная формула* Φ *ИВ представима в одном и только одном из следующих видов*: $(\Psi \wedge X)$, $(\Psi \vee X)$, $(\Psi \to X)$, *или* $\neg\Psi$ *для однозначно определенных формул* Ψ *и* X.

Для доказательства предложения установим сначала один технический факт.

Лемма 1. *Если* Φ *и* Ψ — *формулы ИВ и* Φ — *начало* Ψ, *то* $\Phi = \Psi$.

Доказательство. Доказывать лемму будем индукцией по длине формулы Φ. Если Φ атомарна, то и Ψ должна быть атомарной, так как в противном случае Ψ начинается со скобки или с символа $\neg$ и тогда Φ не может быть началом Ψ. Следовательно, $\Phi = \Psi$.

Пусть Φ не атомарна и имеет вид $\neg\Phi'$, тогда Ψ должна иметь вид $\neg\Psi'$, причем, как нетрудно усмотреть из определения формулы, Φ' и Ψ' должны быть формулами. Кроме того, Φ' является, очевидно, началом Ψ'. Индукционное предположение дает $\Phi' = \Psi'$ и, следовательно, $\Phi = \neg\Phi' = \neg\Psi' = \Psi$.

Пусть Φ имеет вид $(\Phi_0 \tau \Phi_1)$, где Φ_0 и Φ_1 — формулы ИВ, τ — один из символов $\wedge$, $\vee$, $\to$. Тогда Ψ начинается со скобки (и поэтому может быть представлена в виде $(\Psi_0 \tau' \Psi_1)$, где Ψ_0 и Ψ_1 — формулы и τ' — один из символов $\wedge$, $\vee$, $\to$. Так как $(\Phi_0 \tau \Phi_1)$ есть начало $(\Psi_0 \tau' \Psi_1)$, то слово Φ_0 есть начало слова $\Psi_0 \tau' \Psi_1$, Ψ_0 — тоже начало этого слова. Из двух начал одного и того же слова одно из них есть начало другого (нужно взять начало меньшей длины). Следовательно, Φ_0 — начало Ψ_0 или Ψ_0 — начало Φ_0. В любом случае применимо индукционное предположение и, следовательно, $\Phi_0 = \Psi_0$, $\tau = \tau'$ и Φ_1 — начало Ψ_1. Снова, применив индукционное предположение, получаем, что $\Phi_1 = \Psi_1$ и $\Phi = (\Phi_0 \tau \Phi_1) = (\Psi_0 \tau' \Psi_1) = \Psi$. □

Доказательство предложения 1. Если формула Φ начинается с символа $\neg$, то доказывать нечего. Пусть Φ представлена в виде $(\Phi_0\tau\Phi_1)$, где τ — один из символов $\wedge$, $\vee$ или $\rightarrow$, а Φ_0, Φ_1 — формулы ИВ, и в виде $(\Phi_0'\tau'\Phi_1')$, где τ' — один из символов $\wedge$, $\vee$ или $\rightarrow$, а Φ_0', Φ_1' — формулы ИВ. Тогда Φ_0 — начало Φ_0' или Φ_0' — начало Φ_0. По лемме $\Phi_0 = \Phi_0'$, поэтому $\tau = \tau'$ и $\Phi_1 = \Phi_1'$. Следовательно, представление $\Phi = (\Phi_0\tau\Phi_1)$ единственно. □

Следствие 1. *Пусть Φ — формула ИВ. Тогда с каждым вхождением символа (или $\neg$ в формулу Φ однозначно связано некоторое вхождение подформулы формулы Φ, первым символом которого является рассматриваемое вхождение (или $\neg$ соответственно.*

Доказательство. Индукцией по построению формулы с каждым вхождением символа (или $\neg$ можно связать *некоторое* такое вхождение подформулы, а лемма 1 позволяет утверждать единственность такого вхождения. □

Предложение 2. *Если Φ — формула ИВ, η, θ — вхождения в Φ подформул Ψ, X соответственно, то либо η и θ не имеют общих вхождений символов алфавита ИВ, либо одно из них целиком содержится в другом.*

Доказательство. Если η и θ имеют общие вхождения символов, то первое вхождение первого символа η или θ должно быть общим. Пусть первое вхождение первого символа η входит в θ. Если Ψ — атомарная формула, то утверждение очевидно. Пусть Ψ не атомарна, тогда первый символ Ψ есть (или $\neg$. По следствию 1 этот символ однозначно определяет вхождение некоторой подформулы Ψ' в X. Но эта подформула будет подформулой и в Φ. В формуле Φ с рассматриваемым вхождением символа (или $\neg$ связано вхождение η подформулы Ψ. В силу единственности Ψ должна совпадать с Ψ' и η целиком содержится в θ. □

Если все вхождения подформулы Ψ в формулу Φ заменить на формулу X, то получим новую формулу, которую обозначим через $(\Phi)^{\Psi}_{X}$. Такое определение корректно, так как из предложения 2 следует, что два различных вхождения подформулы Ψ в Φ не имеют общих вхождений символов алфавита ИВ.

Определение. *Секвенциями* ИВ называются последовательности следующих четырех видов:

$$\Phi_0, \ldots, \Phi_n \vdash \Psi; \quad \Phi_0, \ldots, \Phi_n \vdash; \quad \vdash \Psi; \quad \vdash,$$

где $\Phi_0, \ldots, \Phi_n$, Ψ — формулы ИВ, n — натуральное число.

Часто секвенции будут обозначаться через $\Gamma \vdash \Psi$ или $\Gamma \vdash$, где Γ обозначает последовательность формул ИВ, может быть, пустую.

Если формулы ИВ можно рассматривать как «формы» сложных высказываний нашего языка, то секвенции являются «формами» утверждений, теорем, в которых можно отчетливо выделить условия (посылки) и заключение. А именно, рассматривая знак $\vdash$ как знак (логического) следования, секвенцию $\Phi_0, \ldots, \Phi_n \vdash \Psi$ можно понимать как утверждение вида «Из (истинности) посылок $\Phi_0, \ldots, \Phi_n$ (логически) следует высказывание Ψ». Секвенция вида $\Phi_0, \ldots, \Phi_n \vdash$ может пониматься как утверждение о совместной противоречивости посылок (условий) $\Phi_0, \ldots, \Phi_n$.

Правила вывода ИВ, которые будут описаны в следующем параграфе, отражают (формализуют) некоторые простейшие стандартные логические способы рассуждения, позволяющие переходить от одних истинных утверждений (теорем) к другим истинным утверждениям (теоремам).

Упражнения

1. Используя предложение 1, показать, что для любого слова α алфавита ИВ мы через конечное число шагов сможем определить, является ли α формулой ИВ или нет.

2. Заменим в определении формулы ИВ п. 2 на следующий: если Φ и Ψ — формулы, то $(\Phi) \wedge (\Psi)$, $(\Phi) \wedge (\Psi)$, $(\Phi) \to (\Psi)$ и $\neg(\Phi)$ — формулы. Показать, что при таком определении имеют место утверждения, аналогичные предложениям 1 и 2.

§ 3. Система аксиом и правил вывода

Ниже мы часто будем иметь дело не с конкретными формулами и секвенциями, а с так называемыми схемами формул и секвенций. Буквы Φ, Ψ, X (буквы Γ, Δ, Θ), возможно с индексами из множества натуральных чисел, будем называть *переменными для формул* (*последовательностей формул*). Пусть алфавит B содержит кроме символов алфавита ИВ переменные для формул и последовательностей формул.

Схемой секвенций (*формул*) ИВ мы будем называть такое слово в алфавите B, что при любых подстановках в это слово вместо переменных для формул и последовательностей формул соответственно конкретных формул и последовательностей конкретных формул получаются секвенции (формулы) ИВ. Результаты таких подстановок будут называться *частными случаями* этой схемы. Например, Ψ, $\Gamma \vdash \Phi \vee \Psi$ и $\Phi \rightarrow (\mathrm{X}_1 \wedge \mathrm{X}_2)$ будут схемами секвенций и формул соответственно, а

$$Q_0 \wedge \neg Q_1,\ \neg Q_0,\ \neg(Q_2 \rightarrow Q_1) \vdash Q_3 \vee (Q_0 \wedge \neg Q_1),$$
$$((Q_1 \rightarrow \neg Q_1) \wedge Q_0) \rightarrow (Q_3 \wedge \neg(Q_2 \vee \neg Q_0))$$

— частными случаями соответствующих схем *).

Определение. Схема секвенций

$$\Phi \vdash \Phi$$

называется *схемой аксиом* ИВ. Частный случай схемы аксиом будем называть *аксиомой*.

Правилами вывода ИВ являются следующие:

1. $\dfrac{\Gamma \vdash \Phi;\ \Gamma \vdash \Psi}{\Gamma \vdash \Phi \wedge \Psi}$;

2. $\dfrac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Phi}$;

3. $\dfrac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Psi}$;

4. $\dfrac{\Gamma \vdash \Phi}{\Gamma \vdash \Phi \vee \Psi}$;

5. $\dfrac{\Gamma \vdash \Psi}{\Gamma \vdash \Phi \vee \Psi}$;

6. $\dfrac{\Gamma, \Phi \vdash \Psi;\ \Gamma, \mathrm{X} \vdash \Psi;\ \Gamma \vdash \Phi \vee \mathrm{X}}{\Gamma \vdash \Psi}$,

7. $\dfrac{\Gamma, \Phi \vdash \Psi}{\Gamma \vdash \Phi \rightarrow \Psi}$;

8. $\dfrac{\Gamma \vdash \Phi;\ \Gamma \vdash \Phi \rightarrow \Psi}{\Gamma \vdash \Psi}$;

9. $\dfrac{\Gamma, \neg\Phi \vdash}{\Gamma \vdash \Phi}$;

10. $\dfrac{\Gamma \vdash \Phi;\ \Gamma \vdash \neg\Phi}{\Gamma \vdash}$,

11. $\dfrac{\Gamma, \Phi, \Psi, \Gamma_1 \vdash \mathrm{X}}{\Gamma, \Psi, \Phi, \Gamma_1 \vdash \mathrm{X}}$;

12. $\dfrac{\Gamma \vdash \Phi}{\Gamma, \Psi \vdash \Phi}$.

Как отмечалось в конце предыдущего параграфа, правила вывода ИВ формализуют определенные стандартные логические способы рассуждений. Прокомментируем на содержательном уровне, не очень строго, правила 1—12 с этой точки зрения. Правила 1—3 — это просто пра-

*) Когда значения переменных для формул и последовательностей формул в схеме C секвенций (формул) в тексте зафиксированы, схему C будем называть просто секвенцией (формулой).

вила, разъясняющие смысл союза «и» (конъюнкции). Правила 4, 5 так же относятся к пояснению смысла союза «или» (дизъюнкции). Правило 6 формализует способ рассуждения «разбором (двух) возможных случаев». Если при выполнении посылок Г справедливо Ф или Х, а Ψ справедливо при выполнении условий Г и Ф, а также и при выполнении условий Г и Х, то Ψ всегда справедливо при выполнении посылок Г, что устанавливается рассмотрением двух возможных случаев (один из которых обязательно выполняется): 1) выполнены условия Г и условие Ф, 2) выполнены условия Г и условие Х. Правило 7 формализует прием эквивалентной переформулировки теоремы, позволяющий одно из условий теоремы помещать в ее заключение в виде посылки. Правило 8 — это одно из логических правил (правило modus ponens или правило отделения), отмеченных еще Аристотелем; оно указывает, как можно освобождаться от посылки в заключении. Правило 9 формализует правило «рассуждения от противного». Предположим, что условия Г и $\neg$Ф могут одновременно выполняться; приходя к противоречию, заключаем, что из выполнимости условий Г всегда вытекает выполнимость Ф. Правило 10 — это правило «обнаружения (выведения) противоречия» для последовательности посылок Г. Правило 11 носит совершенно технический формальный характер: перестановка посылок не влияет на истинность заключения. Правило 12, называемое иногда «утончением» или правилом лишней посылки, отражает тривиальный факт, что, добавляя к условиям теоремы лишнее условие, мы не нарушаем истинности заключения теоремы.

Если в правилах вывода в качестве Г и Γ_1 берутся конкретные последовательности формул ИВ, а в качестве Ф, Ψ, Х — конкретные формулы, то получаются *частные случаи* (или *применения*) *правил вывода*. Правила 1—10 называются *основными*, а правила 11—12 — *структурными*. Если Θ — применение правила вывода k, то будем говорить, что секвенция, стоящая в Θ под чертой, получается из секвенций, стоящих над чертой, при помощи правила k.

Определение. *Линейным доказательством* в ИВ называется конечная последовательность $S_0, \ldots, S_n$ секвенций ИВ, которая удовлетворяет следующему условию: каждая секвенция S_i, $i \leqslant n$, либо является аксиомой, либо получается из некоторых S_j, $j<i$, при помощи одного из правил вывода 1—12. Секвенция S называется *доказуемой* в ИВ или *теоремой* ИВ, если существует доказательство $S_0, \ldots, S_n$ в ИВ, у которого $S_n = S$. Формула Φ ИВ называется *доказуемой* в ИВ, если в ИВ доказуема секвенция $\vdash \Phi$.

Заметим, что если $S_0, \ldots, S_n$ — доказательство в ИВ и $S'_0, \ldots, S'_k$ — доказательство в ИВ, то $S_0, \ldots, S_n$, $S'_0, \ldots, S'_k$ — тоже доказательство в ИВ.

Определим индуктивно понятие *дерева*:

1) Всякая секвенция является деревом.

2) Если $D_0, \ldots, D_n$ — деревья и S — секвенция, то

$$\frac{D_0, \ldots, D_n}{S}$$

— также дерево.

Одна и та же секвенция может входить в дерево несколько раз. Секвенцию вместе с ее местом расположения в дереве D будем называть *вхождением секвенции в дерево D*. Вхождение секвенции в дерево D, над которым нет горизонтальной черты, будем называть *начальным* в D. Вхождение секвенции в D, под которым нет горизонтальной черты, будем называть *заключительным* в D. Часто будет употребляться слово «секвенция» вместо «вхождение секвенции», если из контекста ясно, о каком вхождении идет речь. Ясно, что дерево может иметь много начальных секвенций, но заключительная секвенция только одна. Часть дерева, состоящую из секвенций, расположенных непосредственно над некоторой чертой, под той же чертой, и самой черты, называется *переходом*.

Определение. Дерево D назовем *доказательством* в ИВ *в виде дерева*, если все его начальные секвенции — аксиомы ИВ, а переходы — применения правил вывода 1—12. Если S является заключительной секвенцией доказательства D в ИВ в виде дерева, то D называется *доказательством S в виде дерева* или *деревом вывода S* в ИВ.

Пусть h — функция, определенная на секвенциях (точнее: на вхождениях секвенций) дерева D и принимающая в качестве значений натуральные числа, со следующими свойствами:

1) $h(S) = 0$, если S является заключительной секвенцией дерева D.

2) Если

$$\frac{S_0, \ldots, S_n}{S}$$

— переход в дереве D, то

$$h(S_0) = \ldots = h(S_n) = h(S) + 1.$$

Очевидно, что условия 1), 2) определяют функцию h однозначно. Число $h(S)$ назовем *высотой* (вхождения) *секвенции S в дереве D*. Максимальную высоту секвенций, входящих в D, назовем *высотой дерева D*.

Предложение 1. *Секвенция S имеет доказательство в ИВ в виде дерева тогда и только тогда, когда S — теорема ИВ.*

Доказательство. Пусть $S_0, \ldots, S_{n-1}$, S — линейное доказательство в ИВ. Если S — аксиома, то S будет доказательством секвенции S в виде дерева. Пусть $D_0, \ldots, D_{n-1}$ — доказательства секвенций $S_0, \ldots, S_{n-1}$ в виде дерева. Если $\frac{S_{i_1}; \ldots; S_{i_k}}{S}$, $i_1, \ldots, i_k < n$, — применение некоторого правила, то дерево

$$\frac{D_{i_1}; \ldots; D_{i_k}}{S}$$

будет доказательством секвенции S в виде дерева.

Пусть теперь дано доказательство секвенции S в виде дерева D. Построим линейное доказательство секвенции S. Построение будем вести индукцией по высоте секвенций в дереве D. Начальные секвенции в дереве D будут линейными доказательствами. Если для всех секвенций $S_0, \ldots, S_m$ высоты $k+1$ уже построены линейные доказательства $L_1, \ldots, L_m$, то очевидно, что последовательность

$$L_1, \ldots, L_m, S$$

будет линейным доказательством секвенции S высоты k. □

Схема секвенций H называется *доказуемой* в ИВ, если ее добавление к ИВ в качестве схемы аксиом не расширяет множество доказуемых секвенций. Ясно, что это эквивалентно тому, что все частные случаи схемы H доказуемы в ИВ.

Пример 1. Следующее дерево показывает доказуемость схемы $\Phi, \Psi \vdash \Phi \wedge \Psi$ *):

$$\dfrac{\dfrac{\Phi \vdash \Phi}{\Phi, \Psi \vdash \Phi}\text{ — правило 12} \qquad \dfrac{\dfrac{\Psi \vdash \Psi}{\Psi, \Phi \vdash \Psi}\text{ — правило 12}}{\Phi, \Psi \vdash \Psi}\text{ — правило 11}}{\Phi, \Psi \vdash \Phi \wedge \Psi}\text{ — правило 1}$$

Правило вывода называется *допустимым* в ИВ, если добавление его в исчисление ИВ не расширяет множество доказуемых секвенций. В частности, правила 1—12 ИВ допустимы.

Предложение 2. *Следующие правила являются допустимыми в ИВ*:

$$\left.\begin{array}{l} \text{а)}\ \dfrac{\Psi_1, \ldots, \Psi_n \vdash \Phi}{X_1, \ldots, X_m \vdash \Phi}, \\ \text{б)}\ \dfrac{\Psi_1, \ldots, \Psi_n \vdash}{X_1, \ldots, X_n \vdash}, \end{array}\right\} \text{ где } \{\Psi_1, \ldots, \Psi_n\} \subseteq \{X_1, \ldots, X_m\},$$

$$\text{в)}\ \dfrac{\Gamma \vdash \Psi;\ \Gamma, \Psi \vdash X}{\Gamma \vdash X}, \qquad \text{г)}\ \dfrac{\Gamma_1, \Phi, \Psi, \Gamma_2 \vdash X}{\Gamma_1, \Phi \wedge \Psi, \Gamma_2 \vdash X},$$

$$\text{д)}\ \dfrac{\Gamma \vdash \Phi \wedge \neg\Phi}{\Gamma \vdash}, \qquad \text{е)}\ \dfrac{\Gamma \vdash}{\Gamma \vdash \Psi},$$

$$\text{ж)}\ \dfrac{\Gamma, \Phi \vdash}{\Gamma \vdash \neg\Phi}, \qquad \text{з)}\ \dfrac{\Gamma \vdash \Phi}{\Gamma, \neg\Phi \vdash},$$

$$\text{и)}\ \dfrac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg\Psi \vdash \neg\Phi}, \qquad \text{к)}\ \dfrac{\Gamma, \neg\Phi \vdash \neg\Psi}{\Gamma, \Psi \vdash \Phi}.$$

Доказательство. Дерево

$$\dfrac{\dfrac{\Gamma, \Phi, \Phi \vdash \Psi}{\Gamma, \Phi \vdash \Phi \to \Psi} \quad \Gamma, \Phi \vdash \Phi}{\Gamma, \Phi \vdash \Psi}$$

показывает допустимость правила

$$\text{а}')\ \dfrac{\Gamma, \Phi, \Phi \vdash \Psi}{\Gamma, \Phi \vdash \Psi}.$$

Ясно, что допустимость правила а) следует из допустимости правила а′) с помощью правил 11, 12. Допустимость правила б) следует из правил а), д) и е). Покажем еще допустимость правил е) и ж), оставляя другие читателю в качестве упражнения.

*) Вместо слов «применение правила 12» и т. д. будем писать короче: «правило 12».— *Прим. ред.*

Ясно, что секвенцию $\Gamma \vdash$ можно получить лишь по правилу 10. Поэтому, если секвенция $\Gamma \vdash$ доказуема, то доказуемы секвенции $\Gamma \vdash \Phi_0$ и $\Gamma \vdash \neg\Phi_0$ для некоторой формулы Φ_0. Для доказательства допустимости правила вида

$$\frac{\Gamma \vdash}{S}$$

достаточно построить дерево, начальными секвенциями которого будут либо доказуемые схемы, либо $\Gamma \vdash \Phi_0$ и $\Gamma \vdash \neg\Phi_0$, заключительной — секвенция S, а переходами — правила 1—12.

$$\text{е)}\quad \dfrac{\dfrac{\dfrac{\dfrac{\Gamma \vdash \Phi_0}{\Gamma, \neg\Psi \vdash \Phi_0} \qquad \dfrac{\Gamma \vdash \neg\Phi_0}{\Gamma, \neg\Psi \vdash \neg\Phi_0}}{\Gamma, \neg\Psi \vdash}}{\Gamma \vdash \Psi}}{}.$$

ж) Воспользуемся доказуемостью схемы $\Gamma, \neg\Psi, \Psi \vdash$, установить которую предлагаем читателю в качестве упражнения.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, \Phi \vdash \Phi_0}{\Gamma, \Phi, \neg\neg\Phi \vdash \Phi_0}}{\Gamma, \neg\neg\Phi, \Phi \vdash \Phi_0}}{\Gamma, \neg\neg\Phi \vdash \Phi \to \Phi_0}; \quad \dfrac{\Gamma, \neg\neg\Phi, \neg\Phi \vdash}{\Gamma, \neg\neg\Phi \vdash \Phi}}{\Gamma, \neg\neg\Phi \vdash \Phi_0} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\Gamma, \Phi \vdash \neg\Phi_0}{\Gamma, \Phi, \neg\neg\Phi \vdash \neg\Phi_0}}{\Gamma, \neg\neg\Phi, \Phi \vdash \neg\Phi_0}}{\Gamma, \neg\neg\Phi \vdash \Phi \to \neg\Phi_0}; \quad \dfrac{\Gamma, \neg\neg\Phi, \neg\Phi \vdash}{\Gamma, \neg\neg\Phi \vdash \Phi}}{\Gamma, \neg\neg\Phi \vdash \neg\Phi_0}}{\Gamma, \neg\neg\Phi \vdash}}{\Gamma \vdash \neg\Phi}. \ \square$$

Конечная последовательность секвенций $S_0, \ldots, S_n$ называется *квазивыводом секвенции S_n в ИВ*, если каждая входящая в нее секвенция является доказуемой в ИВ или получается из предыдущих по допустимому в ИВ правилу вывода. Дерево D называется *квазивыводом секвенции S в ИВ в виде дерева*, если всякая начальная секвенция D доказуема в ИВ, заключительной секвенцией является S, а переходы представляют собой применения допустимых в ИВ правил вывода.

Очевидно, что всякая секвенция, для которой существует квазивывод или квазивывод в виде дерева, является доказуемой.

Пример 2. Докажем секвенцию $\vdash Q_0 \vee \neg Q_0$.

$$\begin{array}{c}
\neg Q_0 \vdash \neg Q_0 \\ \hline
\neg Q_0 \vdash Q_0 \vee \neg Q_0;\ \neg(Q_0 \vee \neg Q_0) \vdash \neg(Q_0 \vee \neg Q_0) \\ \hline
\neg(Q_0 \vee \neg Q_0),\ \neg Q_0 \vdash \\ \hline
\neg(Q_0 \vee \neg Q_0) \vdash Q_0 \\ \hline
\neg(Q_0 \vee \neg Q_0) \vdash Q_0 \vee \neg Q_0;\ \neg(Q_0 \vee \neg Q_0) \vdash \neg(Q_0 \vee \neg Q_0) \\ \hline
\neg(Q_0 \vee \neg Q_0) \vdash \\ \hline
\vdash Q_0 \vee \neg Q_0
\end{array}$$

Заметим, что приведенное выше дерево не является доказательством в ИВ, так как второй переход не является применением ни одного из правил. Однако ясно, что, дополнив это дерево применениями правил 11 и 12, можно получить доказательство. В дальнейшем без оговорок будем пользоваться допустимыми правилами, которые получаются из основных правил комбинацией со структурными правилами, например, таким:

$$\frac{\Phi_1, \ldots, \Phi_n, \Phi \vdash \Psi;\ \Psi_1, \ldots, \Psi_m, \mathrm{X} \vdash \Psi;\ \mathrm{X}_1, \ldots, \mathrm{X}_k \vdash \Phi \vee \mathrm{X}}{\Phi_{n+1}, \ldots, \Phi_{n+r} \vdash \Psi},$$

где $\{\Phi_1, \ldots, \Phi_n, \Psi_1, \ldots, \Psi_m, \mathrm{X}_1, \ldots, \mathrm{X}_k\} \subseteq \{\Phi_{n+1}, \ldots, \Phi_{n+r}\}$.

Упражнения

1. Установить доказуемость в ИВ следующих схем:
а) $\Gamma_1, \Phi, \Gamma_2 \vdash \Phi$; б) $\Gamma, \neg\Phi, \Phi \vdash$; в) $\Phi \wedge \Psi \vdash \Psi \wedge \Phi$;
г) $\Phi \vee \Psi \vdash \Psi \vee \Phi$.

2. Доказать допустимость в ИВ следующих правил:
л) $\dfrac{\Gamma, \neg\Phi \vdash \Psi}{\Gamma, \neg\Psi \vdash \Phi}$; м) $\dfrac{\Gamma, \Phi \vdash \neg\Psi}{\Gamma, \Psi \vdash \neg\Phi}$.

§ 4. Эквивалентность формул

Обозначим через F множество всех формул ИВ. Пусть s: $F \to F$ — отображение множества F в F, удовлетворяющее условиям:

1) $s(\Phi \to \Psi) = (s(\Phi) \to s(\Psi))$,

2) $s(\Phi \wedge \Psi) = (s(\Phi) \wedge s(\Psi))$,

3) $s(\Phi \vee \Psi) = (s(\Phi) \vee s(\Psi))$,

4) $s(\neg\Phi) = \neg s(\Phi)$.

Всякое такое отображение будем называть *подстановкой*. Предоставляем читателю возможность самостоятельно убедиться в том, что всякая подстановка однозначно определяется своими значениями на атомарных формулах, т. е. если $P_0, \ldots, P_n$ — все атомарные подформулы формулы Φ, а s_0 и s_1 — такие подстановки, что $s_0(P_i) = s_1(P_i)$ для $i \leqslant n$, то $s_0(\Phi) = s_1(\Phi)$. Для результата подстановки $s(\Phi)$ введем обозначение $s(\Phi) = (\Phi)^{P_0, \ldots, P_n}_{s(P_0), \ldots, s(P_n)}$, которое согласуется с обозначением $(\Phi)^{\Psi}_{X}$, введенным в § 2.

Распространим отображение s на секвенции:

5) $s(\Phi_1, \ldots, \Phi_n \vdash \Psi) = s(\Phi_1), \ldots, s(\Phi_n) \vdash s(\Psi)$; $s(\Phi_1, \ldots, \Phi_n \vdash) = s(\Phi_1), \ldots, s(\Phi_n) \vdash$; $s(\vdash \Phi) = \vdash s(\Phi)$; $s(\vdash) = \vdash$.

По индукции можно определить продолжение s на деревья:

6) $s\left(\dfrac{D_1; \ldots; D_k}{S}\right) = \dfrac{s(D_1); \ldots; s(D_k)}{s(S)}$.

Теорема 1 (о подстановке). *Пусть отображение $s\colon F \to F$ удовлетворяет условиям* 1)—6) *и S — доказуемая в ИВ секвенция. Тогда секвенция $s(S)$ доказуема в ИВ.*

Доказательство. Индукцией по высоте дерева будем доказывать, что если D — доказательство секвенции S в ИВ в виде дерева, то $s(D)$ — доказательство секвенции $s(S)$ в ИВ. Если S — аксиома, то $s(S)$ также будет аксиомой. Пусть

$$D = \cfrac{\dfrac{D^0_0; \ldots; D^0_{i_0}}{S_0} \quad \cdots \quad \dfrac{D^k_0; \ldots; D^k_{i_k}}{S_k}}{S},$$

тогда

$$s(D) = \cfrac{\dfrac{s\left(D^0_0\right); \ldots; s\left(D^0_{i_0}\right)}{s\left(S_0\right)} \quad \cdots \quad \dfrac{s\left(D^k_0\right); \ldots; s\left(D^k_{i_k}\right)}{s\left(S_k\right)}}{s(S)}.$$

В силу индукционного предположения достаточно доказать, что в дереве $s(D)$ последний переход является применением того же правила, что и в последнем переходе дерева D. Но это очевидно, так как свойства 1)—5) гарантируют сохранение переходов. Например, если

$$\frac{\Phi_0,\ \Phi\vdash\Psi;\ \Phi_0,\ X\vdash\Psi;\ \Phi_0\vdash\Phi\vee X}{\Phi_0\vdash\Psi}$$

— последний переход в дереве D, то

$$\frac{s(\Phi_0),\ s(\Phi)\vdash s(\Psi);\ s(\Phi_0),\ s(X)\vdash s(\Psi);\ s(\Phi_0)\vdash s(\Phi)\vee s(X)}{s(\Phi_0)\vdash s(\Psi)}$$

— применение правила 4 и последний переход в дереве $s(D)$. □

Теорема о подстановке, иными словами, утверждает, что если в доказуемой секвенции вместо пропозициональных переменных подставить произвольные формулы, то полученная секвенция будет доказуемой.

Определение. Две формулы Φ и Ψ назовем *эквивалентными* (обозначаем $\Phi\equiv\Psi$), если в ИВ доказуемы две секвенции $\Phi\vdash\Psi$ и $\Psi\vdash\Phi$.

Отметим, что символ $\equiv$ не является символом языка исчисления высказываний. Он является символом языка, на котором мы доказываем утверждения об исчислении. Иногда этот язык называют *метаязыком*. Понятия схемы и доказательства также являются понятиями метаязыка.

Лемма 1. *Отношение $\Phi\equiv\Psi$ является отношением эквивалентности, т. е. для любых формул Φ, Ψ, X ИВ справедливы следующие утверждения:*

а) $\Phi\equiv\Phi$;

б) *если* $\Phi\equiv\Psi$, *то* $\Psi\equiv\Phi$;

в) *если* $\Phi\equiv\Psi$ *и* $\Psi\equiv X$, *то* $\Phi\equiv X$.

Доказательство. а) следует из того, что $\Phi\vdash\Phi$ — аксиома. б) следует из симметричности Φ и Ψ в определении отношения $\Phi\equiv\Psi$. Если $\Phi\vdash\Psi$ и $\Psi\vdash X$ доказуемы, то по предложению 3.2 в) $\Phi\vdash X$ доказуема. Аналогично, если $X\vdash\Psi$, $\Psi\vdash\Phi$ доказуемы, то $X\vdash\Phi$ доказуема. □

Лемма 2. а) *Если $\Phi\equiv\Psi$, то Φ доказуема в ИВ тогда и только тогда, когда в ИВ доказуема Ψ.*

б) *Если* $\Phi_1\equiv\Psi_1$ *и* $\Phi_2\equiv\Psi_2$, *то* $(\Phi_1\wedge\Phi_2)\equiv(\Psi_1\wedge\Psi_2)$, $(\Phi_1\vee\Phi_2)\equiv(\Psi_1\vee\Psi_2)$, $(\Phi_1\to\Phi_2)\equiv(\Psi_1\to\Psi_2)$ *и* $\neg\Phi_1\equiv\neg\Psi_1$.

Доказательство. Если доказуемы $\vdash\Phi$ и $\Phi\vdash\Psi$, то дерево

$$\frac{\dfrac{\Phi\vdash\Psi}{\vdash\Phi\to\Psi};\ \vdash\Phi}{\vdash\Psi}$$

будет квазивыводом $\vdash\Psi$. Аналогично из доказуемости $\vdash\Psi$ и $\Psi\vdash\Phi$ получаем доказуемость $\vdash\Phi$. Утверждение а) доказано.

В силу симметричности Φ_i и Ψ_i в б) достаточно доказать секвенции $\neg\Phi_1\vdash\neg\Psi_1$, $\Phi_1\wedge\Phi_2\vdash\Psi_1\wedge\Psi_2$, $\Phi_1\vee\Phi_2\vdash\Psi_1\vee\Psi_2$ и $\Phi_1\to\Phi_2\vdash\Psi_1\to\Psi_2$. Следующие 4 квазивывода завершают доказательство леммы 2:

1) $$\dfrac{\Psi_1\vdash\Phi_1;\ \neg\Phi_1\vdash\neg\Phi_1}{\dfrac{\Psi_1,\ \neg\Phi_1\vdash}{\neg\Phi_1\vdash\neg\Psi_1}};$$

2) $$\dfrac{\dfrac{\Phi_1\wedge\Phi_2\vdash\Phi_1;\ \Phi_1\vdash\Psi_1}{\Phi_1\wedge\Phi_2\vdash\Psi_1}\qquad\dfrac{\Phi_1\wedge\Phi_2\vdash\Phi_2;\ \Phi_2\vdash\Psi_2}{\Phi_1\wedge\Phi_2\vdash\Psi_2}}{\Phi_1\wedge\Phi_2\vdash\Psi_1\wedge\Psi_2};$$

3) $$\dfrac{\dfrac{\Phi_1\vdash\Psi_1}{\Phi_1\vdash\Psi_1\vee\Psi_2}\qquad\dfrac{\Phi_2\vdash\Psi_2}{\Phi_2\vdash\Psi_1\vee\Psi_2}\qquad\Phi_1\vee\Phi_2\vdash\Phi_1\vee\Phi_2}{\Phi_1\vee\Phi_2\vdash\Psi_1\vee\Psi_2};$$

4) $$\dfrac{\dfrac{\Psi_1\vdash\Phi_1;\ \Phi_1\to\Phi_2\vdash\Phi_1\to\Phi_2}{\Phi_1\to\Phi_2,\ \Psi_1\vdash\Phi_2}\qquad\dfrac{\Phi_2\vdash\Psi_2}{\vdash\Phi_2\to\Psi_2}}{\dfrac{\Phi_1\to\Phi_2,\ \Psi_1\vdash\Psi_2}{\Phi_1\to\Phi_2\vdash\Psi_1\to\Psi_2}}.\ \square$$

Теорема 2 (о замене). *Пусть Φ — формула ИВ, Ψ — ее подформула. Пусть Φ' получается из Φ путем замены некоторого вхождения Ψ на формулу Ψ'. Тогда если $\Psi\equiv\Psi'$, то $\Phi\equiv\Phi'$.*

Доказательство. Если $\Psi=\Phi$, то теорема тривиальна. Далее индукцией по длине формулы Φ. Если $\Phi=Q_i$, то $\Psi=\Phi$.

Индукционный шаг распадается на 4 случая:

а) $\Phi=\Phi_1\wedge\Phi_2$; б) $\Phi=\Phi_1\vee\Phi_2$;

в) $\Phi=\Phi_1\to\Phi_2$; г) $\Phi=\neg\Phi_1$.

По предложению 2.2 любое вхождение $\Psi\neq\Phi$ содержится либо в Φ_1, либо в Φ_2, поэтому эквивалентность $\Phi\equiv\Phi'$ следует из индукционного предположения и леммы 2 б). $\square$

Упражнения

1. Пусть формулы Φ и Ψ ИВ содержат лишь одну пропозициональную переменную P, и для некоторых подстановок s_1, s_2 имеем $s_1(\Phi)=\Psi$ и $s_2(\Psi)=\Phi$. Показать, что $\Phi\equiv\Psi$.

2. Пусть $\Phi \equiv \Psi$ и существует пропозициональная переменная P, входящая как в Φ, так и в Ψ. Показать, что существует формула X, эквивалентная формулам Φ и Ψ, все пропозициональные переменные которой содержатся как в Φ, так и в Ψ. (Указание. Воспользоваться теоремой 1.)

§ 5. Нормальные формы

Понятие эквивалентности формул ИВ будет иметь для нас большое значение, так как основные изучаемые нами свойства формул ИВ сохраняются при переходе к эквивалентным формулам. Поэтому очень важно уметь находить для каждой формулы ИВ эквивалентную ей формулу, но устроенную по возможности более просто. В этом параграфе будут определены такие «канонические» представители для формул ИВ.

Лемма 1. *Пусть Φ и Ψ — формулы ИВ. Тогда имеют место следующие эквивалентности:*

а) $(\Phi \to \Psi) \equiv (\neg\Phi \vee \Psi)$;

б) $\neg\neg\Phi \equiv \Phi$;

в) $\neg(\Phi \wedge \Psi) \equiv (\neg\Phi \vee \neg\Psi)$;

г) $\neg(\Phi \vee \Psi) \equiv (\neg\Phi \wedge \neg\Psi)$;

д) $\Phi \equiv (\Phi \vee \Phi)$;

е) $\Phi \equiv (\Phi \wedge \Phi)$.

Доказательство. Приведем квазивыводы для утверждения а):

$$\dfrac{\dfrac{\dfrac{\Phi \vdash \Phi;\ \Phi \to \Psi \vdash \Phi \to \Psi}{\Phi \to \Psi,\ \Phi \vdash \Psi}}{\Phi \to \Psi,\ \Phi \vdash \neg\Phi \vee \Psi;} \quad \dfrac{\neg\Phi \vdash \neg\Phi}{\neg\Phi \vdash \neg\Phi \vee \Psi;} \quad \vdash \Phi \vee \neg\Phi}{\Phi \to \Psi \vdash \neg\Phi \vee \Psi};$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\Phi \vdash \Phi;\ \neg\Phi \vdash \neg\Phi}{\Phi,\ \neg\Phi \vdash}}{\Phi,\ \neg\Phi \vdash \Psi;} \quad \Psi \vdash \Psi; \quad \neg\Phi \vee \Psi \vdash \neg\Phi \vee \Psi}{\neg\Phi \vee \Psi,\ \Phi \vdash \Psi}}{\neg\Phi \vee \Psi \vdash \Phi \to \Psi}.$$

Заметим, что доказуемость $\vdash \Phi \vee \neg\Phi$ следует из примера 3.2 и теоремы о подстановке.

Доказательство остальных утверждений леммы 1 предоставляется читателю. □

Лемма 2. *Любая формула* Φ *исчисления высказываний эквивалентна формуле* Ψ, *которая не содержит символа импликации.*

Доказательство. Определим отображение α: $F \to F$ индукцией по построению формулы:

1) $\alpha(Q_i) = Q_i$,
2) $\alpha(\Phi \wedge \Psi) = \alpha(\Phi) \wedge \alpha(\Psi)$,
3) $\alpha(\Phi \vee \Psi) = \alpha(\Phi) \vee \alpha(\Psi)$,
4) $\alpha(\neg\Phi) = \neg\alpha(\Phi)$,
5) $\alpha(\Phi \to \Psi) = \neg\alpha(\Phi) \vee \alpha(\Psi)$.

Тогда $\alpha(\Phi)$ не содержит символа импликации и $\alpha(\Phi) \equiv \Phi$ следует по индукции из леммы 4.2 б) и леммы 1 а). □

Лемма 3. *Любая формула* Φ *ИВ эквивалентна формуле* Ψ *без символа импликации, у которой символы отрицания стоят только перед атомарными подформулами.*

Доказательство. Пусть $F^{\to}$ — множество формул, не содержащих символа импликации. Определим отображение β: $F^{\to} \to F^{\to}$ по индукции:

1) $\beta(Q_i) = Q_i$,
2) $\beta(\neg Q_i) = \neg Q_i$,
3) $\beta(\Phi \wedge \Psi) = \beta(\Phi) \wedge \beta(\Psi)$,
4) $\beta(\Phi \vee \Psi) = \beta(\Phi) \vee \beta(\Psi)$,
5) $\beta(\neg(\Phi \wedge \Psi)) = \beta(\neg\Phi) \vee \beta(\neg\Psi)$,
6) $\beta(\neg(\Phi \vee \Psi)) = \beta(\neg\Phi) \wedge \beta(\neg\Psi)$,
7) $\beta(\neg\neg\Phi) = \beta(\Phi)$.

Пусть $X = \alpha(\Phi)$, где α — отображение из леммы 2. Эквивалентность $X \equiv \beta(X)$ легко получить индукцией по длине X, используя лемму 1 и лемму 4.2 б). Очевидно, что $\Psi = \beta(X)$ удовлетворяет требованиям леммы 3. □

Лемма 4. *Пусть* Φ, Ψ *и* X — *формулы ИВ. Тогда*

а) $(\Phi \wedge \Psi) \equiv (\Psi \wedge \Phi)$;

а′) $(\Phi \vee \Psi) \equiv (\Psi \vee \Phi)$;

б) $((\Phi \wedge \Psi) \wedge X) \equiv (\Phi \wedge (\Psi \wedge X))$;

б′) $((\Phi \vee \Psi) \vee X) \equiv (\Phi \vee (\Psi \vee X))$;

в) $(\Phi \wedge (\Psi \vee X)) \equiv ((\Phi \wedge \Psi) \vee (\Phi \wedge X))$;

в′) $(\Phi \vee (\Psi \wedge X)) \equiv ((\Phi \vee \Psi) \wedge (\Phi \vee X))$.

Доказательство. Чтобы не загромождать изложение, докажем лишь в). Остальные эквивалентности читатель легко докажет сам, используя навык, приобретенный при разборе ранее приведенных доказательств.

$$\dfrac{\dfrac{\dfrac{\Phi\wedge(\Psi\vee X)\vdash\Phi;\ \Psi\vdash\Psi}{\Phi\wedge(\Psi\vee X),\Psi\vdash\Phi\wedge\Psi}}{\Phi\wedge(\Psi\vee X),\Psi\vdash(\Phi\wedge\Psi)\vee(\Phi\wedge X)};\ \dfrac{\dfrac{\Phi\wedge(\Psi\vee X)\vdash\Phi;\ X\vdash X}{\Phi\wedge(\Psi\vee X),X\vdash\Phi\wedge X}}{\Phi\wedge(\Psi\vee X),X\vdash(\Phi\wedge\Psi)\vee(\Phi\wedge X)};\ \Phi\wedge(\Psi\vee X)\vdash\Psi\vee X}{\Phi\wedge(\Psi\vee X)\vdash(\Phi\wedge\Psi)\vee(\Phi\wedge X)};$$

$$\dfrac{\dfrac{\dfrac{\Phi\wedge\Psi\vdash\Psi}{\Phi\wedge\Psi\vdash\Psi\vee X};\ \Phi\wedge\Psi\vdash\Phi}{\Phi\wedge\Psi\vdash\Phi\wedge(\Psi\vee X)};\ \dfrac{\Phi\wedge X\vdash\Phi;\ \dfrac{\Phi\wedge X\vdash X}{\Phi\wedge X\vdash\Psi\vee X}}{\Phi\wedge X\vdash\Phi\wedge(\Psi\vee X)};\ (\Phi\wedge\Psi)\vee(\Phi\wedge X)\vdash(\Phi\wedge\Psi)\vee(\Phi\wedge X)}{(\Phi\wedge\Psi)\vee(\Phi\wedge X)\vdash\Phi\wedge(\Psi\vee X)}\ \square$$

Определим теперь важные понятия *дизъюнктивного* и *конъюнктивного* члена формулы. Для любой формулы Φ через $D(\Phi)$ будем обозначать множество всех дизъюнктивных членов формулы Φ, а через $K(\Phi)$ — множество всех ее конъюктивных членов, которые определим индукцией по длине Φ.

а) Если формула Φ не представима в виде дизъюнкции, т. е. в виде $\Phi=(\Phi_0\vee\Phi_1)$, то $D(\Phi)=\{\Phi\}$, т. е. Φ является своим единственным дизъюнктивным членом.

б) Если $\Phi=(\Phi_0\vee\Phi_1)$, то $D(\Phi)=D(\Phi_0)\cup D(\Phi_1)$.

Множество $K(\Phi)$ определяется двойственно. а) Если формула Φ не имеет вида $\Phi_0\wedge\Phi_1$, то $K(\Phi)=\{\Phi\}$; б) если $\Phi=(\Phi_0\wedge\Phi_1)$, то $K(\Phi)=K(\Phi_0)\cup K(\Phi_1)$.

Предложение 1. *Пусть Φ и Ψ — формулы ИВ. Если $D(\Phi)\subseteq D(\Psi)$, то секвенция $\Phi\vdash\Psi$ доказуема в ИВ.*

Доказательство. Установим, что из $\Phi\in D(\Psi)$ следует доказуемость секвенции $\Phi\vdash\Psi$. Докажем это индукцией по длине формулы Ψ при фиксированной формуле Φ. Если Ψ' имеет минимальную длину, то $\Psi=\Phi$ и доказывать нечего. В случае, когда Ψ не представима в виде дизъюнкции, то также имеем $\Psi=\Phi$. Пусть $\Psi=\Psi'\vee\Psi''$. Тогда $\Phi\in D(\Psi')$ или $\Phi\in D(\Psi'')$. Если, скажем, $\Phi\in D(\Psi')$, то

$$\frac{\Phi\vdash\Psi'}{\Phi\vdash\Psi'\vee\Psi''}$$

— квазивывод секвенции $\Phi\vdash\Psi$.

Установим теперь предложение индукцией по длине Φ при фиксированном Ψ. Если $D(\Phi)=\{\Phi\}$, то $\Phi\in\in D(\Psi)$ и выше уже установлена доказуемость $\Phi\vdash\Psi$. Если $\Phi=\Phi'\vee\Phi''$, то $D(\Phi')\cup D(\Phi'')=D(\Phi)\subseteq D(\Psi)$ и по индукционному предложению секвенции $\Phi'\vdash\Psi$ и $\Phi''\vdash\Psi$ доказуемы. Тогда

$$\frac{\Phi\vdash\Phi'\vee\Phi'';\ \Phi'\vdash\Psi;\ \Phi''\vdash\Psi}{\Phi\vdash\Psi}$$

— квазивывод нужной секвенции. □

Следствие 1. *Если* $D(\Phi)=D(\Psi)$, *то* $\Phi\equiv\Psi$. □

Полученное следствие показывает, что с точностью до эквивалентности формул можно пользоваться обозначением $\bigvee\limits_{i=1}^{n}\Phi^{i}$ или $\Phi_1\vee\ldots\vee\Phi_n$ для формул Φ таких, что $D(\Phi)=\{\Phi_1, \ldots, \Phi_n\}$.

Для конъюнктивных членов ситуация вполне аналогичная. Оставляем читателю доказательство следующего предложения.

Предложение 2. *Пусть* Φ *и* Ψ *— формулы ИВ. Если* $K(\Psi)\subseteq K(\Phi)$, *то доказуема секвенция* $\Phi\vdash\Psi$. □

Следствие 2. *Если* $K(\Phi)=K(\Psi)$, *то* $\Phi\equiv\Psi$. □

Это позволяет использовать обобщенную запись вида $\bigwedge\limits_{i=1}^{n}\Phi_i$ или $\Phi_1\wedge\ldots\wedge\Phi_n$ для всех формул Φ таких, что $K(\Phi)=\{\Phi_1, \ldots, \Phi_n\}$.

Лемма 5. *Для любой конечной последовательности* Γ *и любой формулы* Φ *секвенция* $\Gamma\vdash\Phi$ *доказуема тогда и только тогда, когда доказуемы секвенции* $\Gamma\vdash\Phi'$ *для всех* $\Phi'\in K(\Phi)$.

Доказательство. В одну сторону лемма вытекает из предложения 2. Пусть для любого $\Phi'\in K(\Phi)$ секвенция $\Gamma\vdash\Phi'$ доказуема. Индукцией по длине Φ покажем, что $\Gamma\vdash\Phi$ доказуема. Если Φ не представима в виде $\Phi_0\wedge\Phi_1$, то доказывать нечего. Если $\Phi=\Phi_0\wedge\Phi_1$, то по индукционному предположению $\Gamma\vdash\Phi_0$ и $\Gamma\vdash\Phi_1$ доказуемы (так как $K(\Phi_i)\subseteq K(\Phi)$). Следовательно,

$$\frac{\Gamma\vdash\Phi_0;\ \Gamma\vdash\Phi_1}{\Gamma\vdash\Phi_0\wedge\Phi_1}$$

есть квазивывод секвенции $\Gamma\vdash\Phi$. □

Определение. Будем говорить, что формула Φ есть *элементарная дизъюнкция*, если каждый дизъюнктивный член Φ есть либо атомарная формула, либо отрицание атомарной формулы. Будем говорить, что формула Φ находится в *конъюнктивной нормальной форме* (*к. н. ф.*), если каждый конъюнктивный член Φ является элементарной дизъюнкцией. Формулу Φ, находящуюся в конъюнктивной нормальной форме, с точностью до эквивалентности можно записать в виде $\bigwedge\limits_{i=0}^{n}(\Phi_0^i\vee\ldots\vee\Phi_{m_i}^i)$, где Φ_j^i — атомарные формулы или отрицания атомарных формул, а $\Phi_0^i\vee\ldots\vee\Phi_{m_i}^i$ — обобщенные обозначения для конъюнктивных членов Φ.

Двойственным образом (т. е. заменой $\wedge$ на $\vee$ и $\vee$ на $\wedge$) определяются понятия *элементарной конъюнкции* и *дизъюнктивной нормальной формы* (*д. н. ф.*).

Теорема 3. *Для любой формулы Φ ИВ существует эквивалентная ей формула Ψ, находящаяся в к. н. ф.*

Доказательство. Пусть Ψ_1 — формула, эквивалентная Φ, не содержащая символа импликации и все символы отрицания которой стоят перед атомарными подформулами. Будем доказывать теорему индукцией по длине Ψ_1. Если Ψ_1 — атомарная формула или ее отрицание, то Ψ_1 уже находится в к. н. ф. Если $\Psi_1 = \Phi_1\wedge\Phi_2$ и X_1, X_2 — формулы, эквивалентные Φ_1, соответственно Φ_2, находящиеся в к. н. ф., то очевидно, что формула $X_1\wedge X_2$ эквивалентна Ψ_1 и находится в к. н. ф.

Пусть $\Psi_1=\Phi_1\vee\Phi_2$. Пусть X_1 и X_2 уже находятся в к. н. ф., $X_1\equiv\Phi_1$ и $X_2\equiv\Phi_2$. По теореме о замене $\Psi_1\equiv X_1\vee X_2$. Доказательство того, что $X_1\vee X_2$ эквивалентна некоторой Ψ, находящейся в к. н. ф., будем вести индукцией по $n=m_1+m_2$, где m_i — число символов $\wedge$ в X_i, $i=1, 2$. Если $m_1=m_2=0$, то $X_1\vee X_2$, будучи элементарной дизъюнкцией, находится в к. н. ф. Пусть, например, m_2 не равно нулю. Тогда $X_2 = X_3\wedge X_4$. По лемме 4 в′) получаем

$$X_1\vee X_2 = X_1\vee(X_3\wedge X_4)\equiv(X_1\vee X_3)\wedge(X_1\vee X_4).$$

По индукционному предположению $X_1\vee X_3$ и $X_1\vee X_4$ эквивалентны Ψ_2 и соответственно Ψ_3, которые находятся в к. н. ф. Ясно, что $\Psi=\Psi_2\wedge\Psi_3$ удовлетворяет требованиям теоремы. □

Доказательство следующей теоремы аналогично доказательству теоремы 3 и оставляется читателю.

Теорема 4. *Для любой формулы Φ ИВ существует эквивалентная ей формула Ψ, находящаяся в д. н. ф.* □

Определение. Будем говорить, что формула Φ ИВ находится в *совершенной к. н. ф.* (*д. н. ф.*), если выполнены следующие условия:

1) Φ находится в к. н. ф. (д. н. ф.);

2) любая пропозициональная переменная P, входящая в формулу Φ, имеет в любом конъюнктивном (дизъюнктивном) члене Φ ровно одно вхождение;

3) любые два различных вхождения конъюнктивных (дизъюнктивных) членов Φ имеют различные множества дизъюнктивных (конъюнктивных) членов.

Например, из формул

$$(Q_1 \vee Q_3) \vee \neg Q_0, \quad (Q_2 \wedge Q_4) \vee (Q_4 \wedge Q_2),$$
$$(Q_1 \wedge \neg Q_2) \vee (Q_2 \wedge \neg Q_1),$$

находящихся в д. н. ф., первая находится в совершенной к. н. ф., а третья — в совершенной д. н. ф.; первая и вторая формулы не находятся в совершенной д. н. ф. (Почему?)

Теорема 5. *Если формула Φ ИВ не доказуема в ИВ, то существует эквивалентная ей формула Ψ, находящаяся в совершенной к. н. ф.*

Докажем сначала три вспомогательных утверждения.

Лемма 6. *Если для некоторой формулы Φ ИВ существует формула Ψ такая, что* $\Psi, \neg\Psi \in D(\Phi)$, *то Φ доказуема.*

Доказательство. Действительно, формула $\Psi \vee \vee \neg\Psi$ доказуема и $D(\Psi \vee \neg\Psi) \subseteq D(\Phi)$. По предложению 1 $\Psi \vee \neg\Psi \vdash \Phi$ — доказуемая секвенция, но тогда и Φ — доказуемая формула. □

Лемма 7. *Если Φ — доказуемая в ИВ формула, то* $\Phi \wedge \Psi \equiv \Psi$ *для любой формулы Ψ ИВ.*

Доказательство. Следующие деревья являются квазивыводами нужных секвенций:

$$\frac{\Phi \wedge \Psi \vdash \Phi \wedge \Psi}{\Phi \wedge \Psi \vdash \Psi}, \quad \frac{\vdash \Phi; \ \Psi \vdash \Psi}{\Psi \vdash \Phi \wedge \Psi}. \quad \square$$

Лемма 8. *Для любых формул Φ и Ψ ИВ имеет место эквивалентность* $\Phi \equiv \Phi \vee (\Psi \wedge \neg\Psi)$.

Доказательство. Следующие квазивыводы устанавливают доказуемость нужных секвенций:

$$\frac{\Phi \vdash \Phi}{\Phi \vdash \Phi \vee (\Psi \wedge \neg\Psi)},$$

$$\frac{\Phi \vdash \Phi;\ \dfrac{\dfrac{\Psi \wedge \neg\Psi \vdash \Psi;\ \Psi \wedge \neg\Psi \vdash \neg\Psi}{\Psi \wedge \neg\Psi \vdash}}{\Psi \wedge \neg\Psi \vdash \Phi};\ \Phi \vee (\Psi \wedge \neg\Psi) \vdash \Phi \vee (\Psi \wedge \neg\Psi)}{\Phi \vee (\Psi \wedge \neg\Psi) \vdash \Phi}. \quad \square$$

Доказательство теоремы 5. Пусть X — формула, эквивалентная Φ и находящаяся в к. н. ф. Такая формула существует по теореме 3. Пусть $X_0, \ldots, X_k$ — все конъюнктивные члены X, для которых нет пропозициональных переменных P таких, что $P, \neg P \in D(X_i)$. Такие члены существуют, так как в противном случае по лемме 6 и лемме 5 формула X, а следовательно, и Φ была бы доказуема.

Пусть $D(X_i) = \{X_i^0, \ldots, X_i^{k_i}\}$, где $X_i^r \neq X_i^s$ для $r \neq s$. По следствию 1 элементарная дизъюнкция X_i эквивалентна элементарной дизъюнкции $X_i' = (\ldots (X_i^0 \vee X_i^1) \vee \ldots) \vee \vee X_i^{k_i}$, в которую каждая пропозициональная переменная входит не более одного раза. По леммам 6, 7 и теореме о замене формула X эквивалентна формуле $X' = (\ldots (X_0' \wedge X_1') \wedge \ldots) \wedge X_k'$. Пусть $P_0, \ldots, P_n$ — все атомарные подформулы формулы X'. Если некоторая X_j' не содержит какой-нибудь P_i в качестве подформулы, то в силу

$$X_j' \equiv X_j' \vee (P_i \wedge \neg P_i) \equiv (X_j' \vee P_i) \wedge (X_j' \vee \neg P_i)$$

формула

$$X'' = (X')^{X_j'}_{(X_j' \vee P_i) \wedge (X_j' \vee \neg P_i)}$$

эквивалентна X, находится в к. н. ф., любая пропозициональная переменная имеет не более одного вхождения в любом ее конъюнктивном члене и число ее конъюнктивных членов, не содержащих P_i, меньше, чем у X'. Проделав конечное число таких преобразований, мы можем получить формулу X^*, эквивалентную Φ и удовлетворяющую условиям 1) и 2) определения формулы, находящейся в совершенной к. н. ф. Выберем максимальное множество $\{\Psi_0, \ldots, \Psi_k\}$ попарно не эквивалентных конъюнктивных членов X*. Из следствия 1 получаем $D(\Psi_i) \neq D(\Psi_j)$ для $i \neq j$. По теореме о замене и следствию 2 получаем, что X* эквивалентна формуле $\Psi = (\ldots(\Psi_0 \wedge \Psi_1) \wedge \ldots) \wedge \Psi_k$, следовательно, Ψ удовлетворяет требованиям теоремы. □

Доказательство следующей теоремы проводится аналогичным способом и мы оставляем его читателю.

Теорема 5′. *Если формула $\neg\Phi$ ИВ не доказуема в ИВ, то существует формула Ψ, эквивалентная Φ и находящаяся в совершенной д. н. ф.* □

Упражнения

1. Доказать утверждения б) — е) леммы 1 и утверждения а), а′), б), б′), в′) леммы 4.
2. Доказать предложение 2, теорему 4 и теорему 5′.
3. Показать, что в теоремах 4 и 5 можно потребовать, чтобы Φ и Ψ содержали одни и те же переменные.
4. Показать, что секвенция $\Gamma, \Phi \vdash \Psi$ тогда и только тогда доказуема в ИВ, когда для любого $X \in D(\Phi)$ секвенция $\Gamma, X \vdash \Psi$ доказуема в ИВ.

§ 6. Семантика исчисления высказываний

Исчисление называется *непротиворечивым*, если в нем не все формулы этого исчисления доказуемы.

Пусть X — некоторое множество, f_X — некоторое отображение элементарных формул ИВ в множество $P(X)$ всех подмножеств X. Такое f_X назовем *интерпретацией ИВ в* X. Продолжим f_X до отображения формул ИВ в $P(X)$ (обозначим его также через f_X) по индукции:

1) $f_X(\Phi \wedge \Psi) = f_X(\Phi) \cap f_X(\Psi)$,

2) $f_X(\Phi \vee \Psi) = f_X(\Phi) \cup f_X(\Psi)$,

3) $f_X(\neg\Phi) = X \setminus f_X(\Phi)$,

4) $f_X(\Phi \to \Psi) = f_X(\neg\Phi) \cup f_X(\Psi)$.

Каждой секвенции S ИВ сопоставим утверждение $f_X(S)$ про подмножества X следующим образом:

а) $f_X(\Phi_0, \ldots, \Phi_n \vdash \Phi) \Leftrightarrow (f_X(\Phi_0), \ldots, f_X(\Phi_n) \to f_X(\Phi))$;

б) $f_X(\vdash \Phi) \Leftrightarrow f_X(\Phi) = X$;

в) $f_X(\Phi_0, \ldots, \Phi_n \vdash) \Leftrightarrow (f_X(\Phi_0), \ldots, f_X(\Phi_n) \to)$;

г) $f_X(\vdash) \Leftrightarrow X \to$.

Напомним (§ 1) определение отношения $\to$ на множествах:

$$X_0, \ldots, X_n \to Y \Leftrightarrow \left(\bigcap_{i \leqslant n} X_i \subseteq Y\right);$$

$$(X_0, \ldots, X_n \to) \Leftrightarrow \left(\bigcap_{i \leqslant n} X_i = \varnothing\right).$$

Теорема 6. *Для любой интерпретации f_X ИВ в X и любой доказуемой в ИВ секвенции S утверждение $f_X(S)$ справедливо.*

Доказательство. Пусть D — дерево вывода в ИВ секвенции S. Очевидно, что если S' — аксиома, то $f_X(S')$ истинно. Поэтому достаточно доказать, что если f_X от секвенций над чертой дерева D справедливо, то f_X от секвенции под той же чертой также справедливо. Пусть, например,

$$\frac{\Phi_0, \ldots, \Phi_n, \Psi_0 \vdash \Psi;\ \Phi_0, \ldots, \Phi_n, \Psi_1 \vdash \Psi;\ \Phi_0, \ldots, \Phi_n \vdash \Psi_0 \vee \Psi_1}{\Phi_0, \ldots, \Phi_n \vdash \Psi}$$

— переход в дереве D и $f_X(\Phi_0, \ldots, \Phi_n, \Psi_0 \vdash \Psi)$, $f_X(\Phi_0, \ldots, \Phi_n, \Psi_1 \vdash \Psi)$, $f_X(\Phi_0, \ldots, \Phi_n \vdash \Psi_0 \vee \Psi_1)$ имеют место. Пусть $x \in \bigcap_{i \leqslant n} f_X(\Phi_i)$. Так как $\bigcap_{i \leqslant n} f_X(\Phi_i) \subseteq f_X(\Psi_0) \cup \cup f_X(\Psi_1)$, то $x \in f_X(\Psi_j)$ для некоторого $j \leqslant 1$. Так как $\bigcap_{i \leqslant n} f_X(\Phi_i) \cap f_X(\Psi_j) \subseteq f_X(\Psi)$, то $x \in f_X(\Psi)$. Следовательно, $f_X(\Phi_0, \ldots, \Phi_n \vdash \Psi)$ имеет место.

Проверка для других переходов D также проста и предоставляется читателю. □

Следствие 1. *ИВ непротиворечиво.*

Доказательство. Пусть X — непустое множество, f_X — некоторая интерпретация ИВ в X. По определению интерпретации $f_X(Q_0 \wedge \neg Q_0) = f_X(Q_0) \cap (X \setminus f_X(Q_0)) = \varnothing$. Очевидно, что утверждение $f_X(\vdash Q_0 \wedge \neg Q_0)$ ложно. По теореме 6 секвенция $\vdash Q_0 \wedge \neg Q_0$ не доказуема. Следовательно, формула $Q_0 \wedge \neg Q_0$ не доказуема в ИВ. □

Мы рассмотрели интерпретацию ИВ, при которой пропозициональные переменные интерпретировались как подмножества некоторого множества X, а логические связки как операции на этих подмножествах. Это позволило доказать непротиворечивость ИВ. Представляет интерес и сама параллельность теоретико-множественных операций и логических связок *).

*) Полезное обобщение этой интерпретации приведено в упражнении 2 к § 11.

Конечно, понятие интерпретации выходит за рамки самого исчисления. Оно относится к так называемой *семантике исчисления*, в отличие от понятий формулы, правил вывода, доказательства, которые относятся к *синтаксису исчисления*.

Сейчас рассмотрим другую интерпретацию ИВ, которая очень тесно связана с этим исчислением и которую будем называть *главной интерпретацией ИВ*. На множестве $\{0, 1\}$ определим операции $\wedge$, $\vee$, $\rightarrow$, $\neg$ при помощи следующей таблицы:

x	y	$x \wedge y$	$x \vee y$	$x \rightarrow y$	$\neg x$
0	0	0	0	1	1
0	1	0	1	1	1
1	0	0	1	0	0
1	1	1	1	1	0

Эта таблица соответствует правилам 1)—4) определения интерпретации $f_{\{\varnothing\}}$, когда $0 = \varnothing$, $1 = \{\varnothing\}$. Иногда употребляют вместо символов 0, 1 слова «ложно» и «истинно». Тогда эта таблица укажет правила приписывания значений истинности для связок $\wedge$, $\vee$, $\rightarrow$, $\neg$, довольно хорошо согласующиеся с употреблением соответствующих связок в русском языке.

Зафиксируем пропозициональные переменные $P_0, \ldots, P_k$. Если задано отображение f множества элементарных формул $\{P_0, \ldots, P_k\}$ в $\{0, 1\}$, то по таблице (1) f однозначно продолжается на множество формул ИВ, пропозициональные переменные которых находятся среди $P_0, \ldots, P_k$. Если при этом $f(\Phi) = 1$ $(f(\Phi) = 0)$, то будем говорить, что *на наборе* $\langle f(P_0), \ldots, f(P_k) \rangle$ *значение истинности формулы* Φ равно 1 (0) или просто, что Φ *истинна* (*ложна*) *на этом наборе*.

Таким образом, для любой формулы Φ с пропозициональными переменными среди $P_0, \ldots, P_k$ мы имеем $(k+1)$-местную функцию на множестве $\{0, 1\}$, которая заданным значениям истинности переменных $P_0, \ldots, P_k$ сопоставляет значение истинности формулы Φ. Эту функцию назовем *истинностной функцией формулы* Φ (обозначаем ее через $T_\Phi(P_0, \ldots, P_k)$). Формулу Φ с переменными среди P_i, $i \leqslant k$, назовем *тождественно истинной* (*тождественно ложной*), если $T_\Phi(P_0, \ldots, P_k)$ принимает значение истины (лжи) на всех наборах значений переменных $P_0, \ldots, P_k$. Ясно, что это понятие не зависит от выбора $P_0, \ldots, P_k$. Секвенция $\Gamma \vdash \Phi$ называется *истинной на наборе* $\langle t_0, \ldots, t_k \rangle$ значений истинности переменных $P_0, \ldots, P_k$, среди которых содержатся все переменные секвенции $\Gamma \vdash \Phi$, если на наборе $\langle t_0, \ldots, t_k \rangle$ либо одна из формул Γ ложна, либо Φ истинна. Секвенция $\Gamma \vdash$ называется *истинной* на наборе $\langle t_0, \ldots, t_k \rangle$ значений истинности переменных $P_0, \ldots, P_k$, среди которых содержатся все переменные из элементов Γ, если одна из формул Γ на наборе $\langle t_0, \ldots, t_k \rangle$ ложна. Секвенция $\vdash$ является ложной на любом наборе по определению, а истинность секвенции $\vdash \Phi$ совпадает с истинностью Φ.

Секвенция S называется *тождественно истинной*, если она истинна на любом наборе $\langle t_0, \ldots, t_k \rangle$ значений истинности переменных $P_0, \ldots, P_k$, среди которых содержатся все переменные, входящие в S. Очевидно, что это понятие также не зависит от выбора $P_0, \ldots, P_k$.

Теорема 7. *Если секвенция S ИВ доказуема в ИВ, то S тождественно истинна.*

Доказательство. Пусть D — доказательство секвенции S в ИВ в виде дерева. Индукцию проводим по высоте доказательства D. Если S — аксиома, то утверждение теоремы тривиально. Чтобы завершить доказательство теоремы, нужно проверить, что правила 1—12 сохраняют тождественную истинность. Пусть, например,

$$\frac{\Gamma \vdash \Phi;\ \Gamma \vdash \Phi \to \Psi}{\Gamma \vdash \Psi}$$

— применение правила 8. Если на некотором наборе истинности пропозициональных переменных все формулы из Γ истинны, то по индукционному предположению Φ и $\Phi \to \Psi$ истинны на этом наборе. Тогда по определению операции $\to$ формула Ψ тоже истинна.

Проверка других правил также проста и предоставляется читателю. □

Из теоремы 7 получаем другое доказательство следствия 1. В самом деле, ясно, что $Q_0 \wedge \neg Q_0$ — тождественно ложная формула. Поэтому в силу теоремы 7 секвенция $\vdash Q_0 \wedge \neg Q_0$ не доказуема в ИВ.

Следствие 2. *Если $\Phi \equiv \Psi$, а пропозициональные переменные из Φ и Ψ содержатся среди $P_0, \ldots, P_k$, то $T_\Phi(P_0, \ldots, P_k) = T_\Psi(P_0, \ldots, P_k)$.*

Доказательство. Пусть на наборе $\bar{t}$ $T_\Phi(\bar{t})=1$. По условию $\Phi \vdash \Psi$ доказуема. По теореме 7 получаем, что $T_\Psi(\bar{t})=1$. Аналогично из $T_\Psi(\bar{t})=1$ следует $T_\Phi(\bar{t})=1$. □

Введем обозначения $P^0=P$, $P^1=\neg P$. Пусть $\bar{t}=\langle t_0, \ldots, t_n\rangle$ — набор нулей и единиц.

Лемма 1. *Элементарная дизъюнкция* Φ *вида* $P_0^{t_0}\vee\ldots\vee P_n^{t_n}$ *принимает значение* 0 *на единственном наборе* $\bar{t}=\langle t_0, \ldots, t_n\rangle$ *значений истинности переменных* $P_0, \ldots, P_n$.

Доказательство. Формула Φ построена из формул $P_i^{t_i}$ при помощи операции $\vee$. Из таблицы истинности для дизъюнкции следует, что если бы одна из формул $P_i^{t_i}$ приняла значение 1, то Φ также приняла бы значение 1. Следовательно, P_i должна принимать значение t_i. □

Теорема 8 (о функциональной полноте ИВ). *Пусть* f — *функция, определенная на наборах* $\langle t_0, \ldots, t_n\rangle$ *нулей и единиц и принимающая нуль или единицу в качестве значений. Тогда существует такая формула* Φ *ИВ, переменные которой содержатся среди* $Q_0, \ldots, Q_n$ *и* $T_\Phi(Q_0, \ldots, Q_n)=f$.

Доказательство. Если f тождественно равна единице, то в качестве Φ можно взять формулу $Q_0\vee\neg Q_0$.

Будем обозначать набор $\langle t_0, \ldots, t_n\rangle$ элементов множества $\{0, 1\}$ через $\bar{t}$, а через $f(\bar{t})$ — значение функции $f(t_0, \ldots, t_n)$. Пусть множество $X=\{\bar{t}\mid f(\bar{t})=0\}$ не пусто. Возьмем в качестве Φ формулу вида $\bigwedge\limits_{\bar{t}\in X}\left(Q_0^{t_0}\vee\ldots\vee Q_n^{t_n}\right)$.

Докажем, что $T_\Phi(\bar{t})=0$ эквивалентно $\bar{t}\in X$. Пусть $T_\Phi(\bar{t})=0$. Так как Φ построена из конъюнктивных членов с помощью операции $\wedge$, то существует конъюнктивный член Ψ, который ложен на наборе $\bar{t}$. Ψ имеет вид $Q_0^{t'_0}\vee\ldots\vee Q_n^{t'_n}$, где $\bar{t}'\in X$. В силу предыдущей леммы $\bar{t}'=\bar{t}$ и, следовательно, $\bar{t}\in X$. Пусть теперь $\bar{t}\in X$. По лемме 1 конъюнктивный член Ψ вида $Q_0^{t_0}\vee\ldots\vee Q_n^{t_n}$ ложен на наборе $\bar{t}$. Используя опять то, что Φ построена из конъюнктивных членов (среди которых находится Ψ) при помощи операции $\wedge$, заключаем, что $T_\Phi(\bar{t})=0$. □

Упражнения

1. Предположим, что ваши вычислительные возможности состоят только в следующем: если вам дают пару чисел $t_1, t_2\in\{0, 1\}$, то вы можете вычислить максимум $\max(t_1, t_2)$ этих чисел, а когда вам дадут $t \in \{0, 1\}$, то вы можете назвать $\bar{t} \in \{0, 1\}$, который не равен t. Показать, что вы тогда способны вычислить любую функцию f, сопоставляющую наборам $\langle t_0, \ldots, t_n \rangle$ нулей и единиц нуль или единицу. А именно, для любой такой функции f существует такая последовательность $s_0, \ldots, s_k$, что для любого $i \leqslant k$ s_i есть либо пара $\langle j, m \rangle$ чисел, меньших i, либо одно число, меньшее i. При этом, если вы по заданному набору $\langle t_0, \ldots \ldots, t_n \rangle$ нулей и единиц напишете последовательность $q_0, \ldots, q_k$ нулей и единиц по следующему правилу:

а) если $i \leqslant n$, то $q_i = t_i$;

б) если $n < i \leqslant k$ и $s_i = \langle j, m \rangle$, то $q_i = \max(q_j, q_m)$;

в) если $n < i \leqslant k$ и $s_i < i$, то $q_i = \widetilde{q}_{s_i}$,

то тогда q_k будет значением f на наборе $\langle t_0, \ldots, t_n \rangle$. (Указание. Воспользоваться теоремой 8, следствием 2 и эквивалентностью $\Phi \wedge \Psi \equiv \neg(\neg \Phi \vee \neg \Psi)$.)

2. Показать, что если формулы $\Phi \equiv \Psi$ находятся в совершенной к. н. ф. (совершенной д. н. ф.) и содержат одни и те же переменные, то $\{D(X) \mid X \in K(\Phi)\} = \{D(X) \mid X \in K(\Psi)\}$ $(\{K(X) \mid X \in D(\Phi)\} = \{K(X) \mid X \in D(\Psi)\})$.

§ 7. Характеризация доказуемых формул

Теорема 9. *Пусть Φ — формула ИВ. Следующие три условия эквивалентны:*

1) *Φ доказуема в ИВ.*

2) *Для всякой $\Phi' \equiv \Phi$, находящейся в к. н. ф., и любого ее конъюнктивного члена Ψ существует такая атомарная формула P, что $P, \neg P \in D(\Psi)$.*

3) *Существует $\Phi' \equiv \Phi$, находящаяся в к. н. ф. и такая, что для любого ее конъюнктивного члена Ψ существует такая атомарная P, что $P, \neg P \in D(\Psi)$.*

Доказательство. 2) $\Rightarrow$ 3) тривиально. 3) $\Rightarrow$ 1) следует из лемм 5.5, 5.6 и 4.2 а).

Докажем 1) $\Rightarrow$ 2). Пусть Φ доказуема. Тогда любой конъюнктивный член Ψ формулы Φ' в силу леммы 5.5 доказуем. Пусть $D(\Psi)$ не содержит никакой атомарной формулы P вместе с ее отрицанием $\neg P$. Рассмотрим два множества атомарных формул $X = \{P \mid P \in D(\Psi)\}$ и $Y = \{P \mid \neg P \in E(\Psi)\}$. По предположению, $X \cap Y = \varnothing$. Пусть Ψ_1 получается из Ψ заменой всех подформул $P \in X$ на Q_0 и всех $P \in Y$ на $\neg Q_0$. По теореме о подстановке Ψ_1 доказуема. Пусть Ψ_2 получается из Ψ_1 заменой $\neg\neg Q_0$ на Q_0. В силу леммы 5.1 б) и теоремы о замене $\Psi_2 \equiv \Psi_1$. Следовательно, Ψ_2 доказуема. Очевидно, что $D(\Psi_2) = \{Q_0\}$. По следствию 5.1 $Q_0 \equiv \Psi_2$. Следовательно, Q_0 доказуема. По теореме о подстановке получаем, что любая формула

Х доказуема. Это невозможно в силу непротиворечивости ИВ. □

Теорема 9 дает характеризацию доказуемых в ИВ формул, основанную на строении эквивалентных им формул, находящихся в к. н. ф. Такую характеризацию назовем *дедуктивной*. Сейчас мы получим *семантическую* характеризацию доказуемых в ИВ формул, основанную на понятии истинности.

Лемма 1. *Секвенция* $\Gamma, \Phi \vdash \Psi$ *доказуема тогда и только тогда, когда доказуема секвенция* $\Gamma \vdash \Phi \to \Psi$.

Доказательство. Непосредственно по правилам 7 и 8. □

Лемма 2. *Секвенция* $\Gamma \vdash$ *доказуема тогда и только тогда, когда доказуема секвенция* $\Gamma \vdash Q_0 \wedge \neg Q_0$.

Доказательство. Следует из предложения 3.2 д) и е). □

Теорема 10 (о полноте ИВ). а) *Для того чтобы формула Φ ИВ была доказуема в ИВ, необходимо и достаточно, чтобы Φ была тождественно истинной.*

б) *Для того чтобы секвенция S ИВ была доказуема в ИВ, необходимо и достаточно, чтобы S была тождественно истинной.*

Доказательство. Необходимость утверждает теорема 7. Утверждение б) следует из а), так как в силу лемм 1, 2 и определения тождественной истинности секвенций и формул доказуемость и тождественная истинность секвенций $\Phi_1, \ldots, \Phi_n \vdash \Psi$ и $\Phi_1, \ldots, \Phi_n \vdash$ равносильны доказуемости и тождественной истинности формул $\Phi_1 \to (\Phi_2 \to \ldots \to (\Phi_n \to \Psi) \ldots)$ и $\Phi_1 \to (\Phi_2 \to \ldots \ldots \to (\Phi_n \to (Q_0 \wedge \neg Q_0) \ldots)$ соответственно.

Пусть Φ — тождественно истинная формула и $\Phi' \equiv \Phi$ находится в к. н. ф. Предположим, что Φ не доказуема. Тогда Φ' тоже не доказуема. В силу лемм 5.5 и 5.6 существует конъюнктивный член Ψ формулы Φ', для которого $D(\Psi)$ не содержит атомарной формулы P вместе с ее отрицанием $\neg P$. Пусть $X = \{P \mid P \in D(\Psi)\}$ и $Y = \{P \mid \neg P \in D(\Psi)\}$. Тогда $X \cap Y = \varnothing$. Если переменные из X принимают значение 0, а переменные из Y — значение 1, то по лемме 6.1 Ψ принимает значение 0. Так как Φ' построена из конъюнктивных членов (среди которых есть Ψ) с помощью одной связки $\wedge$, то Φ' принимает значение 0, когда переменные из X принимают значение 0, а из Y — значение 1. Следовательно, Φ' — не тождественно истинная формула. В силу следствия 6.2

Ф — тоже не тождественно истинная формула. Получили противоречие. □

Если задано исчисление и определено понятие истинности (семантика) формул этого исчисления, то говорят, что исчисление *непротиворечиво по отношению к этой семантике*, если в исчислении доказуемы только истинные формулы. Если доказуемы все истинные формулы, то говорят, что исчисление *полно по отношению к этой семантике*. Кроме проблемы непротиворечивости и полноты важное значение имеет *проблема разрешимости* исчисления. Говорят, что исчисление *разрешимо*, если существует эффективная процедура (алгоритм), позволяющая для любой формулы Ф через конечное число шагов определить, доказуема Ф или нет. Если такой процедуры не существует, то говорят, что исчисление *неразрешимо*.

Если истинность формул ИВ определить как тождественную истинность, то предыдущая теорема показывает, что ИВ полно и непротиворечиво по отношению к этой семантике. Очевидно, что за конечное число шагов можно узнать, является ли данная формула Ф ИВ тождественно истинной или нет. Так как тождественная истинность и доказуемость Ф эквивалентны, то ИВ разрешимо.

При задании исчисления с помощью схем аксиом и правил вывода естественно возникает вопрос о независимости этих схем аксиом и правил вывода. *Схема аксиом* называется *независимой* в исчислении, если хотя бы один ее частный случай не доказуем в исчислении без этой схемы. *Правило вывода* называют *независимым* в исчислении, если оно не является допустимым в исчислении без этого правила. *Исчисление* называется *независимым, если* все его схемы аксиом и правила вывода независимы.

При построении исчисления часто стремятся получить его независимым. (Немаловажную роль здесь играют эстетические соображения.) В оставшейся части параграфа на примере ИВ будет изложен важный метод доказательства независимости исчислений *).

Предложение 1. *ИВ независимо.*

Доказательство. Так как в ИВ только одна схема аксиом, то она независима. Для доказательства независимости правил вывода достаточно для каждого правила α найти характеристическое свойство Δ, которым обладают все секвенции, доказуемые при помощи правил,

*) См. также упражнение 1 к § 8.

отличных от α, и которым некоторые доказуемые в ИВ секвенции не обладают. Мы ограничимся только формулировками характеристических свойств для правил 1—12, оставляя необходимую проверку читателю.

Характеристическим свойством для правил 1—8 будет тождественная истинность (§ 6) секвенций при новом определении для каждого правила одной из логических операций $\wedge$, $\vee$, $\to$, $\neg$ на множестве $\{0, 1\}$. Остальные операции при этом определяются по таблице § 6. Приведем новые определения логических операций, соответствующих правилам 1—8.

Правило 1. Конъюнкция определяется как тождественно ложная функция.

Правило 2. Значение конъюнкции $x \wedge y$ равно значению второго члена y.

Правило 3. Значение конъюнкции $x \wedge y$ равно значению первого члена x.

Правило 4. Значение дизъюнкции $x \vee y$ равно значению второго члена y.

Правило 5. Значение дизъюнкции $x \vee y$ равно значению первого члена x.

Правило 6. Дизъюнкция определяется как тождественно истинная функция.

Правило 7. Импликация определяется как тождественно ложная функция.

Правило 8. Импликация определяется как тождественно истинная функция.

Рассмотрим множество $A = \{0, 1, 2\}$. Конъюнкцию на множестве A определим как минимум двух чисел, а дизъюнкцию — как максимум. Отрицание определяется следующим образом: $\neg(2) = 0$, $\neg(1) = 0$, $\neg(0) = 2$. Импликация определяется так:

$$m \to n = \begin{cases} 2, & m \leqslant n; \\ n, & m > n. \end{cases}$$

Правило 9. Характеристическим свойством для секвенций $\Gamma \vdash \Phi$ ($\Gamma \vdash$) является следующее: для значений из множества A пропозициональных переменных минимум значений формул из Γ меньше или равен значению формулы Φ (соответственно равен нулю). При этом минимум пустого множества значений полагается равным двум.

Правило 10. Характеристическим свойством секвенций для этого правила является наличие формулы в правой части.

Правило 11. Характеристическое свойство секвенции $\Gamma \vdash \Phi$ ($\Gamma \vdash$) состоит в следующем: если $\Gamma = \langle \Phi_0, \ldots, \Phi_n \rangle \neq \varnothing$, то секвенция $\Phi_0 \vdash \Phi$ ($\Phi_0 \vdash$) доказуема в ИВ.

Правило 12. Характеристическое свойство секвенций $\Gamma \vdash \Phi$, $\Gamma \vdash$ состоит в том, что Γ одноэлементно или пусто. □

Упражнения

1. Пусть формула Φ ИВ находится в д. н. ф. Для того чтобы Φ была доказуемой в ИВ, необходимо и достаточно, чтобы для любых не содержащих общих элементов множеств X и Y пропозициональных переменных существовали формула $\Psi \in D(\Phi)$ и множества X_1, Y_1 пропозициональных переменных, для которых $(X \cup X_1) \cap (Y \cup Y_1) = \varnothing$ и $K(\Psi) \subseteq \{P \mid P \in (X \cup X_1)\} \cup \{\neg P \mid P \in (Y \cup Y_1)\}$. (Указание. Применить теорему о полноте ИВ.)

2. Провести необходимую проверку характеристических свойств в доказательстве предложения 1.

§ 8. Исчисление высказываний гильбертовского типа

В этом параграфе мы рассмотрим другую, так называемую гильбертовскую, аксиоматизацию исчисления высказываний — ИВ$_1$.

Определение. Понятие формулы в ИВ$_1$ то же, что и в ИВ; секвенций в ИВ$_1$ нет. Аксиомы ИВ$_1$ получаются из следующих 10 схем подстановкой конкретных формул ИВ$_1$ вместо переменных Φ, Ψ, X.

1. $\Phi \to (\Psi \to \Phi)$,
2. $(\Phi \to \Psi) \to ((\Phi \to (\Psi \to X)) \to (\Phi \to X))$,
3. $(\Phi \wedge \Psi) \to \Phi$,
4. $(\Phi \wedge \Psi) \to \Psi$,
5. $(\Phi \to \Psi) \to ((\Phi \to X) \to (\Phi \to (\Psi \wedge X)))$,
6. $\Phi \to (\Phi \vee \Psi)$,
7. $\Phi \to (\Psi \vee \Phi)$,
8. $(\Phi \to X) \to ((\Psi \to X) \to ((\Phi \vee \Psi) \to X))$,
9. $(\Phi \to \Psi) \to ((\Phi \to \neg \Psi) \to \neg \Phi)$,
10. $\neg \neg \Phi \to \Phi$.

Правило вывода в ИВ$_1$ одно:

$$\frac{\Phi, \ \Phi \to \Psi}{\Psi}.$$

Определение. *Доказательством в* $ИВ_1$ *формулы* Φ_n называется такая последовательность формул $\Phi_0, \ldots, \Phi_n$ $ИВ_1$, что каждая Φ_i, $i \leqslant n$, либо является аксиомой, либо получена из некоторых Φ_j, Φ_k, $j, k < i$, по правилу вывода. Если существует доказательство в $ИВ_1$ формулы Φ, то Φ называется *доказуемой в* $ИВ_1$ и обозначается это так: $\rhd \Phi$. *Выводом в* $ИВ_1$ *формулы* Φ_n *из множества* H *формул* $ИВ_1$ называется такая последовательность $\Phi_0, \ldots, \Phi_n$ формул $ИВ_1$, что каждая Φ_i, $i \leqslant n$, либо является аксиомой, либо принадлежит H, либо получается из некоторых Φ_j, Φ_k, $j, k < i$, по правилу вывода. Если существует вывод формулы Φ из H, то Φ называем *выводимой в* $ИВ_1$ *из* H и пишем $H \rhd \Phi$, при этом H называется *множеством гипотез.*

Очевидно, что доказуемость Φ в $ИВ_1$ равносильна выводимости Φ в $ИВ_1$ из пустого множества гипотез. Отметим, что множество гипотез H не обязано быть конечным, но если $H \rhd \Phi$, то в силу конечности вывода Φ из H существует конечное множество $H_1 \subseteq H$, для которого $H_1 \rhd \Phi$. Очевидно также, что если $H \subseteq H'$ и $H \rhd \Phi$, то $H' \rhd \Phi$.

Основной целью данного параграфа является доказательство следующей теоремы, которая показывает в определенном смысле равносильность ИВ и $ИВ_1$.

Теорема 11. а) *Секвенция* $\Psi_1, \ldots, \Psi_n \vdash \Phi$ *тогда и только тогда доказуема в ИВ, когда* Φ *выводима из* $\{\Psi_1, \ldots, \Psi_n\}$ *в* $ИВ_1$. *В частности, множества доказуемых формул в ИВ и в* $ИВ_1$ *совпадают.*

б) *Секвенция* $\Psi_1, \ldots, \Psi_n \vdash$ *тогда и только тогда доказуема в ИВ, когда формула* $Q_0 \wedge \neg Q_0$ *выводима из* $\{\Psi_1, \ldots, \Psi_n\}$ *в* $ИВ_1$.

Прежде чем приступить к доказательству теоремы 11, мы разовьем некоторую теорию выводимости в $ИВ_1$.

Пример 1. Пусть Φ — формула $ИВ_1$. Последовательность из следующих 5 формул будет доказательством формулы $\Phi \to \Phi$ в $ИВ_1$:

1) $\Phi \to (\Phi \to \Phi)$ — аксиома,

2) $\Phi \to ((\Phi \to \Phi) \to \Phi)$ — аксиома,

3) $(\Phi \to (\Phi \to \Phi)) \to ((\Phi \to ((\Phi \to \Phi) \to \Phi)) \to (\Phi \to \Phi))$ — аксиома,

4) $(\Phi \to ((\Phi \to \Phi) \to \Phi)) \to (\Phi \to \Phi)$ — правило вывода к 1) и 3),

5) $\Phi \to \Phi$ — правило вывода к 2) и 4).

Правило вывода

$$\frac{\Phi_0, \ldots, \Phi_k}{\Psi}$$

называется *допустимым* в ИВ$_1$, если его добавление к исчислению ИВ$_1$ не увеличивает семейство выводимых из H формул для любого множества гипотез H.

Квазивыводом в ИВ$_1$ формулы Φ_n из множества гипотез H называется такая последовательность формул $\Phi_0, \ldots, \Phi_n$, что каждая Φ_i, $i \leqslant n$, либо выводима в ИВ$_1$ из H, либо получается из некоторых предыдущих по допустимому в ИВ$_1$ правилу вывода. Очевидно, что если имеется квазивывод в ИВ$_1$ формулы Φ из множества H, то Φ выводима в ИВ$_1$ из H.

Теорема 12 (о дедукции). *Если $H \cup \{\Phi\} \triangleright \Psi$, то $H \triangleright \Phi \to \Psi$.*

Доказательство проводим индукцией по минимальному n, для которого существует вывод $\Psi_0, \ldots, \Psi_n$ формулы Ψ из $H \cup \{\Phi\}$. Если $n = 0$, то либо 1) $\Psi = \Phi$, либо 2) Ψ — аксиома или входит в H. В первом случае, в силу примера 1, формула $\Phi \to \Psi$ выводима из H. Во втором случае последовательность

$$\Psi, \quad \Psi \to (\Phi \to \Psi), \quad \Phi \to \Psi$$

будет выводом в ИВ$_1$ из H. Пусть $n > 0$. Из минимальности n имеем, что Ψ получается из Ψ_i и $\Psi_j = (\Psi_i \to \Psi)$ для $i, j < n$ по правилу вывода. Тогда в силу индукционного предложения последовательность

$$\Phi \to \Psi_i, \quad \Phi \to (\Psi_i \to \Psi),$$
$$(\Phi \to \Psi_i) \to ((\Phi \to (\Psi_i \to \Psi)) \to (\Phi \to \Psi)),$$
$$(\Phi \to (\Psi_i \to \Psi)) \to (\Phi \to \Psi), \quad \Phi \to \Psi$$

будет квазивыводом $\Phi \to \Psi$ из H. □

Теорема о дедукции существенно облегчает для многих формул ИВ$_1$ установление их доказуемости в ИВ$_1$. Так, без применения теоремы о дедукции в следующем примере пришлось бы привести гораздо более длинное доказательство.

Пример 2. Пусть Φ и Ψ — формулы ИВ$_1$. Покажем, что формула $\Phi \to (\Psi \to (\Phi \wedge \Psi))$ доказуема в ИВ$_1$. По теореме о дедукции достаточно показать, что $\{\Phi, \Psi\} \triangleright \Phi \wedge \Psi$. Следующая последовательность будет требуемым выводом:

1) $\Phi \to (\Phi \to \Phi)$ — аксиома,
2) $\Psi \to (\Phi \to \Psi)$ — аксиома,
3) $(\Phi \to \Phi) \to ((\Phi \to \Psi) \to (\Phi \to (\Phi \wedge \Psi)))$ — аксиома,
4) Φ — гипотеза,
5) $\Phi \to \Phi$ — правило к 1) и 4),
6) Ψ — гипотеза,
7) $\Phi \to \Psi$ — правило к 2) и 6),
8) $(\Phi \to \Psi) \to (\Phi \to (\Phi \wedge \Psi))$ — правило к 3) и 5),
9) $\Phi \to (\Phi \wedge \Psi)$ — правило к 7) и 8),
10) $\Phi \wedge \Psi$ — правило к 4) и 9).

Прежде чем приступить к доказательству теоремы 11, установим еще один технический факт.

Следствие 1. $\{\Phi_0, \ldots, \Phi_n\} \rhd \Phi$ *равносильно* $\rhd \Phi_0 \to (\Phi_1 \to \ldots (\Phi_n \to \Phi) \ldots)$, *что в свою очередь равносильно* $\rhd (\Phi_0 \wedge (\Phi_1 \wedge \ldots (\Phi_{n-1} \wedge \Phi_n) \ldots)) \to \Phi$.

Доказательство. В одну сторону $n+1$ раз применяем теорему дедукции. Пусть теперь $\rhd \Phi_0 \to (\Phi_1 \to \ldots \ldots (\Phi_n \to \Phi) \ldots)$. Тогда $\{\Phi_0, \ldots, \Phi_n\} \rhd \Phi_0 \to (\Phi_1 \to \ldots \ldots (\Phi_n \to \Phi) \ldots)$ и, применяя несколько раз правило вывода, получаем $\{\Phi_0, \ldots, \Phi_n\} \rhd \Phi$. Используя несколько раз пример 2 и правило вывода, получаем $\{\Phi_0, \ldots, \Phi_n\} \rhd \Phi_0 \wedge (\Phi_1 \wedge \ldots (\Phi_{n-1} \wedge \Phi_n) \ldots)$, а применяя несколько раз аксиомы 3, 4 и правило вывода, получаем $\{\Phi_0 \wedge (\Phi_1 \wedge \ldots (\Phi_{n-1} \wedge \Phi_n) \ldots)\} \rhd \Phi_i$ для любого $i \leqslant n$. Следовательно, $\{\Phi_0, \ldots, \Phi_n\} \rhd \Phi$ равносильно выводимости $\{\Phi_0 \wedge (\Phi_1 \wedge \ldots (\Phi_{n-1} \wedge \Phi_n) \ldots)\} \rhd \Phi$, что, как уже показано выше, равносильно $\rhd (\Phi_0 \wedge (\Phi_1 \wedge \ldots (\Phi_{n-1} \wedge \wedge \Phi_n) \ldots)) \to \Phi$. □

Доказательство теоремы 11. В силу следствия 1 и лемм 7.1, 7.2 достаточно показать, что доказуемость формулы Φ в ИВ равносильна доказуемости Φ в ИВ$_1$. Легко проверить, что все аксиомы ИВ$_1$ тождественно истинны, а правило вывода ИВ$_1$ сохраняет тождественную истинность. Поэтому по теореме о полноте ИВ из $\rhd \Phi$ следует доказуемость Φ в ИВ.

Будем говорить, что *правило вывода ИВ сохраняет выводимость в ИВ$_1$*, если после замены в нем секвенций $\Psi_1, \ldots, \Psi_n \vdash \Phi$ и $\Psi_1, \ldots, \Psi_n \vdash$ соответственно на $\{\Psi_1, \ldots, \Psi_n\} \rhd \Phi$ и $\{\Psi_1, \ldots, \Psi_n\} \rhd Q_0 \wedge \neg Q_0$ из истинности утверждений над чертой будет следовать истинность утверждения под чертой. Ясно, что для доказательства того, что из доказуемости Φ в ИВ следует $\rhd \Phi$, достаточно показать, что правила 1—12 сохраняют выводимость в $ИВ_1$. Сохранение выводимости для правил 1—5 легко показать, используя пример 2 и аксиомы 3—7. Пусть $\{\Psi_1, \ldots, \Psi_k, \Phi\} \rhd \Psi$; $\{\Psi_1, \ldots, \Psi_k, X\} \rhd \Psi$; $\{\Psi_1, \ldots, \Psi_k\} \rhd \Phi \vee X$. По теореме о дедукции $\{\Psi_1, \ldots, \Psi_k\} \rhd \Phi \to \Psi$ и $\{\Psi_1, \ldots, \Psi_k\} \rhd X \to \Psi$. Применяя три раза правило вывода $ИВ_1$ к аксиоме 8, получаем $\{\Psi_1, \ldots, \Psi_k\} \rhd \Psi$. Следовательно, правило 6 сохраняет выводимость. Правило 7 соответствует теореме о дедукции, правило 8 — правилу вывода $ИВ_1$. Докажем сохранение выводимости правилом 9. Пусть $\{\Psi_1, \ldots, \Psi_k, \neg\Phi\} \rhd Q_0 \wedge \neg Q_0$. Из аксиом 3 и 4 получаем $\{\Psi_1, \ldots, \Psi_k, \neg\Phi\} \rhd Q_0$ и $\{\Psi_1, \ldots, \Psi_k, \neg\Phi\} \rhd \neg Q_0$. По теореме о дедукции получаем $\{\Psi_1, \ldots, \Psi_k\} \rhd \neg\Phi \to Q_0$ и $\{\Psi_1, \ldots, \Psi_k\} \rhd \neg\Phi \to \neg Q_0$. Тогда из аксиом 9 и 10 получаем $\{\Psi_1, \ldots, \Psi_k\} \rhd \Phi$. Рассмотрим правило 10. Пусть $\{\Psi_1, \ldots, \Psi_k\} \rhd \Phi$ и $\{\Psi_1, \ldots, \Psi_k\} \rhd \neg\Phi$. Из аксиомы 1 получаем

$$\{\Psi_1, \ldots, \Psi_k\} \rhd \neg(Q_0 \wedge \neg Q_0) \to \Phi$$

и

$$\{\Psi_1, \ldots, \Psi_k\} \rhd \neg(Q_0 \wedge \neg Q_0) \to \neg\Phi.$$

Из аксиом 9 и 10 тогда следует $\{\Psi_1, \ldots, \Psi_k\} \rhd Q_0 \wedge \neg Q_0$. Сохранение выводимости правилами 11 и 12 следует непосредственно из определения вывода в $ИВ_1$. □

Упражнение

1. Доказать независимость $ИВ_1$. (Указание. Тот же метод, что и для ИВ. Для доказательства независимости схем 1 и 2 логические связки определяются на множестве $\{0, 1, 2\}$, а схем 3—10 — на множестве $\{0, 1\}$. Для схемы 1 связки определяются так: $n \wedge m) = \min (n, m)$, $n \vee m = \max (n, m)$, $\neg 0 = \neg 1 = 2$, $\neg 2 = 0$, $(n \to m) = 2$, если $n \leqslant m$, и $(n \to m) = 0$, если $n > m$. Для схемы 2 имеем $(0 \wedge m) = (m \wedge 0) = 1$, $(0 \vee 0) = 1$, $\neg 2 = 1$, $(0 \to 0) = (2 \to 0) = (2 \to 1) = 1$, $(1 \to 0) = 2$, а остальные значения связок — как для схемы 1. Характеристическое свойство формул при доказательстве независимости схем 1 и 2 — тождественное равенство 2.)

§ 9. Консервативные расширения исчислений

Пусть даны два языка $L_0 \subseteq L_1$ и два исчисления: I_0 языка L_0 и I_1 языка L_1. Исчисление I_1 назовем *консервативным расширением* I_0 (обозначаем $I_0 < I_1$), если выражение Φ языка L_0 доказуемо в I_0 тогда и только тогда, когда Φ доказуемо в I_1. Очевидно, что отношение $<$ рефлексивно, транзитивно и имеет место

Предложение 1. *Если* $I_0 < I_1$ *и* I_0 *непротиворечиво, то* I_1 *непротиворечиво.* □

Пусть ИВ$^{(\to)}$ — исчисление, полученное из ИВ удалением из алфавита символа $\to$ и удалением правил 7 и 8.

Предложение 2. *ИВ*$^{(\to)}$ $<$ *ИВ.*

Доказательство. Пусть α: $F \to F$ — отображение, определенное в доказательстве леммы 5.2. Продолжим α на последовательности формул и секвенции:

$$\alpha(\langle\Phi_1, \ldots, \Phi_n\rangle) = \langle\alpha\Phi_1, \ldots, \alpha\Phi_n\rangle,$$
$$\alpha(\Gamma \vdash \Phi) = \alpha(\Gamma) \vdash \alpha(\Phi), \quad \alpha(\Gamma \vdash) = \alpha(\Gamma) \vdash.$$

Так как $\alpha(\Phi) = \Phi$ для формулы Φ, не содержащей импликации, то достаточно показать, что если секвенция S доказуема в ИВ, то секвенция $\alpha(S)$ доказуема в ИВ$^{(\to)}$. Если D — доказательство секвенции S в ИВ в виде дерева, то индукцией по высоте D будем строить квазивывод D^* секвенции $\alpha(S)$ в ИВ$^{(\to)}$. Если D — аксиома ИВ, то очевидно, что $D^* = \alpha(D)$ — аксиома ИВ$^{(\to)}$. Пусть

$$D = \frac{D_1; \ldots; D_n}{S}.$$

Если последний переход в D осуществляется по правилам, отличным от правил 7 и 8, то очевидно, что

$$D^* = \frac{D_1^*; \ldots; D_n^*}{\alpha(S)}$$

будет квазивыводом в ИВ$^{(\to)}$, у которого последний переход осуществляется по тому же правилу, что у D. Если

$$D = \frac{D_1; D_2}{\Gamma \vdash \Phi},$$

где D_1, D_2 — доказательства в ИВ секвенций $\Gamma \vdash \Psi$, $\Gamma \vdash \Psi \to \Phi$ соответственно, то в качестве D^* берем следующее дерево:

$$\cfrac{D_1^*; \quad \cfrac{\neg\alpha(\Psi) \vdash \neg\alpha(\Psi); \quad \cfrac{\neg\alpha(\Phi), \alpha(\Phi), \neg\neg\alpha(\Psi) \vdash}{\neg\alpha(\Phi), \alpha(\Phi) \vdash \neg\alpha(\Psi)}; \quad D_2^*}{\alpha(\Gamma), \neg\alpha(\Phi) \vdash \neg\alpha(\Psi)}}{\cfrac{\alpha(\Gamma), \neg\alpha(\Phi) \vdash}{\alpha(\Gamma) \vdash \alpha(\Phi)}}.$$

Если

$$D = \frac{D_1}{\Gamma \vdash \Psi \to \Phi},$$

где D_1 — доказательство в ИВ секвенции $\Gamma, \Psi \vdash \Phi$, то в качестве D^* берем следующее дерево:

$$\frac{\dfrac{D_1^*}{\alpha(\Gamma),\ \alpha(\Psi) \vdash \neg\alpha(\Psi) \vee \alpha(\Phi);}\ \ \neg\alpha(\Psi) \vdash \neg\alpha(\Psi) \vee \alpha(\Phi);\ \ \vdash \alpha(\Psi) \vee \neg\alpha(\Psi)}{\alpha(\Gamma) \vdash \neg\alpha(\Psi) \vee \alpha(\Phi)}. \quad \square$$

Пусть $ИВ^{(\to, \vee)}$ — исчисление, полученное из ИВ удалением из алфавита символов $\to$, $\vee$ и удалением правил 4—8.

Предложение 3. *$ИВ^{(\to, \vee)} < ИВ$.*

Доказательство. Обозначим через $F^{(\to)}$ множество формул ИВ, не содержащих символа $\to$. Определим отображение β: $F^{(\to)} \to F^{(\to)}$ следующим образом:

а) если Φ не содержит символа $\vee$, то $\beta(\Phi) = \Phi$;

б) если $\Phi = (\Psi \vee X)$, то $\beta(\Phi) = \neg(\neg\beta(\Psi) \wedge \neg\beta(X))$;

в) если $\Phi = (\Psi \wedge X)$, $\Phi = \neg\Psi$, то $\beta(\Phi) = (\beta(\Psi) \wedge \beta(X))$, $\beta(\Phi) = \neg\beta(\Psi)$.

Продолжим β на последовательности формул и секвенции:

$$\beta(\langle \Phi_1, \ldots, \Phi_n \rangle) = \langle \beta\Phi_1, \ldots, \beta\Phi_n \rangle,$$

$$\beta(\Gamma \vdash \Phi) = \beta(\Gamma) \vdash \beta(\Phi), \quad \beta(\Gamma \vdash) = \beta(\Gamma) \vdash.$$

В силу а) определения β и предложения 2 достаточно показать, что если секвенция S доказуема в исчислении $ИВ^{(\to)}$, то $\beta(S)$ доказуема в $ИВ^{(\to, \vee)}$.

Индукцией по высоте для любого доказательства D секвенции S в $ИВ^{(\to)}$ в виде дерева будем строить квазивывод D^* секвенции $\beta(S)$ в $ИВ^{(\to, \vee)}$. Если D — аксиома $ИВ^{(\to)}$, то очевидно, что $D^* = \beta(D)$ — аксиома $ИВ^{(\to, \vee)}$. Пусть

$$D = \frac{D_0; \ldots; D_n}{S}.$$

Если последний переход в D осуществляется по правилам, отличным от правил 4—6 ИВ, то очевидно, что

$$D^* = \frac{D_0^*; \ldots; D_n^*}{\beta(S)}$$

будет квазивыводом в $ИВ^{(\to, \vee)}$.

Пусть

$$D = \frac{D_1}{\Gamma \vdash \Phi \vee \Psi}$$

и последний переход в D осуществляется по правилу 4 исчисления ИВ. Тогда D_1^* будет квазивыводом секвенции $\beta(\Gamma) \vdash \beta(\Phi)$ и в качестве D^* можно взять следующее дерево:

$$\cfrac{\cfrac{D_1^*;\ \beta(\Gamma),\ \neg\beta(\Phi) \wedge \neg\beta(\Psi) \vdash \neg\beta(\Phi)}{\beta(\Gamma),\ \neg\beta(\Phi) \wedge \neg\beta(\Psi) \vdash}}{\beta(\Gamma) \vdash \neg(\neg\beta(\Phi) \wedge \neg\beta(\Psi))}.$$

Аналогично рассматривается случай, когда последний переход в D — применение правила 5.

Прежде чем рассмотреть случай применения правила 6, докажем допустимость в $ИВ^{(\to,\vee)}$ следующих правил:

а) $\dfrac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg\neg\Phi \vdash \Psi}$; б) $\dfrac{\Gamma, \Phi \vdash}{\Gamma, \neg\neg\Phi \vdash}$;

в) $\dfrac{\Gamma, \Phi \vdash}{\Gamma \vdash \neg\Phi}$; г) $\dfrac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg\Psi \vdash \neg\Phi}$.

Допустимость в $ИВ^{(\to,\vee)}$ правил а) и б) будем показывать одновременной индукцией по высоте доказательства D в $ИВ^{(\to,\vee)}$ секвенций $\Gamma, \Phi \vdash \Psi$ $(\Gamma, \Phi \vdash)$. Если D — аксиома $X \vdash X$, то квазивыводом в $ИВ^{(\to,\vee)}$ секвенции $\neg\neg X \vdash X$ будет следующее дерево:

$$\cfrac{\cfrac{\neg X \vdash \neg X;\ \neg\neg X \vdash \neg\neg X}{\neg\neg X,\ \neg X \vdash}}{\neg\neg X \vdash X}.$$

Если D не является аксиомой, то доказуемость секвенции $\Gamma, \neg\neg\Phi \vdash \Psi$ (секвенции $\Gamma, \neg\neg\Phi \vdash$) сразу следует из индукционного предположения. Пусть секвенция $\Gamma, \Phi \vdash$ доказуема в $ИВ^{(\to,\vee)}$. Тогда по правилу б) получаем доказуемость $\Gamma, \neg\neg\Phi \vdash$ и по правилу 9 получаем доказуемость в $ИВ^{(\to,\vee)}$ секвенции $\Gamma \vdash \neg\Phi$. Покажем теперь допустимость в $ИВ^{(\to,\vee)}$ правила г). Из доказуемой в $ИВ^{(\to,\vee)}$ секвенции $\Gamma, \Phi \vdash \Psi$ и аксиомы $\neg\Psi \vdash \neg\Psi$ с помощью правил 10—12 получаем секвенцию $\Gamma, \neg\Psi, \Phi \vdash$. Из допустимости в $ИВ^{(\to,\vee)}$ правила в) получаем доказуемость в $ИВ^{(\to,\vee)}$ секвенции $\Gamma, \neg\Psi \vdash \neg\Phi$.

Пусть теперь
$$D = \frac{D_1;\ D_2;\ D_3}{\Gamma \vdash \Psi}$$
— доказательство в $\text{ИВ}^{(\to)}$, последний переход в котором осуществляется по правилу 6. По индукционному предположению существуют квазивыводы D_1^*, D_2^* и D_3^* в исчислении $\text{ИВ}^{(\to,\vee)}$ секвенций $\beta(\Gamma),\ \beta(\Phi) \vdash \beta(\Psi)$; $\beta(\Gamma),\ \beta(X) \vdash \beta(\Psi)$ и $\beta(\Gamma) \vdash \neg(\neg\beta(\Phi) \wedge \neg\beta(X))$ соответственно. В силу допустимости в $\text{ИВ}^{(\to,\vee)}$ правила г) следующее дерево будет квазивыводом в $\text{ИВ}^{(\to,\vee)}$ секвенции $\beta(\Gamma) \vdash \beta(\Psi)$:
$$\cfrac{\cfrac{\cfrac{D_1^*}{\beta(\Gamma),\ \neg\beta(\Psi) \vdash \neg\beta(\Phi)} \quad \cfrac{D_2^*}{\beta(\Gamma),\ \neg\beta(\Psi) \vdash \neg\beta(X)}}{\beta(\Gamma),\ \neg\beta(\Psi) \vdash \neg\beta(\Phi) \wedge \neg\beta(X);\ D_3^*}}{\cfrac{\beta(\Gamma),\ \neg\beta(\Psi) \vdash}{\beta(\Gamma) \vdash \beta(\Psi)}}. \ \square$$

До этого мы рассматривали расширения языков исчислений лишь путем расширения алфавитов. Рассмотрим теперь расширение LG языка исчисления $\text{ИВ}^{(\to,\vee)}$, у которого алфавит и формулы те же самые, что у $\text{ИВ}^{(\to,\vee)}$, а секвенции определяются так: если Γ и Θ — последовательности формул исчисления $\text{ИВ}^{(\to,\vee)}$, то $\Gamma \vdash \Theta$ является секвенцией языка LG.

Определим теперь исчисление G_0 языка LG. Аксиомами G_0 будут секвенции вида $P,\ \Gamma \vdash \Theta,\ P$, где P — атомарная формула, а Γ, Θ — последовательности атомарнах формул. Правилами вывода исчисления G_0 будут следующие:

1) $\dfrac{\Gamma \vdash \Theta, \Phi;\ \Gamma \vdash \Theta, \Psi}{\Gamma \vdash \Theta, \Phi \wedge \Psi}$,

2) $\dfrac{\Phi, \Psi, \Gamma \vdash \Theta}{\Phi \wedge \Psi, \Gamma \vdash \Theta}$,

3) $\dfrac{\Phi, \Gamma \vdash \Theta}{\Gamma \vdash \Theta, \neg\Phi}$,

4) $\dfrac{\Gamma \vdash \Theta, \Phi}{\neg\Phi, \Gamma \vdash \Theta}$,

5) $\dfrac{\Gamma \vdash \Delta, \Phi, \Psi, \Theta}{\Gamma \vdash \Delta, \Psi, \Phi, \Theta}$,

6) $\dfrac{\Gamma, \Phi, \Psi, \Delta \vdash \Theta}{\Gamma, \Psi, \Phi, \Delta \vdash \Theta}$,

7) $\dfrac{\Gamma \vdash \Theta, \Phi, \Phi}{\Gamma \vdash \Theta, \Phi}$,

8) $\dfrac{\Phi, \Phi, \Gamma \vdash \Theta}{\Phi, \Gamma \vdash \Theta}$,

где Φ, Ψ — переменные для формул G_0, а Γ, Θ, Δ — переменные для последовательностей формул G_0.

В оставшейся части параграфа формулами и секвенциями, если не оговорено противное, мы называем формулы и секвенции исчисления G_0.

Лемма 1. *Пусть секвенция $\Gamma \vdash \Theta$ доказуема в G_0, а последовательности Γ_1 и Θ_1 содержат среди своих членов все члены последовательностей Γ и Θ соответственно. Тогда секвенция $\Gamma_1 \vdash \Theta_1$ доказуема в G_0.*

Доказательство. Индукцией по длине Φ покажем, что для любых последовательностей формул Γ, Θ из доказуемости в G_0 секвенции $\Gamma \vdash \Theta$ следует доказуемость в G_0 секвенций $\Phi, \Gamma \vdash \Theta$ и $\Gamma \vdash \Theta, \Phi$. Утверждение леммы отсюда получим, используя правила 5)—8).

Если Φ — атомарная формула, а D — доказательство в G_0 секвенции $\Gamma \vdash \Theta$, то очевидно, что, заменив в D каждую секвенцию $\Gamma' \vdash \Theta'$ на $\Gamma', \Phi \vdash \Theta'$ (на $\Gamma' \vdash \Phi, \Theta'$), получим доказательство в G_0 секвенции $\Gamma, \Phi \vdash \Theta$ (секвенции $\Gamma \vdash \Phi, \Theta$). Применяя правила 5), 6), получим доказуемость секвенций $\Phi, \Gamma \vdash \Theta$ и $\Gamma \vdash \Theta, \Phi$.

Пусть $\Phi = \Psi \wedge X$ и секвенции $X, \Gamma \vdash \Theta$; $\Gamma \vdash \Theta, \Psi$; $\Gamma \vdash \Theta, X$ доказуемы в G_0. Из индукционного предположения получаем доказуемость $\Psi, X, \Gamma \vdash \Theta$, а с помощью правила 1) получаем доказуемость $\Gamma \vdash \Theta, \Phi$. С помощью правила 2) получаем также $\Phi, \Gamma \vdash \Theta$.

Если $\Phi = \neg\Psi$ и секвенции $\Psi, \Gamma \vdash \Theta$; $\Gamma \vdash \Theta, \Psi$ доказуемы в G_0, то доказуемость в G_0 секвенций $\Phi, \Gamma \vdash \Theta$ и $\Gamma \vdash \Theta, \Phi$ получаем с помощью правил 3) и 4). □

Лемма 2. а) *Если в G_0 доказуема секвенция* $\Gamma \vdash \Theta, \Phi \wedge \Psi$, *то доказуемы также секвенции* $\Gamma \vdash \Theta, \Phi$ *и* $\Gamma \vdash \Theta, \Psi$.

б) *Если в G_0 доказуема секвенция* $\Phi\wedge$, $\Gamma \vdash \Theta$, *то доказуема также секвенция* $\Phi, \Psi, \Gamma \vdash \Theta$.

в) *Если в G_0 доказуема секвенция* $\Gamma \vdash \Theta, \neg\Phi$, *то доказуема также секвенция* $\Phi, \Gamma \vdash \Theta$.

г) *Если в G_0 доказуема секвенция* $\neg\Phi, \Gamma \vdash \Theta$, *то доказуема также секвенция* $\Gamma \vdash \Theta, \Phi$.

Доказательство. Докажем утверждение б). Доказательства остальных утверждений проводятся аналогично, и мы их оставляем читателю в качестве упражнения.

Переход в доказательстве D будем называть *существенным*, если он осуществляется по правилам, отличным от правил перестановки 5), 6). Если D — доказательство в G_0 в виде дерева, то через D^* обозначим дерево, полученное из D удалением всех секвенций, расположенных ниже секвенции, являющейся заключением при последнем существенном переходе в D.

Индукцией по числу существенных переходов в дереве D будем доказывать следующее утверждение: если D — доказательство в G_0 секвенции $\Gamma_1, \Phi\wedge\Psi, \Gamma_2 \vdash \Theta$, то существует доказательство D_1 секвенции $\Gamma_1, \Phi, \Psi, \Gamma_2 \vdash \Theta$, причем число существенных переходов в D_1 меньше числа существенных переходов в D.

Пусть D^* имеет следующий вид:

$$\cfrac{\cfrac{D'}{\Phi, \Psi, \Gamma' \vdash \Theta'}}{\wedge\Psi, \Gamma' \vdash \Theta'}.$$

Тогда в качестве требуемого D_1 можно взять некоторое дерево D_1, для которого

$$D_1^* = \left(\frac{D'}{\Phi, \Psi, \Gamma' \vdash \Theta'}\right)^*.$$

Пусть D^* имеет следующий вид:

$$\cfrac{\cfrac{D'}{\Phi\wedge\Psi, \Phi\wedge\Psi, \Gamma' \vdash \Theta'}}{\Phi\Delta\Psi, \Gamma' \vdash \Theta'}.$$

Обозначим через n_0 число существенных переходов в D. По индукционному предположению существует доказательство D_2 секвенции $\Phi, \Psi, \Phi\wedge\Psi, \Gamma' \vdash \Theta'$ с числом существенных переходов $< n_0 - 1$. Опять по индукционному предположению существует доказательство D_3 секвенции $\Phi, \Psi, \Phi, \Psi, \Gamma' \vdash \Theta'$ с числом существенных переходов $< n_0 - 2$. Тогда в качестве D_1 можно взять такое доказательство секвенции $\Gamma_1, \Phi, \Psi, \Gamma_2 \vdash \Theta$, что D_1^* есть

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{D_3}{\Phi,\ \Phi,\ \Psi,\ \Psi,\ \Gamma' \vdash \Theta'}}{\Phi,\ \Psi,\ \Psi,\ \Gamma' \vdash \Theta'}}{\Psi,\ \Phi,\ \Psi,\ \Gamma' \vdash \Theta'}}{\Psi,\ \Psi,\ \Phi,\ \Gamma' \vdash \Theta'}}{\Psi,\ \Phi,\ \Gamma' \vdash \Theta'}.$$

Ясно, что число существенных переходов в D_1 меньше $n_0 - 2 + 2 = n_0$.

Пусть D^* имеет следующий вид:

$$\frac{\dfrac{D'}{\Gamma_1',\ \Phi\wedge\Psi,\ \Gamma_2' \vdash \Theta',\ X_1} \qquad \dfrac{D''}{\Gamma_1',\ \Phi\wedge\Psi,\ \Gamma_2' \vdash \Theta',\ X_2}}{\Gamma_1',\ \Phi\wedge\Psi,\ \Gamma_2' \vdash \Theta',\ X_1\wedge X_2}.$$

По индукционному предположению существуют доказательства D_1' и D_1'' секвенций $\Gamma_1', \Phi, \Psi, \Gamma_2' \vdash \Theta', X_1$ и $\Gamma_1', \Phi, \Psi, \Gamma_2' \vdash \Theta', X_2$ соответственно и число существенных переходов в D_1', D_1'' меньше числа существенных переходов в деревьях

$$\frac{D'}{\Gamma_1',\ \Phi\wedge\Psi,\ \Gamma_2' \vdash \Theta',\ X_1}, \qquad \frac{D''}{\Gamma_1',\ \Phi\wedge\Psi,\ \Gamma_2' \vdash \Theta',\ X_2}$$

соответственно. Тогда в качестве требуемого D_1 берем такое доказательство секвенции $\Gamma_1, \Phi, \Psi, \Gamma_2 \vdash \Theta$, для которого

$$D_1^* = \frac{D_1';\ D_1''}{\Gamma_1',\ \Phi,\ \Psi,\ \Gamma_2' \vdash \Theta',\ X_1\wedge X_2}.$$

Оставшиеся виды последнего существенного перехода в D рассматриваются аналогично. □

Лемма 3. *Если секвенции* $\Gamma \vdash \Theta, \Phi$ *и* $\Phi, \Gamma' \vdash \Theta'$ *доказуемы в* G_0, *то секвенция* $\Gamma, \Gamma' \vdash \Theta, \Theta'$ *доказуема в* G_0.

Доказательство. Существенным переходом в доказательстве D в виде дерева называется переход по правилам, отличным от правил перестановки 5) и 6).

Пусть Φ — атомарная формула. Будем доказывать лемму в этом случае индукцией по числу существенных переходов в доказательстве D секвенции $\Gamma \vdash \Theta, \Phi$. Если D не имеет существенных переходов, то $\Gamma \vdash \Theta, \Phi$ отличается от аксиом только перестановкой формул. Тогда либо $\Phi \in \Gamma$, либо $\Psi \in \Gamma$, $\Psi \in \Theta$ для некоторой атомарной Ψ. В первом случае доказуемость $\Gamma, \Gamma' \vdash \Theta, \Theta'$ следует из доказуемости $\Phi, \Gamma' \vdash \Theta$ и леммы 1. Во втором случае доказуемость $\Gamma, \Gamma' \vdash \Theta, \Theta'$ следует из аксиомы $\Psi \vdash \Psi$ с помощью леммы 1. Пусть доказательство D секвенции $\Gamma \vdash \Theta, \Phi$ имеет $n > 0$ существенных переходов. Пусть последний существенный переход в D является применением правила 1):

$$\frac{\Gamma_1 \vdash \Theta_1, \Phi, \Theta_2, \Psi; \Gamma_1 \vdash \Theta_1, \Phi, \Theta_2, X}{\Gamma_1 \vdash \Theta_1, \Phi, \Theta_2, \Psi \wedge X},$$

где последовательности Γ_1 и $\langle \Theta_1, \Phi, \Theta_2, \Psi \wedge X \rangle$ являются перестановками последовательностей Γ и $\langle \Theta, \Phi \rangle$. Из индукционного предположения, используя правила перестановки, получаем доказуемость секвенций $\Gamma, \Gamma' \vdash \Theta_1, \Theta_2, \Theta', \Psi$ и $\Gamma, \Gamma' \vdash \Theta_1, \Theta_2, \Theta', X$. Применяя правило 1) и правила перестановки, получаем доказуемость секвенции $\Gamma, \Gamma' \vdash \Theta, \Theta'$. Случаи применения других правил в последнем существенном переходе для атомарной Φ рассматриваются аналогично.

Продолжим доказательство леммы, применяя индукции по длине формулы Φ. Пусть $\Gamma \vdash \Theta, \Phi$ и $\Phi, \Gamma' \vdash \Theta'$ доказуемы в G_0.

Если $\Phi = \Psi \wedge X$, то по лемме 2 доказуемы секвенции $\Gamma \vdash \Theta, \Psi$; $\Gamma \vdash \Theta, X$ и $\Psi, X, \Gamma' \vdash \Theta'$. Из индукционного предположения получаем сначала доказуемость секвенций $\Gamma, X, \Gamma' \vdash \Theta, \Theta'$, а затем секвенции $\Gamma, \Gamma, \Gamma' \vdash \Theta, \Theta, \Theta'$. Доказуемость секвенции $\Gamma, \Gamma' \vdash \Theta, \Theta'$ получаем теперь с помощью структурных правил 5) — 8).

Если $\Phi = \neg\Psi$, то по лемме 2 доказуемы секвенции $\Psi, \Gamma \vdash \Theta$ и $\Gamma' \vdash \Theta', \Psi$. По индукционному предположению получаем доказуемость $\Gamma', \Gamma \vdash \Theta', \Theta$, а значит, и $\Gamma, \Gamma' \vdash \Theta, \Theta'$. □

Если Θ — последовательность $\Phi_1, \ldots, \Phi_n$ формул исчисления G_0, то через будем обозначать последовательность $\neg\Phi_1, \ldots, \neg\Phi_n$.

Лемма 4. *Если секвенция* $\Gamma \vdash \Theta$ *доказуема в* G_0, *то секвенция* $\neg\Theta, \Gamma \vdash$ *доказуема в ИВ.*

Доказательство проводим индукцией по высоте доказательства D секвенции $\Gamma \vdash \Theta$ в G_0. Предлагаем читателю применить свой опыт по доказательствам в исчислении ИВ, полученный при чтении предыдущих параграфов. □

Предложение 4. $ИВ^{(\to, \vee)} < G_0$.

Доказательство. Если в G_0 доказуема секвенция $\Gamma \vdash \Theta$, где Θ содержит не более одного члена, то из леммы 4 и предложения 3 следует доказуемость $\Gamma \vdash \Theta$ в $ИВ^{(\to, \vee)}$.

Рассмотрим секвенцию S, доказуемую в $ИВ^{(\to, \vee)}$. Индукцией по высоте доказательства D секвенции S в $ИВ^{(\to, \vee)}$ покажем доказуемость S в G_0.

Пусть D — аксиома $\Phi \vdash \Phi$ исчисления $ИВ^{(\to, \vee)}$. Если Φ — атомарная формула, то $\Phi \vdash \Phi$ — аксиома G_0. Если $\Phi = \Psi \wedge X$ и $\Psi \vdash \Psi$, $X \vdash X$ доказуемы в G_0, то по лемме 1 и правилам 1), 2) получаем доказуемость $\Phi \vdash \Phi$ в G_0. Если $\Phi = \neg\Psi$ и $\Psi \vdash \Psi$ доказуема в G, то по правилам 3), 4) и 6) получаем доказуемость в G_0 секвенции $\Phi \vdash \Phi$.

Пусть высота D равна $n > 0$ и для всех секвенций S', имеющих доказательство в $ИВ^{(\to, \vee)}$ с высотой $< n$, доказуемость S' в

G_0 установлена. Если последний переход в D осуществляется по правилам 1 или 11 исчисления ИВ, то доказуемость S в G_0 следует из индукционного предположения с помощью правил 1) и 6) исчисления G_0.

Если D имеет один из следующих видов:

$$\frac{\dfrac{D'}{\Gamma \vdash \Phi \wedge \Psi}}{\Gamma \vdash \Phi}, \quad \frac{\dfrac{D'}{\Gamma \vdash \Phi \wedge \Psi}}{\Gamma \vdash \Psi}, \quad \frac{\dfrac{D'}{\Gamma,\ \neg\Phi \vdash}}{\Gamma \vdash \Phi},$$

то доказуемость S в G_0 следует из индукционного предположения и леммы 2.

Если последний переход в D осуществляется по правилу 12 ИВ, то доказуемость S в G_0 следует из индукционного предположения и леммы 1.

Рассмотрим последний из возможных случаев, когда D имеет вид

$$\frac{\dfrac{D'}{\Gamma \vdash \Phi;} \quad \dfrac{D''}{\Gamma \vdash \neg\Phi}}{\Gamma \vdash}.$$

Из индукционного предположения и леммы 2 следует доказуемость в G_0 секвенций $\Gamma \vdash \Phi$ и $\Phi,\ \Gamma \vdash$. Применяя лемму 3 и правила 6), 8), получаем доказуемость в G_0 секвенции $\Gamma \vdash$. □

Исчисление G_0 является частью исчисления G, предложенного Генценом. Исчисления генценовского типа по сравнению с изученными нами исчислениями являются более удобными при анализе и поиске формальных доказательств. Это объясняется основной особенностью этих исчислений, которая, грубо говоря, состоит в том, что сложность формул при применении правил может только возрастать. Исчисление G будет подробно изучаться в главе 6. Здесь мы лишь применим отмеченное выше свойство исчисления G_0 для получения непротиворечивости ИВ, не прибегая к понятию интерпретации исчисления. В самом деле, рассмотрим секвенцию $\vdash Q_0$. Индукцией по высоте легко заметить, что если D — доказательство секвенции S в исчислении G_0 и существует вхождение формулы в D, содержащее логическую связку $\wedge$ или $\neg$, то эта логическая связка обязана входить в S. Поэтому, если секвенция $\vdash Q_0$ доказуема в G_0, то она может быть получена из аксиомы с помощью только правил 5) — 8), что очевидным образом невозможно. Следовательно, исчисление G_0 непротиворечиво. Применяя предложения 1, 3, 4, получаем непротиворечивость ИВ.

Упражнения

1. Показать, что ИВ$^{(\to,\wedge)} <$ ИВ, где ИВ$^{(\to,\wedge)}$ получено из ИВ$^{(\to)}$ удалением из алфавита символа $\wedge$ и соответствующих правил.

2. Используя теорему полноты для ИВ, показать, что ИВ$^{(\to,\vee,\neg)} <$ ИВ, где ИВ$^{(\to,\vee,\neg)}$ получается из ИВ$^{(\to,\vee)}$ удалением из алфавита символа $\neg$ и соответствующих правил.

Глава 2

ТЕОРИЯ МНОЖЕСТВ

§ 10. Предикаты и отображения

Все изучаемые в этой книге объекты являются множествами, хотя называются они по-разному: слова, символы, совокупности, числа, функции, формулы и др.

С интуитивной точки зрения, конечно, не все математические объекты суть множества, например, трудно думать о скобке и пропозициональной переменной как о множествах. Однако посредством подходящих соглашений (кодирования) их можно отождествить с множествами. В частности, скобку можно отождествить с множеством $\{\{\varnothing\}\}$. Этот метод является плодотворным, и в этой книге принимается такое соглашение*). В качестве аксиомы теории множеств мы принимаем *аксиому экстенсиональности*, которая утверждает, что два множества, имеющих одинаковые элементы, равны,— другими словами, любое множество определяется своими элементами.

Если $a_1, \ldots, a_n$ — все элементы множества A, то в силу аксиомы экстенсиональности множество A можно обозначать через $\{a_1, \ldots, a_n\}$. При этом не предполагается, что $a_1, \ldots, a_n$ попарно различны. Ясно, что одно и то же множество A может иметь много таких обозначений, например,

$$\{a, b, a\} = \{a, b, b\} = \{a, b\} = \{b, a\}.$$

Множества $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$ и т. д. (каждое последующее состоит из всех предыдущих) называются *натуральными числами* и обозначаются соответственно через 0, 1, 2 и т. д. Множество всех натуральных чисел обозначаем через ω. Слова $\alpha_1\alpha_2\ldots\alpha_n$ и конечные последовательности

*) Для некоторых объектов, с интуитивной точки зрения не являющихся множествами, мы фиксируем их кодировку через множества (например, для натуральных чисел), для других мы кодировку не уточняем, так как в наших рассуждениях она не участвует — важно лишь выделение этих объектов среди других множеств, встречающихся в книге.

$\alpha_1, \alpha_2, \ldots, \alpha_n$ будут отождествляться с *упорядоченным набором* $\langle\alpha_1, \ldots, \alpha_n\rangle$ элементов $\alpha_1, \ldots, \alpha_n$, который сейчас определим индукцией по n.

Определение. Упорядоченный набор $\langle\,\rangle$ пустого множества элементов равен $\varnothing$. Упорядоченный набор $\langle a\rangle$ одного элемента a равен a. Упорядоченный набор $\langle a, b\rangle$ двух элементов a и b называется упорядоченной парой и равен $\{\{a\}, \{a, b\}\}$. Если $n > 2$, то упорядоченный набор $\langle a_1, \ldots, a_n\rangle$ элементов $a_1, \ldots, a_n$ равен упорядоченной паре $\langle\langle a_1, \ldots, a_{n-1}\rangle, a_n\rangle$.

Упорядоченный набор $\langle a_1, \ldots, a_n\rangle$ иногда будем называть *кортежем*, а число n — длиной кортежа $\langle a_1, \ldots, a_n\rangle$, при этом длина пустого кортежа $\langle\,\rangle$ равна нулю. Кортеж длины $n > 2$ будем называть *упорядоченной n-кой* или просто n-кой (тройкой, четверкой и т. д.). Отождествление слов и последовательностей с упорядоченными наборами возможно в силу следующего предложения.

Предложение 1. *Если* $\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle$, *то* $a_1 = b_1, \ldots, a_n = b_n$.

Доказательство. Из определения упорядоченного набора следует, что достаточно доказать предложение для $n = 2$. Из условия $\langle a_1, a_2\rangle = \langle b_1, b_2\rangle$ и определения упорядоченной пары имеем $\{a_1\} \in \langle b_1, b_2\rangle$. Так как $\langle b_1, b_2\rangle = \{\{b_1\}, \{b_1, b_2\}\}$, то $\{a_1\} = \{b_1\}$ или $\{a_1\} = \{b_1, b_2\}$, поэтому $b_1 \in \{a_1\}$, т. е. $b_1 = a_1$. Легко заметить, что если $\{x, y\} = \{x, z\}$, то $y = z$. Тогда из установленного равенства $\{\{a_1\}, \{a_1, a_2\}\} = \{\{a_1\}, \{a_1, b_2\}\}$ получаем сначала $\{a_1, a_2\} = \{a_1, b_2\}$, а затем $a_2 = b_2$. □

Определение. а) Множество $\{\langle a_0, \ldots, a_n\rangle \mid a_0 \in A_0, \ldots, a_n \in A_n\}$ называется *декартовым произведением* множеств $A_0, \ldots, A_n$ и обозначается через $A_0 \times \ldots \times A_n$. Если $X \subseteq A_0 \times \ldots \times A_n$, то множество всех $a \in A_i$, для которых существуют такие $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$, что $\langle a_0, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_n\rangle \in X$, называется проекцией X и обозначается через $\pi_i^n X$.

б) Если $A_1 = \ldots = A_n = A$, то $A_1 \times \ldots \times A_n$ называется декартовой n-степенью множества A и обозначается через A^n. Если $n = 0$, то по определению полагаем $A^0 = \{\varnothing\}$.

в) Подмножества $B \subseteq A^n$ будут называться *n-местными отношениями* или *предикатами* на A. Будем говорить, что B — n-местное отношение или предикат, если B является n-местным отношением на A для некоторого множества A.

г) Если B — двухместное отношение, то двухместное отношение $\{\langle a, b\rangle | \langle b, a\rangle \in B\}$ будем называть *обратным* к B и обозначать через B^{-1}.

д) Если B, C — два двухместных отношения, то двухместное отношение

$$\{\langle a, c\rangle | \langle a, b\rangle \in B \quad \text{и} \quad \langle b, c\rangle \in C \text{ для некоторого } b\}$$

будем называть *композицией* или *произведением* двухместных отношений B, C и обозначать через (BC) или $B \cdot C$.

Так как $\langle a\rangle = a$, то $A^1 = A$, поэтому подмножества A будут одноместными предикатами на A.

Заметим, что 0-местных предикатов только два: $\varnothing$ и $\{\varnothing\}$. Из определения B^{-1} сразу следует равенство $B = (B^{-1})^{-1}$.

Предложение 2. *Если B, C и D — двухместные предикаты, то*

а) $((BC)D) = (B(CD))$,

б) $(BC)^{-1} = (C^{-1}B^{-1})$.

Доказательство а). Пусть $\langle x, y\rangle \in ((BC)D)$. Тогда для некоторых u и v имеем $\langle x, u\rangle \in B$, $\langle u, v\rangle \in C$ и $\langle v, y\rangle \in D$. Таким образом, $\langle u, y\rangle \in (CD)$ и $\langle x, y\rangle \in (B(CD))$. Включение $(B(CD)) \subseteq ((BC)D)$ доказывается аналогично. Доказательство б) оставляется читателю. □

Ассоциативность композиции, доказанная в предложении 2, позволяет обозначать композицию $((BC)D) = (B(CD))$ через (BCD). По этой же причине однозначно определена композиция n предикатов $(B_1 \ldots B_n)$. Отметим, что коммутативность $(BC) = (CB)$ для произведения предикатов не имеет места (приведите пример).

Определение. Двухместное отношение U на множестве A называется

а) *диагональю* A^2 и обозначается через id_A, если $U = \{\langle a, a\rangle | a \in A\}$;

б) *рефлексивным* на A, если $\mathrm{id}_A \subseteq U$;

в) *симметричным*, если $U = U^{-1}$;

г) *транзитивным*, если $(UU) \subseteq U$;

д) *эквивалентностью* на A, если U рефлексивно, симметрично и транзитивно;

е) *антисимметричным*, если $U \cap U^{-1} \subseteq \mathrm{id}_A$.

Например, предикат

$\{\langle m, n\rangle | m$ и n — взаимно простые натуральные числа$\}$ является симметричным, но не рефлексивным и не транзитивным на ω, а предикат $\{\langle m, n\rangle | (n - m) > 0,\ n, m \in \omega\}$

является транзитивным на ω, но не симметричным и не рефлексивным на ω.

Если U — n-местное отношение на A и $B \subseteq A$, то отношение $U \cap B^n$ на множестве B будем называть *ограничением отношения U на множество B*. Очевидно, что ограничения отношений типов а) — е) из предыдущего определения на любое $B \subseteq A$ будут также отношениями соответствующих типов а) — е).

Пример 1. Говорим, что $R = \{A_i | i \in I\}$ является разбиением множества A, если $\bigcup\limits_{i \in I} A_i = A$ и для любых $i, j \in I$ либо $A_i = A_j$, либо $A_i \cap A_j = \varnothing$. Пусть $R = \{A_i | i \in I\}$ — разбиение множества A. Определим следующее двухместное отношение на A:

$$E_R = \{\langle a, b\rangle | a, b \in A_i \text{ для некоторого } i \in I\}.$$

Очевидно, что E_R будет эквивалентностью на A.

Если E — эквивалентность на множестве A, то множества $E_x = \{a | \langle a, x\rangle \in E\}$ для $x \in A$ будем называть *классами эквивалентности* по отношению E.

Легко показать, что любую эквивалентность на множестве A можно получить способом, указанным в примере 1. В самом деле, пусть E — эквивалентность на A и $R_E = \{E_x | x \in A\}$. Из рефлексивности E получаем $x \in E_x$, следовательно, $\bigcup\limits_{x \in A} E_x = A$. Из симметричности и транзитивности E следует, что если $\langle x, y\rangle \in E$, то $E_x = E_y$, а если $\langle x, y\rangle \notin E$, то $E_x \cap E_y = \varnothing$. Таким образом, множество R_E классов эквивалентности по E является разбиением A и $E_{R_E} = E$.

Определение. а) Двухместное отношение f называется *отображением* или *функцией*, если для любых a, b, c из $\langle a, b\rangle \in f$ и $\langle a, c\rangle \in f$ следует $b = c$. Если f — отображение, то множество $\pi_1^2 f$ называется *областью определения* f и обозначается $\operatorname{dom} f$, а множество $\pi_2^2 f$ называется *областью значений* f и обозначается $\operatorname{rang} f$.

б) Отображение f называется *разнозначным*, если f^{-1} также является отображением.

в) Отображение f называется отображением A *в* B, если $\operatorname{dom} f = A$ и $\operatorname{rang} f \subseteq B$.

г) Отображение f называется отображением A *на* B, если $\operatorname{dom} f = A$ и $\operatorname{rang} f = B$.

д) Отображение f множества A^n в A называется *n-местной операцией* на A.

Очевидно, что диагональ id_A множества A^2 будет разнозначной одноместной операцией на A. Диагональ id_A множества A^2 в дальнейшем будем называть также тождественной операцией на A.

Запись $f\colon A \to B$ будет в дальнейшем обозначать, что f — отображение A в B, а запись $f\colon A \twoheadrightarrow B$ будет обозначать, что f — отображение A на B.

Предложение 3. а) *Если* $f\colon A \to B$ *и* $g\colon B \to C$, *то* $(fg)\colon A \to C$.

б) *Если* $f\colon A \twoheadrightarrow B$ *и* $g\colon B \twoheadrightarrow C$, *то* $(fg)\colon A \twoheadrightarrow C$.

в) *Если* f — *разнозначное отображение* A *на* B, *то* f^{-1} — *разнозначное отображение* B *на* A, $f \cdot f^{-1} = \mathrm{id}_A$ *и* $f^{-1} \cdot f = \mathrm{id}_B$.

г) *Если* f *и* g — *разнозначные отображения, то* $f \cdot g$ *также разнозначно и* $(fg)^{-1} = (g^{-1}f^{-1})$.

Доказательство этого предложения оставляется читателю в качестве упражнения. □

Если f — отображение и $\langle a, b\rangle \in f$, то b называется *значением* f *на элементе* a и обозначается через $f(a)$ или fa.

Если f — отображение и $A \subseteq \mathrm{dom}\, f$, то множество $\{fa \mid a \in A\}$ называется *образом множества* A *при отображении* f и обозначается через $f[A]$, а отображение $f \cap (A \times \mathrm{rang}\, f)$ называется *ограничением* f *на* A и обозначается через $f \restriction A$.

Ясно, что n-местная операция является $(n+1)$-местным отношением, а 0-местная операция $f\colon A^0 \to A$ есть $\{\langle \varnothing, a\rangle\}$ для некоторого $a \in A$. Часто 0-местную операцию $\{\langle \varnothing, a\rangle\}$ на A будем называть константой на A и отождествлять с элементом a.

Если f — n-местная операция на A, то условие $\langle a_1, \ldots, a_n, b\rangle \in f$ будем записывать так: $f(a_1, \ldots, a_n) = b$. Для $n = 0$ это будет $f(\,) = b$, т. е. $f = b$, что согласуется с принятым нами отождествлением константы с ее значением.

Если f — n-местная операция на A и $B \subseteq A$, то множество B называется *замкнутым относительно операции* f, если из $a_1, \ldots, a_n \in B$ следует $f(a_1, \ldots, a_n) \in B$.

Упражнения

1. Пусть U — транзитивное двухместное отношение на множестве A, $\langle a, a\rangle \notin U$ для любого a и для любого $a \in A$существует такое b, что $\langle a, b\rangle \in U$. Показать, что A бесконечно.

2. Доказать предложение 3.

3. Если $f\colon A \to B$, $g\colon B \twoheadrightarrow A$ и $(gf) = \mathrm{id}_B$, то f разнозначно и $g = f^{-1}$.

§ 11. Частично упорядоченные множества

Среди различных типов отношений некоторые имеют фундаментальное значение не только для математической логики, но и для всей математики. В предыдущем параграфе мы уже рассматривали одно из таких отношений — эквивалентность. Определим еще два очень важных типа отношений.

Определение. а) Отношение U на множестве A называется *частичным порядком на* A, если оно рефлексивно, транзитивно и антисимметрично.

б) Частичный порядок U на A называется *линейным порядком на* A, если для любых a, $b \in A$ выполняется хотя бы одно из следующих двух условий: $\langle a, b\rangle \in U$, $\langle b, a\rangle \in U$.

Очевидно, что ограничение частичного (линейного) порядка на A на любое подмножество $B \subseteq A$ будет частичным (линейным) порядком на B.

Важным примером частичного порядка на множестве A является отношение $\{\langle a, b\rangle | a, b \in A, a \subseteq b\}$, а примером линейного порядка — отношение $\{\langle a, b\rangle | a, b \in X, a \leqslant b\}$, где X — некоторое подмножество действительных чисел.

Определение. а) Если U — частичный порядок на A, то пару $\mathfrak{A} = \langle A, U\rangle$ назовем *частично упорядоченным множеством* (сокращенно ч. у. м.).

б) Если U — линейный порядок на A, то пару $\mathfrak{A} = \langle A, U\rangle$ назовем *линейно упорядоченным множеством*.

Пусть $\mathfrak{A} = \langle A, U\rangle$ — частично упорядоченное множество. Элемент $a_0 \in A$ называется *верхней* (*нижней*) *гранью* в $\mathfrak{A}$ подмножества $A_0 \subseteq A$, если $\langle b, a_0\rangle \in U$ ($\langle a_0, b\rangle \in U$) для всех $b \in A_0$. Верхняя (нижняя) в $\mathfrak{A}$ грань A называется *наибольшим* (*наименьшим*) в $\mathfrak{A}$ элементом. Элемент $a \in A$ называется *максимальным* (*минимальным*) в $\mathfrak{A}$, если из $\langle a, x\rangle \in U$ (соответственно из $\langle x, a\rangle \in U$) следует $x = a$. Ясно, что наибольший (наименьший) элемент является максимальным (минимальным), и если U — линейный порядок, то максимальный (минимальный) в $\mathfrak{A}$ элемент является также наибольшим (наименьшим) в $\mathfrak{A}$. Очевидно, что если наибольший (наименьший) в $\mathfrak{A}$ элемент существует, то все максимальные (минимальные) элементы равны между собой.

Если B — множество верхних граней в $\mathfrak{A} = \langle A, U\rangle$ множества $A_1 \subseteq A$, то наименьший в $\langle B, U \cap B^2\rangle$ элемент называется *наименьшей верхней гранью* (сокращенно н. в. г.) в $\mathfrak{A}$ множества A_1 и обозначается через $\sup(A_1, \mathfrak{A})$. Заменив в предыдущем определении слова «верхних» и «наименьший» соответственно на слова «нижних» и «наибольший», получим определение *наибольшей нижней грани* (сокращенно н. н. г.) A_1 в $\mathfrak{A}$, которую будем обозначать через $\inf(A_1, \mathfrak{A})$. Ясно, что $\sup(A_1, \mathfrak{A})$ и $\inf(A_1, \mathfrak{A})$ определяются по A_1 и $\mathfrak{A}$ однозначно, если они существуют.

Определение. Частично упорядоченное множество $\mathfrak{A} = \langle A, U\rangle$ называется *решеткой*, если для любых $a, b \in A$ в $\mathfrak{A}$ существуют $\sup(\{a, b\}, \mathfrak{A})$ и $\inf(\{a, b\}, \mathfrak{A})$, которые будут обозначаться через $a \cup^{\mathfrak{A}} b$ и $a \cap^{\mathfrak{A}} b$. Решетка $\mathfrak{A} = \langle A, U\rangle$ называется *дистрибутивной*, если для любых $a, b, c \in A$ операции $\cup^{\mathfrak{A}}$ и $\cap^{\mathfrak{A}}$ удовлетворяют следующим условиям:

D) $a \cup^{\mathfrak{A}} (b \cap^{\mathfrak{A}} c) = (a \cup^{\mathfrak{A}} b) \cap^{\mathfrak{A}} (a \cup^{\mathfrak{A}} c)$;

D′) $a \cap^{\mathfrak{A}} (b \cup^{\mathfrak{A}} c) = (a \cap^{\mathfrak{A}} b) \cup^{\mathfrak{A}} (a \cap^{\mathfrak{A}} c)$.

Решетка $\mathfrak{A} = \langle A, U\rangle$ называется *булевой решеткой*, если $\mathfrak{A}$ дистрибутивна, имеет наибольший элемент $1^{\mathfrak{A}}$, наименьший элемент $0^{\mathfrak{A}}$ и для любого $a \in A$ существует такой элемент $\bar{a} \in A$, что $\bar{a} \cup^{\mathfrak{A}} a = 1^{\mathfrak{A}}$ и $\bar{a} \cap^{\mathfrak{A}} a = 0^{\mathfrak{A}}$. Элемент $\bar{a}$, удовлетворяющий в решетке $\mathfrak{A}$ с наибольшим элементом $1^{\mathfrak{A}}$ и наименьшим элементом $0^{\mathfrak{A}}$ указанным условиям, называется *дополнением элемента a* в $\mathfrak{A}$.

Предложение 1. а) *Если дополнение $\bar{a}$ элемента a в дистрибутивной решетке $\mathfrak{A}$ с наибольшим и наименьшим элементами существует, то оно единственно.*

б) *Если $\mathfrak{A} = \langle A, U\rangle$ — булева решетка, то для любых $a, b, c \in A$ операции $\cup^{\mathfrak{A}}$, $\cap^{\mathfrak{A}}$ и $^-$, определенные выше, удовлетворяют следующим условиям (для простоты индекс $\mathfrak{A}$ у $\cup^{\mathfrak{A}}$ и $\cap^{\mathfrak{A}}$ опущен):*

1) $a \cup b = b \cup a$,	4) $a \cap (b \cap c) = (a \cap b) \cap c$,
2) $a \cap b = b \cap a$,	5) $(a \cap b) \cup b = b$,
3) $a \cup (b \cup c) = (a \cup b) \cup c$,	6) $(a \cup b) \cap b = b$,

7) $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$, 9) $(a \cap \bar{a}) \cup b = b$,

8) $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$, 10) $(a \cup \bar{a}) \cap b = b$.

в) *Если на множестве A заданы три операции $\cup$, $\cap$ и $^-$, удовлетворяющие для любых a, b, $c \in A$ условиям 1)—10) утверждения б) (где $\cup(a, b)$, $\cap(a, b)$ и $^-(a)$ пишутся как $a \cup b$, $a \cap b$ и $\bar{a}$), то пара $\mathfrak{A} = \langle A, U\rangle$ для $U = \{\langle a, b\rangle | a \cap b = a\}$ является булевой решеткой, причем $a \cup b = \sup(\{a, b\}, \mathfrak{A})$, $a \cap b = \inf(\{a, b\}, \mathfrak{A})$, $\bar{a} \cup a = 1^{\mathfrak{A}}$, $\bar{a} \cap a = 0^{\mathfrak{A}}$.*

Доказательство. а) Для простоты будем опускать индекс $\mathfrak{A}$ у $\cup^{\mathfrak{A}}$, $\cap^{\mathfrak{A}}$, $1^{\mathfrak{A}}$ и $0^{\mathfrak{A}}$. Если $a \cup a_1 = 1$ и $a \cap a_2 = 0$, то

$$a_1 = a_1 \cup 0 = a_1 \cup (a \cap a_2) = (a_1 \cup a) \cap (a_1 \cup a_2) = 1 \cap (a_1 \cup a_2) = a_1 \cup a_2.$$

Аналогично из $a \cap a_1 = 0$ и $a \cup a_2 = 1$ получаем $a_2 = a_2 \cup a_1$, следовательно, $a_1 = a_2$.

б) Свойства 1) и 2) очевидны. Так как $a \cap \bar{a} = 0^{\mathfrak{A}}$ и $a \cup \bar{a} = 1^{\mathfrak{A}}$, то выполняются 9) и 10). Так как $\mathfrak{A}$ дистрибутивна, то выполняются 7) и 8). В дальнейшем условие $\langle a, b\rangle \in U$ будем обозначать через $a \leqslant b$. Из определения операций $\cup^{\mathfrak{A}}$ и $\cap^{\mathfrak{A}}$ получаем, что для любых d, $m_1, m_2 \in A$

(1) $d \leqslant m_1 \cap m_2 \Leftrightarrow (d \leqslant m_1$ и $d \leqslant m_2)$,

(2) $m_1 \cup m_2 \leqslant d \Leftrightarrow (m_1 \leqslant d$ и $m_2 \leqslant d)$,

(3) $m_1, m_2 \leqslant m_1 \cup m_2$,

(4) $m_1 \cap m_2 \leqslant m_1, m_2$.

Пользуясь этими фактами, легко установить свойства 3)—6). Проверим, например, свойство 6), оставляя проверку 3)—5) читателю. Из (4) получаем $(a \cup b) \cap b \leqslant b$, а из (3) и (1) получаем $b \leqslant (a \cup b) \cap b$, следовательно, из антисимметричности U получаем 6).

в) Из условий 5), 6), 1) и 2) получаем

$$a \cap b = a \Leftrightarrow a \cup b = b. \qquad (*)$$

Покажем сначала, что $U = \{\langle a, b\rangle | a \cap b = a\}$ — частичный порядок. Подставив в 7) вместо b элемент a, а вместо c — элемент $\bar{a}$ и воспользовавшись условиями 2), 1), 6) и 9), получаем $a = a \cap a$, следовательно, U рефлексивно. Пусть $a \cap b = a$ и $b \cap c = b$. Из (*), 7), 5), 1) и 2) получаем

$$\cap c = a \cap (b \cup c) = (a \cap b) \cup (a \cap c) = a \cup (a \cap c) = a,$$

следовательно, U транзитивно. Пусть $a \cap b = a$ и $b \cap a = b$, тогда из 2) получаем $a = b$, т. е. U антисимметрично. Для завершения доказательства нужно показать, что $a \cup b = \sup(\{a, b\}, \mathfrak{A})$ и $a \cap b = \inf(\{a, b\}, \mathfrak{A})$. Докажем первое из этих равенств, оставляя проверку второго читателю. Из

$$a \cap (a \cup b) = (a \cap a) \cup (a \cap b) = a \cup (a \cap b) = a$$

и $a \cup b = b \cup a$ получаем, что $a \cup b$ — верхняя грань множества $\{a, b\}$. Пусть c — верхняя грань $\{a, b\}$, т. е. $a \cap c = a$ и $b \cap c = b$. Тогда

$$(a \cup b) \cap c = c \cap (a \cup b) = (c \cap a) \cup (c \cap b) = a \cup b,$$

т. е. $\langle a \cup b, c\rangle \in U$. □

Условия 1)—10) из предложения 1 называются аксиомами булевых алгебр, а множество A вместе с определенными на нем операциями $\cap$, $\cup$, $^-$, удовлетворяющими аксиомам 1)—10), называется *булевой алгеброй*. Если $\mathfrak{A} = \langle A, \cup, \cap, ^-\rangle$ — булева алгебра, то через $\leqslant$ будет обозначаться частичный порядок на A, определенный условием

$$a \leqslant b \Leftrightarrow a \cap b = a.$$

Из предложеия 1 следует, что булева алгебра $\mathfrak{A}$ определяется отношением $\leqslant$ однозначно.

Примеры. 1) Если $A \subseteq P(B)$ и множество A замкнуто относительно операций объединения и пересечения, то легко проверить, что $\mathfrak{A} = \langle A, \subseteq\rangle$, где $\subseteq$ — отношение включения на A, является дистрибутивной решеткой, причем $\bigcup^{\mathfrak{A}}$ и $\bigcap^{\mathfrak{A}}$ являются операциями объединения и пересечения на A.

2) Если в примере 1) множество A замкнуто относительно операции взятия дополнения в B (т. е. операции $\bar{a} = B \setminus a$), то $\mathfrak{A} = \langle A, \subseteq\rangle$ является булевой решеткой, а $\langle A, \cup, \cap, ^-\rangle$ — булевой алгеброй, где $\cup$, $\cap$, $^-$ — операции объединения, пересечения и дополнения в B. В частности, если $A = P(B)$, то $\langle P(B), \cup, \cap, ^-\rangle$ будет называться *булевой алгеброй всех подмножеств* B и для простоты будет иметь то же обозначение $P(B)$, что и множество всех подмножеств B.

Определение. Частично упорядоченное множество $\mathfrak{A} = \langle A, U\rangle$ называется *фундированным*, если для любого непустого подмножества $A_1 \subseteq A$ ч. у. м. $\mathfrak{A}_1 = \langle A_1, U \cap A_1^2\rangle$ имеет минимальный элемент.

Если $\langle A, U\rangle$ — фундированное частично упорядоченное множество, то очевидно, что $\langle B, U \cap B^2\rangle$ также будет фундированным частично упорядоченным множеством для любого $B \subseteq A$.

На фундированное частично упорядоченное множество можно обобщить метод математической индукции.

Предложение 2 (принцип трансфинитной индукции). *Пусть* $\mathfrak{A} = \langle A, U\rangle$ — *фундированное частично упорядоченное множество и* $B \subseteq A$. *Если для любого* $a \in A$ *из* $\{b \in A \mid \langle b, a\rangle \in U,\ b \neq a\} \subseteq B$ *следует* $a \in B$, то $B = A$.

Доказательство. Предположим, что $B \neq A$, и пусть a_0 — минимальный элемент ч. у. м. $\langle A \setminus B, U \cap \cap (A \setminus B)^2\rangle$. Тогда $\{b \in A \mid \langle b, a_0\rangle \in U,\ b \neq a_0\} \subseteq B$ и по условию имеем $a_0 \in B$, что невозможно. □

Определение. Пусть $\mathfrak{A} = \langle A, U\rangle$ — линейно упорядоченное множество. Множество $X \subseteq A$ будем называть

а) *начальным сегментом* $\mathfrak{A}$, если для любых $a, b \in A$ из $a \in X$ и $\langle b, a\rangle \in U$ следует $b \in X$;

б) *замкнутым начальным сегментом, если* для некоторого $a_0 \in A$ X равно множеству $O[a_0, \mathfrak{A}] = \{b \mid \langle b, a_0\rangle \in U\}$;

в) *открытым начальным сегментом*, если X равно множеству $O(a_0, \mathfrak{A}) = (O[a_0, \mathfrak{A}] \setminus \{a_0\})$ для некоторого $a_0 \in A$.

Часто, когда ясно, о каком $\mathfrak{A}$ идет речь, мы будем писать $O[a_0]$ и $O(a_0)$ вместо $O[a_0, \mathfrak{A}]$ и $O(a_0, \mathfrak{A})$ соответственно. Заметим, что пустое множество $\varnothing$ является начальным сегментом любого линейно упорядоченного множества. Очевидно, что элемент a_0 в б) и в) предыдущего определения определен по X однозначно.

Примеры. Пусть G — отношение «меньше или равно» на действительных числах (т. е. $\langle a, b\rangle \in G \leftrightarrow a \leqslant b$).

1. В линейно упорядоченном множестве $\langle \omega, G \cap \omega^2\rangle$ любой отличный от ω начальный сегмент является одновременно и открытым и замкнутым.

2. В $\langle R, G\rangle$, где R — множество всех действительных чисел, любой отличный от R начальный сегмент является открытым или замкнутым, но никакой начальный сегмент $\langle R, G\rangle$ не является одновременно открытым и замкнутым.

3. В $\langle Q, G \cap Q^2\rangle$, где Q — множество всех рациональных чисел, начальный сегмент $\{r \mid r \leq \sqrt{2}\}$ не является ни открытым, ни замкнутым.

Определение. Если $\mathfrak{A} = \langle A, U\rangle$ — фундированное линейное упорядоченное множество, то $\mathfrak{A}$ называется *вполне упорядоченным множеством.* Если $\mathfrak{A} = \langle A, U\rangle$ — ч. у. м., $X \subseteq A$ и $U \cap X^2$ — линейный порядок на X, то X называется *цепью в* $\mathfrak{A}$. В частности, пустое множество является цепью в любом ч. у. м.

В § 10 была сформулирована одна аксиома теории множеств, которой мы уже пользовались,— это аксиома экстенсиональности. Впредь мы будем использовать также *аксиому выбора*, утверждающую что для любого непустого множества A существует такое отображение (функция выбора) h: $(P(A)\setminus\{\varnothing\})\to A$, что $h(B)\in B$ для любого непустого $B\subseteq A$. Из этой аксиомы вытекают следующие два важных принципа.

Теорема 1 (принцип максимума). *Если в частично упорядоченном множестве $\mathfrak{A}=\langle A, U\rangle$ каждая цепь $X\subseteq A$ имеет верхнюю грань, то существует максимальный в $\mathfrak{A}$ элемент.*

Доказательство. Рассмотрим множество $Y=\{X\subseteq A|X$ — цепь в $\mathfrak{A}\}$ и для $X\in Y$ множество $B(X)=\{a\in A|a$ — верхняя грань X в $\mathfrak{A}\}$. Предположим, что $\mathfrak{A}$ не имеет максимальных элементов. Тогда семейство $S=\{B(X)\setminus X|X\in Y\}$ состоит из непустых подмножеств A. Из аксиомы выбора получаем, что существует такое отображение h множества Y в A, что $h(X)\in(B(X)\setminus X)$ для всех $X\in Y$. В дальнейшем начальный сегмент линейно упорядоченного множества $\langle X, U\cap X^2\rangle$ будем называть начальным сегментом X. Рассмотрим множество $Z\subseteq Y$ всех непустых цепей X в $\mathfrak{A}$, удовлетворяющих следующему условию: $h(X_1)=\inf(X\setminus X_1, \langle X, U\cap X^2\rangle)$ для любого начального сегмента $X_1\subseteq X$, $X_1\neq X$. Очевидно, что $\{h(\varnothing)\}\in Z$. Пусть X_1, $X_2\in Z$. Так как $h(\varnothing)$ — наименьший элемент в $\langle X_1, U\cap X_1^2\rangle$ и $\langle X_2, U\cap X_2^2\rangle$, то X_1 и X_2 имеют общие непустые начальные сегменты. Пусть C — объединение общих начальных сегментов X_1 и X_2. Ясно, что C — начальный сегмент X_1 и X_2. Тогда $C=X_1$ или $C=X_2$, так как в противном случае $C\cup\{h(C)\}\neq C$ было бы общим начальным сегментом X_1 и X_2, что противоречит определению C. Таким образом, для любых X_1, $X_2\in Z$ или $X_1\subseteq X_2$, или $X_2\subseteq X_1$. Следовательно, $C^*=\bigcup\limits_{X\in Z}X$ будет цепью в $\mathfrak{A}$ и $C^*\cup\{h(C^*)\}\in Z$, что противоречит определению C^* и условию $h(C^*)\in B(C^*)\setminus C^*$. □

Теорема 2 (принцип полного упорядочения). *Каждое множество A может быть вполне упорядочено, т. е. для каждого множества A существует $U\subseteq A^2$, для которого $\mathfrak{A}=\langle A, U\rangle$ — вполне упорядоченное множество.*

Доказательство. Рассмотрим множество $W=\{\langle X, U\rangle|\langle X, U\rangle$ — вполне упорядоченное множество, $X\subseteq A\}$.

Определим на множестве W порядок $\preccurlyeq$:

$$\langle X_1, U_1\rangle \preccurlyeq \langle X_2, U_2\rangle \Leftrightarrow U_1 \subseteq U_2 \text{ и } X_1 \text{ — начальный сегмент } \langle X_2, U_2\rangle.$$

Пусть $\{\langle X_i, U_i\rangle \mid i \in I\}$ — цепь в $\langle W, \preccurlyeq\rangle$. Очевидно, что $\mathfrak{A} = \left\langle \bigcup_{i\in I} X_i, \bigcup_{i\in I} U_i\right\rangle$ является линейно упорядоченным множеством. Пусть $Y \subseteq \bigcup_{i\in I} X_i$ и $Y \neq \varnothing$. Тогда $Y \cap X_{i_0} \neq \varnothing$ для некоторого $i_0 \in I$. Так как $\langle X_{i_0}, U_{i_0}\rangle$ — вполне упорядоченное множество, то $\langle Y \cap X_{i_0}, U_{i_0} \cap Y^2\rangle$ имеет минимальный элемент y_0. Так как X_{i_0} — начальный сегмент $\mathfrak{A}$, то y_0 — минимальный элемент $\left\langle Y, \left(\bigcup_{i\in I} U_i\right) \cap Y^2\right\rangle$. Таким образом, $\mathfrak{A} \in W$. Ясно, что $\mathfrak{A}$ является верхней гранью для цепи $\{\langle X_i, U_i\rangle \mid i \in I\}$ в $\langle W, \preccurlyeq\rangle$. Поэтому по теореме 1 $\langle W, \preccurlyeq\rangle$ имеет максимальный элемент $\langle A_0, U_0\rangle$. Если существует $a_0 \in A \setminus A_0$, то $\langle A_0 \cup \{a_0\}, U_1\rangle \in W$, где $U_1 = U_0 \cup \cup \{\langle a, a_0\rangle \mid a \in A_0\} \cup \{\langle a_0, a_0\rangle\}$, что противоречит максимальности $\langle A_0, U_0\rangle$ в $\langle W, \preccurlyeq\rangle$. Таким образом, $\langle A, U_0\rangle$ — вполне упорядоченное множество. □

Определение. Пусть $\mathfrak{A} = \langle A, U\rangle$ и $\mathfrak{B} = \langle B, V\rangle$ — два линейно упорядоченных множества. Отображение $f\colon A \twoheadrightarrow B$ назовем *подобием* $\mathfrak{A}$ на $\mathfrak{B}$, если

$$\langle a, b\rangle \in U \Leftrightarrow \langle fa, fb\rangle \in V. \tag{1}$$

Будем говорить, что $\mathfrak{A}$ и $\mathfrak{B}$ *подобны*, если существует подобие одного из них на другое.

Заметим, что подобие $f\colon A \twoheadrightarrow B$ разнозначно. В самом деле, если $fa = fb$, то из рефлексивности V и (1) получаем $\langle a, b\rangle \in U$ и $\langle b, a\rangle \in U$, следовательно, из антисимметричности U получаем $a = b$. Если f — подобие $\mathfrak{A}$ на $\mathfrak{B}$, то очевидно, что f^{-1} — подобие $\mathfrak{B}$ на $\mathfrak{A}$.

Предложение 3. *Если f — подобие линейно упорядоченного множества $\mathfrak{A}$ на линейно упорядоченное множество $\mathfrak{B}$ и X — (открытый, замкнутый) начальный сегмент $\mathfrak{A}$, то $f(X)$ — (открытый, замкнутый) начальный сегмент $\mathfrak{B}$.*

Доказательство оставляется читателю в качестве легкого упражнения. □

В оставшейся части параграфа мы докажем важные свойства вполне упорядоченных множеств.

Предложение 4. *Любой начальный сегмент X вполне упорядоченного множества $\mathfrak{A} = \langle A, U\rangle$, отличный от A, является открытым.*

Доказательство. Очевидно, что $X = O(a_0, \mathfrak{A})$, где a_0 — минимальный элемент множества $A \setminus X$. □

Если X и Y — начальные сегменты линейно упорядоченных множеств $\mathfrak{A} = \langle A, U\rangle$ и $\mathfrak{B} = \langle B, V\rangle$ соответственно и $\langle X, U \cap X^2\rangle$ подобно $\langle Y, V \cap Y^2\rangle$, то в дальнейшем будем говорить просто, что X подобно Y.

Предложение 5. *Если $f: A \to B$ и $g: A \to B$ — два подобия вполне упорядоченного множества $\mathfrak{A} = \langle A, U\rangle$ на некоторые начальные сегменты линейно упорядоченного множества $\mathfrak{B} = \langle B, V\rangle$, то $f = g$.*

Доказательство. Рассмотрим множество $Q = \{a \in A \mid fa = ga\}$. Если $O(b, \mathfrak{A}) \subseteq Q$, то $fb = \inf(B \setminus g[O(b, \mathfrak{A})], \mathfrak{B})$, следовательно, $fb = gb$. По предложению 2 имеем $Q = A$, и предложение 5 доказано. □

Предложение 6. *Никакие два различных начальных сегмента вполне упорядоченного множества $\mathfrak{A}$ не подобны между собой.*

Доказательство. Пусть f — подобие начального сегмента X на начальный сегмент Y. Так как id_X является подобием X на X, то по предложению 5 $f = \mathrm{id}_X$, следовательно, $X = Y$. □

Теорема 3. *Если $\mathfrak{A} = \langle A, U\rangle$ и $\mathfrak{B} = \langle B, V\rangle$ — вполне упорядоченные множества, то либо $\mathfrak{A}$ подобно начальному сегменту $\mathfrak{B}$, либо $\mathfrak{B}$ подобно начальному сегменту $\mathfrak{A}$.*

Доказательство. Рассмотрим множество $P = \{f \mid f$ — подобие некоторого начального сегмента $\mathfrak{A}$ на начальный сегмент $\mathfrak{B}\}$.

В силу предложений 3 и 5 для любых $f, g \in P$ либо $f \subseteq g$, либо $g \subseteq f$. Поэтому $F = \bigcup\limits_{f \in P} f$ будет подобием начального сегмента X множества $\mathfrak{A}$ на начальный сегмент Y множества $\mathfrak{B}$. Если $X = A$ или $Y = B$, то все доказано. Предположим, что это не так. Тогда по предложению 4 $X = O(a_0, \mathfrak{A})$ и $Y = O(b_0, \mathfrak{B})$. Очевидно, что $F \cup \{\langle a_0, b_0\rangle\}$ будет тогда подобием начального сегмента $O[a_0, \mathfrak{A}]$ на начальный сегмент $O[b_0, \mathfrak{B}]$, следовательно, $F \cup \{\langle a_0, b_0\rangle\} \subseteq F$, что невозможно. □

Упражнения

1. Показать, что если $\mathfrak{A} = \langle A, U\rangle$ — ч. у. м. с наименьшим элементом, A конечно и для любых $a, b \in A$ существует $\sup(\{a, b\}, \mathfrak{A})$, то $\mathfrak{A}$ — решетка.

2. Пусть $\mathfrak{A} = \langle A, \cup, \cap, ^-\rangle$ — булева алгебра и A содержит более одного элемента. Отображение γ множества F формул ИВ в A,

обладающее свойствами:

1) $\gamma(\Phi \vee \Psi) = \gamma(\Phi) \cup \gamma(\Psi)$, 3) $\gamma(\Phi \to \Psi) = \overline{\gamma(\Phi)} \cup \gamma(\Psi)$,
2) $\gamma(\Phi \wedge \Psi) = \gamma(\Phi) \cap \gamma(\Psi)$, 4) $\gamma(\neg \Phi) = \overline{\gamma(\Phi)}$,

называется интерпретацией ИВ в $\mathfrak{A}$. Показать, что доказуемые в ИВ формулы — это в точности такие Φ, что $\gamma(\Phi) = 1^{\mathfrak{A}}$ для любой интерпретации γ ИВ в $\mathfrak{A}$. (Указание. В одну сторону установить $\gamma(\Phi) = 1^{\mathfrak{A}}$ для аксиом ИВ$_1$ и проверить, что правило ИВ$_1$ сохраняет это свойство, в другую сторону воспользоваться тем, что на множестве $\{1^{\mathfrak{A}}, 0^{\mathfrak{A}}\}$ операции $\cup$, $\cap$ и $^-$ определяются так же, как на множестве $\{1, 0\}$ в § 6 определяются операции $\vee$, $\wedge$ и $\neg$.)

3. Показать, что ч. у. м. $\langle A, U\rangle$ тогда и только тогда не является фундированным, когда существует последовательность $a_0, \ldots, a_n, \ldots$ попарно различных элементов A, для которой $\langle a_{n+1}, a_n\rangle \in U$, $n \in \omega$.

§ 12. Фильтры булевой алгебры

Пусть на протяжении этого параграфа $\mathfrak{B} = \langle B, \cap, \cup, {}^-\rangle$ — булева алгебра. Как показано в предложении 11.1, $\mathfrak{B}^* = \langle B, \leqslant\rangle$, где отношение $a \leqslant b$ определяется равенством $a \cap b = a$, является булевой решеткой и для любых $a, b \in B$ выполняются условия:

(1) $a \cup b = \sup(\{a, b\}, \mathfrak{B}^*)$, $a \cap b = \inf(\{a, b\}, \mathfrak{B}^*)$;

(2) $a \cup \bar{a} = 1$ — наибольший элемент $\mathfrak{B}^*$;

(3) $a \cap \bar{a} = 0$ — наименьший элемент $\mathfrak{B}^*$;

(4) $\bar{a}$ является единственным элементом B, для которого выполняются условия $a \cup \bar{a} = 1$ и $a \cap \bar{a} = 0$.

Отметим еще некоторые свойства булевых операций.

Лемма 1. а) $\bar{0} = 1$, $\bar{1} = 0$;

б) $0 \cap a = 0$, $0 \cup a = a$;

в) $1 \cap a = a$, $1 \cup a = 1$;

г) $a = \bar{\bar{a}}$;

д) $\overline{a \cap b} = \bar{a} \cup \bar{b}$;

е) $\overline{a \cup b} = \bar{a} \cap \bar{b}$;

ж) $a \cap b = a \Leftrightarrow a \cup b = b$.

Доказательство. Свойство а) непосредственно вытекает из (1)—(4). Свойства б), в) следуют из (1)—(3), а г) следует из (4), так как $\bar{a} \cup a = a \cup \bar{a} = 1$ и $\bar{a} \cap a = a \cap \bar{a} = 0$. Свойство ж) следует из (1), так как $a \cap b = a \Leftrightarrow a \leqslant b$. Для доказательства д) в силу (4) достаточно показать, что

$$(a \cap b) \cup (\bar{a} \cup \bar{b}) = 1 \quad \text{и} \quad (a \cap b) \cap (\bar{a} \cup \bar{b}) = 0.$$

Эти равенства следуют из аксиом 1)—6) булевых алгебр, например,

$$(a \cap b) \cap (\bar{a} \cup \bar{b}) = ((a \cap b) \cap \bar{a}) \cup ((a \cap b) \cap \bar{b}) = \\ = (0 \cap b) \cup (0 \cap a) = 0.$$

Проверка другого равенства, а также доказательство свойства е) проводится аналогично. □

Часто для простоты обозначений мы будем отождествлять $\mathfrak{B}^*$ с $\mathfrak{B}$. Пусть далее B неодноэлементно.

Определение. Множество $D \subseteq B$ называется *фильтром булевой алгебры* $\mathfrak{B}$, если выполняются следующие условия:

1) $0 \notin D$;
2) если $a, b \in D$, то $a \cap b \in D$;
3) если $a \in D$ и $a \leqslant b$, то $b \in D$.

Множество $D \subseteq P(X)$ называется *фильтром на множестве* X, если D является фильтром булевой алгебры $\langle P(X), \cup, \cap, ^-\rangle$ и $D \neq \varnothing$.

Примеры. 1. Множество $\{1\}$ является фильтром булевой алгебры $\mathfrak{B}$. С другой стороны, из условия 3) вытекает, что $1 \in D$ для любого непустого фильтра D в булевой алгебре $\mathfrak{B}$.

2. Если $a_0 \in B$, $a_0 \neq 0$, то множество $\{b \mid b \in B,\ a_0 \leqslant b\}$ будет фильтром алгебры $\mathfrak{B}$.

3. Множество $\{Y \subseteq X \mid (X \setminus Y)$ — конечное множество$\}$ является фильтром на бесконечном множестве X, который иногда называют фильтром Фреше на X.

Так как операции $\cup$ и $\cap$ булевой алгебры $\mathfrak{B}$ удовлетворяют аксиомам коммутативности 1), 2) и аксиомам ассоциативности 3), 4), то можно говорить об объединении (пересечении) в $\mathfrak{B}$ конечного множества элементов $a_1, \ldots$ $\ldots, a_n \in B$ и обозначать его так: $a_1 \cup \ldots \cup a_n$ $(a_1 \cap \ldots \cap a_n)$. Индукцией по n легко устанавливаются следующие обобщенные законы дистрибутивности:

$$b \cup (a_1 \cap \ldots \cap a_n) = (b \cup a_1) \cap \ldots \cap (b \cup a_n),$$
$$b \cap (a_1 \cup \ldots \cup a_n) = (b \cap a_1) \cup \ldots \cup (b \cap a_n),$$

а также обобщения свойств д), е) леммы 1:

$$\overline{a_1 \cap \ldots \cap a_n} = \bar{a}_1 \cup \ldots \cup \bar{a}_n,$$
$$\overline{a_1 \cup \ldots \cup a_n} = \bar{a}_1 \cap \ldots \cap \bar{a}_n.$$

Определение. а) Множество $Y \subseteq B$ называется *центрированным в булевой алгебре* $\mathfrak{B}$, если пересечение в $\mathfrak{B}$ любого конечного множества элементов из Y не равно 0. Центрированное в $\langle P(X), \cup, \cap, ^- \rangle$ множество (т. е. такое множество $Y \subseteq P(X)$, у которого любое конечное подмножество имеет непустое пересечение) будем просто называть *центрированным.*

б) Фильтр булевой алгебры $\mathfrak{B}$, не содержащийся ни в каком отличном от него фильтре алгебры $\mathfrak{B}$, называется *ультрафильтром.*

Ясно, что любой фильтр булевой алгебры $\mathfrak{B}$ будет центрированным в $\mathfrak{B}$ множеством.

Предложение 1. *Каждое центрированное в булевой алгебре $\mathfrak{B}$ множество Y содержится в некотором ультрафильтре алгебры $\mathfrak{B}$.*

Доказательство. Рассмотрим множество $U = \{X \mid X$ — центрированное в $\mathfrak{B}$ множество и $Y \subseteq X\}$. Так как $Y \in U$, то $U \neq \varnothing$. Очевидно, что в ч. у. м. $\langle U, \subseteq \rangle$ объединение любой цепи является элементом U. По теореме 1 в $\langle U, \subseteq \rangle$ имеется максимальный элемент X_0. Достаточно показать, что X_0 является фильтром. Условие 1) для X_0 тривиально выполнено. Для проверки условий 2) и 3) в силу максимальности X_0 достаточно показать, что если $a, b \in X_0$ и $a \leqslant c$, то $X_0 \cup \{a \cap b\}$ и $X_0 \cup \{c\}$ центрированы в $\mathfrak{B}$. Центрированность $X_0 \cup \{a \cap b\}$ очевидна. Предположим, что $a_1 \cap \ldots \cap a_n \cap c = 0$ для некоторых $a_1, \ldots, a_n \in X_0$. Тогда из равенства $c \cap a = a$ получаем

$$0 = 0 \cap a = (a_1 \cap \ldots \cap a_n \cap c) \cap a = (a_1 \cap \ldots \cap a_n) \cap (c \cap a) = \\ = a_1 \cap \ldots \cap a_n \cap a,$$

что противоречит центрированности X_0. □

Предложение 2. *Для того чтобы фильтр D булевой алгебры $\mathfrak{B}$ был ультрафильтром, необходимо и достаточно, чтобы для любого $b \in B$ было либо $b \in D$, либо $\bar{b} \in D$.*

Доказательство. В силу предложения 1 для доказательства необходимости нужно лишь показать, что для любого $b \in B$ либо $D \cup \{b\}$, либо $D \cup \{\bar{b}\}$ является центрированным в $\mathfrak{B}$ множеством. Предположим, что это не так. Тогда $b_1 \cap \ldots \cap b_n \cap b = 0$ и $b_{n+1} \cap \ldots \cap b_{n+m} \cap \bar{b} = 0$ для некоторых $b_1, \ldots, b_{n+m} \in D$. В силу свойства 2) фильтра D можно считать $n = m = 1$. Из свойств операций $\cup, \cap, ^-$ в булевой алгебре $\mathfrak{B}$ получаем

$$b_1 \cap b_2 = b_1 \cap b_2 \cap (b \cup \bar{b}) = (b_1 \cap b_2 \cap b) \cup (b_1 \cap b_2 \cap \bar{b}) = \\ = (0 \cap b_2) \cup (b_1 \cap 0) = 0 \cup 0 = 0,$$

что противоречит свойствам 1), 2) фильтра D.

Достаточность. Если существует фильтр $D^* \supseteq D$ и элемент $b \in D^* \setminus D$, то $\bar{b} \notin D$, так как в противном случае $0 = b \cap \bar{b} \in D^*$, что невозможно. □

Определение. Фильтр D булевой алгебры $\mathfrak{B}$ называется *главным*, если существует такой $a_0 \in D$, что

$$D = \{b \in B \mid a_0 \leqslant b\}.$$

Элемент $a \in B$ называется *атомом булевой алгебры* $\mathfrak{B}$, если $a \neq 0$ и

$$b \leqslant a \Rightarrow (b = a \text{ или } b = 0).$$

Ясно, что если a — атом $\mathfrak{B}$, то $b \cap a$ равно a или 0 для любого $b \in B$.

Лемма 2. *Если D — главный ультрафильтр алгебры $\mathfrak{B}$, то $D = \{b \in B \mid a_0 \leqslant b\}$ для некоторого атома a_0 алгебры $\mathfrak{B}$.*

Доказательство. Пусть $D = \{b \in B \mid b_0 \leqslant b\}$ для некоторого $b_0 \neq 0$. Предположим, что b_0 — не атом. Тогда существует $b_1 \leqslant b_0$, $b_1 \neq b_0$, $b_1 \neq 0$. Так как $b_1 \notin D$, то по предложению 2 $\bar{b}_1 \in D$, откуда $b_0 \leqslant \bar{b}_1$, т. е. $b_0 \cap \bar{b}_1 = b_0$. Следовательно,

$$b_1 = b_1 \cap b_0 = b_1 \cap (b_0 \cap \bar{b}_1) = b_0 \cap (b_1 \cap \bar{b}_1) = 0,$$

получили противоречие. □

Предложение 3. *Следующие условия для булевой алгебры $\mathfrak{B}$ эквивалентны:*

1) *B — конечное множество;*
2) *все непустые фильтры $\mathfrak{B}$ главные;*
3) *все ультрафильтры $\mathfrak{B}$ главные.*

Доказательство. 1) $\Rightarrow$ 2). Если B — конечное множество и $D = \{b_1, \ldots, b_n\}$ — фильтр алгебры $\mathfrak{B}$, то пересечение $a_0 = b_1 \cap \ldots \cap b_n$ принадлежит D и $a_0 \leqslant b_i$ для $i = 1, \ldots, n$. Утверждение 2) $\Rightarrow$ 3) тривиально. Докажем 3) $\Rightarrow$ 1). Пусть выполняется 3). Пусть $A_0 \subseteq B$ — множество всех атомов алгебры $\mathfrak{B}$. Рассмотрим множество $A_1 = \{\bar{a} \mid a \in A_0\}$. Покажем, что A_1 не центрированное. В самом деле, если A_1 центрированное, то по предложению 1 $A_1 \subseteq D$ для некоторого ультрафильтра D. Из условия 3) и леммы 2 получаем, что существует такой $a_0 \in A_0$, что $a_0 \leqslant b$ для всех $b \in D$. В частности, $a_0 \leqslant \bar{a}_0$, т. е. $a_0 = a_0 \cap \bar{a}_0 = 0$, что противоречит условию $a \neq 0$ для атомов $a \in A_0$. Так как A_1 не центрированное, то $\bar{a}_1 \cap \ldots \cap \bar{a}_n = 0$

для некоторых a_1, .

$1 = \bar{0} = \bar{a}_1 \cap \ldots$

Пусть b — произво

$b = b \cap 1 = b \cap ($

Так как $b \cap a_i$ равн
нию некоторых эле
вательно, B — конс

Предложени
на множестве I,
$i_0 \in I$.

Доказатель
очевидно, что в P
множества. □

1. Пусть D — не
$= \langle B, \cup, \cap, ^- \rangle$. На м
щим образом:

$a\bar{D}b$

где $\bar{D}$ равно $\{\bar{d} \mid d \in D$
и D — ультрафильтр
отношением $\bar{D}$ на два

2. Фильтр D на
если для любых $a_i \in$

Ясно, что любой глав
Показать, что на мно
полного ультрафильтр

3. Пусть $\bar{D}$ — отно
ния 1. Пусть $B(D) =$
и равно $\{a \mid a\bar{D}b,\ a \in B$
дующим образом:

а) $m_1 \cup m_2 = \widetilde{D}_{(a_1}$

где $a_i \in m_i$, $i = 1, 2$.
от выбора элементов
алгеброй.

§ 1

Для бесконечны
ла элементов може

Определение
жества A меньше

обозначать $|A| \leqslant |B|$), если существует разнозначное отображение $f: A \to B$. Говорим, что *мощности множеств* A и B *равны* или что A и B *равномощны* (обозначаем $|A| = |B|$), если существует разнозначное отображение A на B.

Заметим, что мы пока не определили, что такое мощность множества A, а определили только два двухместных отношения на множествах. Именно эти отношения и являются основными понятиями этого параграфа, а введенная ниже мощность появляется лишь для удобства изложения.

Отметим свойства введенных отношений, вытекающие непосредственно из определения:

а) $|A| \leqslant |A|$;

б) $(|A| \leqslant |B|$ и $|B| \leqslant |C|) \Rightarrow |A| \leqslant |C|$;

в) $|A| = |B| \Rightarrow (|A| \leqslant |B|$ и $|B| \leqslant |A|)$.

Следующая теорема показывает, что в свойстве в) можно заменить $\Rightarrow$ на $\Leftrightarrow$.

Теорема 4 (Кантора — Бернштейна). *Если для множеств A и B имеем $|A| \leqslant |B|$ и $|B| \leqslant |A|$, то $|A| = |B|$.*

Доказательство. Пусть $f: A \to B$, $g: B \to A$ — разнозначные отображения, $A_0 = A$, $A_1 = g[B]$ и $A_{n+2} = (fg)[A_n]$. Индукцией по n легко установить, что $A_{n+1} \subseteq A_n$, $n \in \omega$. Пусть $D = \bigcap\limits_{k \in \omega} A_k$ и $M_i = A_i \setminus A_{i+1}$. Очевидно, что $\left(\bigcup\limits_{k \leqslant i \in \omega} M_i\right) \cup D = A_k$ и $M_i \cap M_j = \varnothing$ для $i \neq j$. Так как $f \cdot g$ разнозначно отображает M_i на M_{i+2} для любого $i \in \omega$, то отображение $h: A \to A$, определенное следующим образом:

$$ha = \begin{cases} a, \text{ если } a \in \left(\bigcup\limits_{i \in \omega} M_{2i+1}\right) \cup D, \\ (fg)'a), \text{ если } a \in \bigcup\limits_{i \in \omega} M_{2i}, \end{cases}$$

является разнозначным отображением A на

$$\left(\bigcup_{1 \leqslant i \in \omega} M_i\right) \cup D = A_1.$$

Так как $|B| = |A_1|$, то получаем $|B| = |A|$. □

Теорема 5 (Кантора). *Условие $|P(A)| \leqslant |A|$ не имеет места для любого множества A.*

Доказательство. Предположим, что существует разнозначное отображение $f: P(A) \to A$. Рассмотрим множество $X = \{a \in f[P(A)] \mid a \notin f^{-1}(a)\}$. Если $f(X) \in X$, то из определения X получаем $f(X) \notin f^{-1}(f(X)) = X$. Если $f(X) \notin X$, то $f(X) \notin f^{-1}(f(X))$, следовательно, $f(X) \in X$. Полученное противоречие показывает, что такого f не может существовать. □

Теорема 6. *Для любых множеств A и B либо $|A| \leqslant |B|$, либо $|B| \leqslant |A|$.*

Доказательство. По теореме 2 существуют такие $U \subseteq A^2$ и $V \subseteq B^2$, что $\mathfrak{A} = \langle A, U\rangle$ и $\mathfrak{B} = \langle B, V\rangle$ — вполне упорядоченные множества. Утверждение теоремы теперь следует из теоремы 3. □

Для множества X определим двухместное отношение $\varepsilon(X)$, состоящее из таких пар $\langle a, b\rangle \in X^2$, что $a \in b$ или $a = b$. Множество X называется *транзитивным*, если из $b \in X$ следует $b \subseteq X$.

Определение. Множество α называется *ординалом*, если оно транзитивно и $\langle \alpha, \varepsilon(\alpha)\rangle$ — вполне упорядоченное множество.

Предложение 1. *Элементы ординала α являются ординалами.*

Доказательство. Так как $\beta \subseteq \alpha$ для любого $\beta \in \alpha$, то отношение $\varepsilon(\beta) = \varepsilon(\alpha) \cap \beta^2$ является фундированным линейным порядком на $\beta \in \alpha$. Если бы элемент β ординала α не был транзитивным, то для некоторых γ_1 и γ_2 было бы $\gamma_1 \in \gamma_2 \in \beta$ и $\gamma_1 \notin \beta$. Так как α транзитивно, то $\gamma_1, \gamma_2 \in \alpha$. Это противоречит транзитивности отношения $\varepsilon(\alpha)$. □

Очевидно, что натуральные числа

$$\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \ldots$$

(каждый последующий содержит все предыдущие) будут ординалами. Множество ω всех натуральных чисел также является ординалом. Ординалами являются множества $\omega \cup \{\omega\}$, $\omega \cup \{\omega\} \cup \{\omega, \{\omega\}\}$ и т. д. Вообще, если α — ординал, то ясно, что множество $\alpha \cup \{\alpha\}$ также является ординалом, который иногда по аналогии с натуральными числами обозначают через $\alpha + 1$.

Предложение 2. *Если α_1, α_2 — два различных ординала, то либо $\alpha_1 \in \alpha_2$, либо $\alpha_2 \in \alpha_1$.*

Доказательство. Покажем сначала, что либо $\alpha_1 \subseteq \alpha_2$, либо $\alpha_2 \subseteq \alpha_1$. Если это не так, то в силу транзитивности α_1, α_2 и вполне упорядоченности $\langle \alpha_1, \varepsilon(\alpha_1)\rangle$, $\langle \alpha_2, \varepsilon(\alpha_2)\rangle$ существуют такие $\gamma_1 \in \alpha_1$, $\gamma_2 \in \alpha_2$, что $\gamma_1 \subseteq \alpha_2$, $\gamma_2 \subseteq \alpha_1$, $\gamma_1 \notin \alpha_2$, $\gamma_2 \notin \alpha_1$. Пусть $\delta \in \gamma_1$. Тогда $\delta \in$

$\in \alpha_2$, и если $\delta \notin \gamma_2$, то в силу линейной упорядоченности $\langle \alpha_2, \varepsilon(\alpha_2) \rangle$ либо $\delta = \gamma_2$, либо $\gamma_2 \in \delta$. В обоих случаях из транзитивности α_1 получаем $\gamma_2 \in \alpha_1$, что невозможно. Таким образом, $\gamma_1 \subseteq \gamma_2$. Аналогично показывается $\gamma_2 \subseteq \gamma_1$, следовательно, по аксиоме экстенсиональности $\gamma_1 = \gamma_2$, что противоречит условиям $\gamma_1 \in \alpha_1$ и $\gamma_2 \notin \alpha_1$.

Итак, показано, что $\alpha_1 \subseteq \alpha_2$ или $\alpha_2 \subseteq \alpha_1$. Пусть, например, $\alpha_2 \subseteq \alpha_1$. Так как $\alpha_1 \neq \alpha_2$, то по вполне упорядоченности $\langle \alpha_1, \varepsilon(\alpha_1) \rangle$ существует такой $\beta \in \alpha_1$, что $\beta \subseteq \alpha_2$ и $\beta \notin \alpha_2$. Пусть $\delta \in \alpha_2$, тогда $\delta \in \alpha_1$ и $\delta \subseteq \alpha_2$. По линейной упорядоченности $\langle \alpha_1, \varepsilon(\alpha_1) \rangle$ имеем одно из следующих условий: $\beta \in \delta$, $\beta = \delta$ или $\delta \in \beta$. Первые два невозможны в силу транзитивности α_2 и $\beta \notin \alpha_2$. Таким образом, $\alpha_2 \subseteq \beta$, что вместе с $\beta \subseteq \alpha_2$ дает $\alpha_2 = \beta \in \alpha_1$. □

Для множества X определим множество

$$\bigcup X = \{a \mid a \in x \text{ для некоторого } x \in X\},$$

которое называется *объединением* или *суммой* множества X.

Ординал, отличный от 0 и не имеющий вид $\alpha + 1$, называется *предельным*. Ясно, что ординал $\delta \neq 0$ тогда и только тогда является предельным, когда $\bigcup \delta = \delta$. Множество натуральных чисел ω можно определить как такой ординал, все элементы которого не предельны.

Предложение 3. *Если X — множество ординалов, то $\bigcup X$ является ординалом.*

Доказательство. Транзитивность $\bigcup X$ следует из транзитивности элементов X. Линейная упорядоченность $\langle \bigcup X, \varepsilon(\bigcup X) \rangle$ следует из предложения 2. Если $Y \subseteq \bigcup X$, $\langle Y, \varepsilon(Y) \rangle$ не имеет минимального элемента и Y не пусто, то для любого $a \in Y$ множество a не пусто и $\langle a \cap Y, \varepsilon(a \cap Y) \rangle$ не имеет минимального элемента. Так как по предложению 1 a является ординалом, то это невозможно, следовательно, $\langle \bigcup X, \varepsilon(\bigcup X) \rangle$ — вполне упорядоченное множество. □

Предложение 4. *Если X — множество ординалов, то $\langle X, \varepsilon(X) \rangle$ — вполне упорядоченное множество.*

Доказательство. Если $a \in X$, то в силу предложения 2 либо $a \in b$ для некоторого $b \in X$, либо $a = \bigcup X$. Следовательно, $X \subseteq ((\bigcup X) + 1)$ и утверждение следует из предложения 3. □

Предложение 5. *Для любого вполне упорядоченного множества $\mathfrak{A} = \langle A, U \rangle$ существует единственный ординал $\alpha(\mathfrak{A})$ такой, что $\langle \alpha(\mathfrak{A}), \varepsilon(\alpha(\mathfrak{A})) \rangle$ подобно $\mathfrak{A}$.*

Назовем этот ординал типом вполне упорядоченного множества $\mathfrak{A}$.

Доказательство. Единственность следует из предложения 11.5, так как в силу предложения 2 из любых двух различных ординалов α, β один является начальным сегментом другого.

Рассмотрим множество $X \subseteq A$ всех таких $a \in A$, что существует ординал $\alpha(a)$ и подобие f_a вполне упорядоченного множества $\langle \alpha(a), \varepsilon(\alpha(a)) \rangle$ на $\langle O[a], U \cap \cap (O[a])^2 \rangle$, где $O[a] = O[a, \mathfrak{A}]$. По предложению 11.5 подобие f_a определено по $a \in X$ однозначно. Пусть $c \in X$ и $\langle b, c \rangle \in U$. Очевидно, что $\alpha_0 = \{f_c^{-1} a \mid a \in O[b]\}$ — ординал. Так как $f_c \restriction \alpha_0$ — подобие $\langle \alpha_0, \varepsilon(\alpha_0) \rangle$ на $\langle O[b], U \cap (O[b])^2 \rangle$, то $b \in X$ и $f_b = f_c \restriction \alpha_0$, следовательно, $f_b \subseteq f_c$. Таким образом, отображение $f_0 = \bigcup \{f_a \mid a \in X\}$ будет подобием $\langle \beta_0, \varepsilon(\beta_0) \rangle$ на $\langle X, U \cap X^2 \rangle$, где β_0 — ординал, равный $\bigcup \{\alpha(a) \mid a \in X\}$. Если $X = A$, то все доказано. Предположим, что $X \neq A$. Так как X — начальный сегмент $\mathfrak{A}$ и так как $\mathfrak{A}$ — вполне упорядоченное множество, то существует такое $a_0 \in A$, что $X = O(a_0)$. Очевидно, что $f_0 \cup \{\langle \beta_0, a_0 \rangle\}$ является подобием ординала $\beta_0 \cup \{\beta_0\}$ на $X \cup \{a_0\} = O[a_0]$, поэтому $a_0 \in X$, что противоречит выбору a_0. □

Будем говорить, что ординал β меньше ординала α (обозначать $\beta < \alpha$), если $\beta \in \alpha$. Если $\beta < \alpha$ или $\beta = \alpha$, то будем писать $\beta \leqslant \alpha$. В силу предложения 4 любое множество ординалов вполне упорядочено отношением $\leqslant$. Если $\alpha_1, \ldots, \alpha_n$ — ординалы, то наибольший по отношению $\leqslant$ элемент множества $\{\alpha_1, \ldots, \alpha_n\}$ будем обозначать через $\max\{\alpha_1, \ldots, \alpha_n\}$.

Определение. Ординал $\varkappa$ называется *кардиналом*, если он не является равномощным никакому меньшему ординалу.

Предложение 6. *Натуральные числа* $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, ... *и множество* ω *всех натуральных чисел являются кардиналами.*

Доказательство. Для того чтобы показать, что все натуральные числа являются кардиналами, достаточно индукцией по $n \in \omega$ показать, что любое натуральное число n не равномощно никакому своему подмножеству $w \neq n$. Для $n = 0$ это выполняется, так как $\varnothing$ не имеет подмножеств, отличных от $\varnothing$. Пусть $f\colon n+1 \to n+1$ — разнозначное отображение и $\operatorname{rang} f \neq n+1$. Если $n \notin \operatorname{rang} f$ или $f(n) = n$, то $f \restriction n$ отображает n на подмножество $w \subseteq n$, $w \neq n$, что невозможно по индукционному предположению. (Напомним, что $n+1 = \{0, 1, \ldots, n\}$.) Если $f(k) = n$, $k < n$, то определяем отображение $g\colon n \to n$, для которого $g(i) = f(i)$ для $i < n$, $i \neq k$, и $g(k) = f(n)$. Так как $\operatorname{rang} g = \operatorname{rang} f \setminus \{n\}$ и $n \neq \operatorname{rang} f \setminus \{n\}$, то g отображает n на $w \subseteq n$, $w \neq n$, что опять противоречит индукционному предположению. Если бы ω не был кардиналом, то $|\omega| \leqslant |n|$ для некоторого натурального числа n. Тогда было бы $|n+1| \leqslant |\omega| \leqslant |n|$, т. е. $n+1$ — не кардинал, что противоречит предыдущему. □

Следующая теорема позволяет выделить среди равномощных множеств канонического представителя — кардинал.

Теорема 7. *Для любого множества X существует единственный кардинал $|X|$, равномощный X.*

Доказательство. Единственность $|X|$ следует из определения кардинала и предложения 4.

По теореме 2 существует такое $U \subseteq X^2$, что $\langle X, U \rangle$ — вполне упорядоченное множество. По предложению 5 существует ординал α_0, равномощный X. В качестве $|X|$ берем ординал $\beta \leqslant \alpha_0$, равномощный α_0, все элементы которого не равномощны α_0. Такой ординал существует по вполне упорядоченности $\langle \alpha_0, \varepsilon(\alpha_0) \rangle$. □

Определение. Для множества X кардинал $|X|$ из теоремы 7 называется *мощностью множества* X.

Очевидно, что $|\alpha| \leqslant \alpha$ для ординала α и α тогда и только тогда является кардиналом, когда $|\alpha| = \alpha$. Заметим, что определенное в начале параграфа отношение $|X| \leqslant |Y|$ на множествах X и Y соответствует отношению $\leqslant$ на кардиналах $|X|$ и $|Y|$, введенному выше так: $\varkappa_1 \leqslant \varkappa_2 \Leftrightarrow (\varkappa_1 \in \varkappa_2$ или $\varkappa_1 = \varkappa_2)$. Дадим точное определение свойства быть конечным множеством, которым ранее мы пользовались интуитивно.

Определение. Множество X называется *конечным*, если $|X| \in \omega$, и *счетным*, если $|X| = \omega$.

Если X — не конечное множество, то говорим, что X бесконечно. Заметим, что существуют бесконечные несчетные множества, более того, в силу теоремы 5 мощность любого множества X меньше мощности множества $P(X)$. Так как ω — наименьший бесконечный кардинал, то счетные множества имеют наименьшую мощность среди бесконечных множеств. Очевидно, что конечное или счетное множество X можно представить в виде $X = \{a_n | n \in \omega\}$, при этом последовательность

$$a_0, a_1, \ldots, a_n, \ldots, \quad n \in \omega,$$

будем называть *нумерацией множества* X. Ясно, что если $Y \subseteq X$, то $|Y| \leqslant |X|$. Заметим, что бесконечный кардинал $\varkappa$ не может иметь вид $\alpha + 1 = \alpha \cup \{\alpha\}$. В самом деле, так как α — бесконечный ординал, то по предложению 2 $\omega \subseteq \alpha$, поэтому отображение $f\colon \alpha + 1 \twoheadrightarrow \alpha$, для которого

$$f(\beta) = \begin{cases} \beta, & \text{если} \quad \beta \notin \omega \cup \{\alpha\}, \\ \varnothing, & \text{если} \quad \beta = \alpha, \\ \beta + 1, & \text{если} \quad \beta \in \omega, \end{cases}$$

будет разнозначным, следовательно, $|\alpha + 1| = |\alpha| \leqslant \alpha$. Докажем следующую важную теорему.

Теорема 8. *Если множество A бесконечно, то* $|A| = |A^2|$.

Доказательство. Отображение $f\colon A \to A^2$, для которого $f(a) = \langle a, a \rangle$, будет разнозначным, следовательно, $|A| \leqslant |A^2|$. Предположим, что $|A^2| \leqslant |A|$ не выполняется. Тогда множество

$$X = \{\alpha | \alpha \text{ — бесконечный кардинал, } \alpha \leqslant |A| \text{ и } \alpha < |\alpha^2|\}$$

не пусто, и пусть α_0 — наименьший элемент множества X. Определим на множестве α_0^2 отношение $\preccurlyeq$:

$$\langle \beta_1, \beta_2 \rangle \preccurlyeq \langle \gamma_1, \gamma_2 \rangle \Leftrightarrow \begin{cases} \max\{\beta_1, \beta_2\} < \max\{\gamma_1, \gamma_2\} \text{ или} \\ \max\{\beta_1, \beta_2\} = \max\{\gamma_1, \gamma_2\},\ \beta_1 < \gamma_1, \text{ или} \\ \max\{\beta_1, \beta_2\} = \max\{\gamma_1, \gamma_2\},\ \beta_1 = \gamma_1,\ \beta_2 \leqslant \gamma_2. \end{cases}$$

Очевидно, что $\preccurlyeq$ — линейный порядок на α_0^2. Кроме того $\langle \alpha_0^2, \preccurlyeq \rangle$ — вполне упорядоченное множество, так как для любого непустого подмножества $Y \subseteq \alpha_0^2$ существуют непустые подмножества

$$Y_1 = \{\langle \beta, \gamma \rangle \in Y | \max\{\beta, \gamma\} \leqslant \max\{\beta', \gamma'\} \text{ для любых } \langle \beta', \gamma' \rangle \in Y\},$$
$$Y_2 = \{\langle \beta, \gamma \rangle \in Y_1 | \beta \leqslant \beta' \text{ для любых } \langle \beta', \gamma' \rangle \in Y_1\},$$
$$Y_3 = \{\langle \beta, \gamma \rangle \in Y_2 | \gamma \leqslant \gamma' \text{ для любых } \langle \beta', \gamma' \rangle \in Y_2\}$$

и очевидно, что Y_3 содержит ровно один элемент и он является наименьшим по отношению $\preccurlyeq$ элементом Y. Так как $\alpha_0 < |\alpha_0^2|$, то по теореме 3 $\langle \alpha_0, \varepsilon(\alpha_0) \rangle$ подобно начальному сегменту $Z = O(\langle\beta_0, \gamma_0\rangle)$ вполне упорядоченного множества $\langle\alpha_0^2, \preccurlyeq\rangle$.

Пусть $\delta_0 = \max\{\beta_0, \gamma_0\}$, тогда очевидно, что $Z \subseteq (\delta_0 + 1)^2$. Так как α_0 бесконечно, то Z и δ_0 также бесконечны и $|\delta_0 + 1| = |\delta_0| < \alpha_0$. Тогда по выбору кардинала α_0 имеем

$$\alpha_0 = |Z| \leqslant |(\delta_0 + 1)^2| \leqslant |\delta_0 + 1| < \alpha_0,$$

получили противоречие. □

Следствие 1. *Пусть A, B — множества и хотя бы одно из них бесконечно, тогда*

а) *если $A \neq \varnothing$ и $B \neq \varnothing$, то* $|A \times B| = \max\{|A|, |B|\}$;

б) $|A \cup B| = \max\{|A|, |B|\}$.

Доказательство. Пусть $|A| = \max\{|A|, |B|\}$.

а) Пусть $b_0 \in B$. Тогда отображение $f\colon A \to A \times B$, для которого $f(a) = \langle a, b_0\rangle$, разнозначно, поэтому $|A| \leqslant |A \times B|$. Из $|B| \leqslant |A|$ и предыдущей теоремы получаем

$$|A \times B| \leqslant |A^2| = |A|.$$

б) Очевидно, что $|A| \leqslant |A \cup B|$. Пусть $f\colon B \to A$ — разнозначное отображение, тогда отображение $g\colon A \cup B \to A \times \{0, 1\}$, для которого

$$g(a) = \begin{cases} \langle a, 0\rangle, & \text{если } a \in A, \\ \langle fa, 1\rangle, & \text{если } a \in B \setminus A, \end{cases}$$

будет разнозначным, поэтому из утверждения а) получаем

$$|A \cup B| \leqslant |A \times \{0, 1\}| = |A|. \ \square$$

Следствие 2. а) *Если A бесконечно, то $|A^k| = |A|$ для любого натурального $k > 0$.*

б) *Если A бесконечно и $A^* = \bigcup\{A^k \mid k \in \omega\}$, то $|A^*| = |A|$.*

в) *Если W — множество слов алфавита $A \neq \varnothing$, то $|W| = \max\{|A|, \omega\}$.*

Доказательство. а) следует из следствия 1 а) индукцией по k.

б) Пусть $f_k\colon A^k \to A$, $0 < k < \omega$, — разнозначные отображения, существующие в силу утверждения а). Тогда отображение $f\colon A^* \to \omega \times A$, для которого

$$fa = \begin{cases} \langle 0, a\rangle, & \text{если } a = \varnothing \in A^0, \\ \langle k, f_k a\rangle, & \text{если } a \in A^k \setminus (A^0 \cup \ldots \cup A^{k-1}), k > 0, \end{cases}$$

будет разнозначным, поэтому в силу следствия 1 а) получаем $|A^*| \leqslant |\omega \times A| = |A|$. Обратное неравенство $|A| \leqslant |A^*|$ очевидно.

в) Так как для $a \in A$ слова a, aa, aaa, ... попарно различны, то $\omega \leqslant |W|$. Если A бесконечно, то утверждение в) следует из утверждения б). Если $|A| = n \in \omega$, то очевидно, что $|W| \leqslant |\omega^*|$, и снова по б) получаем $|W| \leqslant \omega$. □

Упражнения

1. Показать, что множества целых, рациональных и алгебраических чисел счетны.

2. Показать, что множества действительных и комплексных чисел равномощны, а множества действительных и натуральных чисел не равномощны. (Указание. Заметить, что мощность множества действительных чисел равна $|P(\omega)|$, и применить теорему, Кантора.)

§ 14. Аксиома выбора

Определим множества V_α, где α — ординал, следующим образом:

а) $V_0 = \varnothing$;

б) $V_\alpha = P(V_\beta)$, если $\alpha = \beta + 1$;

в) $V_\alpha = \bigcup\limits_{\beta<\alpha} V_\beta$, если α — предельный ординал.

Аксиома, утверждающая, что для любого множества X существует ординал α, для которого $X \in V_\alpha$, называется *аксиомой регулярности*. Таким образом, по аксиоме регулярности каждое множество получается на некотором шаге «регулярного процесса», при котором, исходя из пустого множества, на каждом шаге получаются все множества, элементы которых уже получены на предыдущих шагах. Это вполне согласуется с нашими интуитивными представлениями об образовании множеств.

Аксиома регулярности позволяет каждому множеству X сопоставить ординал $\rho(X)$, который называется *рангом* X и определяется как наименьший ординал, для которого $X \in V_{\rho(X)}$. Очевидно, что если $X \in Y$, то $\rho(X) < \rho(Y)$, поэтому в силу предложения 13.4 из аксиомы регулярности следуют следующие два утверждения:

1) не существует последовательности X_0, X_1, ..., X_n, ..., для которой $X_{n+1} \in X_n$, $n \in \omega$;

2) любое непустое множество X имеет элемент $a \in X$, для которого $a \cap X = \varnothing$.

Аксиома регулярности на самом деле равносильна каждому из утверждений 1) и 2). Действительно, если $X_{n+1} \in X_n$ для $n \in \omega$, то множество $\{X_n | n \in \omega\}$ противоречит условию 2), следовательно, 2) $\Rightarrow$ 1). Заметим, что если для любого элемента a множества X существует ординал $\beta(a)$, для которого $a \in V_{\beta(a)}$, то $X \in V_\gamma$, где $\gamma = (\bigcup \{\beta(a) | a \in X\} + 1)$. Поэтому если a_0 не принадлежит V_α ни для какого ординала α, то существует $a_1 \in a_0$, который также не принадлежит V_α ни для какого α. Таким образом, если аксиома регулярности не выполняется, то существует такая последовательность a_n, $n \in \omega$, что $a_{n+1} \in a_n$, $n \in \omega$, т. е. 1) также не выполняется.

Аксиомы экстенсиональности и регулярности налагают определенные условия на отношение $\in$ (принадлежности) и $=$ (равенства), т. е. в определенном смысле ограничивают «универсум», состоящий из множеств. Аксиома выбора, наоборот, утверждает, что в этом «универсуме» должны существовать определенные множества, если некоторые уже существуют. Однако в доказательствах мы свободно пользовались и другими условиями существования множеств, например, мы образовывали объединение $A \cup B$ двух множеств A и B, рассматривали множество-степень $P(A)$, считали, что в нашем распоряжении «имеются» натуральные числа $n \in \omega$. Все условия существования множеств, которые мы использовали (кроме аксиомы выбора), вытекают из следующих аксиом «существования»:

1) Существует пустое множество $\varnothing$.

2) Если существуют множества a и b, то существует множество $\{a, b\}$.

3) Если существует множество X, то существует множество $\bigcup X = \{t | t \in x$ для некоторого $x \in X\}$.

4) Существует множество $\omega = \{0, 1, \ldots, n, \ldots\}$, где $0 = \varnothing$ и $n + 1 = n \cup \{n\}$.

5) Если существует множество A, то существует множество $P(A) = \{B | B \subseteq A\}$.

6) Если $\Phi(x, y)$ — некоторое условие на множества x, y такое, что для любого множества x существует не более одного множества y, удовлетворяющего условию $\Phi(x, y)$, то для любого множества a существует множество

$$\{b | \Phi(c, b) \text{ для некоторого } c \in a\}.$$

Пример 1. Покажем, что из аксиом 5) и 6) следует существование множества $A^2 = \{\langle a, b\rangle | a, b \in A\}$ для любого множества A.

Так как $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$, то $A^2 \subseteq P(P(A))$. Пусть

$$\Phi_0(x, y) \Leftrightarrow (\text{существуют такие } a, b \in A, \text{ что } x = \{\{a\}, \{a, b\}\} \text{ и } y = x).$$

Тогда множество A^2 равно $\{b | \Phi_0(c, b), c \in P(P(A))\}$ и по аксиоме 6) оно существует.

Систему аксиом 1)—6) вместе с аксиомами экстенсиональности и регулярности называют *системой аксиом Цермело — Френкеля* (обозначают ZF). Систему ZF вместе с аксиомой выбора обозначают через ZFC *).

В рамках теории ZFC можно изложить все общепринятые в современной математике способы рассуждений. Можно даже сказать, что на современном этапе развития математики такая «переводимость» в ZFC является мерилом математической строгости. (Правда, это оспаривается интуиционистами и конструктивистами, но их воззрений мы в этой книге не касаемся.) Таким образом, формальный вывод из аксиом ZFC можно принять в качестве разумного уточнения понятия математического доказательства **). Точная формулировка этого понятия имеет большое значение и составляет одну из центральных задач математической логики. Только при наличии соответствующих точных определений можно установить недоказуемость и независимость некоторых утверждений. Так было доказано, что множеству действительных чисел можно без противоречия приписать практически любую мощность. То обстоятельство, что правильность формального доказательства легко проверить на машине, явилось отправным пунктом для перспективных исследований по машинному поиску доказательств. Исторически главную роль в создании ZFC сыграли противоречия «наивной» теории множеств. Как же обстоят дела с непротиворечивостью ZFC? В рамках ZFC ника-

*) Для точного определения понятия условия $\Phi(x, y)$ в аксиоме 6) мы отсылаем читателя к понятию формулы сигнатуры Σ_0, содержащей лишь один двухместный предикатный символ $\in$ (см. главу 3). Заметим, что все аксиомы ZFC можно записать в виде предложений сигнатуры Σ_0.

**) Под формальным выводом понимается вывод в исчислении предикатов (см. § 22).

ких противоречий до сих пор не обнаружено. С другой стороны, было доказано, что если ZFC непротиворечива, то этот факт нельзя установить средствами этой теории.

В ZFC имеется семь аксиом, утверждающих существование некоторых множеств. Аксиома выбора среди них занимает особое место. Она, по-видимому, является наименее «очевидной». Дело в том, что множества, существование которых утверждается в аксиомах 1)—6), определяются однозначно (например, сумма множества $\bigcup X$ однозначно определена по X), функция же выбора для непустых подмножеств X определена неоднозначно. Более того, если существует условие, определяющее однозначно функцию выбора для непустых подмножеств X, то тогда существование функции выбора для $P(X)\setminus\{\varnothing\}$ можно вывести без аксиомы выбора (т. е. в ZF). Наличие такой неопределенности объекта, существование которого утверждает эта аксиома, а также некоторые ее следствия, не согласующиеся с «наивной» интуицией, вызвало многочисленные споры вокруг аксиомы выбора среди математиков в начале XX в. Некоторые даже считали, что она наверняка должна привести к противоречию. Однако после результата К. Гёделя о равнонепротиворечивости ZF и ZFC эти споры в основном утихли. Тем не менее, до сих пор иногда стараются приводить, если это возможно, доказательства, не использующие аксиому выбора, считая такое доказательство более «конструктивным».

Оставшуюся часть параграфа мы посвятим теореме, показывающей, что аксиома выбора эквивалентна (в ZF) некоторым своим следствиям, доказанным в предыдущих параграфах.

Теорема 9. *Из аксиом ZF можно вывести эквивалентность следующих утверждений:*

а) *аксиома выбора: для любого непустого множества A существует такое отображение h: $(P(A)\setminus\{\varnothing\})\to A$, что $hB\in B$ для всех $B\subseteq A$, $B\neq\varnothing$;*

б) *принцип полного упорядочения: для любого множества A существует отношение $U\subseteq A^2$, для которого $\langle A, U\rangle$ — вполне упорядоченное множество;*

в) *принцип максимума: если в частично упорядоченном множестве $\mathfrak{A}=\langle A, U\rangle$ каждая цепь имеет верхнюю грань, то $\mathfrak{A}$ имеет максимальный элемент;*

г) *если множество A бесконечно, то $|A^2|=|A|$.*

Доказательство. В силу теорем 1, 2 и 8 в ZF имеют место а)$\Rightarrow$в), а)$\Rightarrow$б) и а)$\Rightarrow$г), кроме того, при доказательстве теоремы 2 показано, что в ZF имеет место в)$\Rightarrow$б). Поэтому достаточно из аксиом ZF вывести б)$\Rightarrow$а) и г)$\Rightarrow$б).

б)$\Rightarrow$а). Пусть $\langle A, U\rangle$ — вполне упорядоченное множество. Возьмем в качестве $\Phi(x, y)$ следующее условие: $\Phi(x, y)\Leftrightarrow(\langle x, U\cap x^2\rangle$ — вполне упорядоченное множество, y — упорядоченная пара, $\pi_1^2 y = x$ и $\pi_2^2 y$ — наименьший элемент $\langle x, U\cap x^2\rangle)$. Очевидно, что для любого x существует не более одного y, для которого выполняется $\Phi(x, y)$. Из аксиомы 6) получаем, что существует множество

$$h = \{\langle B, a\rangle \mid \Phi(B, \langle B, a\rangle),\ B\in(P(A)\setminus\{\varnothing\})\}.$$

Ясно, что h: $(P(A)\setminus\{\varnothing\})\to A$ и $h(B)\in B$ для $B\subseteq A$, $B\neq\varnothing$.

г)$\Rightarrow$б). Так как $\langle n, \varepsilon(n)\rangle$ — вполне упорядоченное множество для любого $n\in\omega$, то достаточно рассмотреть случай, когда A бесконечно. Из аксиомы 6) следует существование множества

$$W = \{U\subseteq A^2 \mid \langle D(U), U\rangle \text{ — вполне упорядоченное множество}\},$$

где $D(U) = \{a\in A \mid \langle a, b\rangle\in U$ или $\langle b, a\rangle\in U$ для некоторого $b\in A\}$. Если $U\in W$, то через $\alpha(U)$ обозначим тип множества $\langle D(U), U\rangle$ (предложение 13.5). По аксиоме 6) существует множество $V = \{\alpha(U) \mid U\in W\}$. Ясно, что V равно множеству $\{\alpha \mid \alpha$ — ординал и $|\alpha|\leqslant|A|\}$. По предложению 13.3 $\alpha_0 = \bigcup V$ является ординалом. Если существует разнозначное отображение f: $\alpha_0\to A$, то $\{f\beta \mid \beta\in\alpha_0\} = A$, так как в противном случае отображение $f\cup\{\langle\alpha_0, a_0\rangle\}$, где $a_0\in A\setminus\{f\beta \mid \beta\in\alpha_0\}$, будет разнозначно отображать α_0+1 в A, следовательно, $\alpha_0+1\subseteq\alpha_0$, что невозможно. Таким образом, либо имеет место $|\alpha_0| = |A|$, либо $|\alpha_0|\leqslant|A|$ не имеет места. Если $|\alpha_0| = |A|$, то из вполне упорядоченности $\langle\alpha_0, \varepsilon(\alpha_0)\rangle$ получаем вполне упорядоченность $\langle A, U\rangle$ для некоторого $U\subseteq A^2$. Пусть $|\alpha_0|\leqslant|A|$ не имеет места. Индукцией по $n\in\omega$ легко получить, что $|n|\leqslant|A|$ для любого $n\in\omega$, следовательно, α_0 — бесконечный ординал. Рассмотрим множество $X = \{\langle\alpha_0, a\rangle \mid a\in A\}$. Очевидно, что $|X| = |A|$ и $X \cap \alpha_0 = \varnothing$. Для простоты равномощность $|E| = |F|$ будем обозначать через $E \sim F$.

Заметим, что если $|Y| \leqslant |Z|$ и Z бесконечно, то $Y \cup Z \sim Z$. В самом деле, если g: $Y \to Z$ — разнозначное отображение, z_1, $z_2 \in Z$, $z_1 \neq z_2$, то отображение f: $Y \cup Z \to Z^2$, для которого

$$fa = \begin{cases} \langle z_1, ga\rangle, & \text{если} \quad a \in Y, \\ \langle z_2, a\rangle, & \text{если} \quad a \in Z \setminus Y, \end{cases}$$

разнозначно, поэтому $|Y \cup Z| \leqslant |Z^2|$. Из г) имеем $|Z^2| = |Z|$, следовательно, $|Y \cup Z| \leqslant |Z|$. Условие $|Z| \leqslant |Y \cup Z|$ очевидно. Пользуясь этим фактом и условием г), получаем

$$\alpha_0 \cup X \sim (\alpha_0 \cup X)^2 = \alpha_0^2 \cup (\alpha_0 \times X) \cup X^2 \cup (X \times \alpha_0) \sim$$
$$\sim \alpha_0 \cup (\alpha_0 \times X) \cup X \cup (X \times \alpha_0) \sim (\alpha_0 \times X) \cup (X \times \alpha_0) \sim \alpha_0 \times X.$$

Таким образом, $\alpha_0 \times X = C \cup D$, где $C \sim \alpha_0$ и $D \sim X \sim A$. Покажем, что $(\alpha_0 \times \{x\}) \cap C \neq \varnothing$ для любого $x \in X$. В самом деле, в противном случае $(\alpha_0 \times \{x_0\}) \subseteq D$ для некоторого $x_0 \in X$, следовательно, $|\alpha_0 \times \{x_0\}| \leqslant |D|$. Так как $\alpha_0 \sim (\alpha_0 \times \{x_0\})$ и $D \sim A$, то это противоречит тому, что условие $|\alpha_0| \leqslant |A|$ не выполняется. Так как $C \sim \alpha_0$ и $\langle \alpha_0, \varepsilon(\alpha_0)\rangle$ — вполне упорядоченное множество, то существует $U \subseteq C^2$, для которого $\langle C, U\rangle$ — вполне упорядоченное множество. Используя аксиому 6), легко получить отображение f: $X \to C$, для которого fa равно наименьшему по отношению U элементу из $(\alpha_0 \times \{a\}) \cap C$. Очевидно, что f — разнозначное отображение. Утверждение г)$\Rightarrow$б) получаем теперь из $A \sim X$ и вполне упорядоченности $\langle f[X], U \cap (f[X])^2\rangle$. □

Упражнение

1. Показать, что аксиома выбора эквивалентна в ZF следующему утверждению: если M — разбиение множества A (см. пример 10.1), то существует отображение g: $M \to A$, для которого $g(m) \in m$, $m \in M$, $m \neq \varnothing$. (Указание. Рассмотреть разбиение $\{m(B) \mid B \in P(A) \setminus \{\varnothing\}\}$, где $m(B) = \{\langle B, a\rangle \mid a \in B\}$.)

Глава 3

ИСТИННОСТЬ НА АЛГЕБРАИЧЕСКИХ СИСТЕМАХ

§ 15. Алгебраические системы

Часто объектом изучения в математике служит множество вместе с определенной на нем структурой, например, множество треугольников с отношением подобия, множество действительных чисел с операциями сложения и умножения, множество вещественных функций со свойством дифференцируемости и операцией дифференцирования и другие. В этом параграфе мы дадим одно из уточнений этого понятия, введя определение алгебраической системы.

Определение. Упорядоченная тройка $\Sigma = \langle R, F, \mu \rangle$ называется *сигнатурой*, если выполняются следующие условия:

а) множества R и F не имеют общих элементов;

б) μ является отображением множества $R \cup F$ в ω.

Элементы множества R называются *символами отношений* или *предикатов*. Элементы множества F называются *символами операций* или *функций*. Отображение μ называется *отображением местности* или *арности для* Σ. Если $\mu(q) = n$, то q называется n-местным предикатным символом при $q \in R$ и n-местным функциональным символом при $q \in F$. 0-местный функциональный символ называется символом константы или просто константой.

Часто для удобства будем представлять конечную или счетную сигнатуру $\Sigma = \langle R, F, \mu \rangle$ в виде

$$\Sigma = \left\langle r_1^{\mu(r_1)}, \ldots, r_n^{\mu(r_n)}, \ldots; f_1^{\mu(f_1)}, \ldots; f_k^{\mu(f_k)}, \ldots; c_1, \ldots, c_m, \ldots \right\rangle,$$

где r_i, f_j — символы отношений и функций, не являющихся константами, c_k — константы сигнатуры Σ. Все сигнатуры в дальнейшем будут обозначаться буквой Σ (возможно, с индексами), множество их символов отношений — через R, множество символов операций — через F, а отображение арности — через μ (с соответствующими индексами). Будем говорить, что сигнатура Σ содержится в сигнатуре Σ_1 (обозначаем $\Sigma \subseteq \Sigma_1$), если $R \subseteq R_1$, $F \subseteq F_1$ и $\mu \subseteq \mu_1$. Если $X \subseteq R \cup F$, то сигнатуру $\Sigma_1 = \langle R \cap X, F \cap X, \mu \restriction X \rangle$ назовем ограничением сигнатуры Σ на множество X (обозначаем $\Sigma_1 = \Sigma \restriction X$). Мощность множества $R \cup F$ называется мощностью сигнатуры $\Sigma = \langle R, F, \mu \rangle$ и обозначается через $|\Sigma|$. Если $\Sigma_n \subseteq \Sigma_{n+1}$, $n \in \omega$, то через $\bigcup\limits_{n \in \omega} \Sigma_n$ обозначаем сигнатуру $\left\langle \bigcup\limits_{n \in \omega} R_n, \bigcup\limits_{n \in \omega} F_n, \bigcup\limits_{n \in \omega} \mu_n \right\rangle$.

Если $R \cup F \neq \varnothing$ и $F = \varnothing$ $(R = \varnothing)$, то сигнатура Σ называется *предикатной* (*функциональной*). Если $R \cup F = \varnothing$, то сигнатура Σ называется пустой.

Определение. Упорядоченная пара $\mathfrak{A} = \langle A, \nu^{\mathfrak{A}} \rangle$ называется *алгебраической системой сигнатуры* Σ, если выполняются следующие условия:

а) A — непустое множество;

б) $\nu^{\mathfrak{A}}$ — отображение множества $R \cup F$ в множество отношений и операций на множестве A;

в) $r \in R \Rightarrow \nu^{\mathfrak{A}}(r)$ является $\mu(r)$-местным отношением на A;

г) $f \in F \Rightarrow \nu^{\mathfrak{A}}(f)$ — $\mu(f)$-местная операция на A.

Множество A называется *носителем* $\mathfrak{A}$, $\nu^{\mathfrak{A}}$ — *интерпретацией сигнатуры* Σ *в* A. В дальнейшем вместо $\nu^{\mathfrak{A}}(r)$ будем часто писать просто $r^{\mathfrak{A}}$ или даже r, если ясно, о какой $\mathfrak{A}$ идет речь.

Алгебраические системы в дальнейшем будут обозначаться готическими буквами $\mathfrak{A}$, $\mathfrak{B}$, ... (возможно, с индексами), а их носители — соответствующими латинскими буквами A, B, ... (с соответствующими индексами). *Мощностью алгебраической системы* $\mathfrak{A}$ будем называть мощность ее носителя A. Для краткости будем часто опускать слово «алгебраическая» и называть $\mathfrak{A}$ просто системой.

Определение. Отображение $f\colon A \to B$ называется *гомоморфизмом* алгебраической системы $\mathfrak{A}$ сигнатуры Σ в систему $\mathfrak{B}$ той же сигнатуры Σ, если выполняются следующие условия:

а) если $q \in R$ и $\mu(q) = n$, то для всех $a_1, \ldots, a_n \in A$

$$\langle a_1, \ldots, a_n \rangle \in q^{\mathfrak{A}} \Rightarrow \langle fa_1, \ldots, fa_n \rangle \in q^{\mathfrak{B}};$$

б) если $q \in F$ и $\mu(q) = n$, то для всех $a_1, \ldots, a_n \in A$

$$f\left(q^{\mathfrak{A}}(a_1, \ldots, a_n)\right) = q^{\mathfrak{B}}(fa_1, \ldots, fa_n).$$

Если f — гомоморфизм $\mathfrak{A}$ и $\mathfrak{B}$ и $f[A] = B$, то f называется *гомоморфизмом* $\mathfrak{A}$ *на* $\mathfrak{B}$, а $\mathfrak{B}$ — *гомоморфным образом* $\mathfrak{A}$.

Разнозначный гомоморфизм f $\mathfrak{A}$ на $\mathfrak{B}$, для которого f^{-1} — также гомоморфизм, называется *изоморфизмом* $\mathfrak{A}$ *на* $\mathfrak{B}$ и обозначается через f: $\mathfrak{A} \rightleftarrows \mathfrak{B}$. Если существует *изоморфизм* f: $\mathfrak{A} \rightleftarrows \mathfrak{B}$, то системы $\mathfrak{A}$ и $\mathfrak{B}$ называются *изоморфными* и обозначается это так: $\mathfrak{A} \simeq \mathfrak{B}$. Изоморфизм f системы $\mathfrak{A}$ на $\mathfrak{A}$ называется *автоморфизмом* системы $\mathfrak{A}$.

Предложение 1. а) *Если* f: $\mathfrak{A} \rightleftarrows \mathfrak{B}$, *то* f^{-1}: $\mathfrak{B} \rightleftarrows \mathfrak{A}$.

б) *Если* f: $\mathfrak{A} \rightleftarrows \mathfrak{A}_1$ *и* g: $\mathfrak{A}_1 \rightleftarrows \mathfrak{A}_2$, *то* (fg): $\mathfrak{A} \rightleftarrows \mathfrak{A}_2$.

в) id_A: $\mathfrak{A} \rightleftarrows \mathfrak{A}$.

Доказательство получается непосредственно из определения изоморфизма. □

Определение. Система $\mathfrak{A}$ называется *подсистемой* системы $\mathfrak{B}$ (обозначаем $\mathfrak{A} \subseteq \mathfrak{B}$), если выполняются следующие условия:

а) $\mathfrak{A}$ и $\mathfrak{B}$ имеют одну и ту же сигнатуру;

б) $A \subseteq B$;

в) множество A замкнуто относительно операций $\nu^{\mathfrak{B}}(f)$, $f \in F$;

г) отношения и операции $\nu^{\mathfrak{A}}(q)$, $q \in R \cup F$, в $\mathfrak{A}$ являются ограничением на A соответствующих отношений и операций $\nu^{\mathfrak{B}}(q)$, $q \in R \cup F$, в $\mathfrak{B}$.

Если $A \neq B$, то $\mathfrak{A} \subseteq \mathfrak{B}$ называется *собственной* подсистемой $\mathfrak{B}$. Если $\mathfrak{A} \subseteq \mathfrak{B}$, то $\mathfrak{B}$ называется *надсистемой* $\mathfrak{A}$.

Из определения подсистемы следует, что две подсистемы $\mathfrak{A}_1$, $\mathfrak{A}_2$ системы $\mathfrak{B}$ с одинаковыми носителями совпадают. С другой стороны, если непустое подмножество $B_1 \subseteq B$ замкнуто относительно операций системы $\mathfrak{B}$, то B_1 является носителем некоторой подсистемы $\mathfrak{B}_1 \subseteq \mathfrak{B}$. Таким образом, существует разнозначное отображение множества непустых замкнутых относительно операций $\mathfrak{B}$ подмножеств B на множество подсистем $\mathfrak{B}$. Это отображение можно продолжить на все непустые подмножества B. А именно, имеет место

Предложение 2. *Если* $\mathfrak{B}$ — *алгебраическая система,* $X \subseteq B$, $X \neq \varnothing$, *то существует такая единственная подсистема* $\mathfrak{B}(X) \subseteq \mathfrak{B}$ *с носителем* $B(X)$, *что* $X \subseteq$

$\subseteq B(X)$ и $\mathfrak{B}(X)\subseteq\mathfrak{A}$ для любой подсистемы $\mathfrak{A}\subseteq\mathfrak{B}$, для которой $X\subseteq A$.

Доказательство. В качестве $B(X)$ берем пересечение носителей A всех подсистем $\mathfrak{A}\subseteq\mathfrak{B}$, содержащих X. Так как $X\subseteq B(X)$, то $B(X)\neq\varnothing$. Как уже отмечалось выше, $B(X)$ является носителем единственной подсистемы $\mathfrak{B}(X)\subseteq\mathfrak{B}$. □

Определение. Подсистема $\mathfrak{B}(X)\subseteq\mathfrak{B}$ из предложения 2 называется *подсистемой, порожденной множеством X в $\mathfrak{B}$*. Если $X=\{a_1, \ldots, a_n\}$, то $\mathfrak{B}(X)$ обозначаем также через $\mathfrak{B}(a_1, \ldots, a_n)$. Если $\mathfrak{B}(X)=\mathfrak{B}$, то говорим, что система $\mathfrak{B}$ порождается множеством X.

Множество алгебраических систем $\{\mathfrak{A}_i | i\in I\}$ называется *направленным множеством алгебраических систем*, если $I\neq\varnothing$ и для любых $i, j\in I$ существует $k\in I$, для которого $\mathfrak{A}_i\subseteq\mathfrak{A}_k$ и $\mathfrak{A}_j\subseteq\mathfrak{A}_k$. Из определения следует, что все системы направленного множества систем имеют одну сигнатуру.

Предложение 3. *Если $\{\mathfrak{A}_i | i\in I\}$ — направленное множество алгебраических систем сигнатуры Σ, то существует единственная система $\mathfrak{A}$ такая, что $\mathfrak{A}_i\subseteq\mathfrak{A}$ для всех $i\in I$ и $\mathfrak{A}\subseteq\mathfrak{B}$ для любой системы $\mathfrak{B}$, для которой $\mathfrak{A}_i\subseteq\mathfrak{B}$, $i\in I$.*

Доказательство. Носителем $\mathfrak{A}$ будет множество $A=\bigcup\limits_{i\in I} A_i$. Пусть $\{a_1, \ldots, a_n\}\subseteq A$. Тогда из определения направленного множества следует, что существует такое $i\in I$, что $\{a_1, \ldots, a_n\}\subseteq A_i$. Пусть $\langle a_1, \ldots, a_n\rangle$ принадлежит $\nu^{\mathfrak{A}}(s)$, $s\in R\cup F$, точно тогда, когда $\langle a_1, \ldots, a_n\rangle$ принадлежит $\nu^{\mathfrak{A}_i}(s)$. Такое определение не зависит от выбора $i\in I$, так как если $\{a_1, \ldots, a_n\}\subseteq A_j$, то существует такая $\mathfrak{A}_k$, что $\mathfrak{A}_i\subseteq\mathfrak{A}_k$ и $\mathfrak{A}_j\subseteq\mathfrak{A}_k$. Следовательно, $\nu^{\mathfrak{A}_\tau}(r)\cap\{\langle a_1, \ldots, a_n\rangle\}$, $r\in R$, и $\nu^{\mathfrak{A}_\tau}(f)(a_1, \ldots, a_n)$, $f\in F$, для $\tau\in\{i, j\}$ совпадают с соответствующими $\nu^{\mathfrak{A}_k}(r)\cap\cap\{\langle a_1, \ldots, a_n\rangle\}$, $r\in R$, и $\nu^{\mathfrak{A}_k}(f)(a_1, \ldots, a_n)$, $f\in F$. Второе утверждение предложения 3 и единственность $\mathfrak{A}$ очевидны. □

Система $\mathfrak{A}$ из предложения 3 называется *объединением систем $\mathfrak{A}_i$, $i\in I$*, и обозначается так: $\mathfrak{A}=\bigcup\limits_{i\in I}\mathfrak{A}_i$.

Определение. Алгебраическая система $\mathfrak{A}$ сигнатуры Σ называется *обогащением системы $\mathfrak{A}_1$* сигнатуры Σ_1, если выполняются следующие условия:

а) $A = A_1$;

б) $\Sigma_1 = \Sigma \restriction (R_1 \cup F_1)$;

в) $\nu^{\mathfrak{A}_1} = \nu^{\mathfrak{A}} \restriction (R_1 \cup F_1)$.

Если система $\mathfrak{A}$ сигнатуры Σ является обогащением системы $\mathfrak{A}_1$ сигнатуры Σ_1, то $\mathfrak{A}_1$ называется *обеднением системы* $\mathfrak{A}$ до сигнатуры Σ_1 и обозначается через $\mathfrak{A} \restriction \Sigma_1$.

Если $\Sigma = \left\langle r_1^{\mu(r_1)}, \ldots, r_n^{\mu(r_n)}, \ldots; f_1^{\mu(f_1)}, \ldots, f_k^{\mu(f_k)}, \ldots; c_1, \ldots, c_m, \ldots \right\rangle$, то алгебраическую систему $\mathfrak{A}$ сигнатуры Σ часто будем обозначать так: $\mathfrak{A} = \langle A, \underline{r}_1, \ldots, \underline{r}_n, \ldots; \underline{f}_1, \ldots, \underline{f}_k, \ldots; \underline{c}_1, \ldots, \underline{c}_m, \ldots \rangle$, где $\underline{r}_n$, $\underline{f}_k$, $\underline{c}_m$ обозначают соответственно отношение $\nu^{\mathfrak{A}}(r_n)$, операцию $\nu^{\mathfrak{A}}(f_k)$ и значение константы $\nu^{\mathfrak{A}}(c_m)$ на множестве A.

Пример 1. Алгебраическая система $\mathfrak{N} = \langle N, \underline{+}, \underline{\cdot}; \underline{0}, \underline{1} \rangle$, где $N = \omega$ — множество натуральных чисел, $\underline{+}$ и $\underline{\cdot}$ — операции сложения и умножения, $\underline{0} = 0$, $\underline{1} = 1$, называется *арифметикой натуральных чисел* или просто *арифметикой*. Заметим, что $\mathfrak{N}$ не имеет подсистем, отличных от нее самой. Функциональная сигнатура $\Sigma_1 = \langle +^2, \cdot^2; 0, 1 \rangle$ называется сигнатурой колец с единицей. Однако не все алгебраические системы сигнатуры Σ_1 будут кольцами. Для этого необходимо, чтобы операции удовлетворяли определенным условиям (аксиомам колец). Арифметика $\mathfrak{N}$ не является кольцом, а система $\mathfrak{Z} = \langle Z, \underline{+}, \underline{\cdot}; \underline{0}, \underline{1} \rangle$, где Z — множество всех целых чисел ($Z = \{0, 1, 2, \ldots; -1, -2, \ldots\}$), $\underline{+}$, $\underline{\cdot}$ — операции сложения и умножения, $\underline{0} = 0$, $\underline{1} = 1$, будет кольцом. Заметим, что $\mathfrak{N} \subseteq \mathfrak{Z}$. Система $\mathfrak{Z}$ называется *кольцом целых чисел*. Система $\mathfrak{R} = \langle R, \underline{+}, \underline{\cdot}, \underline{0}, \underline{1} \rangle$, где R — действительные числа, $\underline{+}$, $\underline{\cdot}$ — операции сложения и умножения, $\underline{0} = 0$, $\underline{1} = 1$, также является кольцом. Система $\mathfrak{Z}$ является подсистемой $\mathfrak{R}$.

Пример 2. Функциональная сигнатура $\Sigma_2 = \langle \cdot^2, (^{-1})^1; e \rangle$ называется групповой. *Группой подстановок множества* X называется система $\langle S(X), \underline{\cdot}, (\underline{^{-1}}); \underline{e} \rangle$ сигнатуры Σ_2, где $S(X)$ обозначает множество всех разнозначных отображений непустого множества X на себя, $\underline{\cdot}$ — композицию отображений, $(\underline{^{-1}})$ — обращение отображения, $\underline{e}$ — тождественное отображение. Вообще система $\mathfrak{A} = \langle A, \underline{\cdot}, (\underline{^{-1}}); \underline{e}\rangle$ сигнатуры Σ_2 называется *группой*, если для любых $a, a_1, a_2 \in A$ в $\mathfrak{A}$ выполняются следующие равенства:

1) $a \cdot (a_1 \cdot a_2) = (a \cdot a_1) \cdot a_2$,

2) $a \cdot e = e \cdot a = a$,

3) $a \cdot a^{-1} = a^{-1} \cdot a = e$,

где $\underline{\cdot}\,(a, a_1)$, $(\underline{^{-1}})(a)$ записаны более кратко как $a \cdot a_1$ и a^{-1}. Если для любых $a, a_1 \in A$ в $\mathfrak{A}$ выполняются еще равенства

а) $a \cdot a_1 = a_1 \cdot a$,

то группа $\mathfrak{A}$ называется абелевой. Часто, чтобы подчеркнуть, что группа $\mathfrak{A}$ абелева, символы $\cdot$, $(^{-1})$ и e обозначаются через $+$, $(-)$ и 0 соответственно. Примером абелевой группы может служить группа целых чисел $\langle Z, \underline{+}, (\underline{-}); \underline{0}\rangle$, где $\underline{+}$ — сложение, $(\underline{-})$ — операция, переводящая m в $-m$, и $\underline{0} = 0$.

Пример 3. Если предикатная сигнатура $\Sigma = \langle Q^2\rangle$ системы $\mathfrak{A}$ состоит из одного символа двухместного отношения Q, то $\mathfrak{A} = \langle A, \underline{Q}\rangle$ называется графом. Если $\underline{Q}$ — частичный (линейный) порядок на A (см. § 11), то $\mathfrak{A}$ называется частично (линейно) упорядоченным множеством или просто частичным (линейным) порядком*). В этом случае $\langle a, b\rangle \in \underline{Q}$ обозначается через $a \leqslant^{\mathfrak{A}} b$ или просто через $a \leqslant b$. Частичный порядок $\mathfrak{A}$ называется плотным, если из $a \leqslant b$ и $a \neq b$ следует существование такого $c \in A$, что $c \neq a$, $c \neq b$, $a \leqslant c$ и $c \leqslant b$. Будем говорить, что два линейных порядка $\mathfrak{A}$ и $\mathfrak{B}$ *имеют одинаковые концы*, если существование в $\mathfrak{A}$ первого и последнего элемента эквивалентно существованию соответствующего элемента в $\mathfrak{B}$. Заметим, что подсистема частичного (линейного) порядка будет частичным (линейным) порядком, однако подсистема плотного линейного порядка не обязана быть плотным линейным порядком (приведите контрпример).

Предложение 4. *Если $\mathfrak{A}$ и $\mathfrak{B}$ — два счетных плотных линейных порядка с одинаковыми концами, то $\mathfrak{A} \simeq \mathfrak{B}$.*

Доказательство. Пусть $A = \{a_n | n \in \omega\}$, $B = \{b_n | n \in \omega\}$. Рассмотрим множество G, состоящее из

*) Это определение не совсем совпадает с определением ч. у. м. в § 11 (ч. у. м. в § 11 — пара, а граф — тройка), однако в силу нашего соглашения обозначать граф через $\langle A, P\rangle$, где $P \subseteq A^2$, это не будет вызывать путаницы.

отображений $g\colon A_1 \twoheadrightarrow B_1$, удовлетворяющих следующим условиям:

1) A_1 и B_1 — конечные подмножества A и B соответственно;

2) $g\colon \mathfrak{A}(A_1) \rightarrowtail \mathfrak{B}(B_1)$, если $A_1 \neq \varnothing$;

3) если $|A_1| = 2n > 0$, то $\{a_0, \ldots, a_{n-1}\} \subseteq A_1$ и $\{b_0, \ldots \ldots, b_{n-1}\} \subseteq B_1$;

4) если $|A_1| = 2n+1$, то $\{a_0, \ldots, a_n\} \subseteq A_1$ и при $n > 0$ $\{b_0, \ldots, b_{n-1}\} \subseteq B_1$;

5) если $a \in A_1$ — первый (последний) элемент $\mathfrak{A}$, то ga — первый (последний) элемент $\mathfrak{B}$.

Так как $\varnothing \in G$, то $G \neq \varnothing$. Пусть $g\colon A_1 \twoheadrightarrow B_1$ принадлежит G и $|A_1| = 2n$. Из условия 3) получаем, что можно выбрать $a \in A \setminus A_1$, для которого $\{a_0, \ldots, a_n\} \subseteq \subseteq A_1 \cup \{a\}$. Возьмем такой элемент $b \in B \setminus B_1$, что $b \leqslant \leqslant gc \Leftrightarrow a \leqslant c$ для всех $c \in A_1$ и b — первый (последний) элемент в $\mathfrak{B}$ тогда и только тогда, когда a — первый (последний) элемент в $\mathfrak{A}$. Такой элемент существует в силу плотности $\mathfrak{B}$ и условий 2), 5) для g. Ясно, что $g \cup \{\langle a, b\rangle\} \in G$. Если $|A_1| = 2n+1$, то, поменяв местами $\mathfrak{A}$ и $\mathfrak{B}$, точно так же можно найти пару $\langle a, b\rangle \notin g$, для которой $g \cup \{\langle a, b\rangle\} \in G$. Следовательно, в частичном порядке $\langle G, \subseteq\rangle$, где $\subseteq$ — отношение включения, нет максимальных элементов. Тогда в G существует бесконечная цепь $X \subseteq G$. Из условий 2)—4) следует, что объединение элементов X будет изоморфизмом $\mathfrak{A}$ на $\mathfrak{B}$. □

Упражнения

1. Показать, что любая алгебраическая система $\mathfrak{A}$ счетной сигнатуры Σ имеет счетную или конечную подсистему $\mathfrak{B} \subseteq \mathfrak{A}$. (Указание. Определим не более чем счетные множества B_n, $n \in \omega$, следующим образом: $B_0 = \{a\}$, где $a \in A$, $B_{n+1} = B_n \cup \{b \mid b$ является значением функции системы $\mathfrak{A}$ на элементах множества $B_n\}$. Тогда в качестве носителя $\mathfrak{B}$ можно взять множество $B = \bigcup\limits_{n \in \omega} B_n$.)

2. Для данной алгебраической системы $\mathfrak{A}$ пусть $S(\mathfrak{A})$ обозначает множество ее подсистем. Тогда система $\langle S(\mathfrak{A}); \subseteq\rangle$, где $\langle \mathfrak{B}_1, \mathfrak{B}_2\rangle \in \subseteq \Leftrightarrow \mathfrak{B}_1 \subseteq \mathfrak{B}_2$, является решеткой (см. § 11), если сигнатура Σ системы $\mathfrak{A}$ содержит символы констант.

3. Пусть система $\mathfrak{A}$ имеет собственную изоморфную себе подсистему. Тогда $\mathfrak{A}$ имеет собственную изоморфную себе надсистему.

4. Показать, что система $\langle N; \underline{+}\rangle$ имеет счетное число подсистем, а система $\langle N; \underline{\cdot}\rangle$ — несчетное.

5. Показать, что если $|\Sigma| < \omega$, то для любого $n \in \omega$ существует такое конечное множество X систем сигнатуры Σ, что любая

система сигнатуры Σ, имеющая мощность n, изоморфна одной из систем множества X.

6. Чему равна минимальная мощность множества X из упражнения 5, если Σ содержит лишь $k \in \omega$ одноместных предикатов?

7. Показать, что разнозначный гомоморфизм: $h: A \twoheadrightarrow B$ системы $\mathfrak{A}$ на систему $\mathfrak{B}$ функциональной сигнатуры Σ является изоморфизмом $\mathfrak{A}$ на $\mathfrak{B}$. Построить пример, показывающий, что условие $R \neq \varnothing$ на сигнатуру Σ в этом утверждении опустить нельзя.

§ 16. Формулы сигнатуры Σ

Зафиксируем некоторое счетное множество $V = \{v_i | i \in \omega\}$, элементы которого будем называть *символами переменных* или просто *переменными* и обозначать буквами x, y и z, возможно, с индексами. Если в тексте встречается последовательность $x_0, \ldots, x_n$ переменных, то всегда предполагается, что $x_i \neq x_j$ для $i \neq j$.

Определение. Множество $T(\Sigma)$ *термов сигнатуры* $\Sigma = \langle R, F, \mu \rangle$ определяется по индукции:

1) переменные $x \in V$ являются термами сигнатуры Σ;

2) если $t_1, \ldots, t_n$ — термы сигнатуры Σ, $f \in F$ и $\mu(f) = n$, то $f(t_1, \ldots, t_n)$ — терм сигнатуры Σ.

Напомним, что запись $\Theta(\tau_1, \ldots, \tau_n)$ при $n = 0$ обозначает Θ; в частности, из 2) получаем, что символ $c \in F$ константы сигнатуры Σ является термом сигнатуры Σ.

Таким образом, термы — это слова (конечно, не все слова) алфавита $V \cup F \cup \{(,)\} \cup \{,\}$. Множество переменных, входящих в терм t, обозначаем через $FV(t)$. Если $FV(t) = \varnothing$, то терм t называется константным или замкнутым. Если t — терм сигнатуры Σ, то запись $t(x_1, \ldots, x_n)$ будет обозначать, что $FV(t) \subseteq \{x_1, \ldots, x_n\}$. Эту запись также будем называть термом *).

Определение. Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры Σ. Отображение γ множества $X \subseteq V$ в A называется *интерпретацией переменных* множества X в A. Если $FV(t) \subseteq X$ для терма t сигнатуры Σ, то индукцией по длине t определяем *значение* $t^{\mathfrak{A}}[\gamma] \in A$ *терма* t *в* $\mathfrak{A}$ *при интерпретации* γ:

---

*) Эта запись, конечно, как и буква t, есть не терм, а обозначение («имя») терма.

1) если $t = x$, $x \in V$, то $t^{\mathfrak{A}}[\gamma] = \gamma x$;

2) если $t = f(t_1, \ldots, t_n)$, $f \in F$, то $t^{\mathfrak{A}}[\gamma] = \nu^{\mathfrak{A}}(f)\left(t_1^{\mathfrak{A}}[\gamma], \ldots \ldots, t_n^{\mathfrak{A}}[\gamma]\right)$.

Ясно, что если $\gamma_1\colon X_1 \to A$, $\gamma_2\colon X_2 \to A$ — две интерпретации, $t \in T(\Sigma)$, $FV(t) \subseteq X_1 \cap X_2$ и $\gamma_1 \upharpoonright FV(t) = \gamma_2 \upharpoonright FV(t)$, то $t^{\mathfrak{A}}[\gamma_1] = t^{\mathfrak{A}}[\gamma_2]$. Часто для краткости вместо $t^{\mathfrak{A}}(x_1, \ldots \ldots, x_n)[\gamma]$ мы будем писать $t^{\mathfrak{A}}(a_1, \ldots, a_n)$, где $a_1 = \gamma(x_1), \ldots, a_n = \gamma(x_n)$. Если в тексте встречается запись $t(x_1, \ldots, x_n)$, то следующая за этим запись $t^{\mathfrak{A}}(a_1, \ldots, a_n)$, $a_1, \ldots, a_n \in A$, будет обозначать $t^{\mathfrak{A}}(x_1, \ldots, x_n)[\gamma]$, где γ определяется так: $\gamma x_i = a_i$, $i = 1, \ldots, n$.

Предложение 1. а) *Если $\mathfrak{A}$ — алгебраическая система сигнатуры Σ, $X \subseteq A$, $X \neq \varnothing$, то носитель $A(X)$ подсистемы $\mathfrak{A}(X)$ равен множеству $\{t^{\mathfrak{A}}[\gamma] \mid t \in T(\Sigma), \gamma\colon FV(t) \to X\}$.*

б) *Если h — гомоморфизм алгебраической системы $\mathfrak{A}$ сигнатуры Σ в систему $\mathfrak{B}$, $t(x_1, \ldots, x_n) \in T(\Sigma)$ и $a_1, \ldots \ldots, a_n \in A$,* то $h\left(t^{\mathfrak{A}}(a_1, \ldots, a_n)\right) = t^{\mathfrak{B}}(ha_1, \ldots, ha_n)$.

Доказательство. а) Пусть $Y = \{t^{\mathfrak{A}}[\gamma] \mid t \in T(\Sigma), \gamma\colon FV(t) \to X\}$. Индукцией по длине терма t получаем, что если $t(x_1, \ldots, x_n) \in T(\Sigma)$ и $a_1, \ldots, a_n \in X$, то $t^{\mathfrak{A}}(a_1, \ldots, a_n) \in B$ для любой подсистемы $\mathfrak{B} \subseteq \mathfrak{A}$, для которой $X \subseteq B$. Поэтому достаточно показать, что Y замкнуто относительно операций системы $\mathfrak{A}$. Пусть $f \in F$, $\mu(f) = m$, $t_1, \ldots, t_m \in T(\Sigma)$ и $\gamma\colon (FV(t_1) \cup \ldots \cup FV(t_m)) \to \to X$. Тогда $\nu^{\mathfrak{A}}(f)\left(t_1^{\mathfrak{A}}[\gamma], \ldots, t_n^{\mathfrak{A}}[\gamma]\right) = t_0^{\mathfrak{A}}[\gamma] \in Y$, где $t_0 = f(t_1, \ldots, t_n)$.

б) Легко доказывается индукцией по длине t. □

Определение. Множество $F(\Sigma)$ *формул сигнатуры* $\Sigma = \langle R, F, \mu\rangle$ определяется по индукции.

1) Если $r \in R$, $\mu(r) = n$ и $t_1, \ldots, t_n \in T(\Sigma)$, то слово $r(t_1, \ldots, t_n)$ является формулой сигнатуры Σ.

2) Если $t_1, t_2 \in T(\Sigma)$, то слово $t_1 \approx t_2$ является формулой сигнатуры Σ.

3) Если Φ, Ψ — формулы сигнатуры Σ, то $(\Phi \wedge \Psi)$, $(\Phi \vee \Psi)$, $(\Phi \to \Psi)$ и $\neg\Phi$ — формулы сигнатуры Σ.

4) Если Φ — формула сигнатуры Σ, $x \in V$, то $\forall x \Phi$ и $\exists x \Phi$ — формулы сигнатуры Σ.

Таким образом, множество $F(\Sigma)$ формул сигнатуры Σ состоит из некоторых слов алфавита $V \cup R \cup F \cup \{\wedge, \vee,$

$\to, \neg, \approx\} \cup \{\forall, \exists\} \cup \{(\ ,\ )\} \cup \{\ ,\ \}$. Например, если $r \in R$, $f,\ g,\ c \in F,\ \mu(r) = \mu(g) = 2,\ \mu(f) = 1,\ \mu(c) = 0$, то слово

$$(\forall v_1 \exists v_2 r(v_2, f(v_3)) \vee \neg v_4 \approx g(v_1, c))$$

является формулой сигнатуры Σ, в то время как слова $v_1 \approx v_2 \forall v_1$, $c \approx v_1 \vee v_2 \approx c$, $(\forall v_1 r(f(v_3), v_2))$,

$$(\exists v_1 r(v_1, v_2, v_1) \vee c \approx v_3)$$

формулами сигнатуры Σ не являются (почему?). При этом последнее слово является формулой, только другой сигнатуры.

Последовательность Φ некоторых символов будем называть просто *формулой*, если она является формулой некоторой сигнатуры. Если Φ — формула, то через $\Sigma(\Phi)$ будем обозначать сигнатуру, все символы которой входят в Φ, и Φ является формулой сигнатуры $\Sigma(\Phi)$. Ясно, что $\Sigma(\Phi)$ определяется по Φ однозначно.

Подслово формулы Φ, которое само является формулой, называется *подформулой* формулы Φ. Формулы вида $r(t_1, \ldots, t_n)$ и $t_1 \approx t_2$, где r — предикатный символ, $t_1, t_2, \ldots$ — термы, называются *атомарными* *). Атомарные формулы, содержащие не более одного сигнатурного символа, называются *атомными*. Таким образом, атомная формула сигнатуры Σ имеет один из следующих видов:

$$v_i \approx v_j,\quad c \approx v_i,\quad v_i \approx c,\quad v_j \approx f(v_{i_0}, \ldots, v_{i_n}),$$
$$f(v_{i_0}, \ldots, v_{i_n}) \approx v_j,\quad r(v_{i_0}, \ldots, v_{i_n}),\quad r,$$

где c — константа, f — функциональный символ, а r — предикатный символ сигнатуры Σ. Символ $\approx$ называется *символом равенства* или просто равенством. Символы $\forall$ и $\exists$ называются соответственно *кванторами всеобщности* и *существования*. Запись $\forall x$ (запись $\exists x$) читается «для всех x» («существует x»). Формулу, не содержащую кванторов, будем называть бескванторной.

Доказательство следующих трех предложений является по существу повторением доказательств предложений 2.1, 2.2 и следствия 2.1 соответственно. (Рассмотрение случаев, когда формула начинается с кванторов, не отличается по существу от рассмотрения в указанных

*) В некоторых книгах такие формулы называются элементарными, но мы этот термин употреблять не будем.

предложениях случая, когда формула начинается с отрицания.)

Предложение 2. *Всякая неатомарная формула Φ сигнатуры Σ представима в одном и только одном из следующих видов:*

$$(\Psi \wedge X), \quad (\Psi \vee X), \quad (\Psi \to X), \quad \forall x \Psi, \exists x \Psi, \quad \neg \Psi$$

для однозначно определенных формул Ψ и X сигнатуры Σ. □

Предложение 3. *Если Φ — формула сигнатуры Σ, а η и θ — вхождения в Φ подформул Ψ и X соответственно, то либо η и θ не имеют общих вхождений символов, либо одно из них целиком содержится в другом.* □

Предложение 4. *С каждым вхождением в формулу Φ сигнатуры Σ символов (, $\neg$, $\forall$ или $\exists$ однозначно связано некоторое вхождение подформулы формулы Φ, первым символом которого является рассматриваемое вхождение соответствующего символа.* □

Определение. Подформула формулы Φ сигнатуры Σ, связанная по предложению 4 с вхождением квантора $\forall$ (квантора $\exists$), называется *областью действия этого вхождения квантора* $\forall$ (квантора $\exists$).

Мы будем в дальнейшем пользоваться соглашением об опускании внешних скобок, принятом в § 2 главы 1. Заметим, что формулу исчисления высказываний можно рассматривать как формулу некоторой сигнатуры, если считать, что символы пропозициональных переменных являются нульместными предикатными символами.

Определение. Для каждой формулы Φ сигнатуры Σ определим множество $FV(\Phi)$ *свободных переменных формулы* Φ следующим образом.

1) Если Φ — атомарная формула вида r, $r(t_1, \ldots, t_n)$ или $t_1 \approx t_2$, то множество $FV(\Phi)$ равно $\varnothing$, $FV(t_1) \cup \ldots \cup FV(t_n)$ или $FV(t_1) \cup FV(t_2)$ соответственно.

2) Если $\Phi = \neg\Psi$, то $FV(\Phi) = FV(\Psi)$.

3) Если $\Phi = \Phi_1 \tau \Phi_2$, где $\tau \in \{\wedge, \vee, \to\}$, то $FV(\Phi) = FV(\Phi_1) \cup FV(\Phi_2)$.

4) Если $\Phi = \mathsf{Q} x \Psi$, где $\mathsf{Q} \in \{\forall, \exists\}$, то $FV(\Phi) = FV(\Psi) \setminus \{x\}$.

Ясно, что для любой формулы Φ через конечное число шагов можно найти все элементы $FV(\Phi)$.

Вхождение η переменной x в формулу Φ сигнатуры Σ будем называть *связанным*, если η лежит в области действия некоторого вхождения квантора $\forall$ или $\exists$, за которым сразу следует символ x. Если вхождение η переменной x в формулу Φ не является связанным, то будем его называть *свободным*. Если формула Φ содержит свободные (связанные) вхождения переменной x, то будем говорить, что *x входит свободно* (*связанно*) в формулу Φ.

Предложение 5. *Если Φ — формула сигнатуры Σ, то переменная x тогда и только тогда принадлежит $FV(\Phi)$, когда существует свободное вхождение x в Φ.*

Доказательство легко проводится индукцией по длине Φ, и мы оставляем его читателю. $\square$

Если Φ — формула, то запись $\Phi(x_1, \ldots, x_n)$ в дальнейшем будет обозначать формулу Φ, а также то, что $FV(\Phi) \subseteq \{x_1, \ldots, x_n\}$.

Определим главное понятие этой главы.

Определение. Для алгебраической системы $\mathfrak{A}$ сигнатуры Σ, интерпретации переменных γ: $X \to A$ и формулы $\Phi \in F(\Sigma)$, для которой $FV(\Phi) \subseteq X$, определим отношение $\mathfrak{A} \vDash \Phi[\gamma]$ (читается «*в $\mathfrak{A}$ истинно* $\Phi[\gamma]$») индукцией по длине Φ.

1) Если $\Phi = r$, $r \in R$, $\mu(r) = 0$, то $\mathfrak{A} \vDash \Phi[\gamma]$ эквивалентно $\varnothing \in \nu^{\mathfrak{A}}(r)$.

2) Если $\Phi = r(t_1, \ldots, t_n)$, $r \in R$, $\mu(r) = n$, $t_1, \ldots, t_n \in T(\Sigma)$, то $\mathfrak{A} \vDash \Phi[\gamma]$ эквивалентно $\left\langle t_1^{\mathfrak{A}}[\gamma], \ldots, t_n^{\mathfrak{A}}[\gamma]\right\rangle \in \nu^{\mathfrak{A}}(r)$ *).

3) Если Φ равна $t_1 \approx t_2$, $t_1, t_2 \in T(\Sigma)$, то $\mathfrak{A} \vDash \Phi[\gamma]$ эквивалентно $t_1^{\mathfrak{A}}[\gamma] = t_2^{\mathfrak{A}}[\gamma]$.

4) Если $\Phi = \neg \Psi$, то $\mathfrak{A} \vDash \Phi[\gamma]$ тогда и только тогда, когда неверно, что $\mathfrak{A} \vDash \Psi[\gamma]$.

5) Если $\Phi = (\Phi_1 \wedge \Phi_2)$, то $\mathfrak{A} \vDash \Phi[\gamma] \Leftrightarrow (\mathfrak{A} \vDash \Phi_1[\gamma]$ и $\mathfrak{A} \vDash \Phi_2[\gamma])$.

6) Если $\Phi = (\Phi_1 \vee \Phi_2)$, то $\mathfrak{A} \vDash \Phi[\gamma] \Leftrightarrow (\mathfrak{A} \vDash \Phi_1[\gamma]$ или $\mathfrak{A} \vDash \Phi_2[\gamma])$.

7) Если $\Phi = (\Phi_1 \to \Phi_2)$, то $\mathfrak{A} \vDash \Phi[\gamma] \Leftrightarrow$ (если имеет место $\mathfrak{A} \vDash \Phi_1[\gamma]$, то имеет место и $\mathfrak{A} \vDash \Phi_2[\gamma]$).

8) Если $\Phi = \exists x \Psi$, то $\mathfrak{A} \vDash \Phi[\gamma]$ имеет место тогда и только тогда, когда существует такая интерпретация

---

*) Конечно, 2) включает 1), так как мы договорились считать $r(t_1, \ldots, t_n)$ при $n = 0$ равным r. Мы здесь включили 1), чтобы подчеркнуть специфику нульместных предикатов.

$\gamma_1\colon X_1 \to A$, для которой $x \in X_1$, $\gamma_1 \restriction FV(\Phi) = \gamma \restriction FV(\Phi)$ и $\mathfrak{A} \models \Psi[\gamma_1]$.

9) Если $\Phi = \forall x \Psi$, то $\mathfrak{A} \models \Phi[\gamma]$ имеет место тогда и только тогда, когда для любой интерпретации $\gamma_1\colon X_1 \to A$, для которой $x \in X_1$ и $\gamma_1 \restriction FV(\Phi) = \gamma \restriction FV(\Phi)$, имеет место $\mathfrak{A} \models \Psi[\gamma_1]$.

Из этого определения видно, что при установлении истинности формулы Φ сигнатуры Σ свободные и связанные вхождения переменных в формулу Φ играют совершенно различные роли. А именно, свободным вхождениям переменной x «приписывается» постоянное значение $\gamma(x)$, в то время как связанным вхождениям переменных никакие постоянные значения не «приписываются», а рассматриваются всевозможные их значения.

Предложение 6. *Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры Σ и $\Phi \in F(\Sigma)$. Если $\gamma_1\colon X_1 \to A$, $\gamma_2\colon X_2 \to A$ — две интерпретации, для которых $FV(\Phi) \subseteq X_1 \cap X_2$ и $\gamma_1 \restriction FV(\Phi) = \gamma_2 \restriction FV(\Phi)$, то $\mathfrak{A} \models \Phi[\gamma_1] \Leftrightarrow \mathfrak{A} \models \Phi[\gamma_2]$.*

Доказательство легко проводится индукцией по длине Φ. □

Мы часто будем использовать вместо $\mathfrak{A} \models \Phi(x_1, \ldots, x_n)[\gamma]$ более удобную запись $\mathfrak{A} \models \Phi(a_1, \ldots, a_n)$, где $a_1 = \gamma(x_1), \ldots, a_n = \gamma(x_n)$. А именно, если в тексте встречается запись $\Phi(x_1, \ldots, x_n)$, то следующая за этим запись $\mathfrak{A} \models \Phi(a_1, \ldots, a_n)$, $a_1, \ldots, a_n \in A$, будет обозначать $\mathfrak{A} \models \Phi(x_1, \ldots, x_n)[\gamma]$, где γ определяется так: $\gamma x_i = a_i$, $i = 1, \ldots, n$. В силу предложения 6 такое сокращение возможно.

Определение. Если Φ — формула сигнатуры Σ и $FV(\Phi) = \varnothing$, то Φ называется *замкнутой формулой* или *предложением*.

Если Φ — предложение сигнатуры Σ, $\mathfrak{A}$ — система сигнатуры Σ, то отношение $\mathfrak{A} \models \Phi[\gamma]$ не зависит от интерпретации γ, и мы его будем обозначать просто $\mathfrak{A} \models \Phi$. Ясно также, что если для формулы Φ, системы $\mathfrak{A}$ и интерпретации γ определено отношение $\mathfrak{A} \models \Phi[\gamma]$, то $\mathfrak{A} \models \Phi[\gamma] \Leftrightarrow \mathfrak{A} \restriction \Sigma(\Phi) \models \Phi[\gamma]$. Если $\Phi[\gamma]$ не истинно в $\mathfrak{A}$, то говорим, что $\Phi[\gamma]$ *ложно в* $\mathfrak{A}$.

Определение. Формула Φ называется *тождественно истинной или общезначимой, если* $\mathfrak{A} \models \Phi[\gamma]$ для любой системы $\mathfrak{A}$ сигнатуры $\Sigma(\Phi)$ и любой интерпретации $\gamma\colon FV(\Phi) \to A$. Ясно, что сигнатуру $\Sigma(\Phi)$ в этом определении можно заменить на любую $\Sigma \supseteq \Sigma(\Phi)$. Множество формул $Y \subseteq F(\Sigma)$ называется *выполнимым в системе* $\mathfrak{A}$ сигнатуры Σ, если существует такая интерпретация γ: $\bigcup_{\Phi \in Y} FV(\Phi) \to A$, что $\mathfrak{A} \models \Phi[\gamma]$ для всех $\Phi \in Y$. Формула Φ называется *выполнимой в системе* $\mathfrak{A}$, если множество $\{\Phi\}$ выполнимо в $\mathfrak{A}$.

Понятие истинности формулы на системе наряду с понятием выводимости принадлежит к основным понятиям математической логики. Важность этого понятия объясняется тем, что многие теоремы математики можно выразить как утверждения об истинности некоторых формул на алгебраических системах из некоторого класса. В отличие от свойств «быть формулой» и «быть тождественно истинной формулой ИВ», в общем случае не существует эффективного способа, позволяющего для предложения Φ за конечное число шагов установить, верно ли $\mathfrak{A} \models \Phi$. Это связано с тем, что при бесконечном A пп. 8) и 9) требуют проверки бесконечного числа условий *). Пункты 2) и 3) в общем случае также не «эффективны», так как предикаты и функции бесконечной системы $\mathfrak{A}$ могут быть заданы не «эффективно».

Установим теперь простой, но важный факт.

Предложение 7. *Если f — изоморфизм системы $\mathfrak{A}$ на систему $\mathfrak{B}$, $\Phi(x_1, \ldots, x_n)$ — формула сигнатуры системы $\mathfrak{A}$, то для любых $a_1, \ldots, a_n \in A$ свойство $\mathfrak{A} \models \Phi(a_1, \ldots, a_n)$ эквивалентно $\mathfrak{B} \models \Phi(fa_1, \ldots, fa_n)$. В частности, если Φ — предложение, то $\mathfrak{A} \models \Phi$ эквивалентно $\mathfrak{B} \models \Phi$.*

Доказательство легко проводится индукцией по длине Φ. Если Φ — атомарная формула, то утверждение следует из определения изоморфизма и предложения 1 б). Индукционный шаг оставляется читателю в качестве упражнения. □

В отличие от бесконечных систем, проверку истинности формулы Φ на конечной системе $\mathfrak{A}$ сигнатуры $\Sigma(\Phi)$ можно осуществить за конечное число шагов. Это легко показать индукцией по длине Φ.

Определение. Пусть $n \in \omega$, $n > 0$. Предложение Φ называется *n-общезначимым*, если $\mathfrak{A} \models \Phi$ для любой алгебраической системы $\mathfrak{A}$ мощности n и сигнатуры $\Sigma(\Phi)$.

Предложение 8. *Существует эффективная процедура (алгоритм), позволяющая для любого $n \in \omega$,*

*) В главе 7 будет показано, что эту трудность нельзя обойти.

$n > 0$, *и любого предложения* Φ *за конечное число шагов установить, является ли* Φ *n-общезначимым или нет.*

Доказательство. Очевидно, что для конечного множества X множества $P(X)$ и X^n, $n \in \omega$, конечны. Поэтому для любой конечной сигнатуры Σ имеется лишь конечное число систем сигнатуры Σ с конечным носителем X. Тогда процедура проверки n-общезначимости сведется к выписыванию всех систем сигнатуры $\Sigma(\Phi)$ с носителем $\{1, 2, \ldots, n\}$ и проверке истинности Φ на каждой из выписанных систем. Такая проверка, как отмечалось выше, осуществляется за конечное число шагов. □

Можно определить аналогично n-общезначимости, $0 < n < \omega$, понятие $\varkappa$-общезначимости формулы Φ для бесконечного кардинала $\varkappa$. Как будет показано в § 24, эти понятия для всех бесконечных кардиналов $\varkappa$ совпадают. Какие еще зависимости существуют между этими понятиями? Как будет показано в следующем параграфе, если предложение Φ бесконечно общезначимо, то существует такое число $n_0 \in \omega$, что Φ является k-общезначимым для любого $k \geqslant n_0$. Из n-общезначимости предложения Φ для любого $n \in \omega$, $n \neq 0$, в общем случае не следует (упражнение 4) общезначимость Φ. Отметим, что полного описания множества

$$S = \{X \subseteq \omega \mid X \text{ равно } \{n \mid \Phi\ n\text{-общезначимо}\} \text{ для некоторого предложения } \Phi\}$$

пока не получено. Неизвестно даже, замкнуто ли множество S относительно дополнения в множестве ω. Мы отметим здесь простой факт.

Предложение 9. *Для любого* $n \in \omega$, $n \geqslant 1$, *существует такое предложение* Φ_n *пустой сигнатуры* Σ_0 (т. е. $\Sigma_0 = \langle \varnothing, \varnothing, \varnothing \rangle$), *для которого* Φ_n *является n-общезначимым, а* $\neg \Phi_n$ *является k-общезначимым для любого* $k \neq n$, $k \geqslant 1$.

Доказательство. В качестве Φ_n можно взять предложение

$$\exists v_1, \ldots \exists v_n ((\neg v_1 \approx v_2 \wedge (\neg v_1 \approx v_3 \wedge \wedge (\ldots \wedge \neg v_{n-1} \approx v_n) \ldots)) \wedge \forall v_0 (v_0 \approx v_1 \vee \vee (\ldots \vee v_0 \approx v_n) \ldots)). \quad \square$$

Формула $\forall v_1 \forall v_2 (P(v_1) \to P(v_2))$ не содержит символов равенства и функций, является 1-общезначимой и не является n-общезначимой для $n > 1$. Легко строится (упражнение 3) также формула Ψ_n без равенства и функций, являющаяся k-общезначимой для $0 < k \leqslant n$ и не являющаяся m-общезначимой для $m > n$. Построить формулу Φ_n из предложения 9 без равенства и функций нельзя в силу следующего факта (упражнение 5): если предложение Φ не содержит символов равенства и функций, то из n-общезначимости Φ следует k-общезначимость Φ для любого $k \leqslant n$, $k \neq 0$.

Упражнения

1. Показать, что для любой конечной сигнатуры Σ существует процедура, позволяющая по любой конечной последовательности символов определить, является ли она формулой сигнатуры Σ или нет.

2. Пусть h — гомоморфизм системы $\mathfrak{A}$ сигнатуры Σ в систему $\mathfrak{B}$. Тогда для любой атомарной $\Phi(x_1, \ldots, x_n) \in F(\Sigma)$ и любых $a_1, \ldots, a_n \in A$ имеем $\mathfrak{A} \models \Phi(a_1, \ldots, a_n) \Rightarrow \mathfrak{B} \models \Phi(ha_1, \ldots, ha_n)$.

3. Показать, что следующая формула Ψ_n является k-общезначимой тогда и только тогда, когда $1 \leqslant k \leqslant n$:

$$\exists v_2 \ldots \exists v_{n+1} \forall v_0 (\forall v_1 (r(v_2, v_1) \to r(v_0, v_1)) \vee$$
$$\vee (\ldots \vee \forall v_1 (r(v_{n+1}, v_1) \to r(v_0, v_1)) \ldots)).$$

4. Показать, что следующая формула является n-общезначимой для любого $n \in \omega$, $n \neq 0$, и не является общезначимой:

$$\exists v_0 \forall v_1 \neg f(v_1) \approx v_0 \to \exists v_0 \exists v_1 (f(v_0) \approx f(v_1) \wedge \neg v_0 \approx v_1).$$

5. Пусть $0 < k < n < \omega$, предложение Φ n-общезначимо, не содержит символов равенства и функций. Тогда Φ k-общезначимо. (Указание. Пусть $\mathfrak{A} \models \neg \Phi$, где $\mathfrak{A}$ — система сигнатуры $\Sigma(\Phi)$ с носителем $\{1, 2, \ldots, k\}$. Строим систему $\mathfrak{B} \supseteq \mathfrak{A}$ мощности n, определяя на множестве $B = \{1, 2, \ldots, n\}$ предикаты r сигнатуры $\Sigma(\Phi)$ следующим образом:

$$\langle i_1, \ldots, i_m \rangle \in \nu^{\mathfrak{B}}(r) \Leftrightarrow \langle j_1, \ldots, j_m \rangle \in \nu^{\mathfrak{A}}(r),$$

где $j_s = i_s$, если $i_s \leqslant k$, $j_s = k$ в противном случае. Тогда $\mathfrak{B} \models \neg \Phi$.)

§ 17. Теорема компактности

Теорема компактности была доказана А. И. Мальцевым в 1936 г. Он же впервые показал ее важное значение как нового метода для доказательства не только теорем математической логики, но и теорем алгебры. Мы дадим доказательство этой теоремы с помощью ультрапроизведений, введенных Лосем в 1955 г.

Пусть дано семейство множеств $S = \{X_i \mid i \in I\}$. *Декартовым произведением* семейства S называется множество

$$I\text{-prod}\,X_i = \left\{f\colon\ I \to \bigcup_{i\in I} X_i \mid fi \in X_i\right\}.$$

Для $j \in I$ отображение множества I-prod X_i в X_j, сопоставляющее элементу f элемент $f(j)$, называется *проекцией* декартова произведения на j-ю координату и обозначается той же буквой j.

Пусть на I задан фильтр D. Определим на I-prod X_i отношение $\overset{D}{\sim}$ следующим образом:

$$f \overset{D}{\sim} g \Leftrightarrow \{i \mid fi = gi\} \in D.$$

Лемма 1. *Отношение $\overset{D}{\sim}$ является эквивалентностью на I-prod X_i.*

Доказательство. Рефлексивность и симметричность $\overset{D}{\sim}$ очевидна. Пусть $f \overset{D}{\sim} g$ и $g \overset{D}{\sim} h$. Тогда множество $Y = \{i | fi = hi\}$ содержит пересечение множеств $\{i | fi = gi\}$ и $\{i | gi = hi\}$, являющихся элементами D. Из условий 2) и 3) определения фильтра получаем $Y \in D$. □

Отображение, сопоставляющее элементу $f \in I$-prod X_i класс эквивалентности по отношению $\overset{D}{\sim}$, содержащий f, будем обозначать той же буквой D, что и фильтр. Множество

$$D\text{-prod}\,X_i = \{Df \mid f \in I\text{-prod}\,X_i\}$$

называется *фильтрованным произведением множеств X_i, $i \in I$, по фильтру D.*

Определение. *Фильтрованным произведением по фильтру D семейства алгебраических систем $\{\mathfrak{A}_i | i \in I\}$ сигнатуры Σ* называется алгебраическая система $\mathfrak{A} = D$-prod $\mathfrak{A}_i$ сигнатуры Σ с носителем $A = D$-prod A_i и следующей интерпретацией $\nu^{\mathfrak{A}}$ сигнатуры Σ в $\mathfrak{A}$.

1) Если $c \in F$ и $\mu(c) = 0$, то для $f \in I$-prod A_i

$$Df = \nu^{\mathfrak{A}}(c) \Leftrightarrow \left\{i \mid fi = \nu^{\mathfrak{A}_i}(c)\right\} \in D.$$

2) Если $s \in R \cup F$, то для $f_1, \ldots, f_n \in I$-prod A_i

$$\langle Df_1, \ldots, Df_n\rangle \in \nu^{\mathfrak{A}}(s) \Leftrightarrow \left\{i \mid \langle f_1 i, \ldots, f_n i\rangle \in \nu^{\mathfrak{A}_i}(s)\right\} \in D,$$

где $n = \mu(s)$, если $s \in R$, и $n = \mu(s) + 1$, если $s \in F$.

Проверим, что определение корректно, т. е. множества $\nu^{\mathfrak{A}}(s)$ и $\nu^{\mathfrak{A}}(c)$ не зависят от выбора представителей $f_1, \ldots, f_n$ и f в классах $Df_1, \ldots, Df_n$ и Df. В самом деле, пусть $Y_k = \{i \mid f_k i = g_k i\} \in D$, $1 \leqslant k \leqslant n$. Множества $W_1 = \left\{i \mid \langle f_1 i, \ldots, f_n i\rangle \in \nu^{\mathfrak{A}_i}(s)\right\}$ и $W_2 = \left\{i \mid \langle g_1 i, \ldots \right.$ $\left. \ldots, g_n i\rangle \in \nu^{\mathfrak{A}_i}(s)\right\}$ имеют одинаковые пересечения с элементом $Y_1 \cap \ldots \cap Y_n$ фильтра D. Следовательно, $W_1 \in$ $\in D \Leftrightarrow W_2 \in D$. Аналогично показывается корректность 1). Для того чтобы утверждать, что $\mathfrak{A}$ является системой сигнатуры Σ, нужно еще показать, что $\nu^{\mathfrak{A}}(s)$ — операция на A, если $s \in F$. Пусть $s \in F$ и $\mu(s) = n$. Для элементов $f_1, \ldots, f_n \in I\text{-prod}\, A_i$ определим $f \in I\text{-prod}\, A_i$ так: $fi = \nu^{\mathfrak{A}_i}(s)(f_1 i, \ldots, f_n i)$, $i \in I$. Тогда $\langle Df_1, \ldots, Df_n,$ $Df\rangle \in \nu^{\mathfrak{A}}(s)$. Пусть для некоторой $g \in I\text{-prod}\, A_i$ имеет место

$$\langle Df_1, \ldots, Df_n, Dg\rangle \in \nu^{\mathfrak{A}}(s).$$

Так как $\nu^{\mathfrak{A}_i}(s)$, $i \in I$, — функции, то множество $\{i \mid fi = gi\}$ содержит пересечение множеств $\left\{i \mid \langle f_1 i, \ldots, f_n i, fi\rangle \in \right.$ $\left. \in \nu^{\mathfrak{A}_i}(s)\right\}$ и $\left\{i \mid \langle f_1 i, \ldots, f_n i, gi\rangle \in \nu^{\mathfrak{A}_i}(s)\right\}$, которые принадлежат D. Следовательно, $Df = Dg$.

Фильтрованное произведение $\{I\}\text{-prod}\, \mathfrak{A}_i$ называется *декартовым* или *прямым произведением* систем $\mathfrak{A}_i$, $i \in I$. Дадим независимое определение для этого важного частного случая. Пусть $\mathfrak{A} = I\text{-prod}\, \mathfrak{A}_i$ является системой сигнатуры Σ с носителем $A = I\text{-prod}\, A_i$ и следующей интерпретацией Σ в A.

1) Если $c \in F$ и $\mu(c) = 0$, то

$$\nu^{\mathfrak{A}}(c)(i) = \nu^{\mathfrak{A}_i}(c).$$

2) Если $s \in R \cup F$, то

$$\langle f_1, \ldots, f_n\rangle \in \nu^{\mathfrak{A}}(s) \Leftrightarrow \langle f_1 i, \ldots, f_n i\rangle \in \nu^{\mathfrak{A}_i}(s)$$

для всех $i \in I$, где $n = \mu(s)$, если $s \in R$, и $n = \mu(s) + 1$, если $s \in F$.

Ясно, что отображение, сопоставляющее элементу f элемент $\{f\}$, будет изоморфизмом $I\text{-prod}\, \mathfrak{A}_i$ на $\{I\}\text{-prod}\, \mathfrak{A}_i$, поэтому, не опасаясь путаницы, систему $I\text{-prod}\, \mathfrak{A}_i$ будем также называть декартовым или прямым произведением. Декартово произведение $I\text{-prod}\, \mathfrak{A}_i$ часто обозначается через $\prod\limits_{i \in I} \mathfrak{A}_i$ и через $\mathfrak{A}_{i_1} \times \ldots \times \mathfrak{A}_{i_n}$, если $I = \{i_1, \ldots, i_n\}$ —

конечное множество. Укажем один простой, но полезный факт, связывающий декартовы произведения с фильтрованными.

Предложение 1. *Для любого фильтра D на I и систем $\{\mathfrak{A}_i | i \in I\}$ сигнатуры Σ отображение D: I-$\mathrm{prod}\, A_i \to D$-$\mathrm{prod}\, A_i$ является гомоморфизмом системы $\mathfrak{A} = I$-$\mathrm{prod}\, \mathfrak{A}_i$ на систему $\mathfrak{A}' = D$-$\mathrm{prod}\, \mathfrak{A}_i$.*

Доказательство. Пусть $s \in R \cup F$ — не константа и $\langle f_1, \ldots, f_n \rangle \in \nu^{\mathfrak{A}}(s)$. По определению декартова произведения $\left\{i \mid \langle f_1 i, \ldots, f_n i \rangle \in \nu^{\mathfrak{A}_i}(s)\right\} = I$. Так как $I \in D$, то $\left\{i \mid \langle f_1 i, \ldots, f_n i \rangle \in \nu^{\mathfrak{A}_i}(s)\right\} \in D$, т. е. $\langle Df_1, \ldots, Df_n \rangle \in \nu^{\mathfrak{A}'}(s)$. Случай, когда s — константа, рассматривается аналогично. □

Под *классом* в дальнейшем мы понимаем некоторое свойство Θ множеств *). При этом множества, удовлетворяющие свойству Θ, будут называться элементами класса Θ. В частности, все множества образуют класс V, который, как уже отмечалось, не является множеством. Свойство «быть элементом множества X» определяет множество X, поэтому любое множество можно считать классом. Конечно, с классами нельзя поступать, как с множествами, например, нельзя рассматривать класс всех подклассов данного класса K. Однако если K_1, K_2 — классы, то очевидным образом определены классы $K_1 \cap K_2$, $K_1 \cup K_2$ и $K_1 \setminus K_2$. Если a — элемент класса K, то так же, как и в случае множеств, мы будем говорить, что a принадлежит K, и обозначать $a \in K$.

Пусть даны некоторый класс K алгебраических систем сигнатуры Σ и фильтр D на I. Говорим, что класс K *замкнут относительно фильтрованных произведений по фильтру* D, если для любого множества $\{\mathfrak{A}_i | i \in I\}$ систем из класса K имеем D-$\mathrm{prod}\, \mathfrak{A}_i \in K$. Если для $\Phi(x_1, \ldots, x_n) \in F(\Sigma)$ определить $K(\Phi)$ как класс таких систем $\mathfrak{A}$ сигнатуры Σ, что для всех $a_1, \ldots, a_n \in A$ в $\mathfrak{A}$ истинно $\Phi(a_1, \ldots, a_n)$, то легко проверить, что для атомарной формулы Φ класс $K(\Phi)$ замкнут относительно

*) Так как мы взяли за основу систему ZFC, то под свойством Θ мы понимаем свойство, записанное формулой $\Phi(x, y_1, \ldots, y_n)$ сигнатуры $\langle \in^2 \rangle$, где переменные $y_1, \ldots, y_n$ играют роль параметров. В качестве «кода» класса K, определенного с помощью параметров $a_1, \ldots, a_n$, можно взять множество $\langle \langle y_1, a_1 \rangle, \ldots, \langle y_n, a_n \rangle, \Phi(x\ y_1, \ldots, y_n) \rangle$, где $\Phi(x, y_1, \ldots, y_n)$ — формула сигнатуры $\langle \in^2 \rangle$, для которой $\Phi(b, a_1, \ldots, a_n) \Leftrightarrow$ (b — элемент K).

любых декартовых произведений. В силу предложения 1 и упражнения 2 к § 16 $K(\Phi)$ для атомарной формулы Φ замкнут также относительно всех фильтрованных произведений. Как будет показано в дальнейшем, это верно не только для атомарных формул. Если же D — ультрафильтр, то для любой формулы $\Phi \in F(\Sigma)$ класс $K(\Phi)$ замкнут относительно фильтрованных произведений по D (теорема 1 ниже).

Определение. Формула $\Phi(x_1, \ldots, x_n)$ называется *фильтрующейся по фильтру D* (на множестве I), если для любого множества $\{\mathfrak{A}_i | i \in I\}$ алгебраических систем сигнатуры $\Sigma(\Phi)$ и любых $Df_1, \ldots, Df_n \in$ $\in D\text{-prod}\, A_i$

$$D\text{-prod}\, \mathfrak{A}_i \vDash \Phi(Df_1, \ldots, Df_n) \Leftrightarrow \{i | \mathfrak{A}_i \vDash \Phi(f_1 i, \ldots, f_n i)\} \in D.$$

Если в этом определении вместо эквивалентности $\Leftrightarrow$ выполняется $\Leftarrow$, то формула Φ называется *условно фильтрующейся по D*. Формула Φ называется (*условно*) *фильтрующейся*, если она (условно) фильтруется по любому фильтру D.

Если γ — интерпретация некоторого множества переменных в $I\text{-prod}\, A_i$, то через $D(\gamma)$ обозначаем композицию отображений γ и D. Через $i(\gamma)$ обозначаем композицию отображений γ и проекции на i-ю координату.

Лемма 2. *Если Φ и Ψ (условно) фильтруются по фильтру D, то формулы $\forall x\Phi$, $\exists x\Phi$ и $\Phi \wedge \Psi$ (условно) фильтруются по фильтру D.*

Доказательство. Зафиксируем некоторую интерпретацию γ свободных переменных формулы $\forall x\Phi$ в множестве $I\text{-prod}\, A_i$.

Пусть $\{i | \mathfrak{A}_i \vDash \forall x\Phi [i(\gamma)]\} \in D$. Тогда для любой $f \in I\text{-prod}\, A_i$, если рассмотреть $\gamma' \supseteq \gamma$, для которой $\gamma'(x) = f$, имеем

$$\{i | \mathfrak{A}_i \vDash \Phi[i(\gamma')]\} \in D.$$

Если Φ условно фильтруется, то $D\text{-prod}\, \mathfrak{A}_i \vDash \Phi[D(\gamma')]$ для любого γ': $FV(\Phi) \to I\text{-prod}\, A_i$, $\gamma \subseteq \gamma'$, т. е. $D\text{-prod}\, \mathfrak{A}_i \vDash \forall x\Phi [D(\gamma)]$.

Пусть $D\text{-prod}\, \mathfrak{A}_i \vDash \forall x\Phi [D(\gamma)]$ и Φ фильтруется. Рассмотрим множество $X = \{i | \mathfrak{A}_i \vDash \forall x\Phi [i(\gamma)]\}$. Возьмем такую функцию $f \in I\text{-prod}\, A_i$, что для $i \in I \setminus X$ имеет место $\mathfrak{A}_i \vDash \neg \Phi [i(\gamma')]$, где $\gamma' \supseteq \gamma$, $\gamma'(x) = f$. Тогда из фильтруемости Φ и того, что $D\text{-prod}\, \mathfrak{A}_i \vDash \Phi[D(\gamma')]$, следует, что $X = \{i | \mathfrak{A}_i \vDash \Phi[i(\gamma')]\} \in D$.

Случаи $\exists x\Phi$ и $\Phi \wedge \Psi$ рассматриваются аналогично, и мы оставляем их читателю в качестве упражнения. □

Лемма 3. *Атомарные формулы фильтруются по любому фильтру D.*

Доказательство. Пусть $\Phi(x_1, \ldots, x_n)$ — атомарная формула вида $s(t_1, \ldots, t_m)$, где $s \in R$, $\mu(s) = m$, $t_1, \ldots, t_m$ — термы, пусть $\gamma\colon \{x_1, \ldots, x_n\} \to I\text{-prod}\, A_i$ — интерпретация переменных и $f_i = \gamma(x_i)$, $i \in \{1, \ldots, n\}$. Тогда для $\mathfrak{A} = D\text{-prod}\,\mathfrak{A}_i$

$$\mathfrak{A} \models \Phi(Df_1, \ldots, Df_n) \Leftrightarrow \left\langle t_1^{\mathfrak{A}}[\gamma D], \ldots, t_m^{\mathfrak{A}}[\gamma D]\right\rangle \in v^{\mathfrak{A}}(s).$$

По предложению 1 и 16.1 б) имеем $t_j^{\mathfrak{A}}[\gamma D] = Dt_j^{\mathfrak{B}}[\gamma]$, $1 \leqslant j \leqslant m$, где $\mathfrak{B} = I\text{-prod}\,\mathfrak{A}_i$, поэтому

$$\left\langle t_1^{\mathfrak{A}}[\gamma D], \ldots, t_m^{\mathfrak{A}}[\gamma D]\right\rangle \in$$
$$\in v^{\mathfrak{A}}(s) \Leftrightarrow \left\langle Dt_1^{\mathfrak{B}}[\gamma], \ldots, Dt_m^{\mathfrak{B}}[\gamma]\right\rangle \in$$
$$\in v^{\mathfrak{A}}(s) \Leftrightarrow \left\{i \,\middle|\, \left\langle t_1^{\mathfrak{B}}[\gamma](i), \ldots, t_m^{\mathfrak{B}}[\gamma](i)\right\rangle \in v^{\mathfrak{A}_i}(s)\right\} \in D.$$

Но $t_j^{\mathfrak{B}}[\gamma](i) = \left[t_j^{\mathfrak{B}}(f_1, \ldots, f_n)\right](i) = t_j^{\mathfrak{A}_i}(f_1 i, \ldots, f_n i)$, поэтому $\left\langle t_1^{\mathfrak{B}}[\gamma](i), \ldots, t_m^{\mathfrak{B}}[\gamma](i)\right\rangle \in v^{\mathfrak{A}_i}(s) \Leftrightarrow \mathfrak{A}_i \models \Phi(f_1 i, \ldots, f_n i)$. Таким образом,

$$D\text{-prod}\,\mathfrak{A}_i \models \Phi(Df_1, \ldots, Df_n) \Leftrightarrow \{i \mid \mathfrak{A}_i \models \Phi(f_1 i, \ldots, f_n i)\} \in D.$$

Случай, когда Φ имеет вид $t_1 \approx t_2$, разбирается аналогично. □

Теорема 1 (Лось). *Любая формула Φ фильтруется по любому ультрафильтру D.*

Доказательство. Индукцией по длине Φ. Так как истинность формул $\Phi \to \Psi$ и $\Phi \vee \Psi$ эквивалентна истинности формул $\neg(\Phi \wedge \neg\Psi)$ и $\neg(\neg\Phi \wedge \neg\Psi)$ соответственно, то в силу лемм 2 и 3 достаточно показать фильтруемость по D формулы $\neg\Phi$ для фильтрующейся по D формулы Φ. Из свойства $\varnothing \notin D$ и предложения 12.2 следует $X \notin D \Leftrightarrow I \setminus X \in D$. Поэтому из фильтруемости Φ получаем

$$D\text{-prod}\,\mathfrak{A}_i \models \neg\Phi[\gamma] \Leftrightarrow \{i \mid \mathfrak{A}_i \models \Phi[\gamma i]\} \notin D \Leftrightarrow$$
$$\Leftrightarrow \{i \mid \mathfrak{A}_i \models \neg\Phi[\gamma i]\} \in D. \quad □$$

Определение. Алгебраическая система $\mathfrak{A}$ сигнатуры Σ называется *моделью множества формул* Γ сигнатуры Σ, если существует такая интерпретация γ в A переменных, входящих свободно в элементы Γ, что $\mathfrak{A} \models \Phi[\gamma]$ для всех $\Phi \in \Gamma$. Множество Γ называется *выполнимым*, если Γ имеет модель. Множество называется *локально выполнимым*, если каждое конечное подмножество Γ имеет модель.

В качестве следствия теоремы 1 получаем следующую очень важную теорему, которая называется *теоремой компактности*.

Теорема 2. *Каждое локально выполнимое множество Γ формул сигнатуры Σ выполнимо.*

Доказательство. Рассмотрим множество I конечных подмножеств Γ. Для $i \in I$ выберем такие системы $\mathfrak{A}_i$ сигнатуры Σ и интерпретации γ_i в A_i свободных переменных, входящих в формулы из i, что $\mathfrak{A}_i \models \Phi[\gamma_i]$ для всех $\Phi \in i$. Для $i \in I$ рассмотрим множества $X_i = \{j \in I | i \subseteq j\}$. Система множеств $\{X_i | i \in I\}$ является центрированной. Действительно, если $i_0, \ldots, i_k \in I$ и $j = i_0 \cup \ldots \cup i_k$, то $j \in X_{i_0} \cap \ldots \cap X_{i_k}$. По предложению 12.1 существует такой ультрафильтр D, что $X_i \in D$ для всех $i \in I$. Для переменной x, входящей свободно в какой-нибудь элемент Γ, определим $\gamma(x) \in I\text{-prod}\, A_i$ следующим образом:

$$\gamma(x)(i) = \begin{cases} \gamma_i(x), & \text{если } x \in \operatorname{dom} \gamma_i, \\ \text{произвольный } a \in A_i & \text{в противном случае.} \end{cases}$$

Пусть $\Phi \in \Gamma$. Ясно, что

$$X_{\{\Phi\}} \subseteq \{i | \mathfrak{A}_i \models \Phi[\gamma i]\}.$$

Так как $X_{\{\Phi\}} \in D$, то $\{i | \mathfrak{A}_i \models \Phi[\gamma i]\} \in D$. По теореме 1 получаем $D\text{-prod}\, \mathfrak{A}_i \models \Phi[\gamma D]$. □

Теорема 2 будет широко применяться в следующих главах, особенно в главе 5. Здесь мы дадим простое, но довольно типичное применение этой теоремы (см. также упражнение 7).

Следствие 1. *Если для любого $n \in \omega$ множество формул Γ сигнатуры Σ имеет модель мощности $\geqslant n$, то Γ имеет бесконечную модель.*

Доказательство. Возьмем бесконечное множество символов C, для которого $C \cap (R \cup F) = \varnothing$, и пусть $\Sigma_1 = \langle R, F \cup C, \mu_1 \rangle$, где $\mu_1 \restriction (R \cup F) = \mu$ и $\mu_1(c) = 0$ для $c \in C$. Рассмотрим множество $X = \Gamma \cup \{\neg\, c \approx d \,|\, c, d \in C, c \neq d\}$ предложений сигнатуры Σ_1. Если $Y = \Gamma_1 \cup \{\neg\, c_1 \approx d_1, \ldots, \neg\, c_n \approx d_n\}$, где $\Gamma_1 \subseteq \Gamma$ — конечное подмножество X, то Y выполнимо в подходящем обогащении модели $\mathfrak{A}$ множества Γ, имеющей мощность $\geqslant n$. По теореме компактности X имеет модель $\mathfrak{A}$. Так как $\nu^{\mathfrak{A}}(c) \neq \nu^{\mathfrak{A}}(d)$ для $d, c \in C$, $c \neq d$, то $\mathfrak{A}$ — бесконечная модель Γ. □

Так как в доказательстве следствия множество C произвольно, то мы на самом деле показали, что при условии следствия 1 множество Γ имеет модель мощности, превосходящей любую наперед заданную мощность.

Упражнения

1. Показать, что фильтрованное произведение частично упорядоченных множеств является частично упорядоченным множеством.

2. Показать, что декартово произведение $K_1 \times K_2$ двух полей не может быть полем. (Указание. В $K_1 \times K_2$ имеются делители нуля.)

3. Если все $\mathfrak{A}_i$, $i \in I$, равны одной системе $\mathfrak{B}$, то декартово (фильтрованное) произведение $I\text{-prod}\,\mathfrak{A}_i$ ($D\text{-prod}\,\mathfrak{A}_i$) называется декартовой (фильтрованной) степенью $\mathfrak{B}$ и обозначается через $\mathfrak{B}^I$ ($\mathfrak{B}^D$). Показать, что

а) на всех декартовых степенях $\mathfrak{B}^I$ при $|I| > 1$ ложна формула

$$\exists v_0 \exists v_1 (r(v_0) \wedge (r(v_1) \wedge (\neg\, v_0 \approx v_1 \wedge \forall v_2 (r(v_2) \to$$
$$\to (v_2 \approx v_0 \vee v_2 \approx v_1)))));$$

б) декартова степень $\mathfrak{B}^I$, когда носитель $\mathfrak{B}$ и множество I имеют более одного элемента, не может быть линейно упорядоченным множеством.

4. Найти неизоморфные алгебраические системы $\mathfrak{A}$ и $\mathfrak{B}$, для которых система $\mathfrak{A} \times \mathfrak{A}$ изоморфна $\mathfrak{B} \times \mathfrak{B}$. (Указание. Пусть $\Sigma = \langle r^1 \rangle$, $A = B = \omega$, $\nu^{\mathfrak{A}}(r) = \omega \setminus \{0\}$, $\nu^{\mathfrak{B}}(r) = \omega \setminus \{0, 1\}$.)

5. Если $D_1 \subseteq D_2$ — два фильтра на множестве I, то существует гомоморфизм системы $D_1\text{-prod}\,\mathfrak{B}_i$ на $D_2\text{-prod}\,\mathfrak{B}_i$. (Указание. Рассмотреть отображение, сопоставляющее элементу $D_1 f$ элемент $D_2 f$.)

6. Пусть D — главный ультрафильтр на I и $\bigcap D = \{i_0\}$. Тогда система $D\text{-prod}\,\mathfrak{A}_i$ изоморфна системе $\mathfrak{A}_{i_0}$.

7. Пусть Γ — такое множество предложений сигнатуры Σ, что для любой алгебраической системы $\mathfrak{A}$ сигнатуры Σ существует предложение $\Phi \in \Gamma$, истинное на $\mathfrak{A}$. Показать, что существует такое конечное множество $\{\Phi_1, \ldots, \Phi_n\} \subseteq \Gamma$, что предложение $(\Phi_1 \vee (\Phi_2 \vee \ldots \vee \Phi_n)\ldots)$ — тождественно истинная формула.

Глава 4

ИСЧИСЛЕНИЕ ПРЕДИКАТОВ

§ 18. Аксиомы и правила вывода

Зафиксируем некоторую произвольную сигнатуру Σ. В этом параграфе мы определим *исчисление предикатов сигнатуры* Σ (сокращенно $ИП^\Sigma$).

Формулами $ИП^\Sigma$ будут формулы сигнатуры Σ. *Секвенциями* $ИП^\Sigma$ называются последовательности следующих 4 типов:

$$\Phi_0, \ldots, \Phi_n \vdash \Psi; \ \Phi_0, \ldots, \Phi_n \vdash; \ \vdash \Psi; \ \vdash,$$

где $\Phi_0, \ldots, \Phi_n, \Psi$ — формулы $ИП^\Sigma$.

Примем следующие соглашения. Пусть $x_1, \ldots, x_n$ — переменные, $t_1, \ldots, t_n$ — термы сигнатуры Σ и Φ — формула сигнатуры Σ. Запись $(\Phi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ будет обозначать результат подстановки термов $t_1, \ldots, t_n$ вместо всех свободных вхождений в Φ переменных $x_1, \ldots, x_n$ соответственно, причем, если в тексте встречается запись $(\Phi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$, то предполагается, что для всех $i = 1, \ldots, n$ ни одно свободное вхождение в Φ переменной x_i не входит в подформулу Φ вида $\forall y \Phi_1$ или $\exists y \Phi_1$ для $y \in FV(t_i)$. Запись $[\Phi]^x_y$ будет обозначать формулу $(\Phi)^x_y$, и при ее появлении предполагается, что кроме условия на запись $(\Phi)^x_y$ еще выполняется условие $y \notin FV(\Phi)$. Когда в тексте уже встречалась запись $\Phi(x_1, \ldots, x_n)$, вместо громоздкой записи $(\Phi)^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}$ часто будем писать просто $\Phi(t_1, \ldots, t_n)$. Заметим, что по соглашению в начале § 16 переменные $x_1, \ldots, x_n$ попарно различны, в то время как среди $t_1, \ldots, t_n$ могут быть равные термы.

Определение. *Аксиомами* $ИП^\Sigma$ являются следующие секвенции:

1) $\Phi \vdash \Phi$, Φ — формула $ИП^\Sigma$;
2) $\vdash x \approx x$, x — переменная;

3) $x \approx y, (\Phi)_x^z \vdash (\Phi)_y^z$, x, y, z — переменные, Φ — формула ИП$^\Sigma$, удовлетворяющая условию на запись $(\Phi)_x^z$ и $(\Phi)_y^z$.

Определение. *Правила вывода* ИП$^\Sigma$ таковы:

1. $\dfrac{\Gamma \vdash \Phi;\ \Gamma \vdash \Psi}{\Gamma \vdash \Phi \wedge \Psi}$;

2. $\dfrac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Phi}$;

3. $\dfrac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Psi}$;

4. $\dfrac{\Gamma \vdash \Phi}{\Gamma \vdash \Phi \vee \Psi}$;

5. $\dfrac{\Gamma \vdash \Psi}{\Gamma \vdash \Phi \vee \Psi}$;

6. $\dfrac{\Gamma, \Phi \vdash X;\ \Gamma, \Psi \vdash X;\ \Gamma \vdash \Phi \vee \Psi}{\Gamma \vdash X}$;

7. $\dfrac{\Gamma, \Phi \vdash \Psi}{\Gamma \vdash \Phi \to \Psi}$;

8. $\dfrac{\Gamma \vdash \Phi;\ \Gamma \vdash \Phi \to \Psi}{\Gamma \vdash \Psi}$;

9. $\dfrac{\Gamma, \neg \Phi \vdash}{\Gamma \vdash \Phi}$;

10. $\dfrac{\Gamma \vdash \Phi;\ \Gamma \vdash \neg \Phi}{\Gamma \vdash}$;

11. $\dfrac{\Gamma, \Phi, \Psi, \Gamma_1 \vdash X}{\Gamma, \Psi, \Phi, \Gamma_1 \vdash X}$;

12. $\dfrac{\Gamma \vdash \Phi}{\Gamma, \Psi \vdash \Phi}$;

13. $\dfrac{\Gamma \vdash \Phi}{\Gamma \vdash \forall x \Phi}$, где x не входит в члены Γ свободно;

14. $\dfrac{\Gamma, (\Phi)_t^x \vdash \Psi}{\Gamma, \forall x \Phi \vdash \Psi}$;

15. $\dfrac{\Gamma \vdash (\Phi)_t^x}{\Gamma \vdash \exists x \Phi}$;

16. $\dfrac{\Gamma, \Phi \vdash \Psi}{\Gamma, \exists x \Phi \vdash \Psi}$, где x не входит в Ψ и члены Γ свободно.

Как и в ИВ, в правилах вывода Φ, Ψ, X — переменные для формул ИП$^\Sigma$, а Γ, Γ_1 — переменные для последовательностей таких формул. При этом в правилах 13—16 формулы Φ, Ψ и последовательности Γ должны удовлетворять указанным условиям, а также условиям на запись $(\Phi)_t^x$. Так же как и в ИВ, если в правилах вывода вместо переменных Φ, Ψ, X и переменных Γ, Γ_1 берутся конкретные формулы и конкретные последовательности формул, то получаются частные случаи (или применения) правил вывода. Если Θ — частный случай правила вывода α, то будем говорить, что секвенция, стоящая в Θ под чертой, получается из секвенций, стоящих в Θ над чертой, при помощи правила α. Следующее определение является почти дословным повторением соответствующего определения ИВ.

Определение. *Линейным доказательством в* $ИП^{\Sigma}$ называется конечная последовательность $C_0, \ldots, C_n$ секвенций $ИП^{\Sigma}$, которая удовлетворяет следующему условию: каждая секвенция C_i, $i \leqslant n$, либо является аксиомой, либо получается из некоторых предыдущих при помощи одного из правил вывода 1—16. Линейное доказательство $C_0, \ldots, C_n$ называется линейным доказательством своей последней секвенции C_n. Если существует линейное доказательство в $ИП^{\Sigma}$ секвенции C, то C называется *доказуемой в* $ИП^{\Sigma}$ или теоремой $ИП^{\Sigma}$. Формула Ф $ИП^{\Sigma}$ называется доказуемой в $ИП^{\Sigma}$ или теоремой $ИП^{\Sigma}$, если в $ИП^{\Sigma}$ доказуема секвенция $\vdash Ф$. Дерево D называется *доказательством в виде дерева* или *деревом доказательства секвенции* C *в* $ИП^{\Sigma}$, если все его начальные секвенции — аксиомы $ИП^{\Sigma}$, переходы — применения правил 1—16, а заключительная секвенция равна C.

Определения допустимого правила и квазивывода совпадают с соответствующими определениями из § 3 с заменой ИВ на $ИП^{\Sigma}$.

Предложение 1. *Секвенция C является теоремой $ИП^{\Sigma}$ тогда и только тогда, когда существует ее доказательство в виде дерева в $ИП^{\Sigma}$.*

Доказательство. Почти дословное повторение доказательства предложения 3.1. □

Формула Ψ $ИП^{\Sigma}$ называется *тавтологией*, если она получается из формулы Ф исчисления высказываний, доказуемой в ИВ, путем замены всех ее пропозициональных переменных $P_1, \ldots, P_n$ на формулы $ИП^{\Sigma}$ $\Psi_1, \ldots, \Psi_n$ соответственно. Формулу Ф при этом назовем *основой тавтологии*.

Предложение 2. *Любая тавтология Ψ сигнатуры Σ доказуема в $ИП^{\Sigma}$.*

Доказательство. Пусть Ψ получена из основы Ф заменой переменных $P_1, \ldots, P_n$ на формулы $\Psi_1, \ldots$ $\ldots, \Psi_n$ соответственно.

Пусть дерево D_1 получено из дерева доказательства D в ИВ секвенции $\vdash Ф$ заменой переменных $P_1, \ldots, P_n$ соответственно на $\Psi_1, \ldots, \Psi_n$ и заменой остальных пропозициональных переменных на произвольную формулу Ψ_{n+1} сигнатуры Σ. Очевидно, что дерево D_1 является деревом доказательства секвенции $\vdash\Psi$ в $ИП^{\Sigma}$. □

Предложение 3. *Пусть* Φ — *формула* $ИП^{\Sigma}$, $x_1, \ldots$ $\ldots, x_n$ — *переменные*, $t_1, \ldots, t_n$ — *термы сигнатуры* Σ *и выполняются условия на запись* $(\Phi)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$. *Тогда в* $ИП^{\Sigma}$ *доказуемы следующие секвенции*:

а) $\forall x_1 \ldots \forall x_n \Phi \vdash (\Phi)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$;

б) $(\Phi)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n} \vdash \exists x_1 \ldots \exists x_n \Phi$.

Доказательство. Пусть $y_1, \ldots, y_n$ — попарно различные переменные, не входящие в формулу Φ, в термы $t_1, \ldots, t_n$ и отличные от $x_1, \ldots, x_n$.

а) Для всех $1 < k < n$ имеет место равенство

$$\left(\forall x_{k+1} \ldots \forall x_n (\Phi)^{x_1,\ldots,x_{k-1}}_{y_1,\ldots,y_{k-1}}\right)^{x_k}_{y_k} = \forall x_{k+1} \ldots \forall x_n (\Phi)^{x_1,\ldots,x_k}_{y_1,\ldots,y_k},$$

и выполнены все условия на такую запись. Поэтому следующее дерево будет доказательством в $ИП^{\Sigma}$:

$$\dfrac{\dfrac{\dfrac{(\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \vdash (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}}{\forall x_n (\Phi)^{x_1,\ldots,x_{n-1}}_{y_1,\ldots,y_{n-1}} \vdash (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}}}{\forall x_{n-1} \forall x_n (\Phi)^{x_1,\ldots,x_{n-2}}_{y_1,\ldots,y_{n-2}} \vdash (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}} \\ \vdots \qquad\qquad \vdots}{\forall x_1 \ldots \forall x_n \Phi \vdash (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}}.$$

Применяя теперь n раз правило 13, получаем доказуемость в $ИП^{\Sigma}$ секвенции

$$\forall x_1 \ldots \forall x_n \Phi \vdash \forall y_1 \ldots \forall y_n (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}.$$

Обозначим формулу $(\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}$ через Ψ. Тогда для Ψ выполнено условие на запись $(\Psi)^{y_1,\ldots,y_n}_{t_1,\ldots,t_n}$. Для всех $1 < k < n$ имеем

$$\left(\forall y_{k+1} \ldots \forall y_n (\Psi)^{y_1,\ldots,y_{k-1}}_{t_1,\ldots,t_{k-1}}\right)^{y_k}_{t_k} = \forall y_{k+1} \ldots \forall y_n (\Psi)^{y_1,\ldots,y_k}_{t_1,\ldots,t_k}$$

и условия на такую запись. Снова применяя n раз правило 14, получаем доказуемость в $ИП^{\Sigma}$ секвенции

$$\forall y_1 \ldots \forall y_n \Psi \vdash (\Psi)^{y_1,\ldots,y_n}_{t_1,\ldots,t_n}.$$

Так как $(\Psi)^{y_1,\ldots,y_n}_{t_1,\ldots,t_n} = (\Phi)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$, то следующее дерево будет квазивыводом в ИП$^\Sigma$:

$$\cfrac{\cfrac{\forall y_1 \ldots \forall y_n \Psi \vdash (\Phi)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}}{\vdash \forall y_1 \ldots \forall y_n \Psi \to (\Phi)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n};\quad \forall x_1 \ldots \forall x_n \Phi \vdash \forall y_1 \ldots \forall y_n \Psi}}{\forall x_1 \ldots \forall x_n \Phi \vdash (\Phi)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}}.$$

б) Доказательство аналогично а). Сначала, применяя несколько раз правило 15, получаем теорему

$$(\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \vdash \exists x_1 \ldots \exists x_n \Phi.$$

Затем, применяя несколько раз правило 16, получаем теорему ИП$^\Sigma$:

$$\exists y_1 \ldots \exists y_n (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \vdash \exists x_1 \ldots \exists x_n \Phi. \qquad (1)$$

Опять, применяя несколько раз правило 15, получаем доказуемость в ИП$^\Sigma$ секвенции

$$(\Psi)^{y_1,\ldots,y_n}_{t_1,\ldots,t_n} \vdash \exists y_1 \ldots \exists y_n \Psi, \qquad (2)$$

где $\Psi = (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}$. Из (1) и (2) так же, как в а), следует доказуемость в ИП$^\Sigma$ секвенции б). □

Предложение 4. *В ИП$^\Sigma$ допустимы правила* а) — м) *из предложения* 3.2 *и упражнения* 2 *к* § 3, *а также правило*

н) $$\frac{\Phi_1, \ldots, \Phi_k \vdash \Psi}{(\Phi_1)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}, \ldots, (\Phi_k)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n} \vdash (\Psi)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}}.$$

Доказательство. Для правил а) — м) доказательство по существу совпадает с доказательством допустимости соответствующих правил из § 3.

н) Пусть секвенция $\Phi_1, \ldots, \Phi_k \vdash \Psi$ доказуема в ИП$^\Sigma$. Применяя несколько раз правило 7, получаем доказуемость в ИП$^\Sigma$ секвенции

$$\vdash \Phi_1 \to (\Phi_2 \to \ldots (\Phi_k \to \Psi) \ldots).$$

Применяя несколько раз правило 13, получаем доказуемость секвенции

$$\vdash \forall x_1 \ldots \forall x_n (\Phi_1 \to (\Phi_2 \to \ldots (\Phi_k \to \Psi) \ldots)).$$

Из предложения 3 а) и допустимого правила в) получаем доказуемость в ИП$^\Sigma$ секвенции

$$\vdash (\Phi_1 \to (\Phi_2 \to \ldots (\Phi_k \to \Psi) \ldots))_{t_1, \ldots, t_n}^{x_1, \ldots, x_n}. \qquad (3)$$

Из (3) и аксиомы $(\Phi_1)_{t_1, \ldots, t_n}^{x_1, \ldots, x_n} \vdash (\Phi_1)_{t_1, \ldots, t_n}^{x_1, \ldots, x_n}$ по правилам 8 и 12 получаем секвенцию

$$(\Phi_1)_{t_1, \ldots, t_n}^{x_1, \ldots, x_n} \vdash (\Phi_2 \to (\ldots (\Phi_k \to \Psi) \ldots))_{t_1, \ldots, t_n}^{x_1, \ldots, x_n}.$$

Аналогично применяя еще несколько раз правило 8, получаем доказуемость в ИП$^\Sigma$ секвенции

$$(\Phi_1)_{t_1, \ldots, t_n}^{x_1, \ldots, x_n}, \ldots, (\Phi_k)_{t_1, \ldots, t_n}^{x_1, \ldots, x_n} \vdash (\Psi)_{t_1, \ldots, t_n}^{x_1, \ldots, x_n}. \quad \square$$

Если C — секвенция ИП$^\Sigma$, то объединение всех множеств $FV(\Phi)$, где Φ — формула из C, называется множеством свободных переменных секвенции C и обозначается через $FV(C)$.

Определение. Пусть C — секвенция ИП$^\Sigma$, $\mathfrak{A}$ — алгебраическая система сигнатуры Σ и γ — интерпретация переменных из $FV(C)$ в множестве A. Секвенция C называется *истинной в* $\mathfrak{A}$ *при интерпретации* γ (обозначаем $\mathfrak{A} \models C[\gamma]$) тогда и только тогда, когда выполняются следующие условия:

1) если $C = \Gamma \vdash \Psi$, то либо $\mathfrak{A} \models \Psi[\gamma]$, либо $\mathfrak{A} \models \neg\Phi[\gamma]$ для некоторой формулы Φ из Γ;

2) если $C = \Gamma \vdash$, то $\mathfrak{A} \models \neg\Phi[\gamma]$ для некоторой формулы Φ из Γ; в частности, Γ — непустая последовательность.

Если секвенция C не истинна в $\mathfrak{A}$ при γ, то говорим, что C *ложна в* $\mathfrak{A}$ *при* γ. Из определения получаем, что секвенция $\vdash$ ложна на любой алгебраической системе $\mathfrak{A}$.

Определение. Секвенция C исчисления ИП$^\Sigma$ называется *тождественно истинной*, если $\mathfrak{A} \models C[\gamma]$ для любой алгебраической системы $\mathfrak{A}$ сигнатуры Σ и любой интерпретации γ: $FV(C) \to A$.

Ясно, что свойство секвенции C быть тождественно истинной не зависит от того, в каком исчислении ИП$^\Sigma$ она рассматривается (т. е. от сигнатуры Σ).

Основной целью для нас в этой главе будет доказательство следующего замечательного результата К. Гёделя: класс доказуемых в ИП$^\Sigma$ секвенций совпадает с классом тождественно истинных секвенций ИП$^\Sigma$. Это утверждение называется теоремой полноты исчисления предикатов. Одна часть этого утверждения доказывается легко.

Теорема 1. *Все доказуемые в* ИП$^\Sigma$ *секвенции C являются тождественно истинными. В частности, исчисление* ИП$^\Sigma$ *непротиворечиво, т. е. не все формулы* ИП$^\Sigma$ *доказуемы в* ИП$^\Sigma$.

Доказательство проводим индукцией по высоте доказательства секвенции C в виде дерева. Очевидно, что аксиомы ИП$^\Sigma$ являются тождественно истинными. Проверку того, что правила вывода 1—16 сохраняют тождественную истинность, мы оставляем читателю в качестве упражнения. Заметим только, что для проверки правил 14 и 15 следует сначала установить следующий факт. Пусть Φ — формула, t — терм и выполняются условия на запись $(\Phi)^x_t$, $X = FV(\Phi)$, $Y = FV((\Phi)^x_t)$, γ: $X \to A$, γ^*: $Y \to A$. Тогда если $\gamma \restriction (X \setminus \{x\}) = \gamma^* \restriction (X \setminus \{x\})$ и $x^{\mathfrak{A}}[\gamma] = t^{\mathfrak{A}}[\gamma^*]$, то

$$\mathfrak{A} \models \Phi[\gamma] \Leftrightarrow \mathfrak{A} \models (\Phi)^x_t[\gamma^*].$$

Этот факт легко устанавливается индукцией по длине Φ. □

Вторую часть теоремы полноты мы докажем в § 21. Для этого нам нужно сначала получить достаточное количество доказуемых в ИП$^\Sigma$ секвенций. Следующее предложение показывает, что обычные свойства равенства доказуемы в ИП$^\Sigma$.

Если $t_1, \ldots, t_n, t$ — термы сигнатуры Σ, $x_1, \ldots, x_n$ — переменные, то через $(t)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$ обозначаем результат подстановки вместо $x_1, \ldots, x_n$ термов $t_1, \ldots, t_n$ соответственно.

Предложение 5. *Пусть t, q, s; $q_1, \ldots, q_n$; $s_1, \ldots, s_n$ — термы сигнатуры Σ, Φ — формула ИП$^\Sigma$, удовлетворяющая условиям на запись $(\Phi)^{x_1,\ldots,x_n}_{q_1,\ldots,q_n}$ и на запись $(\Phi)^{x_1,\ldots,x_n}_{s_1,\ldots,s_n}$. Тогда в ИП$^\Sigma$ доказуемы следующие секвенции:*

а) $\vdash t \approx t$;

б) $t \approx q \vdash q \approx t$;

в) $t \approx q,\ q \approx s \vdash t \approx s$;

г) $q_1 \approx s_1, \ldots, q_n \approx s_n \vdash (t)^{x_1,\ldots,x_n}_{q_1,\ldots,q_n} \approx (t)^{x_1,\ldots,x_n}_{s_1,\ldots,s_n}$;

д) $q_1 \approx s_1, \ldots, q_n \approx s_n, (\Phi)^{x_1,\ldots,x_n}_{q_1,\ldots,q_n} \vdash (\Phi)^{x_1,\ldots,x_n}_{s_1,\ldots,s_n}$.

Доказательство. а) Секвенция $\vdash t \approx t$ получается из аксиомы $\vdash x \approx x$ по производному правилу н) из предложения 4.

Пусть x, x_1, y, z — попарно различные переменные. Рассмотрим дерево

$$\cfrac{\cfrac{\vdash x \approx x;\ x \approx y,\ (z \approx x)^z_x \vdash (z \approx x)^z_y}{x \approx y \vdash y \approx x}}{t \approx q \vdash q \approx t}.$$

Так как начальные секвенции у него — аксиомы, а переходы — применения правил из предложения 4, то рассматриваемое дерево является квазивыводом секвенции б). Доказуемость в) получаем аналогично из квазивывода

$$\cfrac{\cfrac{y \approx z,\ (x \approx x_1)^{x_1}_y \vdash (x \approx x_1)^{x_1}_z}{x \approx y,\ y \approx z \vdash x \approx z}}{t \approx q,\ q \approx s \vdash t \approx s}.$$

Пусть $y_1, \ldots, y_n$; $z_1, \ldots, z_n$ — попарно различные переменные, отличные от $x_1, \ldots, x_n$, не входящие в термы $q_1, \ldots, q_n$, $s_1, \ldots, s_n$, t и в формулу Φ. Из а), предложения 4 в) и из того, что термы $(t)^{x_1}_{y_1}$ и $\left((t)^{x_1}_{z_1}\right)^{z_1}_{y_1}$ равны, получаем, что дерево

$$\frac{\vdash (t)^{x_1}_{y_1} \approx (t)^{x_1}_{y_1};\ y_1 \approx z_1,\ (t)^{x_1}_{y_1} \approx \left((t)^{x_1}_{z_1}\right)^{z_1}_{y_1} \vdash (t)^{x_1}_{y_1} \approx (t)^{x_1}_{z_1}}{y_1 \approx z_1 \vdash (t)^{x_1}_{y_1} \approx (t)^{x_1}_{z_1}}$$

является квазивыводом в ИП$^\Sigma$. Если $n > 1$, то в силу предложения 4 н) в ИП$^\Sigma$ доказуема секвенция $y_1 \approx z_1 \vdash (t)^{x_1, x_2}_{y_1, y_2} \approx (t)^{x_1, x_2}_{z_1, y_2}$. Применяя к этой секвенции и аксиоме

$$y_2 \approx z_2,\quad (t)^{x_1, x_2}_{y_1, y_2} \approx \left((t)^{x_1, x_2}_{z_1, z_2}\right)^{z_2}_{y_2} \vdash (t)^{x_1, x_2}_{y_1, y_2} \approx (t)^{x_1, x_2}_{z_1, z_2}$$

правило в) из предложения 4, получаем секвенцию

$$y_1 \approx z_1;\quad y_2 \approx z_2 \vdash (t)^{x_1, x_2}_{y_1, y_2} \approx (t)^{x_1, x_2}_{z_1, z_2}.$$

Проделав несколько таких шагов, получаем доказуемость в ИП$^\Sigma$ секвенции

$$y_1 \approx z_1,\ \ldots,\ y_n \approx z_n \vdash (t)^{x_1, \ldots, x_n}_{y_1, \ldots, y_n} \approx (t)^{x_1, \ldots, x_n}_{z_1, \ldots, z_n}.$$

Из этой секвенции с помощью правила н) из предложения 4 получаем секвенцию г).

д) Так как справедливо равенство $\left((\Phi)^{x_1,x_2,\ldots,x_n}_{y_1,y_2,\ldots,y_n}\right)^{y_1}_{z_1} = (\Phi)^{x_1,x_2,\ldots,x_n}_{z_1,y_2,\ldots,y_n}$, то секвенция

$$y_1 \approx z_1,\quad (\Phi)^{x_1,x_2,\ldots,x_n}_{y_1,y_2,\ldots,y_n} \vdash (\Phi)^{x_1,x_2,\ldots,x_n}_{z_1,y_2,\ldots,y_n}$$

является аксиомой. Если $n > 1$, то из этой аксиомы и аксиомы

$$y_2 \approx z_2,\quad (\Phi)^{x_1,x_2,\ldots,x_n}_{z_1,y_2,\ldots,y_n} \vdash \left((\Phi)^{x_1,x_2,\ldots,x_n}_{z_1,y_2,\ldots,y_n}\right)^{y_2}_{z_2}$$

по правилу в) из предложения 4 получаем

$$y_1 \approx z_1,\quad y_2 \approx z_2,\quad (\Phi)^{x_1,x_2,x_3,\ldots,x_n}_{y_1,y_2,y_3,\ldots,y_n} \vdash (\Phi)^{x_1,x_2,x_3,\ldots,x_n}_{z_1,z_2,y_3,\ldots,y_n}.$$

Проделав несколько таких шагов, получаем доказуемость в ИП^{Σ} секвенции

$$y_1 \approx z_1,\ \ldots,\ y_n \approx z_n,\quad (\Phi)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \vdash (\Phi)^{x_1,\ldots,x_n}_{z_1,\ldots,z_n}.$$

Отсюда в силу предложения 4 н) следует доказуемость в ИП^{Σ} секвенции д). □

Следующая теорема является, конечно, следствием упомянутой выше теоремы Гёделя, однако ее легко доказать и непосредственно.

Теорема 2. *Если $\Sigma_1 \subseteq \Sigma$, то исчисление ИП^{Σ} является консервативным расширением исчисления ИП^{Σ_1}.*

Доказательство. Пусть D — дерево доказательства в ИП^{Σ} секвенции C, являющейся также секвенцией ИП^{Σ_1}. Пусть y — переменная, не входящая ни в одну формулу из D. Определим отображение $\delta\colon T(\Sigma) \to T(\Sigma_1)$ индукцией по длине терма $t \in T(\Sigma)$:

а) если t — переменная, то $\delta t = t$;

б) если $t = f(t_1, \ldots, t_n)$, где f — символ из Σ_1, то $\delta t = f(\delta t_1, \ldots, \delta t_n)$;

в) если $t = f(t_1, \ldots, t_n)$, где f — символ не из Σ_1, то $\delta t = y$.

Если Φ — атомарная формула сигнатуры Σ, то пусть $\delta\Phi$ равняется: а) формуле $r(\delta t_1, \ldots, \delta t_n)$, если $\Phi = r(t_1, \ldots, t_n)$ и r — символ сигнатуры Σ_1; б) формуле $\delta t_1 \approx \delta t_2$, если $\Phi = t_1 \approx t_2$; в) формуле $\forall y\,(y \approx y)$, если $\Phi = r(t_1, \ldots, t_n)$, где r — символ не из Σ_1. Для любой формулы Φ сигнатуры Σ определим формулу $\delta\Phi$ сигнатуры Σ_1 как результат замены в формуле Φ всех атомарных подформул Ψ на $\delta\Psi$. Пусть δD получается из D заменой всех секвенций $\Psi_1, \ldots, \Psi_n \vdash \Phi$ и $\Psi_1, \ldots \ldots, \Psi_n \vdash$ на $\delta\Psi_1, \ldots, \delta\Psi_n \vdash \delta\Psi$ и $\delta\Psi_1, \ldots, \delta\Psi_n \vdash$ соответственно. Очевидно, что начальные секвенции δD будут аксиомами ИП^{Σ_1}. Легко проверяется, что все переходы в δD будут применениями тех же правил, что и соответствующие переходы в D. В самом деле, проверка для правил 1—13 и 16 тривиальна, а для правил 14 и 15 нужно сначала индукцией по длине формулы Φ заметить (учитывая $x \neq y$), что $\delta(\Phi)_t^x = (\delta\Phi)_{\delta t}^x$, для чего в свою очередь индукцией по длине терма t_1 нужно для любого терма t_2 установить равенство $\delta(t_1)_{t_2}^x = (\delta t_1)_{\delta t_2}^x$. Так как $\delta\Phi = \Phi$ для всех формул Φ из секвенции C, то δD будет доказательством C в ИП^{Σ_1}. □

В дальнейшем мы свободно будем пользоваться теоремой 2, чтобы не упоминать исчисление ИП^{Σ}, когда речь идет о доказуемости некоторой секвенции C. В частности, мы будем говорить, что секвенция C *доказуема в исчислении предикатов* или просто *доказуема*, если C доказуема в некотором ИП^{Σ}.

Упражнения

1. Пусть сигнатура Σ содержит пропозициональные переменные исчисления ИВ в качестве нульместных предикатных символов. Показать, что ИП^{Σ} является консервативным расширением ИВ. (Указание. Воспользоваться теоремой полноты для ИВ и теоремой 1.)

2. Показать, что если в одном из правил 13—16 убрать ограничение на применения этого правила (в частности, для правил 14 и 15 снять условие на запись $(\Phi)_t^x$), то в полученном исчислении будет доказуема не тождественно истинная формула.

3. Показать, что если во всех правилах 13—16 убрать все ограничения на применения этих правил, то все теоремы полученного исчисления J будут 1-общезначимыми, в частности, J будет непротиворечивым.

§ 19. Эквивалентность формул

Все изучаемые нами свойства алгебраических систем инвариантны относительно изоморфизма, многие же интересующие нас свойства формул инвариантны относительно определенного ниже отношения эквивалентности.

Зафиксируем на дальнейшее произвольную сигнатуру Σ. Все формулы и алгебраические системы в этом параграфе имеют сигнатуру Σ, а доказательства рассматриваются в исчислении ИП^Σ.

Определение. Формулы Φ и Ψ называются *эквивалентными* (обозначается $\Phi \equiv \Psi$), если доказуемы две секвенции $\Phi \vdash \Psi$ и $\Psi \vdash \Phi$.

Очевидно, что отношение $\equiv$ является эквивалентностью на множестве $F(\Sigma)$ и все доказуемые формулы из $F(\Sigma)$ образуют один класс эквивалентности. В силу теоремы 1 для любых формул $\Phi \equiv \Psi$, любой системы $\mathfrak{A}$ и любой интерпретации $\gamma\colon FV(\Phi) \cup FV(\Psi) \to A$ из $\mathfrak{A} \vDash \Phi[\gamma]$ следует $\mathfrak{A} \vDash \Psi[\gamma]$.

Заметим, что в силу теоремы 2 отношение $\Phi \equiv \Psi$ не зависит от сигнатуры Σ.

Определение. Формулы Φ и Ψ называются *пропозиционально эквивалентными* (обозначается $\Phi \overset{s}{\equiv} \Psi$), если $\Phi \to \Psi$ и $\Psi \to \Phi$ — тавтологии.

Из предложения 18.2 и правила 8 получаем

Предложение 1. *Пропозиционально эквивалентные формулы Φ и Ψ эквивалентны.* □

Предложение 2. *Пусть Φ, Ψ — формулы и x не входит свободно в Ψ. Тогда имеем эквивалентности:*

а) $\neg \exists x \Phi \equiv \forall x \neg \Phi$; б) $\neg \forall x \Phi \equiv \exists x \neg \Phi$;

в) $\exists x \Phi \wedge \Psi \equiv \exists x (\Phi \wedge \Psi)$; г) $\forall x \Phi \wedge \Psi \equiv \forall x (\Phi \wedge \Psi)$;

д) $\exists x \Phi \vee \Psi \equiv \exists x (\Phi \vee \Psi)$; е) $\forall x \Phi \vee \Psi \equiv \forall x (\Phi \vee \Psi)$;

ж) $\forall x \Phi \equiv \forall y [\Phi]^x_y$; з) $\exists x \Phi \equiv \exists y [\Phi]^x_y$.

Доказательство. Приведем квазивыводы для эквивалентностей а), в), д) и ж), оставляя проверку остальных читателю.

а) $$\begin{array}{c} \neg\Phi \vdash \neg\Phi \\ \hline \forall x \neg\Phi \vdash \neg\Phi \\ \hline \Phi \vdash \neg\forall x \neg\Phi \\ \hline \exists x\Phi \vdash \neg\forall x\neg\Phi \\ \hline \forall x\neg\Phi \vdash \neg\exists x\Phi \end{array}; \qquad \begin{array}{c} \Phi \vdash \Phi \\ \hline \Phi \vdash \exists x\Phi \\ \hline \neg\exists x\Phi \vdash \neg\Phi \\ \hline \neg\exists x\Phi \vdash \forall x\neg\Phi \end{array}.$$

в) $$\frac{\dfrac{\begin{array}{c} \Psi, \Phi \vdash \Phi\wedge\Psi \\ \hline \Psi, \Phi \vdash \exists x(\Phi\wedge\Psi) \\ \hline \Psi, \exists x\Phi \vdash \exists x(\Phi\wedge\Psi) \\ \hline \exists x\Phi \vdash \Psi \to \exists x(\Phi\wedge\Psi) \\ \hline \vdash \exists x\Phi \to (\Psi \to \exists x(\Phi\wedge\Psi)); \quad \exists x\Phi\wedge\Psi \vdash \exists x\Phi \end{array}}{\exists x\Phi\wedge\Psi \vdash \Psi \to \exists x(\Phi\wedge\Psi);} \qquad \exists x\Phi\wedge\Psi \vdash \Psi}{\exists x\Phi\wedge\Psi \vdash \exists x(\Phi\wedge\Psi)};$$

$$\dfrac{\dfrac{\dfrac{\Phi\wedge\Psi\vdash\Phi}{\Phi\wedge\Psi\vdash\exists x\Phi};\quad \Phi\wedge\Psi\vdash\Psi}{\Phi\wedge\Psi\vdash\exists x\Phi\wedge\Psi}}{\exists x\,(\Phi\wedge\Psi)\vdash\exists x\Phi\wedge\Psi}.$$

д)
$$\dfrac{\exists x\Phi\vee\Psi\vdash\exists x\,\Phi\vee\Psi;\quad \dfrac{\dfrac{\Phi\vdash\Phi\vee\Psi}{\Phi\vdash\exists x\,(\Phi\vee\Psi)}}{\exists x\Phi\vdash\exists x\,(\Phi\vee\Psi)};\quad \dfrac{\Psi\vdash\Phi\vee\Psi}{\Psi\vdash\exists x\,(\Phi\vee\Psi)}}{\exists x\Phi\vee\Psi\vdash\exists x\,(\Phi\vee\Psi)};$$

$$\dfrac{\dfrac{\Phi\vee\Psi\vdash\Phi\vee\Psi;\quad \dfrac{\dfrac{\Phi\vdash\Phi}{\Phi\vdash\exists x\Phi}}{\Phi\vdash\exists x\Phi\vee\Psi};\quad \Psi\vdash\exists x\Phi\vee\Psi}{\Phi\vee\Psi\vdash\exists x\Phi\vee\Psi}}{\exists x\,(\Phi\vee\Psi)\vdash\exists x\Phi\vee\Psi}.$$

ж)
$$\dfrac{\dfrac{[\Phi]^x_y\vdash[\Phi]^x_y}{\forall x\Phi\vdash[\Phi]^x_y}}{\forall x\Phi\vdash\forall y\,[\Phi]^x_y}.$$

Перед доказательством последней секвенции заметим, что $\left[[\Phi]^x_y\right]^y_x=\Phi$. Это равенство следует из условий на запись $[\Phi]^x_y$.

$$\dfrac{\dfrac{\left[[\Phi]^x_y\right]^y_x\vdash\Phi}{\forall y\,[\Phi]^x_y\vdash\Phi}}{\forall y\,[\Phi]^x_y\vdash\forall x\Phi.}\quad\square$$

Предложение 3. *Имеют место все эквивалентности из §§ 4 и 5, если Φ, Ψ и X считать формулами сигнатуры Σ.*

Доказательство. Очевидно, так как при замене пропозициональных переменных на формулы $ИП^{\Sigma}$ доказательства в ИВ перейдут в доказательства в $ИП^{\Sigma}$. □

Теорема 3 (о замене). *Если формула Φ получается из формулы Ψ сигнатуры Σ заменой некоторого вхождения подформулы Ψ' на формулу Φ' сигнатуры Σ и $\Phi'\equiv\Psi'$, то $\Phi\equiv\Psi$.*

Доказательство проводим индукцией по длине Ψ. Если $\Psi'=\Psi$, то утверждение тривиально. Если $\Psi=\neg\Psi_1$ или $\Psi=\Psi_1\tau\Psi_2$, где $\tau\in\{\wedge,\vee,\to\}$, то доказательство индукционного шага не отличается от соответствующих случаев теоремы о замене для ИВ (§ 4). Таким образом, для завершения доказательства в силу индукционного предположения осталось рассмотреть случаи, когда Ψ имеет вид $\forall x\Psi'$ или $\exists x\Psi'$. По условию секвенции $\Phi' \vdash \Psi'$ и $\Psi' \vdash \Phi'$ доказуемы. В силу симметричности Φ' и Ψ' достаточно доказать секвенции $\forall x\Psi' \vdash \vdash \forall x\Phi'$ и $\exists x\Psi' \vdash \exists x\Phi'$. Приведем их квазивыводы:

$$\frac{\dfrac{\Psi' \vdash \Phi'}{\forall x\Psi' \vdash \Phi'}}{\forall x\Psi' \vdash \forall x\Phi'}; \quad \frac{\dfrac{\Psi' \vdash \Phi'}{\Psi' \vdash \exists x\Phi'}}{\exists x\Psi' \vdash \exists x\Phi'}. \quad \square$$

В определении истинности формул на системах связанные вхождения переменных играют совершенно другую роль, чем свободные. В частности, проверка истинности формул $\forall x\Phi$ и $\forall y[\Phi]^x_y$ одна и та же. В оставшейся части этого параграфа будет показано, что замена связанных переменных преобразует формулу в эквивалентную ей, если при этом новое вхождение переменной связывается тем же вхождением квантора и никакое свободное вхождение переменной не становится при такой замене связанным. Перейдем к точной формулировке такого преобразования.

Определение. Говорим, что формула Φ получается из формулы Ψ *заменой связанной переменной*, если Φ получается из Ψ заменой некоторого вхождения подформулы $\mathrm{Q}x\Psi_1$ на формулу $\mathrm{Q}y[\Psi_1]^x_y$ (здесь $\mathrm{Q} \in \in \{\forall, \exists\}$ и выполняются условия на запись $[\Psi_1]^x_y$). Формулы Φ и Ψ называются *конгруэнтными* (обозначается $\Phi \sim \Psi$), если существует такая последовательность формул $\Phi_0, \ldots, \Phi_n$, что $\Phi_0 = \Phi$, $\Phi_n = \Psi$, а Φ_{k+1}, $k < n$, получается из Φ_k заменой связанной переменной.

Пример. Рассмотрим формулы $\Phi = \forall v_2\exists v_3 r(v_2, v_3)$ и $\Psi = \forall v_3\exists v_2 r(v_3, v_2)$. Последовательность

$$\forall v_2\exists v_3 r(v_2, v_3), \quad \forall v_2\exists v_0 r(v_2, v_0),$$
$$\forall v_3\exists v_0 r(v_3, v_0), \quad \forall v_3\exists v_2 r(v_3, v_2)$$

показывает, что $\Phi \sim \Psi$.

Предложение 4. а) *Отношение $\sim$ является эквивалентностью на множестве формул сигнатуры Σ.*

б) *Если $\Phi \sim \Psi$, то $\Phi \equiv \Psi$.*

Доказательство. а) Из свойства $[[\Psi_1]^x_y]^y_x = \Psi_1$ для любой формулы Ψ_1, для которой выполняются условия на запись $[\Psi_1]^x_y$, следует, что если Ψ получается из Φ заменой связанной переменной, то Φ также получается из Ψ заменой связанной переменной. Отсюда получаем симметричность отношения $\sim$. Рефлексивность и транзитивность отношения $\sim$ очевидна.

б) В силу теоремы о замене достаточно показать, что $\mathrm{Q}x\Psi_1 \equiv \mathrm{Q}y[\Psi_1]^x_y$, $\mathrm{Q} \in \{\forall, \exists\}$. Но это уже доказано в предложении 2 ж), з). □

Как уже отмечалось, нас будут интересовать формулы в основном «с точностью» до эквивалентности, поэтому будут допускаться записи вида $\Phi_1 \wedge \ldots \wedge \Phi_n$, $\bigvee\limits_{k \leqslant n} \Phi_k$ и др., по которым формулы восстанавливаются неоднозначно, но при любых расстановках скобок получаются эквивалентные формулы.

Упражнения

1. Показать, что отношение $\equiv$ является эквивалентностью на $F(\Sigma)$.
2. Доказать утверждения б), г), е) и з) предложения 2.
3. Показать, что для любой формулы Φ и любых переменных $x_1, \ldots, x_n$ существует такая формула Ψ, что $\Psi \equiv \Phi$ и $\{x_1, \ldots, x_n\} \subseteq FV(\Psi)$.

§ 20. Нормальные формы

Так как нас в основном будут интересовать формулы «с точностью» до эквивалентности, то полезно выбрать такие подмножества $P \subseteq F(\Sigma)$ формул, устроенных по возможности более просто по сравнению с произвольными формулами, чтобы для любой $\Phi \in F(\Sigma)$ существовала $\Psi \in P$, для которой $\Phi \equiv \Psi$. Некоторые из таких подмножеств будут определены в настоящем параграфе.

Будем говорить, что формула Φ сигнатуры Σ находится в *дизъюнктивной нормальной форме* (сокращенно *д. н. ф.*), если она получается из формулы Ψ исчисления высказываний, находящейся в д. н. ф., заменой всех входящих в Ψ пропозициональных переменных $P_1, \ldots, P_n$ на некоторые атомарные формулы $\Phi_1, \ldots, \Phi_n$ сигнатуры Σ соответственно.

Определение. Будем говорить, что формула Φ сигнатуры Σ находится в *пренексной нормальной форме*, если она имеет вид

$$\mathrm{Q}_1 x_1 \ldots \mathrm{Q}_n x_n \Phi_1,$$

где Q_i, $1 \leqslant i \leqslant n$,— кванторы, а Φ_1 находится в д. н. ф. Формулу Φ_1 в этом случае назовем *матрицей*, а слово $\mathrm{Q}_1 x_1 \ldots \mathrm{Q}_n x_n$ — *кванторной приставкой* формулы Φ.

Теорема 4. *Для любой формулы Φ сигнатуры Σ существует формула Ψ сигнатуры Σ, находящаяся в пренексной нормальной форме и эквивалентная Φ.*

Доказательство. В силу предложения 19.3 формулы $\Phi_1 \to \Phi_2$ и $\neg\Phi_1 \vee \Phi_2$ эквивалентны для любых $\Phi_1, \Phi_2 \in F(\Sigma)$. Следовательно, для любой $\Phi \in F(\Sigma)$, применяя несколько раз теорему 3, можно получить формулу $\Psi_1 \equiv \Phi$, не содержащую знака $\to$. Индукцией по длине формулы Ψ_1, не содержащей $\to$, покажем, что существует $\Psi_2 \equiv \Psi_1$, имеющая вид

$$Q_1 y_1 \ldots Q_k y_k \Psi_3,$$

где Ψ_3 — бескванторная формула, и длина Ψ_2 равна длине Ψ_1. Если Ψ_1 бескванторная, то в качестве Ψ_2 берем Ψ_1. Если $\Psi_1 = Qx\Psi'$, то нужная Ψ_2 существует по предположению индукции и теореме 3. Таким образом, осталось рассмотреть случаи: 1) $\Psi_1 = \neg\Psi'$ и 2) $\Psi_1 = (\Psi'\tau\Psi'')$, $\tau \in \{\wedge, \vee\}$, где Ψ' имеет кванторы и находится в виде $Q_0 x_0 \ldots Q_n x_n X$, где X — бескванторная формула. (Здесь мы воспользовались эквивалентностью $(\Psi'\tau\Psi'') \equiv (\Psi''\tau\Psi')$ для того, чтобы утверждать, что Ψ' имеет кванторы.) Пусть $\Psi' = \exists x\Psi_4$. Случай с другим квантором рассматривается совершенно аналогично. Из предложения 19.2 а) получаем для случая 1) эквивалентность $\Psi_1 \equiv \forall x \neg\Psi_4$. Нужная Ψ_2 для случая 1) существует тогда по индукционному предположению и теореме 3. Рассмотрим случай 2). Пусть y — переменная, не входящая в Ψ_1. Из предложения 19.2 з) и теоремы 3 получаем $\Psi_1 \equiv (\exists y [\Psi_4]^x_y \tau\Psi'')$. Из эквивалентностей в) и д) того же предложения имеем $\Psi_1 \equiv \exists y ([\Psi_4]^x_y \tau\Psi'')$. Требуемая Ψ_2 найдется теперь по индукционному предположению и теореме 3.

Для завершения доказательства теоремы в силу теоремы 3 нужно для бескванторной Ψ_3 найти $\Phi' \equiv \Psi_3$, находящуюся в д. н. ф. Для этого заменим все атомарные подформулы $\Phi_0, \ldots, \Phi_n$ формулы Ψ_3 на пропозициональные переменные $P_0, \ldots, P_n$ соответственно, получим формулу X исчисления высказываний. Пусть X_1 — формула исчисления высказываний, находящаяся в д. н. ф. с теми же переменными, что и X, для которой $X_1 \vdash X$ и $X \vdash X_1$ — теоремы ИВ. Пусть Φ' получается из X_1 заменой $P_0, \ldots, P_n$ на $\Phi_0, \ldots, \Phi_n$ соответственно, тогда $\Phi' \overset{s}{\equiv} \Psi_3$, следовательно, по предложению 19.1 $\Phi' \equiv \Psi_3$. □

Определение. Говорим, что формула Φ сигнатуры Σ находится в *приведенной нормальной форме*, если все ее атомарные подформулы являются атомными. (См. § 16 для определения атомной формулы.)

Предложение 1. *Для любой формулы Φ сигнатуры Σ существует формула Ψ сигнатуры Σ, находящаяся в приведенной нормальной форме.*

Доказательство. В силу теоремы 3 достаточно доказать предложение для атомарной формулы Φ. Проведем индукцию по числу $n(\Phi)$ вхождений сигнатурных символов в Φ. Если $n(\Phi) \leqslant 1$, то Φ — атомная формула и доказывать нечего. Если $n(\Phi) > 1$, то в Φ существует вхождение терма t, имеющего вид $f(v_{i_1}, \ldots, v_{i_k})$. Тогда $\Phi = (\Phi')^y_t$, где Φ' получается из Φ заменой этого вхождения на переменную y, не входящую в Φ.

Следующие квазивыводы:

$$\cfrac{\cfrac{\Phi \vdash \Phi;\ \vdash t \approx t}{\Phi \vdash (\Phi' \wedge y \approx t)^y_t}}{\Phi \vdash \exists y\,(\Phi' \wedge y \approx t)}; \qquad \cfrac{\cfrac{y \approx t,\ \Phi' \vdash \Phi}{\Phi' \wedge y \approx t \vdash \Phi}}{\exists y\,(\Phi' \wedge y \approx t) \vdash \Phi}$$

показывают, что $\Phi \equiv \exists y\,(\Phi' \wedge y \approx t)$. Теперь применяем индукционное предположение к Φ' и теорему 3. □

Заметим, что в теореме 4 без изменения доказательства можно потребовать, чтобы формула Ψ находилась в приведенной нормальной форме, если Φ находится в приведенной нормальной форме. Поэтому имеет место

Следствие 1. *Для любой формулы Φ сигнатуры Σ существует формула Ψ сигнатуры Σ, находящаяся в пренексной приведенной нормальной форме и эквивалентная Φ.* □

В дальнейшем для краткости вместо «пренексная (приведенная) нормальная форма» будем писать «пренексная (приведенная) н. ф.».

Упражнения

1. Показать, что в теореме 4 можно потребовать, чтобы у формул Φ и Ψ было одно и то же число вхождений кванторов.

2. Показать, что в теореме 4 можно потребовать, чтобы Ψ имела вид

$$\exists x_0 \forall x_1 \ldots \exists x_{n-1} \forall x_n \Psi'.$$

3. Проверить, что в теореме 4 и предложении 1 можно потребовать, чтобы $FV(\Phi) = FV(\Psi)$.

§ 21. Теорема о существовании модели

Определение. Множество формул X сигнатуры Σ называется *противоречивым* или *несовместным*, если в исчислении предикатов доказуема секвенция $\Gamma \vdash$, где все члены Γ принадлежат X. В противном случае X называется *непротиворечивым* или *совместным*.

Отметим простые свойства введенного понятия.

Предложение 1. а) *Пустое множество непротиворечиво.*

б) *Если X — непротиворечивое множество формул сигнатуры Σ и в исчислении предикатов доказуема секвенция $\Phi_1, \ldots, \Phi_n \vdash \Phi$, где $\Phi \in F(\Sigma)$, $\Phi_0 \in X, \ldots$ $\ldots, \Phi_n \in X$, то $X \cup \{\Phi\}$ непротиворечиво.*

в) *Если $X \cup \{\exists x \Phi\}$ непротиворечиво, то $X \cup \{[\Phi]_y^x\}$ непротиворечиво при условии, что y не входит свободно в элементы X.*

г) *Если X_n, $n \in \omega$,— непротиворечивые множества, и $X_n \subseteq X_{n+1}$, $n \in \omega$, то $X = \bigcup\limits_{i \in \omega} X_n$ непротиворечиво.*

д) *Если X — непротиворечивое множество формул сигнатуры Σ, то для любой $\Phi \in F(\Sigma)$ либо $X \cup \{\Phi\}$, либо $X \cup \{\neg \Phi\}$ непротиворечиво.*

Доказательство. Утверждение а) следует из теоремы 1. Утверждение г) очевидно. Если $\Phi_1, \ldots, \Phi_n \vdash$ $\vdash \Phi$ — теорема исчисления предикатов, то из доказуемости секвенции $\Psi_1, \ldots, \Psi_k, \Phi \vdash$ следует доказуемость $\Psi_1, \ldots, \Psi_k, \Phi_1, \ldots, \Phi_n \vdash$, так что имеет место б). Если секвенция $\Phi_1, \ldots, \Phi_n, [\Phi]_y^x \vdash$ доказуема в исчислении предикатов и y не входит свободно ни в одну из формул $\Phi_1, \ldots, \Phi_n$, то по правилу предложения 18.4 ж) и правилу 13 получаем доказуемость $\Phi_1, \ldots, \Phi_n \vdash \forall y \neg [\Phi]_y^x$. Тогда из предложения 19.2 ж) следует доказуемость секвенции $\Phi_1, \ldots, \Phi_n \vdash \forall x \neg \Phi$. Из предложения 19.2 а) тогда следует доказуемость $\Phi_1, \ldots, \Phi_n \vdash \neg \exists x \Phi$. Используя теперь правило 10 и аксиому $\exists x \Phi \vdash \exists x \Phi$, получаем, что $\Phi_1, \ldots, \Phi_n, \exists x \Phi \vdash$ является теоремой исчисления предикатов, откуда получаем в). Если $\Phi_1, \ldots, \Phi_n, \Phi \vdash$ и $\Psi_1, \ldots, \Psi_k, \neg \Phi \vdash$ — теоремы исчисления предикатов, то по правилу 9, предложению 18.4 ж) и правилу 10 получаем доказуемость секвенции $\Phi_1, \ldots, \Phi_n, \Psi_1, \ldots$ $\ldots, \Psi_k \vdash$, т. е. справедливо д). □

Приступим теперь к доказательству одной из важнейших теорем математической логики.

Теорема 5 (о существовании модели). *Любое непротиворечивое множество X формул сигнатуры Σ имеет модель.*

Доказательство. В силу теоремы компактности (§ 17) можно считать, что множество X конечно. Пусть $x_1, \ldots, x_n$ — все переменные, входящие свободно в элементы $X = \{\Psi_1, \ldots, \Psi_k\}$. Так как выполнимость X равносильна выполнимости $X' = \{\exists x_1 \ldots \exists x_n (\Psi_1 \wedge \ldots \wedge \Psi_k)\}$, то можно считать, что X состоит из одного предложения. Наконец, сигнатуру $\Sigma = \langle R, F, \mu \rangle$ можно считать конечной. (Если Σ бесконечна, то нужно взять ограничение Σ на множество символов, входящих в элемент X.)

Пусть $C = \{c_n | n \in \omega\}$ — множество символов, $c_n \neq c_k$ для $n \neq k$ и $C \cap (R \cup F) = \varnothing$. Пусть Σ_1 получается добавлением к Σ элементов множества C в качестве символов новых констант. Так как формулы сигнатуры Σ_1 являются словами некоторого счетного алфавита, то множество всех формул сигнатуры Σ_1 имеет счетную мощность. Пусть $\{\Phi_n | n \in \omega\}$ — множество всех предложений сигнатуры Σ_1.

Строим последовательность

$$X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq \ldots, \quad n \in \omega,$$

конечных множеств предложений сигнатуры Σ_1 следующим образом:

1. $X_0 = X$.

2. Если $X_n \cup \{\Phi_n\}$ противоречиво, то $X_{n+1} = X_n \cup \cup \{\neg \Phi_n\}$.

3. Если $X_n \cup \{\Phi_n\}$ непротиворечиво и Φ_n не начинается с квантора существования, то $X_{n+1} = X_n \cup \{\Phi_n\}$.

4. Если $X_n \cup \{\Phi_n\}$ непротиворечиво и $\Phi_n = \exists x \Phi'$, то $X_{n+1} = X_n \cup \left\{\Phi_n, (\Phi')^x_{c_k}\right\}$, где $c_k \in C$ — константа с наименьшим k, не входящая в Φ_n и элементы X_n.

Положим $X_\omega = \bigcup\limits_{n \in \omega} X_n$. Установим некоторые свойства множества X_ω. Пусть Φ и Ψ — произвольные предложения сигнатуры Σ_1.

а) X_ω непротиворечиво;

б) либо $\Phi \in X_\omega$, либо $\neg \Phi \in X_\omega$;

в) если $\Phi_1, \ldots, \Phi_n \in X_\omega$ и $\Phi_1, \ldots, \Phi_n \vdash \Phi$ доказуема, то $\Phi \in X_\omega$;

г) $\Phi \wedge \Psi \in X_\omega \Leftrightarrow (\Phi \in X_\omega$ и $\Psi \in X_\omega)$;

д) $\Phi \vee \Psi \in X_\omega \Leftrightarrow (\Phi \in X_\omega$ или $\Psi \in X_\omega)$;

е) $\neg \Phi \in X_\omega \Leftrightarrow \Phi \notin X_\omega$;

ж) $\Phi \to \Psi \in X_\omega \Leftrightarrow (\Phi \notin X_\omega$ или $\Psi \in X_\omega)$;

з) $\exists x \Phi \in X_\omega \Leftrightarrow ((\Phi)_c^x \in X_\omega$ для некоторой $c \in C)$;

и) $\forall x \Phi \in X_\omega \Leftrightarrow ((\Phi)_c^x \in X_\omega$ для любой $c \in C)$;

к) если t — замкнутый терм сигнатуры Σ_1, то $c \approx t \in X_\omega$ для некоторой $c \in C$.

Для доказательства а) в силу предложения 1 г) достаточно установить, что X_n, $n \in \omega$, непротиворечивы. Рассуждение проводим индукцией по n. По условию $X_0 = X$ непротиворечиво. Пусть X_n непротиворечиво. Если для Φ_n имеет место случай 2, то X_{n+1} непротиворечиво по предложению 1 д). В случае 3 X_{n+1} непротиворечиво по условию. Пусть $X_n \cup \{\exists x \Phi'\}$ непротиворечиво и D — дерево доказательства в ИП^{Σ_1} секвенции $\Psi_1, \ldots, \Psi_k, \exists x \Phi', (\Phi')_c^x \vdash$, где $c \in C$ не входит в формулы $\Psi_1, \ldots, \Psi_k, \exists x \Phi'$. Пусть y — переменная, не входящая в дерево D, и D' получается из D заменой всех вхождений c на y. Очевидно, что D' будет доказательством в ИП^{Σ_1} секвенции $\Psi_1, \ldots, \Psi_k, \exists x \Phi', [\Phi']_y^x \vdash$, что противоречит предложению 1 в), если $\Psi_i \in X_n$, $1 \leqslant i < k$. Свойство б) вытекает непосредственно из построения X_ω, так как $\Phi = \Phi_n$ для некоторого $n \in \omega$. Свойство в) легко следует из свойств а) и б). Свойства г) — ж) легко следуют из свойств а), б) и в). Докажем свойство з). Пусть $\Phi_n = \exists x \Phi$. Если $\exists x \Phi \in X_\omega$, то по свойству а) $X_n \cup \{\Phi_n\}$ непротиворечиво, тогда по построению $(\Phi)_c^x \in X_{n+1}$ для некоторой $c \in C$. С другой стороны, так как $(\Phi)_c^x \vdash \exists x \Phi$ — теорема исчисления предикатов, то из $(\Phi)_c^x \in X_\omega$ и свойства в) получаем $\exists x \Phi \in X_\omega$. Докажем свойство и). Если $\forall x \Phi \in X_\omega$ и $c \in C$, то из аксиомы $(\Phi)_c^x \vdash (\Phi)_c^x$ по правилу 14 получаем теорему $\forall x \Phi \vdash (\Phi)_c^x$. Отсюда по свойству в) получаем $(\Phi)_c^x \in X_\omega$. Если $\forall x \Phi \notin X_\omega$, то по свойству е) $\neg \forall x \Phi \in X_\omega$. Из эквивалентности $\neg \forall x \Phi \equiv \exists x \neg \Phi$ и в) получаем $\exists x \neg \Phi \in X_\omega$. По свойству з) $(\neg \Phi)_c^x \in X_\omega$ для некоторой $c \in C$. Тогда по свойству е) $(\Phi)_c^x \notin X_\omega$. Докажем теперь последнее свойство к). В силу предложения 18.5 а) $\vdash (x \approx t)_t^x$ — теорема исчисления предикатов. По правилу 15 получаем, что $\vdash \exists x (x \approx t)$ — также теорема. Теперь к) следует из в) и з).

На множестве C определим отношение $\sim$ так:

$$c \sim d \Leftrightarrow c \approx d \in X_\omega.$$

Из свойства в) и предложения 18.5 а) — в) следует, что $\sim$ — эквивалентность на C. Если $c \in C$, то обозначим через $\tilde{c}$ класс эквивалентности по отношению $\sim$, содержащий c. Переходим к определению алгебраической системы $\mathfrak{A} = \langle A, \nu^{\mathfrak{A}} \rangle$. Пусть $A = \{\tilde{c} \mid c \in C\}$. Сигнатура системы $\mathfrak{A}$ равна $\Sigma_1 = \langle R, F \cup C, \mu_1 \rangle$. Определим интерпретацию $\nu^{\mathfrak{A}}$ сигнатуры Σ_1 в A. Пусть $c, d_1, \ldots, d_n \in C$. Тогда

1) $\nu^{\mathfrak{A}}(c) = \tilde{c}$;

2) $\langle \tilde{d}_1, \ldots, \tilde{d}_n \rangle \in \nu^{\mathfrak{A}}(r) \Leftrightarrow r(d_1, \ldots, d_n) \in X_\omega$, где $r \in R$, $\mu(r) = n$;

3) если $f \in F$, $\mu(f) = n$, то $\nu^{\mathfrak{A}}(f)(\tilde{d}_1, \ldots, \tilde{d}_n) = \tilde{c} \Leftrightarrow$ $\Leftrightarrow c \approx f(d_1, \ldots, d_n) \in X_\omega$.

Корректность определения предикатов системы $\mathfrak{A}$ по 2) следует из свойства в) и предложения 18.5 д). Проверим, что если $f \in F$, то 3) действительно является определением операции на A. Пусть $c \approx f(d_1, \ldots, d_n) \in$ $\in X_\omega$, $c' \approx f(e_1, \ldots, e_n) \in X_\omega$ и $\tilde{d}_1 = \tilde{e}_1, \ldots, \tilde{d}_n = \tilde{e}_n$. Тогда $d_1 \approx e_1 \in X_\omega, \ldots, d_n \approx e_n \in X_\omega$, откуда по свойству в) и предложению 18.5 г) получаем $f(d_1, \ldots, d_n) \approx$ $\approx f(e_1, \ldots, e_n) \in X_\omega$, следовательно, по свойству в) и предложению 18.5 б) — г) имеем $c \approx c' \in X_\omega$, т. е. $\tilde{c} = \tilde{c}'$. С другой стороны, для любых $\tilde{d}_1, \ldots, \tilde{d}_n \in A$ по свойству к) имеем $c \approx f(d_1, \ldots, d_n) \in X_\omega$ для некоторого $c \in C$, т. е. $\nu^{\mathfrak{A}}(f)$ определена на любых $a_1, \ldots, a_n \in A$.

Индукцией по длине замкнутого терма t сигнатуры Σ_1 покажем, что

$$t^{\mathfrak{A}} = \tilde{c} \Leftrightarrow c \approx t \in X_\omega. \qquad (1)$$

Если t — константа из C, то (1) следует из определения отношения $\sim$ и из 1) определения $\nu^{\mathfrak{A}}$. Для термов t вида $f(d_1, \ldots, d_n)$, где $d_1, \ldots, d_n \in C$ и $f \in F$ (в частности, когда t — константа из Σ), эквивалентность (1) следует из 3) определения $\nu^{\mathfrak{A}}$. Пусть $t = f(t_1, \ldots, t_n)$, $f \in F$, $\mu(f) = n \geqslant 1$ и $t_1^{\mathfrak{A}} = \tilde{d}_1, \ldots, t_n^{\mathfrak{A}} = \tilde{d}_n$. По индукционному предположению $d_1 \approx t_1 \in X_\omega, \ldots, d_n \approx t_n \in X_\omega$, поэтому из предложения 18.5 г) и свойства в) получаем

$$f(t_1, \ldots, t_n) \approx f(d_1, \ldots, d_n) \in X_\omega. \qquad (2)$$

По определению $\nu^{\mathfrak{A}}(f)$ имеем

$$t^{\mathfrak{A}} = \tilde{c} \Leftrightarrow c \approx f(d_1, \ldots, d_n) \in X_\omega. \tag{3}$$

Из (3), (2), предложения 18.5 б), в) и свойства в) получаем (1).

Индукцией по длине предложения Φ сигнатуры Σ_1 покажем

$$\mathfrak{A} \models \Phi \Leftrightarrow \Phi \in X_\omega. \tag{4}$$

Если $\Phi = t_1 \approx t_2$, то по (1) имеем

$\mathfrak{A} \models \Phi \Leftrightarrow (c \approx t_1 \in X_\omega,\ c \approx t_2 \in X_\omega$ для некоторого $c \in C)$.

Отсюда в силу предложения 18.5 б) — г) и свойств в), к) получаем 4) для этого случая. Пусть $\Phi = r(t_1, \ldots, t_n)$, $r \in R$, и $t_1^{\mathfrak{A}} = \tilde{d}_1, \ldots, t_n^{\mathfrak{A}} = \tilde{d}_n$. Используя определение $\nu^{\mathfrak{A}}(r)$, (1), предложение 18.5 и свойство в), получаем (4) для такого Φ. Для остальных Φ эквивалентность (4) сразу получается из индукционного предположения и соответствующих свойств в) — и).

Так как $X \subseteq X_\omega$, то из (4) получаем, что $\mathfrak{A}$ является моделью для множества X. □

Следствием доказанной теоремы является

Теорема 6 (теорема Гёделя о полноте). *Если Φ — тождественно истинная формула исчисления предикатов, то Φ доказуема в исчислении предикатов.*

Доказательство. Из тождественной истинности Φ получаем, что множество $\{\neg\Phi\}$ не имеет модели. Из теоремы 5 следует, что $\{\neg\Phi\}$ противоречиво, т. е. $\neg\Phi \vdash$ — теорема исчисления предикатов. По правилу 9 получаем, что Φ доказуема. □

Доказательство теоремы 5 дает нам следующий факт: конечное непротиворечивое множество X формул сигнатуры Σ имеет конечную или счетную модель $\mathfrak{A}$. К сожалению, теорема компактности, которую мы применили для произвольного множества X, ничего не говорит нам о мощности модели для X. Однако сила метода доказательства теоремы 5 позволяет обойтись без теоремы компактности и заодно получить информацию о мощности полученной модели. Сначала введем одно понятие.

Определение. Множество предложений X сигнатуры Σ называется *полным* в Σ, если X непротиворечиво и для любого предложения Φ сигнатуры Σ либо $\Phi \in X$, либо $\neg\Phi \in X$.

Предложение 2. *Любое непротиворечивое множество X предложений сигнатуры Σ содержится в некотором полном в Σ множестве предложений Y.*

Доказательство. Рассмотрим семейство P всех непротиворечивых множеств предложений сигнатуры Σ, содержащих X. Отношение включения $\subseteq$ частично упорядочивает множество P. Очевидно, что объединение любой цепи из $\langle P, \subseteq\rangle$ принадлежит P. По принципу максимума $\langle P, \subseteq\rangle$ имеет максимальный элемент Y. Из предложения 1 д) получаем, что Y — полное в Σ множество. □

Теорема 7. *Если бесконечное множество X формул сигнатуры Σ непротиворечиво, то X имеет модель $\mathfrak{A}$ мощности, не превосходящей мощность X.*

Доказательство. Пусть $FV(X)$ — все переменные, входящие хотя бы в одну формулу из X свободно. Рассмотрим такое множество $C' = \{c_x | x \in FV(X)\}$ символов, что $c_x \neq c_y$ для $x \neq y$ и $C' \cap (R \cup F) = \varnothing$. Пусть $\Sigma(X)$ — сигнатура, все символы которой входят хотя бы в одну формулу из X. Пусть Σ_0 получается из $\Sigma(X)$ добавлением элементов множества C' в качестве символов новых констант. В силу следствия 13.2 $|\Sigma_0| \leqslant |X|$. Заменим во всех формулах из X все свободные вхождения переменных $x \in FV(X)$ на константы $c_x \in C'$ соответственно. Ясно, что полученное множество X' предложений сигнатуры Σ_0 имеет модель тогда и только тогда, когда X имеет модель. Множество X' непротиворечиво *). В самом деле, предположим, что D — дерево доказательства секвенции $(\Phi_1)^{x_1,\ldots,x_n}_{c_{x_1},\ldots,c_{x_n}}, \ldots, (\Phi_k)^{x_1,\ldots,x_n}_{c_{x_1},\ldots,c_{x_n}} \vdash$, где $\Phi_1, \ldots, \Phi_k \in X$ и $c_{x_1}, \ldots, c_{x_n}$ — все константы из C', входящие в D. Заменив константы $c_{x_1}, \ldots, c_{x_n}$ на переменные $y_1, \ldots, y_n$, не входящие в D, получим доказательство D' секвенции $(\Phi_1)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n}, \ldots, (\Phi_k)^{x_1,\ldots,x_n}_{y_1,\ldots,y_n} \vdash$. Применяя предложение 18.4 н) (перенеся сначала одну из формул в правую часть с отрицанием), получим доказуемость $\Phi_1, \ldots, \Phi_k \vdash$, что противоречит совместности X.

Переходим к построению множеств предложений X_n, $n \in \omega$, и сигнатур Σ_n, $n \in \omega$. При этом будут выполняться следующие условия:

---

*) По причинам, которые выяснятся в конце данного параграфа, мы даем здесь доказательство, не опирающееся на теорему 5.

1) $X_n \subseteq X_{n+1}$, $n \in \omega$, $X' \subseteq X_0$;

2) X_n — полное в Σ_n множество предложений;

3) сигнатура Σ_{n+1} получается из Σ_n добавлением новых символов констант;

4) $|\Sigma_n| \leqslant |X_n| = |X|$, $n \in \omega$.

В качестве X_0 берем полное в Σ_0 множество предложений, содержащее X'. Если X_n уже построено, то Σ_{n+1} получается из Σ_n добавлением множества $\{c_\Phi^n \mid \Phi \in X_n\}$ новых символов констант. Рассмотрим множество предложений

$$X'_n = X_n \cup \left\{ (\Phi)^x_{c^n_\Psi} \,\middle|\, \Psi = \exists x\Phi,\ \Psi \in X_n \right\}$$

сигнатуры Σ_{n+1}. Множество X'_n непротиворечиво. В самом деле, предположим, что для $\{\Psi'_1, \ldots, \Psi'_k, \Psi_1, \ldots, \Psi_m\} \subseteq X_n$, $\Psi_1 = \exists z_1\Phi_1, \ldots, \Psi_m = \exists z_m\Phi_m$, секвенция

$$\Psi'_1, \ldots, \Psi'_k, (\Phi_1)^{z_1}_{c^n_{\Psi_1}}, \ldots, (\Phi_m)^{z_m}_{c^n_{\Psi_m}} \vdash$$

доказуема и m — минимальное такое число. Заменяя в доказательстве D этой секвенции константу $c^n_{\Psi_1}$ на переменную y, не входящую в D, получим доказательство D' секвенции

$$\Psi'_1, \ldots, \Psi'_k, [\Phi_1]^{z_1}_y, (\Phi_2)^{z_2}_{c^n_{\Psi_2}}, \ldots, (\Phi_m)^{z_m}_{c^n_{\Psi_m}} \vdash.$$

Из предложения 1 в) получаем, что секвенция

$$\Psi'_1, \ldots, \Psi'_k, \exists z_1\Phi_1, (\Phi_2)^{z_2}_{c^n_{\Psi_2}}, \ldots, (\Phi_m)^{z_m}_{c^n_{\Psi_m}} \vdash$$

доказуема, что противоречит минимальности m. В качестве X_{n+1} берем теперь полное в Σ_{n+1} множество предложений, содержащее X'_n. Пусть $X_\omega = \bigcup\limits_{n\in\omega} X_n$ и C есть множество всех констант из всех Σ_n, $n \in \omega$. Так как каждое X_n непротиворечиво, то и X_ω непротиворечиво. Очевидно также, что X_ω — полное в Σ_ω множество, где $\Sigma_\omega = \bigcup\limits_{n\in\omega} \Sigma_n$ получается из Σ добавлением элементов C в качестве символов констант. Следовательно, X_ω имеет свойства а) и б) из доказательства теоремы 5, где вместо сигнатуры Σ_1 рассматривается сигнатура Σ_ω. Из свойств а) и б) следуют свойства в) — ж). Свойство з) следует из построения множеств X'_n, $n \in \omega$. Наконец, свойства и), к) следуют из свойства з) так же, как в теореме 5. Далее нужно в точности повторить конец доказательства теоремы 5, начиная с определения отношения $\sim$ на множестве C.

Осталось только заметить, что мощность модели $\mathfrak{A}$ не превосходит мощности множества C, которое в свою очередь является объединением счетного числа множеств, имеющих мощность, не превосходящую мощность X, и, следовательно, имеет мощность, не превосходящую мощность $\omega \times X$. По следствию 13.1 а) имеем $|\omega \times X| = |X|$. $\square$

Теорема 7 вместе с теоремой 1 дает также новое доказательство теоремы компактности. (См. подстрочное примечание на с. 140.)

Упражнения

1. Привести пример формулы Φ исчисления предикатов, для которой множества $\{\Phi\}$ и $\{\neg\Phi\}$ непротиворечивы.
2. Вывести теорему компактности из теорем 1 и 7.
3. Из теорем 1 и 6 получить характеризацию доказуемых секвенций ИП$^\Sigma$: секвенция C исчисления ИП$^\Sigma$ тогда и только тогда доказуема в ИП$^\Sigma$, когда C тождественно истинна.

§ 22. Исчисление предикатов гильбертовского типа

Зафиксируем произвольную сигнатуру Σ. Все зависящие от сигнатуры понятия этого параграфа будут относиться к сигнатуре Σ.

В этом параграфе мы рассмотрим исчисление ИП$_1^\Sigma$, которое называется *исчислением предикатов гильбертовского типа*, и покажем его эквивалентность в определенном смысле (теорема 9) исчислению ИП$^\Sigma$ подобно тому, как в § 8 была показана эквивалентность ИВ и ИВ$_1$.

Определение *формулы* ИП$_1^\Sigma$ то же, что и для ИП$^\Sigma$. Секвенций в ИП$_1^\Sigma$ нет.

Аксиомы ИП$_1^\Sigma$ получаются из следующих 14 схем заменой переменных Φ, Ψ, X конкретными формулами ИП$_1^\Sigma$; x, y, z — переменными, а t — термами ИП$_1^\Sigma$:

1. $\Phi \to (\Psi \to \Phi)$,
2. $(\Phi \to \Psi) \to ((\Phi \to (\Psi \to X)) \to (\Phi \to X))$,
3. $(\Phi \wedge \Psi) \to \Phi$,
4. $(\Phi \wedge \Psi) \to \Psi$,
5. $(\Phi \to \Psi) \to ((\Phi \to X) \to (\Phi \to (\Psi \wedge X)))$,

6. $\Phi \to (\Phi \vee \Psi)$,
7. $\Phi \to (\Psi \vee \Phi)$,
8. $(\Phi \to X) \to ((\Psi \to X) \to ((\Phi \vee \Psi) \to X))$,
9. $(\Phi \to \Psi) \to ((\Phi \to \neg \Psi) \to \neg \Phi)$,
10. $\neg\neg \Phi \to \Phi$,
11. $\forall x \Phi \to (\Phi)^x_t$,
12. $(\Phi)^x_t \to \exists x \Phi$,
13. $x \approx x$,
14. $x \approx y \to ((\Phi)^z_x \to (\Phi)^z_y)$.

Правила вывода ИП^Σ_1:

1. $\dfrac{\Phi, \Phi \to \Psi}{\Psi}$, 2. $\dfrac{\Psi \to \Phi}{\Psi \to \forall x \Phi}$, 3. $\dfrac{\Phi \to \Psi}{\exists x \Phi \to \Psi}$,

где в правилах 2 и 3 x не входит свободно в Ψ.

Доказательством в ИП^Σ_1 формулы Φ называется такая последовательность $\Phi_0, \ldots, \Phi_n$ формул ИП^Σ_1, что $\Phi_n = \Phi$ и для каждого $i \leqslant n$ формула Φ_i удовлетворяет одному из следующих условий:

1) Φ_i — аксиома ИП^Σ_1,

2) Φ_i получается из некоторых Φ_j, $j < i$, по одному из правил 1—3.

Если существует доказательство в ИП^Σ_1 формулы Φ, то Φ называется *доказуемой* в ИП^Σ_1 или *теоремой* ИП^Σ_1 (обозначаем $\rhd \Phi$).

Выводом в ИП^Σ_1 *формулы* Φ *из множества формул* G называется такая последовательность $\Phi_0, \ldots, \Phi_n$ формул ИП^Σ_1, что $\Phi_n = \Phi$ и для каждого $i \leqslant n$ формула Φ_i удовлетворяет одному из следующих условий:

1) Φ_i доказуема в ИП^Σ_1,

2) Φ_i принадлежит G,

3) Φ_i получается из некоторых Φ_j, $j < i$, по одному из правил 1—3, причем при применении правил 2 и 3 переменная x не должна входить ни в одну формулу из G свободно.

Если существует вывод в ИП^Σ_1 формулы Φ из множества G, то Φ называется *выводимой в* ИП^Σ_1 *из* G. При этом G называется множеством гипотез. Очевидно, что доказуемость формулы эквивалентна ее выводимости из пустого множества гипотез. Поэтому выводимость Φ из G можно обозначать через $G \rhd \Phi$. В этом параграфе, если не оговорено противное, под доказательством и выводом понимаются доказательство и вывод в ИП^Σ_1.

Правило вывода

$$\frac{\Psi_1, \ldots, \Psi_k}{\Phi}$$

называется *допустимым в* ИП_1^Σ, если его добавление к исчислению ИП_1^Σ не изменяет множества доказуемых формул.

Предложение 1. *Следующие правила будут допустимыми в* $ИП_1^\Sigma$:

$$\text{а)}\ \frac{\Phi}{\forall x\Phi};\quad \text{б)}\ \frac{(\Phi)_t^x}{\exists x\Phi};\quad \text{в)}\ \frac{(\Phi)_t^x \to \Psi}{\forall x\Phi \to \Psi};\quad \text{г)}\ \frac{\Psi \to (\Phi)_t^x}{\Psi \to \exists x\Phi}.$$

Доказательство. а) Пусть Ψ — некоторое доказуемое предложение, тогда в силу аксиомы 1, доказуемости Φ и правила 1 получаем $\rhd \Psi \to \Phi$. По правилу 2 получаем $\rhd \Psi \to \forall x\Phi$. Отсюда доказуемость $\forall x\Phi$ следует по правилу 1.

в) Формулу $\forall x\Phi \to \Psi$ получаем из аксиомы $\forall x\Phi \to (\Phi)_t^x$ и теоремы $(\Phi)_t^x \to \Psi$ с помощью аксиом 1, 2 и правила 1.

Доказательство утверждений б) и г) мы оставляем читателю (упражнение 1). □

Формулы Φ и Ψ называются *эквивалентными в* ИП_1^Σ, если в ИП_1^Σ доказуемы формулы $\Phi \to \Psi$ и $\Psi \to \Phi$ (обозначаем это через $\Phi \overset{1}{\equiv} \Psi$).

Предложение 2. *Любая тавтология* Φ *доказуема в* $ИП_1^\Sigma$.

Доказательство. Пусть Ψ — основа Φ. В силу теоремы 8.11 Ψ доказуема в ИВ_1. Ясно, что, заменив пропозициональные переменные в доказательстве в ИВ_1 формулы Ψ на соответствующие формулы ИП_1^Σ, получим доказательство Φ в ИП_1^Σ. □

Следствие 1. *Если* Φ *и* Ψ — *пропозиционально эквивалентные формулы* $ИП_1^\Sigma$, *то доказуемость* Φ *в* $ИП_1^\Sigma$ *равносильна доказуемости* Ψ *в* $ИП_1^\Sigma$. □

Теорема 8 (о дедукции). *Если* $G \cup \{\Phi, \Psi\}$ — *множество формул* $ИП_1^\Sigma$, *то из* $G \cup \{\Phi\} \rhd \Psi$ *следует* $G \rhd \Phi \to \Psi$.

Доказательство. Индукция по длине n минимального вывода $\Psi_1, \ldots, \Psi_n$ формулы Ψ из $G \cup \{\Phi\}$. Случай, когда $n = 1$ (т. е. Ψ — теорема ИП_1^Σ или принадлежит $G \cup \{\Phi\}$), а также случай, когда Ψ_n получается по правилу 1, ничем не отличаются от соответствующих случаев для $ИВ_1$ и уже рассмотрены в доказательстве теоремы 8.12. В силу минимальности вывода осталось рассмотреть случаи, когда Ψ получается из Ψ_{n-1} по правилам 2 или 3. По предположению индукции мы уже имеем $G \rhd \Phi \to \Psi_{n-1}$.

Пусть $\Psi_{n-1} = (\Theta_1 \to \Theta_2)$ и $\Psi = (\Theta_1 \to \forall x\Theta_2)$. При этом в силу определения вывода x не входит свободно в Φ, элементы G и Θ_1. Так как $\Phi \to (X_1 \to X_2)$ и $(\Phi \wedge X_1) \to X_2$ пропозиционально эквивалентны для любых формул X_1, X_2, то в силу следствия 1 последовательность

$$\Phi \to \Psi_{n-1},\ (\Phi \wedge \Theta_1) \to \Theta_2,\ (\Phi \wedge \Theta_1) \to \forall x\Theta_2,\ \Phi \to (\Theta_1 \to \forall x\Theta_2)$$

можно дополнить до вывода $\Phi \to \Psi$ из G.

Пусть теперь Ψ получается по правилу 3. Тогда $\Psi_{n-1} = (\Theta_1 \to \Theta_2)$ и $\Psi = (\exists x\Theta_1 \to \Theta_2)$. Здесь x не входит свободно в Φ, Θ_2 и элементы G. В силу пропозициональных эквивалентностей $\Phi \to \Psi_{n-1} \overset{s}{\equiv} \Theta_1 \to (\Phi \to \Theta_2)$ и $\exists x\Theta_1 \to (\Phi \to \Theta_2) \overset{s}{\equiv} \Phi \to (\exists x\Theta_1 \to \Theta_2)$ следующую последовательность:

$$\Phi \to \Psi_{n-1},\ \Theta_1 \to (\Phi \to \Theta_2),\ \exists x\Theta_1 \to (\Phi \to \Theta_2),\ \Phi \to (\exists x\Theta_1 \to \Theta_2)$$

можно дополнить до вывода $\Phi \to \Psi$ из G. □

С л е д с т в и е 2. *Пусть* $\Phi_1, \ldots, \Phi_n$, Φ — *формулы* $ИП_1^\Sigma$. *Тогда* $\{\Phi_1, \ldots, \Phi_n\} \rhd \Phi$ *равносильно* $\rhd \Phi_1 \to (\Phi_2 \to \ldots (\Phi_n \to \Phi)\ldots)$, *что в свою очередь равносильно* $\rhd (\Phi_1 \wedge (\ldots (\Phi_{n-1} \wedge \Phi_n)\ldots)) \to \Phi$.

Д о к а з а т е л ь с т в о. Для первой эквивалентности n раз применяется теорема 8 и правило 1. Для второй эквивалентности те же рассуждения, что и в следствии 8.1. □

Т е о р е м а 9. *Для того чтобы формула* Φ *была выводима в* $ИП_1^\Sigma$ *из множества всех членов конечной последовательности формул* Γ, *необходимо и достаточно, чтобы секвенция* $\Gamma \vdash \Phi$ *была доказуема в* $ИП^\Sigma$. *В частности, множества формул, доказуемых в* $ИП_1^\Sigma$ *и в* $ИП^\Sigma$, *совпадают.*

Д о к а з а т е л ь с т в о. В силу правил 7 и 8 $ИП^\Sigma$ секвенция $\Psi_1, \ldots, \Psi_n \vdash \Phi$ доказуема в $ИП^\Sigma$ тогда и только тогда, когда доказуема $\vdash \Psi_1 \to (\Psi_2 \to \ldots (\Psi_n \to \Phi)\ldots)$. Тогда из следствия 2 получаем, что для доказательства необходимости можно ограничиться случаем $\Gamma = \varnothing$.

Легко проверить, что аксиомы $ИП_1^\Sigma$ тождественно истинны, а правила вывода $ИП_1^\Sigma$ сохраняют тождественную истинность. Поэтому необходимость следует из теоремы Гёделя о полноте.

Достаточность. Очевидно, что если $\Gamma \vdash \Phi$ — аксиома $ИП^\Sigma$, то $\Gamma \rhd \Phi$. (Здесь и далее мы допускаем некоторую вольность в обозначениях: следовало бы писать $\{\Psi_1, \ldots, \Psi_n\} \rhd \Phi$, если $\Gamma = \langle \Psi_1, \ldots, \Psi_n \rangle$.) Пусть Φ_0 — какое-нибудь предложение сигнатуры Σ. Так как правила

$$\frac{\Gamma \vdash}{\Gamma \vdash \Phi_0 \wedge \neg \Phi_0}, \qquad \frac{\Gamma \vdash \Phi_0 \wedge \neg \Phi_0}{\Gamma \vdash}$$

являются допустимыми в $ИП^\Sigma$, то осталось показать, что если в правилах вывода исчисления $ИП^\Sigma$ заменить знак $\vdash$ на $\rhd$, а $\Gamma \vdash$ на $\Gamma \rhd \Phi_0 \wedge \neg \Phi_0$, то из истинности утверждений над чертой будет следовать утверждение под чертой. Для правил 1—12 проверка та же самая, что и в теореме 8.11. Для правил 13 и 15 при $\Gamma = \varnothing$ это верно в силу предложения 1 а), б). Для остальных случаев это следует из следствия 2, правил 2, 3 исчисления $ИП_1^\Sigma$ и предложения 1 в), г). $\square$

Из этой теоремы и теоремы 2 получаем

Следствие 3. *Если $\Sigma_1 \subseteq \Sigma$, то исчисление $ИП_1^\Sigma$ является консервативным расширением исчисления $ИП_1^{\Sigma_1}$.* $\square$

Из теоремы 9 следует также, что $\Phi \overset{1}{\equiv} \Psi$ равносильно $\Phi \equiv \Psi$.

Следствие 4. *Пусть $X \cup \{\Phi\}$ — множество формул сигнатуры Σ, а Y — множество всех переменных, входящих свободно хотя бы в одну формулу из $X \cup \{\Phi\}$. Для того чтобы имело место $X \rhd \Phi$, необходимо и достаточно, чтобы выполнялось следующее условие: для любой алгебраической системы $\mathfrak{A}$ сигнатуры Σ и интерпретации $\gamma\colon Y \to A$, если имеет место $\mathfrak{A} \models \Psi[\gamma]$ при любом $\Psi \in X$,* то $\mathfrak{A} \models \Phi[\gamma]$.

Доказательство. Так как вывод содержит лишь конечное множество формул, то $X \rhd \Phi$ равносильно тому, что $X_1 \rhd \Phi$ для некоторого конечного $X_1 \subseteq X$. Необходимость тогда следует из теорем 9 и 1. Если из $\mathfrak{A} \models \Psi[\gamma]$, $\Psi \in X$, следует $\mathfrak{A} \models \Phi[\gamma]$ для любых систем $\mathfrak{A}$ сигнатуры Σ и $\gamma\colon Y \to A$, то множество $X \cup \{\neg\Phi\}$ не имеет модели. Тогда по теореме 5 для некоторых $\Psi_1, \ldots, \Psi_n \in X$ секвенция $\Psi_1, \ldots, \Psi_n \vdash \Phi$ доказуема и из теоремы 9 получаем достаточность. $\square$

Упражнения

1. Доказать утверждения б) и г) предложения 1.

2. Доказать, что $\Gamma \rhd \Phi$ тогда и только тогда, когда существует такая последовательность $\Phi_0, \ldots, \Phi_n$ формул ИП_1^Σ, что $\Phi_n = \Phi$ и для каждого $i \leqslant n$ формула Φ_i удовлетворяет одному из следующих условий:

1) Φ_i доказуема в ИП_1^Σ,

2) Φ_i принадлежит Γ,

3) Φ_i получается из некоторых Φ_j, $j < i$, по правилу 1.

§ 23. Чистое исчисление предикатов

В этом параграфе будет определено исчисление ИПЧ, которое называется *чистым исчислением предикатов*, и будет доказана некоторая «универсальность» этого исчисления (теорема 11).

Рассмотрим сигнатуру $\Sigma^* = \langle R^*, F^*, \mu^* \rangle$ со следующими свойствами:

1) $F^* = \varnothing$, $R^* = \{r_m^k \mid k, m \in \omega\}$;

2) $\mu^*(r_m^k) = k$ для любого $m \in \omega$ и $k \in \omega$.

Формулами ИПЧ будут формулы сигнатуры Σ^*, не содержащие символа равенства. *Секвенции* ИПЧ — это секвенции ИП^{Σ^*}, все формулы в которых являются формулами ИПЧ.

Аксиомами ИПЧ будут только секвенции вида $\Phi \vdash \Phi$; *правила вывода* те же, что у ИП^{Σ^*}. Доказательство в ИПЧ определяется так же, как в ИП^{Σ^*}, — конечно, под формулами, секвенциями и аксиомами теперь понимаются формулы, секвенции и аксиомы ИПЧ. Легко проверить, что все результаты в §§ 18—20, относящиеся к ИП^{Σ^*}, за исключением предложения 18.5, предложения 20.1 и теоремы 2, справедливы также для ИПЧ, так как в их доказательствах не используются аксиомы 2), 3). Сейчас мы покажем, что результаты § 21 также распространяются на ИПЧ. На самом деле имеет место

Теорема 10. *Исчисление* ИП^{Σ^*} *является консервативным расширением исчисления ИПЧ.*

Доказательство. Множество X предложений ИПЧ называется совместным в ИПЧ, если для любых $\Phi_1, \ldots, \Phi_n \in X$ секвенция $\Phi_1, \ldots, \Phi_n \vdash$ не доказуема в ИПЧ. Покажем, что любое совместное в ИПЧ множество формул ИПЧ имеет модель. Доказательство этого утверждения мало чем отличается от доказательства теоремы 5.

Построение множества X_ω то же самое. (При этом под формулами и доказательствами, конечно, понимаются формулы и доказательства в ИПЧ.) Доказательства свойств а) — и) для X_ω те же самые. Свойство к) в данном случае не требуется. Отношение $\sim$ на C не определяется и носителем системы $\mathfrak{A}$ является само множество C. Доказательство эквивалентности

$$\mathfrak{A} \vDash \Phi(d_1, \ldots, d_n) \Leftrightarrow \Phi(d_1, \ldots, d_n) \in X_\omega$$

из свойств а) — и) проводится еще проще, чем в теореме 5, так как отпадает необходимость переходить к представителям классов эквивалентности по отношению $\sim$ и нет атомарных формул вида $t_1 \approx t_2$.

Если теперь $S = \Psi_1, \ldots, \Psi_n \vdash \Phi$ — теорема ИП$^{\Sigma *}$, являющаяся секвенцией ИПЧ, то по теореме 1 S — тождественно истинная секвенция. Тогда по только что доказанному $\{\Psi_1, \ldots, \Psi_n, \neg\Phi\}$ — не совместное в ИПЧ множество, следовательно, секвенция $\Psi_1, \ldots, \Psi_n, \neg\Phi \vdash$ доказуема в ИПЧ. По правилу 9 получаем доказуемость S в ИПЧ. Если $S = \Psi_1, \ldots, \Psi_n \vdash$, то $\{\Psi_1, \ldots, \Psi_n\}$ — не совместное в ИПЧ множество, и опять $\Psi_1, \ldots, \Psi_n \vdash$ — теорема ИПЧ. □

Ясно, что из результатов § 21 и теоремы 10 следует справедливость всех теорем, полученных из теорем § 21 заменой ИП$^\Sigma$ на ИПЧ. Конец этого параграфа мы посвятим одному факту, который показывает, что вопросы о доказуемости в различных ИП$^\Sigma$ «сводятся» к вопросам о доказуемости в ИПЧ. Переходим к точным формулировкам.

Зафиксируем предикатный символ $r_0 \in R^*$, для которого $\mu_0(r_0) = 2$.

Определение. Пусть $\Sigma = \langle R, F, \mu\rangle$ — конечная или счетная сигнатура. Разнозначное отображение α: $R \cup F \to R^*$ называется *интерпретацией* Σ в Σ^*, если выполняются следующие условия: а) $r_0 \notin \alpha(R \cup F)$; б) если $s \in R$, то $\mu^*(\alpha s) = \mu(s)$; в) если $f \in F$, то $\mu^*(\alpha f) = \mu(f) + 1$. Для интерпретации α сигнатуры Σ в Σ^* определим отображение α^* множества формул сигнатуры Σ, находящихся в приведенной нормальной форме, в множество формул ИПЧ по индукции. Если Φ — атомная формула вида $x \approx y$, то $\alpha^*(\Phi) = r_0(x, y)$; если Φ — атомная формула вида $s(x_1, \ldots, x_n)$, то $\alpha^*\Phi = \alpha s(x_1, \ldots, x_n)$; если Φ — атомная формула вида $y \approx f(x_1, \ldots, x_n)$ или $f(x_1, \ldots, x_n) \approx y$, то $\alpha^*\Phi = \alpha f(x_1, \ldots, x_n, y)$;

если $\Phi = \neg\Psi$, $\Phi = Qx\Psi$ или $\Phi = \Psi_1\tau\Psi_2$, где $Q \in \{\forall, \exists\}$, $\tau \in \{\wedge, \vee, \rightarrow\}$, то $\alpha^*\Phi$ равна $\neg\alpha^*\Psi$, $Qx\alpha^*\Psi$ или $\alpha^*\Psi_1\tau\alpha^*\Psi_2$ соответственно. Если α — интерпретация Σ в Σ^*, $\Phi \in F(\Sigma)$ находится в приведенной н. ф. и $\Sigma(\Phi) = \langle\{s_0, \ldots, s_k\}, \{f_0, \ldots, f_m\}, \mu'\rangle$, то через $\alpha_0\Phi$ обозначим конъюнкцию следующих предложений сигнатуры Σ^* (где $n_j = \mu'(s_j)$, $l_i = \mu'(f_i)$, $x, y, z, x_1, \ldots, x_n, y_1, \ldots, y_n$ — попарно различные переменные)*):

$$1)\ \forall x_1 \ldots \forall x_{n_j} \forall y_1 \ldots \forall y_{n_j} ((r_0(x_1, y_1) \wedge \ldots$$
$$\ldots \wedge r_0(x_{n_j}, y_{n_j}) \wedge \alpha s_j(x_1, \ldots, x_{n_j})) \rightarrow \alpha s_j(y_1, \ldots, y_{n_j})),\ j \leqslant k;$$

$$2)\ \forall x_0 \ldots \forall x_{l_i} \forall y_0 \ldots \forall y_{l_i} ((r_0(x_0, y_0) \wedge \ldots$$
$$\ldots \wedge r_0(x_{l_i}, y_{l_i}) \wedge \alpha f_i(x_0, \ldots, x_{l_i})) \rightarrow \alpha f_i(y_0, \ldots, y_{l_i})),\ i \leqslant m;$$

$$3)\ \forall x_1 \ldots \forall x_{l_i} \exists y \alpha f_i(x_1, \ldots, x_{l_i}, y),\quad i \leqslant m;$$

$$4)\ \forall x_1 \ldots \forall x_{l_i} \forall y \forall z ((\alpha f_i(x_1, \ldots, x_{l_i}, y) \wedge$$
$$\wedge\ \alpha f_i(x_1, \ldots, x_{l_i}, z)) \rightarrow r_0(y, z)),\quad i \leqslant m;$$

$$5)\ \forall x r_0(x, x);$$

$$6)\ \forall x \forall y (r_0(x, y) \rightarrow r_0(y, x));$$

$$7)\ \forall x \forall y \forall z ((r_0(x, y) \wedge r_0(y, z)) \rightarrow r_0(x, z)).$$

Ясно, что из условия 2) на сигнатуру Σ^* следует, что для любой конечной или счетной сигнатуры Σ существует интерпретация Σ в Σ^*.

Теорема 11. *Пусть Φ — формула исчисления предикатов, $\Phi' \equiv \Phi$, Φ' находится в приведенной н. ф. и α — интерпретация сигнатуры $\Sigma(\Phi')$ в Σ^*. Тогда Φ доказуема в исчислении предикатов тогда и только тогда, когда $\alpha_0\Phi' \rightarrow \alpha^*\Phi'$ доказуема в ИПЧ.*

Доказательство. В силу теорем 1, 6 и 10 достаточно проверить, что тождественная истинность Φ' равносильна тождественной истинности $\alpha_0\Phi' \rightarrow \alpha^*\Phi'$. Для любой системы $\mathfrak{A}$ сигнатуры $\Sigma(\Phi') = \langle\{s_0, \ldots, s_k\},$

---

*) Предложение $\alpha_0\Phi$ зависит только от сигнатуры $\Sigma(\Phi)$, а его истинность на алгебраической системе $\mathfrak{A}$ равносильна тому, что $\nu^{\mathfrak{A}}(r_0)$ есть эквивалентность, предикаты αs_j и αf_i не «различают» $\nu^{\mathfrak{A}}(r_0)$ -эквивалентные элементы, а отношения $\nu^{\mathfrak{A}}(\alpha f_i)$ определяют на классах $\nu^{\mathfrak{A}}(r_0)$ -эквивалентных элементов l_i-местные операции.

$\{f_0, \ldots, f_m\}, \mu\rangle$ определим систему $\alpha\mathfrak{A}$ сигнатуры $\alpha\Sigma = \langle\{r_0, \alpha s_0, \ldots, \alpha s_k, \alpha f_0, \ldots, \alpha f_m\}, \varnothing, \alpha\mu\rangle \in \Sigma^*$ следующим образом:

а) $\alpha A = A$;

б) $\langle a, b\rangle \in \nu^{\alpha\mathfrak{A}}(r_0) \Leftrightarrow a = b$;

в) $\nu^{\alpha\mathfrak{A}}(\alpha s_j) = \nu^{\mathfrak{A}}(s_j),\ j \leqslant k$;

г) $\nu^{\alpha\mathfrak{A}}(\alpha f_i) = \nu^{\mathfrak{A}}(f_i),\ i \leqslant m,\ \mu(f_i) > 0$;

д) $\nu^{\alpha\mathfrak{A}}(\alpha f_i) = \left\{\nu^{\mathfrak{A}}(f_i)\right\},\ i \leqslant m,\ \mu(f_i) = 0.$

Индукцией по длине формулы Ψ сигнатуры $\Sigma(\Phi')$, находящейся в приведенной н. ф., легко проверить, что для любой интерпретации γ в A свободных переменных Ψ

$$\mathfrak{A} \vDash \Psi[\gamma] \Leftrightarrow \alpha\mathfrak{A} \vDash \alpha^*\Psi[\gamma].$$

В частности, для любой $\gamma\colon FV(\Phi') \to A$ имеем

$$\mathfrak{A} \vDash \neg\Phi'[\gamma] \Rightarrow \alpha\mathfrak{A} \vDash \neg\alpha^*\Phi'[\gamma]. \tag{1}$$

Очевидно, что в $\alpha\mathfrak{A}$ истинно $\alpha_0\Phi'$, поэтому из (1) получаем, что из тождественной истинности $\alpha_0\Phi' \to \alpha^*\Phi'$ следует тождественная истинность Φ'.

Пусть $\alpha_0\Phi' \to \alpha^*\Phi'$ не тождественно истинна, тогда для некоторой системы $\mathfrak{A}_0$ сигнатуры $\alpha\Sigma$ и интерпретации γ_0 в A_0 свободных переменных Φ' имеем $\mathfrak{A}_0 \vDash \alpha_0\Phi'$ и $\mathfrak{A}_0 \vDash \neg\alpha^*\Phi'[\gamma_0]$. Из истинности в $\mathfrak{A}_0$ предложений 5) — 7) из определения $\alpha_0\Phi'$ получаем, что отношение $\nu^{\mathfrak{A}_0}(r_0)$ определяет на A_0 эквивалентность. Класс эквивалентности по отношению $\nu^{\mathfrak{A}_0}(r_0)$, содержащий $a \in A_0$, будем обозначать через $\tilde{a}$. Определим систему $\mathfrak{B}_0$ сигнатуры $\Sigma(\Phi')$ следующим образом:

а) $B_0 = \{\tilde{a} \mid a \in A_0\}$;

б) $\langle\tilde{a}_1, \ldots, \tilde{a}_n\rangle \in \nu^{\mathfrak{B}_0}(s_j) \Leftrightarrow \langle a_1, \ldots, a_n\rangle \in$

$$\in \nu^{\mathfrak{A}_0}(\alpha s_j), \qquad j \leqslant k;$$

в) $\langle\tilde{a}_1, \ldots, \tilde{a}_{n+1}\rangle \in \nu^{\mathfrak{B}_0}(f_i) \Leftrightarrow \langle a_1, \ldots, a_{n+1}\rangle \in$

$$\in \nu^{\mathfrak{A}_0}(\alpha f_i), \qquad i \leqslant m,\ \mu(f_i) = n > 0;$$

г) $\tilde{a} = \nu^{\mathfrak{B}_0}(f_i) \Leftrightarrow a \in \nu^{\mathfrak{A}_0}(\alpha f_i), \qquad i \leqslant m,\ \mu(f_i) = 0.$

Из истинности на $\mathfrak{A}_0$ конъюнктивных членов 1) и 2) предложения $\alpha_0\Phi'$ следует корректность этих определений. Из истинности предложений 3) и 4) следует, что $\nu^{\mathfrak{B}_0}(f_i)$, $i \leqslant m$, — операции на B_0. Индукцией по длине формулы $\Psi(x_1, \ldots, x_n)$ сигнатуры $\Sigma(\Phi')$, находящейся в приведенной нормальной форме, легко проверить, что для любых $a_1, \ldots, a_n \in A_0$

$$\mathfrak{B}_0 \models \Psi(\tilde{a}_1, \ldots, \tilde{a}_n) \Leftrightarrow \mathfrak{A}_0 \models \alpha^*\Psi(a_1, \ldots, a_n).$$

Отсюда получаем, что $\mathfrak{B}_0 \models \neg\Phi'[\tilde{\gamma}_0]$, где $\tilde{\gamma}_0(x) = \widetilde{\gamma_0(x)}$, $x \in FV(\Phi')$, т. е. Φ' — не тождественно истинная формула. □

Как будет показано в § 38, существуют эффективно заданные множества формул, для которых нет эффективной процедуры (алгоритма), позволяющей для любой формулы данного множества за конечное число шагов устанавливать, является ли она тождественно истинной формулой или нет. Однако теорема Гёделя о полноте дает нам возможность по любой эффективно заданной сигнатуре Σ построить эффективный процесс (машину) M^Σ, который перечисляет все тождественно истинные формулы сигнатуры Σ, т. е. M в процессе работы выдает такие слова $\Phi_0, \ldots, \Phi_n, \ldots$, что $\{\Phi_0, \ldots, \Phi_n, \ldots\}$ есть множество всех тождественно истинных формул сигнатуры Σ. Этот процесс состоит в выписывании конечных последовательностей секвенций ИП$^\Sigma$ и выдает слово Φ тогда, когда выписанная последовательность есть линейное доказательство секвенции $\vdash \Phi$ в ИП$^\Sigma$. Так как для любого эффективно заданного множества формул X переход от формулы $\Phi \in X$ к формуле $\Phi' \equiv \Phi$ в приведенной н. ф., а затем к формуле $\alpha_0\Phi' \to \alpha^*\Phi'$ можно сделать эффективным, то теорема 11 показывает, что для того чтобы уметь перечислять все тождественно истинные формулы из любого эффективно заданного множества формул, достаточно построить машину M, перечисляющую теоремы ИПЧ.

Упражнение

1. Пусть J — исчисление, полученное добавлением к ИПЧ символа равенства и следующих аксиом:

а) $\vdash x \approx x$;

б) $x \approx y,\ (P)^z_x \vdash (P)^z_y$ где P — атомная формула сигнатуры Σ^*.

Показать, что в J доказуемы все теоремы ИП$^{\Sigma^*}$.

Глава 5

ТЕОРИЯ МОДЕЛЕЙ

§ 24. Элементарная эквивалентность

В § 16 было показано, что на изоморфных системах истинны одни и те же предложения. Обратное неверно для бесконечных систем. В этом параграфе мы покажем (теорема 1), что истинность на $\mathfrak{A}$ и $\mathfrak{B}$ одних и тех же предложений равносильна существованию «достаточно большого» запаса конечных частичных изоморфизмов $\mathfrak{A}$ и $\mathfrak{B}$. В частности, если на конечных системах $\mathfrak{A}$ и $\mathfrak{B}$ истинны одни и те же предложения, то $\mathfrak{A}$ изоморфна $\mathfrak{B}$.

Определение. Две алгебраические системы $\mathfrak{A}$ и $\mathfrak{B}$ сигнатуры Σ называются *элементарно эквивалентными* (обозначаем $\mathfrak{A} \equiv \mathfrak{B}$), если для любого предложения Φ сигнатуры Σ

$$\mathfrak{A} \models \Phi \Leftrightarrow \mathfrak{B} \models \Phi.$$

Множество предложений $\{\Phi \mid \mathfrak{A} \models \Phi\}$ сигнатуры Σ называется *элементарной теорией* системы $\mathfrak{A}$ или просто *теорией* $\mathfrak{A}$ и обозначается через $\mathrm{Th}(\mathfrak{A})$.

Ясно, что отношение $\mathfrak{A} \equiv \mathfrak{B}$ равносильно равенству $\mathrm{Th}(\mathfrak{A}) = \mathrm{Th}(\mathfrak{B})$.

Определение. Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — алгебраические системы сигнатуры $\Sigma = \langle R, F, \mu \rangle$. Разнозначное отображение $f\colon X \to B$, где $X \subseteq A$, называется *частичным изоморфизмом* $\mathfrak{A}$ *в* $\mathfrak{B}$, если для любых $a_1, \ldots, a_n \in X$ выполняются следующие условия:

1) если $s \in R \cup F$ — не константа, то

$$\langle a_1, \ldots, a_n \rangle \in \nu^{\mathfrak{A}}(s) \Leftrightarrow \langle fa_1, \ldots, fa_n \rangle \in \nu^{\mathfrak{B}}(s);$$

2) если $s \in F$ — константа, то

$$\nu^{\mathfrak{A}}(s) = a_1 \Leftrightarrow \nu^{\mathfrak{B}}(s) = fa_1.$$

(Напомним, что если $n = 0$, то $\langle a_1, \ldots, a_n \rangle = \langle\ \rangle = \Lambda = \varnothing$.) Если X — конечное множество, то f называется *конечным частичным изоморфизмом*. Множество конечных частичных изоморфизмов $\mathfrak{A}$ в $\mathfrak{B}$ обозначаем через $P(\mathfrak{A}, \mathfrak{B})$.

Теорема 1. *Пусть* $\mathfrak{A}$ *и* $\mathfrak{B}$ — *системы сигнатуры* Σ. *Для того чтобы системы* $\mathfrak{A}$ *и* $\mathfrak{B}$ *были элементарно эквивалентны, необходимо и достаточно, чтобы для любого* $n \in \omega$ *и любой конечной сигнатуры* $\Sigma_1 \subseteq \Sigma$ *существовали непустые множества* $F_1(\Sigma_1, n), \ldots, F_n(\Sigma_1, n)$ *конечных частичных изоморфизмов* $\mathfrak{A} \upharpoonright \Sigma_1$ *в* $\mathfrak{B} \upharpoonright \Sigma_1$ *со следующим свойством:*

*) *если* $f \in F_i(\Sigma_1, n)$, $1 \leqslant i < n$, *то для любых* $a \in A$, $b \in B$ *существуют* $g_1, g_2 \in F_{i+1}(\Sigma_1, n)$, *для которых* $a \in \operatorname{dom} g_1$, $b \in \operatorname{rang} g_2$, $f \subseteq g_1$ *и* $f \subseteq g_2$.

Доказательство. Достаточность. Индукцией по m докажем, что если длина формулы $\Phi(x_1, \ldots, x_k)$, находящейся в приведенной н. ф., не больше m, множества $F_1(\Sigma(\Phi), n) \subseteq P(\mathfrak{A} \upharpoonright \Sigma(\Phi), \mathfrak{B} \upharpoonright \Sigma(\Phi)), \ldots, F_n(\Sigma(\Phi), n) \subseteq P(\mathfrak{A} \upharpoonright \Sigma(\Phi), \mathfrak{B} \upharpoonright \Sigma(\Phi))$ удовлетворяют условию *) и $i + m \leqslant n$, то для любого $f \in F_i(\Sigma(\Phi), n)$ и любых $a_1, \ldots, a_k \in \operatorname{dom} f$

$$\mathfrak{A} \models \Phi(a_1, \ldots, a_k) \Leftrightarrow \mathfrak{B} \models \Phi(fa_1, \ldots, fa_k).$$

Если Φ — атомная формула, то это утверждение следует из определения частичного изоморфизма. Если $\Phi = \neg\Psi$ или $\Phi = \Psi_1 \tau \Psi_2$, $\tau \in \{\wedge, \vee, \rightarrow\}$, то утверждение следует из индукционного предположения. Так как $\forall x \Psi \equiv \neg \exists x \neg \Psi$ для любой формулы Ψ, то достаточно рассмотреть лишь случай $\Phi(x_1, \ldots, x_k) = \exists y \Psi(y, x_1, \ldots, x_k)$. Пусть $\mathfrak{A} \models \Phi(a_1, \ldots, a_k)$. Тогда $\mathfrak{A} \models \Phi(a_0, a_1, \ldots, a_k)$ для некоторого $a_0 \in A$. Возьмем такое $g \in F_{i+1}(\Sigma(\Phi), n)$, что $f \subseteq g$ и $a_0 \in \operatorname{dom} g$. Так как длина Ψ меньше длины Φ, то по индукционному предположению $\mathfrak{B} \models \Psi(ga_0, fa_1, \ldots, fa_k)$, следовательно, $\mathfrak{B} \models \Phi(fa_1, \ldots, fa_k)$. Пусть $\mathfrak{B} \models \Phi(fa_1, \ldots, fa_k)$. Тогда $\mathfrak{B} \models \Psi(b_0, fa_1, \ldots, fa_k)$ для $b_0 \in B$. Возьмем $g \in F_{i+1}(\Sigma(\Phi), n)$, для которого $f \subseteq g$ и $b_0 \in \operatorname{rang} g$. Тогда по индукционному предположению имеем $\mathfrak{A} \models \Psi(g^{-1}b_0, a_1, \ldots, a_k)$, следовательно, $\mathfrak{A} \models \Phi(a_1, \ldots, a_k)$.

Необходимость. Пусть $\Sigma_1 \subseteq \Sigma$ — конечная сигнатура и $X(n, m)$ для $n, m \in \omega$ — максимальное множество попарно не эквивалентных формул Φ сигнатуры Σ_1, находящихся в приведенной н. ф., содержащих $\leqslant n$ кванторов и $FV(\Phi) \subseteq \{v_1, \ldots, v_m\}$. Так как имеется лишь конечное число атомных формул с переменными из множества $\{v_1, \ldots, v_k\}$, то индукцией по n легко показать, что для любых n и m множество $X(n, m)$ конечно. Очевидно, что функция $|X(n, m)|$ неубывающая по каждой из переменных n и m. Пусть $a_1, \ldots, a_k \in A$ попарно различны. Отображение f: $\{a_1, \ldots, a_k\} \to B$ назовем *(n, m)-изоморфизмом*, если $k \leqslant m$ и для любой формулы $\Phi(x_1, \ldots, x_k) \in X(n, m)$ имеет место

$$\mathfrak{A} \vDash \Phi(a_1, \ldots, a_k) \Leftrightarrow \mathfrak{B} \vDash \Phi(fa_1, \ldots, fa_k).$$

Ясно, что любой частичный изоморфизм $f \in P(\mathfrak{A} \restriction \Sigma_1, \mathfrak{B} \restriction \Sigma_1)$, для которого $|\mathrm{dom}\, f| \leqslant m$, является $(0, m)$-изоморфизмом. Для $i = n, n-1, \ldots, 2, 1$ будем определять неубывающие функции g_i: $\omega \to \omega$ так, чтобы множества

$$F_i(\Sigma_1, n) = \{f \mid f \text{ является } (g_i(m), m)\text{-изоморфизмом для некоторого } m \in \omega\}$$

удовлетворяли условию *).

В качестве g_n берем тождественный нуль. Если $1 < i \leqslant n$, $m \in \omega$, то полагаем

$$g_{i-1}(m) = (g_i(m+1) \cdot |X(g_i(m+1), m+1)|) + 1.$$

Если g_i неубывающая, то очевидно, что g_{i-1} также неубывающая. Из $\mathfrak{A} \equiv \mathfrak{B}$ следует, что $f = \varnothing$ является $(n, 0)$-изоморфизмом для любого $n \in \omega$. Следовательно, классы $F_1(\Sigma_1, n), \ldots, F_n(\Sigma_1, n)$ непустые. Пусть $f \in F_{i-1}(\Sigma_1, n)$ является $(g_{i-1}(m), m)$-изоморфизмом, $1 < i \leqslant n$, $\mathrm{dom}\, f = \{a_1, \ldots, a_k\}$, $k \leqslant m$ и $a \in A$. Обозначим через $\Phi(v_1, \ldots, v_{k+1})$ конъюнкцию всех $\Psi(v_1, \ldots, v_{k+1}) \in X(g_i(k+1), k+1)$, для которых $\mathfrak{A} \vDash \Psi(a_1, \ldots, a_k, a)$. Число кванторов у Φ не превосходит $g_i(k+1) \cdot |X(g_i(k+1), k+1)|$, поэтому существует формула $\mathrm{X}(v_1, \ldots, v_k) \in X(g_{i-1}(k), k)$, эквивалентная формуле $\exists v_{k+1} \Phi(v_1, \ldots, v_{k+1})$. Так как $g_{i-1}(k) \leqslant g_{i-1}(m)$, $\mathfrak{A} \vDash \mathrm{X}(a_1, \ldots, a_k)$ и f — $(g_{i-1}(m), m)$-изоморфизм, то $\mathfrak{B} \vDash \mathrm{X}(fa_1, \ldots, fa_k)$. Тогда $\mathfrak{B} \vDash \Phi(fa_1, \ldots, fa_k, b)$ для некоторого $b \in B$. Из построения Φ вытекает, что для любой $\Psi \in X(g_i(k+1), k+1)$ либо $\Phi \to \Psi$, либо $\Phi \to \neg \Psi$ является тождественно истинной формулой, следовательно, $g = f \cup \langle a, b \rangle$ будет $(g_i(k+1), k+1)$-изоморфизмом, т. е. принадлежит $F_i(\Sigma_1, n)$. Заменив в предыдущем рассуждении $\mathfrak{A}$ на $\mathfrak{B}$ и f на f^{-1}, получим, что для любого $b' \in B$ существует $a' \in A_k$ такое, что $f \cup \{\langle a', b' \rangle\}$ принадлежит $F_i(\Sigma_1, n)$. □

Следствие 1. *Если $\mathfrak{A}$ и $\mathfrak{B}$ — алгебраические системы конечной сигнатуры Σ, то для того чтобы $\mathfrak{A}$ и $\mathfrak{B}$ были элементарно эквивалентны, необходимо и достаточно, чтобы для любого $n \in \omega$ существовали непустые множества*

$F_1(n) \subseteq P(\mathfrak{A}, \mathfrak{B})$, ..., $F_n(n) \subseteq P(\mathfrak{A}, \mathfrak{B})$ *со следующим свойством:*

*) *если* $f \in F_i(n)$, $1 \leqslant i < n$, $a \in A$ *и* $b \in B$, *то существуют* $g_1, g_2 \in F_{i+1}(n)$, *для которых* $f \subseteq g_1$, $f \subseteq g_2$, $a \in \operatorname{dom} g_1$ *и* $b \in \operatorname{rang} g_2$.

Доказательство. В качестве множеств $F_1(n)$, ..., $F_n(n)$ берем множества $F_1(\Sigma, n)$, ..., $F_n(\Sigma, n)$ из теоремы 1. □

Следствие 2. *Если* $\mathfrak{A}$, $\mathfrak{B}$ — *алгебраические системы сигнатуры* Σ *и* $\mathfrak{A}$ *конечна, то* $\mathfrak{A} \equiv \mathfrak{B}$ *тогда и только тогда, когда* $\mathfrak{A} \simeq \mathfrak{B}$.

Доказательство. В предложении 16.7 доказано, что для любых $\mathfrak{A}$ и $\mathfrak{B}$ из $\mathfrak{A} \simeq \mathfrak{B}$ следует $\mathfrak{A} \equiv \mathfrak{B}$. Пусть $\mathfrak{A} \equiv \mathfrak{B}$ и $|A| = m_0 \in \omega$. Так как в $\mathfrak{B}$ истинна формула Φ_{m_0} из предложения 16.9, то $|B| = m_0$. Для каждого $n \in \omega$ имеется лишь конечное число попарно различных n-местных предикатов и функций на конечном множестве, поэтому имеется такая конечная или счетная $\Sigma' \subseteq \Sigma$, что если $s \in R \cup F$, то $\nu^{\mathfrak{A}}(s) = \nu^{\mathfrak{A}}(s')$ для некоторого $s' \in R' \cup F'$. Поэтому достаточно показать, что $\mathfrak{A} \restriction \Sigma' \simeq \mathfrak{B} \restriction \Sigma'$. Пусть $\Sigma' = \bigcup\limits_{i \in \omega} \Sigma_i$, где Σ_i конечна и $\Sigma_i \subseteq \Sigma_{i+1}$. Рассмотрим множества частичных изоморфизмов $F_j(\Sigma_i, n)$, где $n, i \in \omega$ и $1 \leqslant j \leqslant n$, из теоремы 1. Из условия *) теоремы 1 следует, что для любых $n, i \in \omega$, любого $k < n$ и любых $a_1, \ldots, a_k \in A$ существует отображение $f \in F_{k+1}(\Sigma_i, n)$, для которого $a_1, \ldots, a_k \in \operatorname{dom} f$. Следовательно, для любого $n > m_0$ существует $f_n \in F_{m_0+1}(\Sigma_n, n)$, являющийся изоморфизмом $\mathfrak{A} \restriction \Sigma_n$ на $\mathfrak{B}_1 \restriction \Sigma_n$, где $\mathfrak{B}_1 \subseteq \mathfrak{B}$. Так как $|B_1| = |A| = |B|$, то $\mathfrak{B}_1 = \mathfrak{B}$. Существует лишь конечное число отображений $f\colon A \to B$, поэтому существует такое число $n_0 \in \omega$, что $f_{n_0}\colon \mathfrak{A} \restriction \Sigma_n \xrightarrow{\sim} \mathfrak{B} \restriction \Sigma_n$ для всех $n \in \omega$, следовательно, $f_{n_0}\colon \mathfrak{A} \xrightarrow{\sim} \mathfrak{B}$. □

Понятие элементарной эквивалентности с некоторой точки зрения может быть даже более важным, чем понятие изоморфизма. Дело в том, что изоморфизм определяется через существование некоторой бесконечной функции, в то время как элементарная эквивалентность определяется через конечные функции. Рассмотрим алгебраические системы $\mathfrak{A}_0$ и $\mathfrak{B}_0$ пустой сигнатуры, у которых A_0 состоит из всех счетных ординалов, а B_0 состоит из всех подмножеств натуральных чисел. Из результатов П. Коэна о независимости в ZFC следует, что $\mathfrak{A}_0 \simeq \mathfrak{B}_0$ нельзя ни доказать, ни опровергнуть в ZFC. В силу же «финитарности» понятия элементарной эквивалентности для «хорошо заданных» систем $\mathfrak{A}$ и $\mathfrak{B}$ отношение $\mathfrak{A} \equiv \mathfrak{B}$ можно доказать или опровергнуть в ZFC. В частности, легко показать, что $\mathfrak{A}_0 \equiv \mathfrak{B}_0$. Конечно, не надо забывать, что понятие изоморфизма играет исключительную роль, например, в алгебре, так как является «пределом» для различных классификаций алгебраических систем.

Если элементарная эквивалентность является ослаблением понятия изоморфизма, то следующее понятие является усилением понятия подсистемы.

Определение. Подсистема $\mathfrak{B} \subseteq \mathfrak{A}$ системы $\mathfrak{A}$ сигнатуры Σ называется *элементарной подсистемой* (обозначаем $\mathfrak{B} \prec \mathfrak{A}$), если для любой формулы $\Phi(x_1, \ldots, x_n)$ сигнатуры Σ и любых $b_1, \ldots, b_n \in B$ имеет место

$$\mathfrak{B} \models \Phi(b_1, \ldots, b_n) \Leftrightarrow \mathfrak{A} \models \Phi(b_1, \ldots, b_n). \qquad (1)$$

Предложение 1. *Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры Σ и $\mathfrak{B} \subseteq \mathfrak{A}$. Для того, чтобы имело место $\mathfrak{B} \prec \mathfrak{A}$, необходимо и достаточно, чтобы для любой формулы $\Phi(x_0, \ldots, x_n)$ сигнатуры Σ и любых $b_1, \ldots, b_n \in B$*

$$\mathfrak{A} \models \exists x_0 \Phi(x_0, b_1, \ldots, b_n) \Rightarrow (\mathfrak{A} \models \Phi(b_0, b_1, \ldots, b_n) \text{ для некоторого } b_0 \in B).$$

Доказательство. Индукцией по длине формулы $\Phi(x_1, \ldots, x_n)$ сигнатуры Σ покажем, что для любых $b_1, \ldots, b_n \in B$ истинно (1). Если Φ атомарная, то (1) следует из определения подсистемы. Если $\Phi = \neg\Psi$ или $\Phi = \Psi_1 \tau \Psi_2$ для $\tau \in \{\wedge, \vee, \rightarrow\}$, то (1) следует из индукционного предположения. Так как $\forall x \Psi \equiv \neg \exists x \neg \Psi$, то достаточно рассмотреть лишь случай $\Phi(x_1, \ldots, x_n) = \exists x_0 \Psi(x_0, \ldots, x_n)$, но в этом случае (1) следует из условия предложения и индукционного предположения. □

Предложение 2. *Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры Σ и $\mathfrak{B} \subseteq \mathfrak{A}$. Если для любой конечной сигнатуры $\Sigma_1 \subseteq \Sigma$, любых $b_1, \ldots, b_n \in B$ и любого $a \in A$ существует автоморфизм f системы $\mathfrak{A} \upharpoonright \Sigma_1$, для которого $fb_1 = b_1, \ldots, fb_n = b_n$ и $fa \in B$, то $\mathfrak{B} \prec \mathfrak{A}$.*

Доказательство. Воспользуемся предложением 1. Пусть $\mathfrak{A} \models \exists x_0 \Phi(x_0, b_1, \ldots, b_n)$. Тогда $\mathfrak{A} \models \Phi(a, b_1, \ldots, b_n)$ для некоторого $a \in A$. Пусть f — автоморфизм системы $\mathfrak{A} \upharpoonright \Sigma(\Phi)$, оставляющий $b_1, \ldots, b_n$ на месте, и $fa \in B$. Из предложения 16.7 получаем $\mathfrak{A} \models \Phi(fa, b_1, \ldots, b_n)$. □

Ясно, что из $\mathfrak{B} \prec \mathfrak{A}$ следует $\mathfrak{B} \equiv \mathfrak{A}$. Обратное в общем случае неверно. Например, рассмотрим системы $\langle Q^{(1)}; \leqslant\rangle$ и $\langle Q^{(2)}; \leqslant\rangle$, где $Q^{(1)}$, $Q^{(2)}$ — множества рациональных чисел, не меньших 1 и не меньших 2 соответственно, а $\leqslant$ — обычное отношение «меньше или равно» на числах. По предложению 15.4 системы $\langle Q^{(1)}; \leqslant\rangle$ и $\langle Q^{(2)}; \leqslant\rangle$ изоморфны, следовательно, элементарно эквивалентны. Однако в подсистеме $\langle Q^{(2)}; \leqslant\rangle$ системы $\langle Q^{(1)}; \leqslant\rangle$ формула $\Phi(v_1) = \forall v_0 (v_0 \leqslant v_1 \to v_0 \approx v_1)$ истинна на элементе 2, а в системе $\langle Q^{(1)}; \leqslant\rangle$ эта формула ложна на том же элементе 2. Таким образом, $\langle Q^{(2)}; \leqslant\rangle \prec \langle Q^{(1)}; \leqslant\rangle$ не имеет места.

Пример 1. Пусть $\mathfrak{A}$ — счетный плотный линейный порядок, а $\mathfrak{B}$ — плотный в $\mathfrak{A}$ порядок (т. е. $\mathfrak{B} \subseteq \mathfrak{A}$ и для любых $a < b$ из A существует $c \in B$, для которого $a < c < b$), тогда ($\mathfrak{B}$ содержит концевые элементы $\mathfrak{A}$) $\Leftrightarrow \mathfrak{B} \prec \mathfrak{A}$.

Для доказательства $\Leftarrow$ замечаем, что так как $\mathfrak{A} \equiv \mathfrak{B}$, то $\mathfrak{A}$ и $\mathfrak{B}$ имеют одинаковые концы. Теперь пусть, например, b_0 — первый элемент $\mathfrak{B}$. Тогда $\mathfrak{B} \models \forall v_0 (v_0 \leqslant b_0 \to v_0 \approx b_0)$. В силу $\mathfrak{B} \prec \mathfrak{A}$ имеем $\mathfrak{A} \models \forall v_0 (v_0 \leqslant b_0 \to v_0 \approx b_0)$ и, значит, b_0 — первый элемент $\mathfrak{A}$. Для доказательства $\Rightarrow$ нужно воспользоваться предложением 2. Требуемый изоморфизм f строится так же, как в предложении 15.4.

Пример 2. Пусть $\mathfrak{A}$ — свободная группа со свободными образующими $\{a_i | i \in I\}$ и $I' \subseteq I$ — бесконечное множество. Тогда группа $\mathfrak{B} \subseteq \mathfrak{A}$, порожденная в $\mathfrak{A}$ множеством $\{a_i | i \in I'\}$, является элементарной подгруппой $\mathfrak{A}$. Для доказательства воспользуемся предложением 2. Пусть $b_1, \ldots, b_n \in B$ и $a \in A$. Тогда существуют конечные множества $X \subseteq \{a_i | i \in I'\}$ и $Y \subseteq \{a_i | i \in I\} \setminus X$, для которых $b_1, \ldots, b_n \in A(X)$ и $a \in A(X \cup Y)$. Рассмотрим разнозначное отображение f множества $\{a_i | i \in I\}$ на себя, оставляющее элементы X на месте и отображающее Y в $\{a_i | i \in I'\}$. Тогда f однозначно продолжается до автоморфизма группы $\mathfrak{A}$, который удовлетворяет условию из предложения 2.

Хотя во многих случаях признак из предложения 2 легко применяется, он не является необходимым (см. упражнение 2). Отметим, что вопрос о возможности заменить в примере 2 условие бесконечности I' на $|I'| > 1$ является нерешенной проблемой.

Аналог предложения 15.2 для отношения $\prec$ не имеет места (см. упражнение 2), в то время как для предложения 15.3 соответствующее утверждение справедливо. Множество $\{\mathfrak{A}_i | i \in I\}$ алгебраических систем назовем *элементарно направленным*, если для любых $i, j \in I$ существует такое $k \in I$, что $\mathfrak{A}_i \prec \mathfrak{A}_k$ и $\mathfrak{A}_j \prec \mathfrak{A}_k$.

Предложение 3. *Если $\{\mathfrak{A}_i | i \in I\}$ — элементарно направленное множество алгебраических систем сигнатуры Σ, то $\mathfrak{A}_j \prec \mathfrak{A} = \bigcup\limits_{i \in I} \mathfrak{A}_i$, $j \in I$.*

Доказательство. Эквивалентность (1) для $\mathfrak{B} = \mathfrak{A}_j$ докажем индукцией по длине Φ. Как и в доказательстве предложения 1, достаточно рассмотреть случай $\Phi = \exists x \Psi$. Пусть $\mathfrak{A} \models \exists x \Psi(x, a_1, \ldots, a_n)$, где $a_1, \ldots, a_n \in A_j$. Тогда $\mathfrak{A} \models \Psi(a, a_1, \ldots, a_n)$ для некоторого $a \in A_i$. Возьмем $k \in I$, для которого $\mathfrak{A}_i \prec \mathfrak{A}_k$ и $\mathfrak{A}_j \prec \mathfrak{A}_k$. По индукционному предположению $\mathfrak{A}_k \models \Psi(a, a_1, \ldots, a_n)$, следовательно, $\mathfrak{A}_k \models \exists x \Psi(x, a_1, \ldots, a_n)$. Так как $\mathfrak{A}_j \prec \mathfrak{A}_k$, то $\mathfrak{A}_j \models \exists x \Psi(x, a_1, \ldots, a_n)$. Обратно, пусть имеет место $\mathfrak{A}_j \models \exists x \Psi(x, a_1, \ldots, a_n)$. Тогда $\mathfrak{A}_j \models \Psi(a, a_1, \ldots, a_n)$ для некоторого $a \in A_j$ и по индукционному предположению $\mathfrak{A} \models \Psi(a, a_1, \ldots, a_n)$, следовательно, имеет место $\mathfrak{A} \models \exists x \Psi(x, a_1, \ldots, a_n)$. $\square$

Хотя аналог предложения 15.2 для $\prec$ не имеет места, более слабый вариант соответствующего утверждения является очень важным.

Теорема 2. *Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры Σ и $X \subseteq A$. Тогда существует такая элементарная подсистема $\mathfrak{B} \prec \mathfrak{A}$, что $X \subseteq B$ и $|B| \leqslant \max(|X|, |\Sigma|, \omega)$.*

Доказательство. Полагаем $X_0 = X$. Пусть X_n уже определено. Для любой формулы $\Psi = \exists x \Phi(x, x_1, \ldots, x_k)$ сигнатуры Σ и любой интерпретации $\gamma\colon \{x_1, \ldots, x_k\} \to A$ выбираем такой элемент $a(\Psi, \gamma) \in A$, что если $\mathfrak{A} \models \exists x \Phi(x, \gamma x_1, \ldots, \gamma x_k)$, то $\mathfrak{A} \models \Phi(a(\Psi, \gamma), \gamma x_1, \ldots, \gamma x_k)$. Полагаем $X_{n+1} = X_n \cup \{a(\Psi, \gamma) \mid \Psi = \exists x \Phi \in F(\Sigma), \gamma\colon FV(\Psi) \to X_n\}$. Ясно, что подсистема $\mathfrak{B} \subseteq \mathfrak{A}$ с носителем $\bigcup\limits_{n \in \omega} X_n$ удовлетворяет условию предложения 1, следовательно, $\mathfrak{B} \prec \mathfrak{A}$. Если $\lambda = \max(|X|, |\Sigma|, \omega)$, то $|F(\Sigma)| \leqslant \lambda$ и $|X_0| \leqslant \lambda$. Если $|X_n| \leqslant \lambda$, то мощность множества Y_n интерпретаций γ переменных в X_n с конечной областью определения не превосходит $\left|\bigcup\limits_{m \in \omega} X_n^m\right|$. Так как $|X_n^m| \leqslant \max(|X_n|, \omega)$, то $|Y_n| \leqslant \lambda \cdot \omega = \lambda$, поэтому $|X_{n+1}| \leqslant |F(\Sigma)| \cdot |Y_n| \leqslant \lambda^2 = \lambda$. Следовательно, $|B| \leqslant \lambda \cdot \omega = \lambda$. $\square$

Определение. Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры Σ и $X \subseteq A$. Возьмем множество $C_X =$

$=\{c_a | a \in X\}$, не пересекающееся с $R \cup F$ и $c_a \neq c_b$ для $a \neq b$. Определим сигнатуру Σ_X как полученную из Σ добавлением элементов множества C_X в качестве новых констант. Обозначим через $\mathfrak{A}_X$ обогащение системы $\mathfrak{A}$ до сигнатуры Σ_X, в котором константа c_a, $a \in X$, интерпретируется элементом a. Множество $D(\mathfrak{A}, X)$ атомарных предложений сигнатуры Σ_X или их отрицаний, истинных в системе $\mathfrak{A}_X$, называется *диаграммой множества* X *в* $\mathfrak{A}$. Если в определении $D(\mathfrak{A}, X)$ заменить «атомарные предложения или их отрицания» на «предложения», то получим определение *полной диаграммы* $D^*(\mathfrak{A}, X)$ *множества* X *в* $\mathfrak{A}$. Диаграмма (полная диаграмма) A в $\mathfrak{A}$ называется *диаграммой* (*полной диаграммой*) $\mathfrak{A}$ и обозначается через $D(\mathfrak{A})$ (соответственно $D^*(\mathfrak{A})$).

Предложение 4. а) *Если* $\mathfrak{A}$ — *алгебраическая система сигнатуры* Σ *и* $\mathfrak{B}$ — *модель диаграммы* $D(\mathfrak{A})$ (*полной диаграммы* $D^*(\mathfrak{A})$) *сигнатуры* Σ_A, *то* $\mathfrak{A} \simeq \mathfrak{B}_1 \restriction \Sigma$ *для некоторой* $\mathfrak{B}_1 \subseteq \mathfrak{B}$ (*некоторой* $\mathfrak{B}_1 \prec \mathfrak{B}$).

б) *Если* $\mathfrak{A} \subseteq \mathfrak{B}$ — *алгебраические системы сигнатуры* Σ, *то*

$$\mathfrak{A} \prec \mathfrak{B} \Leftrightarrow \mathfrak{A}_A \equiv \mathfrak{B}_A.$$

Доказательство. а) Очевидно, что отображение, сопоставляющее элементу $a \in A$ элемент $\nu^{\mathfrak{B}}(c_a)$, будет требуемым изоморфизмом. б) Непосредственно из определений. □

Теорема 2 позволяет «спускаться» по мощностям, сохраняя элементарные свойства. Следующая теорема позволяет «подниматься».

Теорема 3. *Пусть* $\mathfrak{A}$ — *бесконечная система сигнатуры* Σ, λ — *кардинал, не меньший* $\max\{|A|, |\Sigma|\}$. *Тогда существует такая система* $\mathfrak{B}$, *что* $\mathfrak{A} \prec \mathfrak{B}$ *и* $|B| = \lambda$.

Доказательство. Возьмем множество C символов констант мощности λ, не пересекающееся с множеством $R \cup F$. Рассмотрим множество

$$Y = D^*(\mathfrak{A}) \cup \{\neg c_1 \approx c_2 | c_1, c_2 \in C, c_1 \neq c_2\}.$$

Так как $\mathfrak{A}$ бесконечна, то для любого конечного подмножества $X \subseteq Y$ систему $\mathfrak{A}$ можно обогатить до модели X. По теореме компактности существует модель $\mathfrak{B}_1$ множества Y сигнатуры $\Sigma_{A \cup C}$. Очевидно, что $|B_1| \geqslant \lambda$. По теореме 2 существует $\mathfrak{B}_2 \prec \mathfrak{B}_1$, $|B_2| = \lambda$. По предложению 4 а) существует $\mathfrak{B}_3 \prec \mathfrak{B}_2$ и изоморфизм $f_1: \mathfrak{A} \rightleftarrows \mathfrak{B}_3 \restriction \Sigma$. Теперь нужно лишь переименовать в системе $\mathfrak{B}_2 \restriction \Sigma$ элементы $b \in B_3$ на $f_1^{-1}b$, чтобы получить требуемую $\mathfrak{B}$. Чтобы избежать коллизии при таком переобозначении, поступаем следующим образом. Возьмем множество Z, для которого $Z \cap A = \varnothing$ и $|Z| = |B_2 \setminus B_3|$. Пусть f — разнозначное отображение множества $B = A \cup Z$ на множество B_2 и $f_1 \subseteq f$. Определим систему $\mathfrak{B} = \langle B, \nu^{\mathfrak{B}} \rangle$ сигнатуры Σ следующим образом:

а) если $s \in R \cup F$ — не константа, то

$$\langle b_1, \ldots, b_n \rangle \in \nu^{\mathfrak{B}}(s) \Leftrightarrow \langle fb_1, \ldots, fb_n \rangle \in \nu^{\mathfrak{B}_2}(s);$$

б) если $s \in F$ — константа, то

$$\nu^{\mathfrak{B}}(s) = f^{-1}\left(\nu^{\mathfrak{B}_2}(s)\right).$$

Ясно, что f — изоморфизм $\mathfrak{B}$ на $\mathfrak{B}_2 \upharpoonright \Sigma$ и $\mathfrak{A} \subseteq \mathfrak{B}$. Пусть $\Phi(x_0, x_1, \ldots, x_n) \in F(\Sigma)$; $b_1, \ldots, b_n \in A$ и

$$\mathfrak{B} \models \exists x_0 \Phi(x_0, b_1, \ldots, b_n).$$

Тогда $\mathfrak{B}_2 \models \exists x_0 \Phi(x_0, fb_1, \ldots, fb_n)$. Так как $fb_1, \ldots, fb_n \in B_3$ и $\mathfrak{B}_3 \prec \mathfrak{B}_2$, то существует такой $b_0 \in B_3$, что $\mathfrak{B}_2 \models \Phi(b_0, fb_1, \ldots, fb_n)$. Отображение f^{-1} является изоморфизмом $\mathfrak{B}_2 \upharpoonright \Sigma$ на $\mathfrak{B}$, поэтому $\mathfrak{B} \models \Phi(f^{-1}b_0, b_1, \ldots, b_n)$. Так как $f^{-1}b_0 \in A$, то по предложению 1 имеем $\mathfrak{A} \prec \mathfrak{B}$. Из $|B_2| = \lambda$ и $\mathfrak{B}_2 \simeq \mathfrak{B}$ следует $|B| = \lambda$. □

Упражнения

1. Покажите, что для систем $\mathfrak{A} \subseteq \mathfrak{B}$ сигнатуры Σ имеет место $\mathfrak{A} \prec \mathfrak{B}$, если выполняется одно из следующих условий:

а) Сигнатура Σ содержит лишь бесконечное множество констант. Значения констант в $\mathfrak{B}$ образуют бесконечное множество.

б) Сигнатура Σ содержит лишь символы одноместных предикатов r_k, $k \in \omega$. Рассмотрим множество $2^\omega = \{\nu | \nu\colon \omega \to \{0, 1\}\}$. Пусть $\mathfrak{B}$ — произвольная система сигнатуры Σ. Для любого $\nu \in 2^\omega$ определяем множество $\mathfrak{B}(\nu) = \{b |$ для всех $n \in \omega$ $\mathfrak{B} \models r_n(b)$, если $\nu(n) = 1$, и $\mathfrak{B} \models \neg r_n(b)$, если $\nu(n) = 0\}$. Ясно, что для различных $\nu_1, \nu_2 \in 2^\omega$ множества $\mathfrak{B}(\nu_1)$ и $\mathfrak{B}(\nu_2)$ не пересекаются. Пусть для всех $\nu \in 2^\omega$ $\mathfrak{B}(\nu) \subseteq A$, если $\mathfrak{B}(\nu)$ — конечное множество, и $A \cap \mathfrak{B}(\nu)$ — бесконечное множество, если $\mathfrak{B}(\nu)$ бесконечно.

в) Сигнатура Σ содержит единственный символ $\sim$ двухместного отношения, который интерпретируется в $\mathfrak{B}$ как эквивалентность с бесконечным числом бесконечных классов эквивалентности. Множество A содержит бесконечное число классов эквивалентности системы $\mathfrak{B}$. (Указание. Воспользоваться предложением 4 б) и теоремой 1.)

2. С помощью примера из упражнения 1 в) показать, что

а) признак элементарности подсистем из предложения 2 не является необходимым (указание: Пусть $|A| = \omega$ и все классы эквивалентности, содержащиеся в $B \setminus A$, несчетны);

б) для некоторой системы $\mathfrak{B}$ и бесконечного множества $X \subseteq B$ не существует минимальной по отношению включения $\subseteq$ элементарной подсистемы $\mathfrak{A} \prec \mathfrak{B}$, содержащей X.

§ 25. Аксиоматизируемые классы

Определение. Класс K алгебраических систем называется *аксиоматизируемым*, если существует сигнатура Σ и такое множество предложений Z сигнатуры Σ, что для любой системы $\mathfrak{A}$

$$\mathfrak{A} \in K \Leftrightarrow$$
$$\Leftrightarrow (\text{сигнатура } \mathfrak{A} \text{ равна } \Sigma \text{ и } \mathfrak{A} \models \Phi \text{ для всех } \Phi \in Z). \qquad (1)$$

Если для класса K выполняется (1), то Σ называется *сигнатурой* K, а множество Z называется *множеством аксиом для* K (обозначаем $K = K_\Sigma(Z)$). Если все системы класса K имеют сигнатуру Σ, то множество предложений сигнатуры Σ, истинных на всех системах из K, называется *элементарной теорией* K или просто *теорией* K и обозначается через $\mathrm{Th}(K)$.

Отметим очевидное свойство теорий: если $K_1 \subseteq K_2$ — классы алгебраических систем сигнатуры Σ, то $\mathrm{Th}(K_2) \subseteq \subseteq \mathrm{Th}(K_1)$.

Предложение 1. *Пусть K — класс алгебраических систем сигнатуры Σ.*

а) *Класс K аксиоматизируем тогда и только тогда, когда $K = K_\Sigma(\mathrm{Th}(K))$.*

б) *Существует минимальный по отношению к включению $\subseteq$ аксиоматизируемый класс K_1 сигнатуры Σ, содержащий K.*

Доказательство. а) Пусть $K = K_\Sigma(Z)$. Так как $Z \subseteq \mathrm{Th}(K)$, то $K_\Sigma(\mathrm{Th}(K)) \subseteq K$. Обратное включение $K \subseteq K_\Sigma(\mathrm{Th}(K))$ очевидно.

б) В качестве K_1 нужно взять $K_\Sigma(\mathrm{Th}(K))$. В самом деле, если K_2 — аксиоматизируемый класс сигнатуры Σ и $K \subseteq K_2$, то $\mathrm{Th}(K_2) \subseteq \mathrm{Th}(K)$. Следовательно, $K_\Sigma(\mathrm{Th}(K)) \subseteq \subseteq K_\Sigma(\mathrm{Th}(K_2)) = K_2$. □

Будем говорить, что класс K алгебраических систем замкнут относительно элементарной эквивалентности (изоморфизмов, подсистем, ультрапроизведений и др.), если вместе с алгебраическими системами $\mathfrak{A}_i$, $i \in I$, он содержит все элементарно эквивалентные им системы (все изоморфные им системы, все их подсистемы, ультрапроизведение $D\text{-prod}\,\mathfrak{A}_i$ и др.). Приведем одну полезную характеризацию аксиоматизируемых классов.

Теорема 4. *Класс K алгебраических систем сигнатуры Σ аксиоматизируем тогда и только тогда, когда он замкнут относительно элементарной эквивалентности и ультрапроизведений.*

Доказательство. Пусть K — аксиоматизируемый класс. Очевидно, что K замкнут относительно элементарной эквивалентности. Замкнутость K относительно ультрапроизведений следует из теоремы 17.1. Пусть K замкнут относительно элементарной эквивалентности и ультрапроизведений. Достаточно показать, что $K_\Sigma(\mathrm{Th}(K)) \subseteq K$. Пусть $\mathfrak{A} \in K_\Sigma(\mathrm{Th}(K))$. Для каждого $\Phi \in \mathrm{Th}(\mathfrak{A})$ рассмотрим множества $u_\Phi = \{\Psi \in \mathrm{Th}(\mathfrak{A}) \mid \rhd \Psi \to \Phi\}$. Ясно, что семейство $X = \{u_\Phi \mid \Phi \in \mathrm{Th}(\mathfrak{A})\}$ будет центрированным. По предложению 12.1 существует такой ультрафильтр D на множестве $\mathrm{Th}(\mathfrak{A})$, что $X \subseteq D$. Для любого $\Phi \in \mathrm{Th}(\mathfrak{A})$ существует система $\mathfrak{B}_\Phi \in K$, на которой истинно Φ, так как в противном случае $\neg\Phi \in \mathrm{Th}(K)$, что противоречит $\mathfrak{A} \in K_\Sigma(\mathrm{Th}(K))$. Покажем, что $\mathfrak{A} \equiv D\text{-prod}\,\mathfrak{B}_\Phi$, и этим теорема будет доказана. Если $\mathfrak{A} \vDash \Phi_0$, то $\mathfrak{B}_\Psi \vDash \Phi_0$ для всех $\Psi \in u_{\Phi_0}$. Так как $u_{\Phi_0} \in D$, то по теореме 17.1 получаем $D\text{-prod}\,\mathfrak{B}_\Phi \vDash \Phi_0$. Если $\mathfrak{A} \vDash \Phi_0$ не имеет места, то $\mathfrak{A} \vDash \neg\Phi_0$ и по только что доказанному $D\text{-prod}\,\mathfrak{B}_\Phi \vDash \neg\Phi_0$. Следовательно, $D\text{-prod}\,\mathfrak{B}_\Phi \vDash \Phi_0$ не имеет места. □

Предложение 2. *Пересечение любого множества аксиоматизируемых классов сигнатуры Σ и объединение конечного числа аксиоматизируемых классов сигнатуры Σ являются аксиоматизируемыми классами.*

Доказательство. Если $K_i = K_\Sigma(Z_i)$, $i \in I$, то очевидно, что $\bigcap\limits_{i \in I} K_i = K_\Sigma\left(\bigcup\limits_{i \in I} Z_i\right)$. Пусть $K_1 = K_\Sigma(Z_1)$ и $K_2 = K_\Sigma(Z_2)$. Рассмотрим множество $Z = \{\Phi \vee \Psi \mid \Phi \in Z_1, \Psi \in Z_2\}$. Покажем, что $K_1 \cup K_2 = K_\Sigma(Z)$. Включение $K_1 \cup K_2 \subseteq K_\Sigma(Z)$ очевидно. Пусть $\mathfrak{A} \notin K_1 \cup K_2$ и сигнатура $\mathfrak{A}$ равна Σ. Тогда существуют такие $\Phi_0 \in Z_1$ и $\Psi_0 \in Z_2$, что $\mathfrak{A} \vDash \neg\Phi_0 \wedge \neg\Psi_0$. Так как $\Phi_0 \vee \Psi_0 \in Z$, то $\mathfrak{A} \notin K_\Sigma(Z)$. □

Определение. Если K — класс алгебраических систем и $K = K_\Sigma(Z)$ для некоторого конечного множества аксиом Z, то класс K называется *конечно аксиоматизируемым*.

Заметим, что если K конечно аксиоматизируем, то, взяв конъюнкцию конечного множества Z аксиом для K, получим множество аксиом $\{\Phi\}$ для K, состоящее из одного предложения Φ.

Если K — класс алгебраических систем сигнатуры Σ, то через $\overline{K}$ обозначим дополнение K в классе $K_\Sigma(\varnothing)$ всех систем сигнатуры Σ.

Предложение 3. *Пусть K — класс алгебраических систем сигнатуры Σ. Класс K является конечно аксиоматизируемым тогда и только тогда, когда K и $\overline{K}$ являются аксиоматизируемыми.*

Доказательство. Если K конечно аксиоматизируем, то $K = K_\Sigma(\{\Phi\})$ для некоторого предложения Φ сигнатуры Σ. Тогда $\overline{K} = K_\Sigma(\{\neg\Phi\})$. Пусть K и $\overline{K}$ аксиоматизируемы. Так как $\overline{K} \cap K = \varnothing$, $K = K_\Sigma(\mathrm{Th}(K))$ и $\overline{K} = K_\Sigma(\mathrm{Th}(\overline{K}))$, то по теореме компактности существуют такие конечные множества $X \subseteq \mathrm{Th}(K)$ и $Y \subseteq \mathrm{Th}(\overline{K})$, что $X \cup Y$ не имеет модели. Так как $\mathrm{Th}(K)$ и $\mathrm{Th}(\overline{K})$ замкнуты относительно взятия конъюнкций, то можно считать, что $X = \{\Phi\}$ и $Y = \{\Psi\}$. Так как $\Phi \wedge \Psi$ — тождественно ложная формула и $\Phi \in \mathrm{Th}_\Sigma(K)$, то на всех системах из K истинно предложение $\Phi \wedge \neg\Psi$. Обратно, если на системе $\mathfrak{A}$ сигнатуры Σ истинно предложение $\Phi \wedge \neg\Psi$, то $\mathfrak{A} \notin \overline{K}$ и, следовательно, $\mathfrak{A} \in K$. Значит, $K = K_\Sigma(\{\Phi \wedge \neg\Psi\})$. □

Определение. Формула Φ называется $\forall$-*формулой* ($\exists$-*формулой*, $\forall\exists$-*формулой*), если $\Phi = \forall x_1 \ldots \forall x_k \Psi$ ($\Phi = \exists x_1 \ldots \exists x_k \Psi$, $\Phi = \forall x_1 \ldots \forall x_k \exists y_1 \ldots \exists y_n \Psi$), где Ψ — бескванторная формула. Класс K алгебраических систем называется $\forall$-*аксиоматизируемым* ($\exists$-*аксиоматизируемым*, $\forall\exists$-*аксиоматизируемым*), если $K = K_\Sigma(Z)$, где Z — множество $\forall$-предложений ($\exists$-предложений, $\forall\exists$-предложений) сигнатуры Σ.

Предложение 4. а) *Пусть $\Phi(x_1, \ldots, x_k)$ — $\forall$-формула ($\exists$-формула) сигнатуры Σ, $\mathfrak{A} \subseteq \mathfrak{B}$ — алгебраические системы сигнатуры Σ, $a_1, \ldots, a_k \in A$. Тогда из истинности $\Phi(a_1, \ldots, a_k)$ в $\mathfrak{B}$ (в $\mathfrak{A}$) следует истинность $\Phi(a_1, \ldots, a_k)$ в $\mathfrak{A}$ (в $\mathfrak{B}$).*

б) *Пусть $\{\mathfrak{A}_i \mid i \in I\}$ — направленное семейство алгебраических систем сигнатуры Σ и $\forall\exists$-предложение Φ сигнатуры Σ истинно во всех $\mathfrak{A}_i$, $i \in I$. Тогда Φ истинно в $\mathfrak{A} = \bigcup\limits_{i \in I} \mathfrak{A}_i$.*

Доказательство. а) Так как значение $t^{\mathfrak{A}}[\gamma]$ терма t при интерпретации γ в A совпадает со значением $t^{\mathfrak{B}}[\gamma]$, то а) выполняется для атомарных формул Φ. Для бескванторных формул утверждение а) получается индукцией по длине Φ. Теперь остается лишь воспользоваться определением истинности формул с кванторами $\forall$ и $\exists$.

б) Пусть $\Phi = \forall x_1 \ldots \forall x_k \exists y_1 \ldots \exists y_n \Psi(x_1, \ldots, x_k, y_1, \ldots, y_n)$, где Ψ — бескванторная формула, истинно на всех $\mathfrak{A}_i$, $i \in I$. Возьмем произвольные $a_1, \ldots, a_k \in A$. Тогда $a_1, \ldots, a_k \in A_i$ для некоторого $i \in I$ и, следовательно, $\mathfrak{A}_i \models \exists y_1 \ldots \exists y_n \Psi(a_1, \ldots, a_k, y_1, \ldots, y_n)$. Так как $\mathfrak{A}_i \subseteq \mathfrak{A}$, то в силу а) имеем $\mathfrak{A} \models \exists y_1 \ldots \exists y_n \Psi(a_1, \ldots, a_k, y_1, \ldots, y_n)$. $\square$

Лемма 1. *Пусть Γ — множество предложений сигнатуры Σ и $\Psi_0(x_1, \ldots, x_k)$ — формула сигнатуры Σ. Если для любых моделей $\mathfrak{A} \subseteq \mathfrak{B}$ множества Γ, имеющих сигнатуру Σ, и любых $a_1, \ldots, a_k \in A$ из истинности $\Psi_0(a_1, \ldots, a_k)$ в $\mathfrak{B}$ (в $\mathfrak{A}$) следует истинность $\Psi_0(a_1, \ldots, a_k)$ в $\mathfrak{A}$ (в $\mathfrak{B}$), то существует $\forall$-формула ($\exists$-формула) $X_0(x_1, \ldots, x_k)$ сигнатуры Σ, для которой $\Gamma \rhd (\Psi_0 \to X_0) \wedge (X_0 \to \Psi_0)$.*

Доказательство. Вместо $u_1, \ldots, u_k$ пишем $\bar{u}$. Пусть $\bar{d}$ — набор новых констант, $\Sigma' = \Sigma \cup \bar{d}$, $\Psi_1 = (\Psi_0)^{\bar{x}}_{\bar{d}}$ и $Z = \{\Phi \mid \Phi$ — $\forall$-предложение сигнатуры Σ' и $\Gamma \rhd \Psi_1 \to \Phi\}$.

Рассмотрим множество $\Gamma \cup Z \cup \{\neg\Psi_1\}$. Если оно несовместно, то существуют $\Phi_0, \ldots, \Phi_n \in Z$ такие, что $\Gamma \rhd \bigwedge\limits_{i \leqslant n} \Phi_i \to \Psi_1$. Тогда $\Gamma \rhd \bigwedge\limits_{i \leqslant n} \Phi_i \leftrightarrow \Psi_1$. Пусть D_0 — дерево доказательства секвенции $\Gamma_0 \vdash \left(\bigwedge\limits_{i \leqslant n} \Phi_i \to \Psi_1\right) \wedge \left(\Psi_1 \to \bigwedge\limits_{i \leqslant n} \Phi_i\right)$, где Γ_0 — подходящее конечное подмножество Γ. Так как эта секвенция не содержит свободных переменных, то можно считать, что $x_1, \ldots, x_k$ не встречаются в D_0. Сделаем подстановку $(D_0)^{d_1, \ldots, d_k}_{x_1, \ldots, x_k}$. Это снова дерево доказательства секвенции $\Gamma_0 \vdash \left(\bigwedge\limits_{i<n} (\Phi_i)^{\bar{d}}_{\bar{x}} \to \Psi_0\right) \wedge \left(\Psi_0 \to \bigwedge\limits_{i \leqslant n} (\Phi_i)^{\bar{d}}_{\bar{x}}\right)$. Остается заметить, что формула $\bigwedge\limits_{i<n} (\Phi_i)^{\bar{d}}_{\bar{x}}$ эквивалентна $\forall$-формуле.

Предположим, что $\Gamma \cup Z \cup \{\neg \Psi_1\}$ совместно и $\mathfrak{A}$ — модель этого множества предложений. Установим, что $\Gamma \cup D(\mathfrak{A}) \rhd \neg \Psi_1$. Действительно, если $\mathfrak{B}$ — любая модель $\Gamma \cup D(\mathfrak{A})$, то существует изоморфное вложение φ

модели $\mathfrak{A}$ в $\mathfrak{B} \restriction \Sigma'$. Если бы в $\mathfrak{B}$ было истинно Ψ_1, то по условию Ψ_1 было бы истинно и в подсистеме $\varphi(\mathfrak{A}) \subseteq \mathfrak{B}$, а следовательно, и в $\mathfrak{A}$, что невозможно. Итак, для всех моделей $\mathfrak{B}$ для $\Gamma \cup D(\mathfrak{A})$ имеем $\mathfrak{B} \rhd \neg \Psi_1$. По теореме о полноте имеем $\Gamma \cup D(\mathfrak{A}) \rhd \neg \Psi_1$. Существуют конечное подмножество $\Gamma_0 \subseteq \Gamma$ и предложения $X_0, \ldots, X_n \in D(\mathfrak{A})$ такие, что секвенция $\Gamma_0 \vdash \bigwedge\limits_{i \leqslant n} X_i \to \neg \Psi_1$ доказуема.

Заменяя константы вида c_a на переменные и навешивая на эти переменные кванторы существования, получим доказуемую секвенцию $\Gamma_0 \vdash \exists \bar{y}\Big(\bigwedge\limits_{i \leqslant n} (X_i)^{\bar{c}_a}_{\bar{y}}\Big) \to \neg \Psi_1$. Тогда доказуема секвенция $\Gamma_0 \vdash \Psi_1 \to \forall \bar{y} \neg \Big(\bigwedge\limits_{i \leqslant n} (X_i)^{\bar{c}_a}_{\bar{y}}\Big)$. Следовательно, $\forall \bar{y} \neg \Big(\bigwedge\limits_{i \leqslant n} (X_i)^{\bar{c}_a}_{\bar{y}}\Big) \in Z$, $\mathfrak{A} \models \forall \bar{y} \neg \Big(\bigwedge\limits_{i \leqslant n} (X_i)^{\bar{c}_a}_{\bar{y}}\Big)$, что противоречит тому, что $X_0, \ldots, X_n \in D(\mathfrak{A})$.

Второй вариант леммы получается из первого заменой формулы Ψ_0 на $\neg\Psi_0$. $\square$

Теорема 5. *Пусть K — аксиоматизируемый класс алгебраических систем сигнатуры Σ.*

а) *K $\exists$-аксиоматизируем $\Leftrightarrow$ K замкнут относительно надсистем.*

б) *K $\forall$-аксиоматизируем $\Leftrightarrow$ K замкнут относительно подсистем.*

Доказательство. Утверждения $\Rightarrow$ следуют из предложения 4.

а) Покажем сначала, что для любого предложения $\Phi \in \mathrm{Th}(K)$ существует такое предложение $\Psi_\Phi \in \mathrm{Th}(K)$, что $\rhd \Psi_\Phi \to \Phi$ и для любой пары $\mathfrak{A} \subseteq \mathfrak{B}$ алгебраических систем сигнатуры Σ из $\mathfrak{A} \models \Psi_\Phi$ следует $\mathfrak{B} \models \Phi$. Предположим, что это не так, т. е. существует такое $\Phi_0 \in \mathrm{Th}(K)$, что для любого $\Psi \in \mathrm{Th}(K)$ существуют системы $\mathfrak{A}_\Psi \subseteq \mathfrak{B}_\Psi$ сигнатуры Σ, для которых из $\rhd \Psi \to \Phi_0$ следуют $\mathfrak{A}_\Psi \models \Psi$ и $\mathfrak{B}_\Psi \models \neg\Phi_0$. Пусть D — ультрафильтр на множестве $\mathrm{Th}(K)$, содержащий центрированное семейство $X = \{u_\Phi \mid \Phi \in \mathrm{Th}(K)\}$, где $u_\Phi = \{\Psi \in \mathrm{Th}(K) \mid \rhd \Psi \to \Phi\}$. Рассмотрим системы $\mathfrak{A}_0 = D\text{-prod}\, \mathfrak{A}_\Psi$ и $\mathfrak{B}_0 = D\text{-prod}\, \mathfrak{B}_\Psi$. Так как $\mathfrak{A}_\Psi \subseteq \mathfrak{B}_\Psi$ для всех $\Psi \in \mathrm{Th}(K)$, то существует $\mathfrak{A}_1 \subseteq \mathfrak{B}_0$, $\mathfrak{A}_1 \simeq \mathfrak{A}_0$. Из теоремы 17.1, включения $X \subseteq D$ и из того, что $\mathfrak{A}_0 \simeq \mathfrak{A}_1$, получаем $\mathfrak{A}_1 \in K_\Sigma(\mathrm{Th}(K)) = K$ и $\mathfrak{B}_0 \models \neg\Phi_0$. Это противоречит замкнутости K относительно надсистем.

Для любого предложения $\Phi \in \mathrm{Th}(K)$ по лемме 1 (полагаем $\Gamma = \{\Psi_\Phi \vee \neg\Phi\}$ и $\Psi_0 = \Phi$) существует такое

$\exists$-предложение X_Φ, что $\rhd \Psi_\Phi \vee \neg\Phi \to ((\Phi \to X_\Phi) \wedge (X_\Phi \to \Phi))$. Отсюда получаем, что $X_\Phi \to \Phi$ — тождественно истинное предложение и в силу $\{\Phi, \Psi_\Phi\} \subseteq \mathrm{Th}(K)$ также $X_\Phi \in \mathrm{Th}(K)$. Следовательно, множество $\exists$-предложений $\{X_\Phi \mid \Phi \in \mathrm{Th}(K)\}$ будет системой аксиом для K.

б) Чтобы получить доказательство б), нужно в доказательстве а) заменить $\mathfrak{A} \subseteq \mathfrak{B}$ и $\mathfrak{A}_\Psi \subseteq \mathfrak{B}_\Psi$ на $\mathfrak{B} \subseteq \mathfrak{A}$ и $\mathfrak{B}_\Psi \subseteq \mathfrak{A}_\Psi$ соответственно и применить другую часть леммы 1. □

Определение. Предложение вида $\forall x_1 \ldots \forall x_k Q$, где Q — атомарная формула, называется *тождеством*. Предложение вида

$$\forall x_1 \ldots \forall x_k ((Q_1 \wedge \ldots \wedge Q_n) \to Q_0), \tag{1}$$

где $Q_0, Q_1, \ldots, Q_n$ — атомарные формулы, называется *квазитождеством*. Аксиоматизируемый класс K называется *многообразием* (*квазимногообразием*), если существует система аксиом Z для K, состоящая из *тождеств* (*квазитождеств*).

Так как тождество $\forall x_1 \ldots \forall x_k Q$ эквивалентно квазитождеству $\forall x_1 \ldots \forall x_{k+1} (x_{k+1} \approx x_{k+1} \to Q)$, то многообразие является квазимногообразием.

Систему $E_\Sigma = \langle \{\varnothing\}, \nu^{E_\Sigma} \rangle$ назовем *единичной системой сигнатуры* Σ, если

$$\nu^{E_\Sigma}(s) = \{\varnothing\}^{\mu(s)} \text{ для всех } s \in R. \tag{2}$$

Условие (2) определяет систему E_Σ однозначно, так как на одноэлементном множестве для любого $n \in \omega$ существует только одна n-местная функция.

Предложение 5. а) *Любое квазимногообразие K сигнатуры Σ замкнуто относительно фильтрованных произведений и содержит единичную систему E_Σ.*

б) *Любое многообразие замкнуто относительно гомоморфных образов.*

Доказательство. а) Так как в E_Σ истинно $Q_0(\varnothing, \ldots, \varnothing)$, для любой атомарной формулы $Q_0(x_1, \ldots, x_k)$ сигнатуры Σ, то в E_Σ истинно любое квазитождество (1). Для того чтобы показать замкнутость K относительно фильтрованных произведений, достаточно показать, что любое квазитождество (1) условно фильтруется по любому фильтру D на множестве I. В силу леммы 17.2 достаточно показать, что формула $((Q_1 \wedge \ldots \wedge Q_n) \to Q_0)(x_1, \ldots, x_k)$ условно фильтруется по D. Пусть $f_1, \ldots, f_k \in I\text{-prod}\, A_i$ и $X = \{i \mid \mathfrak{A}_i \vDash ((Q_1 \wedge \ldots \wedge Q_n) \to$

$\to Q_0)(f_1i, \ldots, f_ki)\} \in D$. Предположим, что в D-prod $\mathfrak{A}_i$ истинно $(Q_1 \wedge \ldots \wedge Q_n \wedge \neg Q_0)(Df_1, \ldots, Df_k)$. Из лемм 17.3 и 17.2 получаем $Y = \{i \mid \mathfrak{A}_i \models (Q_1 \wedge \ldots \wedge Q_n)(f_1i, \ldots, f_ki)\} \in D$ и $Z = \{i \mid \mathfrak{A}_i \models Q_0(f_1i, \ldots, f_ki)\} \notin D$. Очевидно, что $X \cap Y$ содержится в Z. Так как $X \cap Y \in D$, то $Z \in D$ — противоречие.

б) Пусть f — гомоморфизм $\mathfrak{A}$ на $\mathfrak{B}$. По предложению 16.1 б) для любого терма t и интерпретации γ: $FV(t) \to A$

$$f\left(t^{\mathfrak{A}}[\gamma]\right) = t^{\mathfrak{B}}[\gamma f].$$

Из этого равенства и определения гомоморфизма получаем, что

$$\mathfrak{A} \models Q[\gamma] \Rightarrow \mathfrak{B} \models Q[\gamma f]$$

для любой атомарной формулы Q сигнатуры Σ. Поэтому в силу того, что f отображает A на B, из истинности любого тождества Φ в $\mathfrak{A}$ следует его истинность в $\mathfrak{B}$. □

Теорема 6. *Для $\forall$-аксиоматизируемого класса K сигнатуры Σ следующие условия эквивалентны:*

1) *K — квазимногообразие,*

2) *K замкнут относительно конечных декартовых произведений и содержит единичную систему E_Σ.*

Доказательство. 1)$\Rightarrow$2) доказано в предложении 5 а). Рассмотрим множество

$$W = \{\Phi \mid \Phi \text{ — квазитождество сигнатуры } \Sigma \text{ и } \Phi \in \mathrm{Th}(K)\}.$$

Пусть $\mathfrak{A}$ — модель W. Покажем, что каждое конечное подмножество $X \subseteq D(\mathfrak{A})$ имеет такую модель $\mathfrak{B}_X$, что $\mathfrak{B}_X \restriction \Sigma \in K$. Пусть $X = Y \cup Z$, где Z состоит из атомных предложений, а Y — из отрицаний атомных. Если $Y = \varnothing$, то в качестве $\mathfrak{B}_X$ можно взять E_{Σ_A}. Пусть $Y = \{\neg Q_1, \ldots, \neg Q_n\}$, Φ — конъюнкция элементов Z, если $Z \neq \varnothing$, и Φ равно $c_a \approx c_a$ для некоторого $a \in A$, если $Z = \varnothing$. Пусть $c_{a_1}, \ldots, c_{a_k}$ — все константы из C_A, входящие в $Q_1, \ldots, Q_n$, Φ, и $Q'_1, \ldots, Q'_n$, Φ' получаются из $Q_1, \ldots, Q_n$, Φ соответственно заменой $c_{a_1}, \ldots, c_{a_k}$ на $x_1, \ldots, x_k$. Так как квазитождества $\forall x_1 \ldots \forall x_k (\Phi \to Q_i)$, $1 \leqslant i \leqslant n$, ложны в $\mathfrak{A}$, то они не принадлежат W. Следовательно, существуют такие системы $\mathfrak{B}_1, \ldots, \mathfrak{B}_n \in K$, что $\mathfrak{B}_i \models (\Phi \wedge \neg Q_i)[\gamma_i]$, $1 \leqslant i \leqslant n$, для некоторых γ_i: $\{x_1, \ldots, x_k\} \to B_i$. Рассмотрим декартово произведение $\mathfrak{B}_1 \times \ldots \times \mathfrak{B}_n \in K$ и интерпретацию γ переменных $x_1, \ldots, x_k$ в B, для которой проекция $i(\gamma)$ на i-ю координату равна γ_i. Из леммы 17.3 получаем, что $\mathfrak{B}_1\times\ldots\times\mathfrak{B}_n\vDash$ $\vDash(\Phi\wedge\neg Q_1\wedge\ldots\wedge\neg Q_n)[\gamma]$. Следовательно, систему $\mathfrak{B}_1\times\ldots\times\mathfrak{B}_n$ можно обогатить до системы $\mathfrak{B}_X$ сигнатуры Σ_A, являющейся моделью X. Из доказательства теоремы 17.2 получаем, что существует ультрапроизведение $\mathfrak{B}=D\text{-prod}\,\mathfrak{B}_X$, являющееся моделью $D(\mathfrak{A})$. В силу предложения 24.4 а) существует такая подсистема $\mathfrak{B}_1\subseteq$ $\subseteq\mathfrak{B}\restriction\Sigma$, что $\mathfrak{A}\simeq\mathfrak{B}_1$. Так как $\mathfrak{B}\restriction\Sigma=D\text{-prod}(\mathfrak{B}_X\restriction\Sigma)$ и $\mathfrak{B}_X\restriction\Sigma\in K$, то из теорем 4, 5 и из того, что $\mathfrak{A}\simeq\mathfrak{B}_1$, вытекает, что $\mathfrak{A}\in K$. Таким образом, получили $K=K_\Sigma(W)$. □

Теорема 7. *Для квазимногообразия K сигнатуры Σ следующие условия эквивалентны:*

1) *K — многообразие;*

2) *K замкнут относительно гомоморфных образов.*

Доказательство. 1)$\Rightarrow$2) показано в предложении 5 б). Пусть выполняется 2) и $\mathfrak{A}$ — модель множества

$$Z=\{\Phi\mid\Phi\text{ — тождество сигнатуры }\Sigma\text{ и }\Phi\in\mathrm{Th}(K)\}.$$

Рассмотрим множество

$$D^-(\mathfrak{A})=\{\neg\Phi\in D^*(\mathfrak{A})\mid\Phi\text{ — атомарная формула}\}.$$

Для любой формулы $\neg\Psi$ из $D^-(\mathfrak{A})$ тождество $\forall y_1\ldots$ $\ldots\forall y_n\Psi_1$ сигнатуры Σ, где $\Psi=(\Psi_1)^{y_1,\ldots,y_n}_{c_{a_1},\ldots,c_{a_n}}$, ложно в $\mathfrak{A}$, поэтому оно не принадлежит Z. Тогда существует $\mathfrak{B}_\Psi\in K$ и интерпретация γ_Ψ: $\{y_1,\ldots,y_n\}\to B_\Psi$, для которых $\mathfrak{B}_\Psi\vDash\neg\Psi_1[\gamma_\Psi]$. Следовательно, $\mathfrak{B}_\Psi$ можно обогатить до системы $\mathfrak{B}'_\Psi$ сигнатуры Σ_A, являющейся моделью $\{\neg\Psi\}$. Рассмотрим декартово произведение $\mathfrak{B}=D^-(\mathfrak{A})\text{-prod}\,\mathfrak{B}'_\Psi$. В силу предложения 5 а) имеем $\mathfrak{B}\restriction\Sigma\in K$. По лемме 17.3 имеет место $\mathfrak{B}\vDash\neg\Psi$ для любого $\neg\Psi\in D^-(\mathfrak{A})$. Пусть $\mathfrak{B}_1$ — подсистема $\mathfrak{B}$, порожденная в $\mathfrak{B}$ множеством $\left\{\nu^{\mathfrak{B}}(c_a)\mid a\in A\right\}$. По теореме 5 б) имеем $\mathfrak{B}_1\restriction\Sigma\in K$.

Определим отображение h: $B_1\to A$ следующим образом: если $t(x_1,\ldots,x_m)$ — терм сигнатуры Σ и $t^{\mathfrak{B}}\left(\nu^{\mathfrak{B}}(c_{a_1}),\ldots\right.$ $\left.\ldots,\nu^{\mathfrak{B}}(c_{a_m})\right)=b$, то $h(b)=t^{\mathfrak{A}}(a_1,\ldots,a_m)$. Корректность определения h следует из импликаций:

$$\mathfrak{B}_1\vDash(t_1\approx t_2)\left(\nu^{\mathfrak{B}}(c_{a_1}),\ldots,\nu^{\mathfrak{B}}(c_{a_m})\right)\Rightarrow$$

$$\Rightarrow(\neg t_1\approx t_2)^{x_1,\ldots,x_m}_{c_{a_1},\ldots,c_{a_m}}\notin D^-(\mathfrak{A})\Rightarrow\mathfrak{A}\vDash(t_1\approx t_2)(a_1,\ldots,a_m);$$

где $t_1(x_1, \ldots, x_m)$ и $t_2(x_1, \ldots, x_m)$ — любые термы сигнатуры Σ. Цепь импликаций, полученная из предыдущей заменой $t_1 \approx t_2$ на любую атомную формулу $Q(x_1, \ldots, x_m)$ сигнатуры Σ, также имеет место, следовательно, h является гомоморфизмом $\mathfrak{B}_1$ на $\mathfrak{A}$. Из 2) получаем, что $\mathfrak{A} \in K$. Таким образом, показано, что $K = K_\Sigma(Z)$. □

Упражнения

1. Пусть K — аксиоматизируемый класс, содержащий системы как угодно больших конечных мощностей. Показать, что класс K_∞, состоящий из бесконечных систем класса K, является аксиоматизируемым, но не является конечно аксиоматизируемым.

2. Показать, что в теореме 4 условие замкнутости относительно элементарной эквивалентности можно заменить на замкнутость относительно изоморфизмов и элементарных подсистем. (Указание. В доказательстве теоремы 4 вместо $\mathrm{Th}(\mathfrak{A})$ рассмотреть $D^*(\mathfrak{A})$.)

3. Показать, что любое квазитождество Φ эквивалентно квазитождеству Ψ в приведенной н. ф.

4. Утверждение, аналогичное упражнению 3, для тождеств не имеет места. Найти многообразие, которое не имеет системы аксиом, состоящей из предложений вида $\forall x_1 \ldots \forall x_n Q$, где Q — атомная формула. (Указание. Рассмотреть многообразие с системой аксиом $\{\forall x P(f(x))\}$.)

§ 26. Скулемовские функции

Определение. Множество T предложений сигнатуры Σ, замкнутое относительно выводимости (т. е. если $T \rhd \Phi$ и Φ — предложение сигнатуры Σ, то $\Phi \in T$), называется *элементарной теорией* или просто *теорией сигнатуры* Σ. Непротиворечивая теория T сигнатуры Σ называется *полной*, если $\Phi \in T$ или $\neg\Phi \in T$ для любого предложения Φ сигнатуры Σ. Непротиворечивая теория T сигнатуры Σ называется *модельно полной*, если $\mathfrak{A} \subseteq \mathfrak{B} \Rightarrow \mathfrak{A} \prec \mathfrak{B}$ для любых моделей $\mathfrak{A}$, $\mathfrak{B}$ теории T, имеющих сигнатуру Σ. Формулы Φ и Ψ сигнатуры Σ называются *эквивалентными относительно теории* T сигнатуры Σ (обозначаем $\Phi \overset{T}{\equiv} \Psi$), если $T \rhd (\Phi \to \Psi) \wedge (\Psi \to \Phi)$. Теория T сигнатуры Σ называется *$\forall$-аксиоматизируемой* или *универсально аксиоматизируемой* (*$\exists$-аксиоматизируемой*, *$\forall\exists$-аксиоматизируемой*), если существует такое множество $Z \subseteq T$ $\forall$-предложений ($\exists$-предложений, $\forall\exists$-предложений), что $Z \rhd \Phi$ для любого $\Phi \in T$. Такое множество Z называется *системой аксиом для теории* T.

Из следствия 22.4 вытекает, что теория T сигнатуры Σ $\forall$-аксиоматизируема ($\exists$-аксиоматизируема, $\forall\exists$-аксиоматизируема) точно тогда, когда класс $K = K_\Sigma(T)$ $\forall$-аксиоматизируем ($\exists$-аксиоматизируем, $\forall\exists$-аксиоматизируем), причем если Z — система аксиом для $K_\Sigma(T)$, то Z является системой аксиом для T, и наоборот.

Теория T сигнатуры Σ называется *теорией с элиминацией кванторов*, если любая формула Φ сигнатуры Σ эквивалентна относительно T некоторой бескванторной формуле Ψ. Очевидно, что непротиворечивая теория с элиминацией кванторов модельно полна. С другой стороны, модельно полная теория T является «почти» теорией с элиминацией кванторов. А именно, имеет место следующая

Теорема 8. *Для того чтобы непротиворечивая теория T сигнатуры Σ была модельно полной, необходимо и достаточно, чтобы любая формула Φ сигнатуры Σ была эквивалентна относительно T некоторой $\forall$-формуле X_1 и некоторой $\exists$-формуле X_2.*

Доказательство. Достаточность следует из предложения 25.4 а). Необходимость получаем из леммы 25.1, взяв в качестве Γ теорию T. □

Конечно, в теореме 8 требование эквивалентности Φ некоторой $\exists$-формуле X_2 можно опустить, так как это следует из эквивалентности $\neg\Psi$ некоторой $\forall$-формуле.

Работать с формулами, содержащими кванторы, гораздо трудней, чем с бескванторными. Поэтому теоремы теории моделей вида: данная теория T является теорией с элиминацией кванторов (является модельно полной) — очень важны. Сейчас мы изложим некоторую конструкцию, впервые предложенную Скулемом, позволяющую любую теорию расширять до $\forall$-аксиоматизируемой модельно полной теории.

Определение. Если Σ — сигнатура, то сигнатура Σ^s получается из Σ добавлением новых n-местных функциональных символов f_Φ для каждой формулы $\Phi = \exists x\Psi$ сигнатуры Σ, начинающейся с квантора существования и имеющей n свободных переменных. Через S обозначим множество предложений

$$\forall x_1 \ldots \forall x_n (\Phi(x_1, \ldots, x_n) \to \Psi(f_\Phi(x_1, \ldots, x_n), x_1, \ldots, x_n))$$

для всех формул $\Phi(x_1, \ldots, x_n) = \exists x\Psi(x, x_1, \ldots, x_n)$ сигнатуры Σ со свободными переменными $x_1, \ldots, x_n$, выписанными в порядке расположения их первых свободных вхождений в формулу Φ. Если T — теория сигнатуры Σ, то через T^s обозначим теорию

$$\{\Phi \mid \Phi \text{ — предложение сигнатуры } \Sigma^s \text{ и } T \cup S \rhd \Phi\}.$$

Сигнатура Σ^s (теория T^s) называется *скулемизацией сигнатуры* Σ (*теории* T). Модель $\mathfrak{A}^s$ теории $(\mathrm{Th}(\mathfrak{A}))^s$, имеющая сигнатуру Σ^s, называется *скулемизацией системы* $\mathfrak{A}$ сигнатуры Σ, если $\mathfrak{A}^s \restriction \Sigma = \mathfrak{A}$.

В отличие от Σ^s и T^s скулемизация $\mathfrak{A}^s$ не определяется по $\mathfrak{A}$ однозначно, две скулемизации $\mathfrak{A}$ могут быть даже не элементарно эквивалентными (см. упражнение 1), более того из упражнения 1 вытекает, что T^s почти всегда не полна.

Предложение 1. а) *Пусть T — теория сигнатуры Σ, $\mathfrak{B}$ — модель теории T^s и $\mathfrak{A} \subseteq \mathfrak{B}$. Тогда* $\mathfrak{A} \restriction \Sigma \prec \mathfrak{B} \restriction \Sigma$

б) *Любая алгебраическая система $\mathfrak{A}$ имеет некоторую скулемизацию $\mathfrak{A}^s$.*

Доказательство. а) Следует непосредственно из предложения 24.1. Докажем б). Если $\Phi = \exists x \Psi(x, x_1, \ldots \ldots, x_n)$, то для $a_1, \ldots, a_n \in A$ берем в качестве значения $\nu^{\mathfrak{A}}(f_\Phi)(a_1, \ldots, a_n)$ элемент $a_0 \in A$, для которого $\mathfrak{A} \models \models \Psi(a_0, a_1, \ldots, a_n)$, если такой $a_0 \in A$ существует, и произвольный элемент $a \in A$, если такой a_0 не существует. □

Из предложения 1 сразу получается теорема 2 из § 24. В качестве $\mathfrak{B}$ в этой теореме нужно взять $\mathfrak{B}_1 \restriction \Sigma$, где $\mathfrak{B}_1$ — подсистема $\mathfrak{A}^s$, порожденная множеством X.

Скулемизация позволяет «убирать» кванторы у формул старой сигнатуры Σ. Однако в формулах новой сигнатуры Σ^s они «остаются». Чтобы избежать этого неудобства, «замкнем» процесс скулемизации.

Определение. Пусть Σ — сигнатура и T — теория сигнатуры Σ. Определим сигнатуры Σ^{ns} и теории T^{ns}, $n \in \omega$, по индукции: $\Sigma^{0s} = \Sigma$, $T^{0s} = T$, $\Sigma^{(n+1)s} = (\Sigma^{ns})^s$, $T^{(n+1)s} = (T^{ns})^s$. Сигнатура $\Sigma^{cS} = \bigcup\limits_{n \in \omega} \Sigma^{nS}$ $\Big($теория $T^{cS} = \bigcup\limits_{n \in \omega} T^{nS}\Big)$ называется *полной скулемизацией сигнатуры* Σ (*теории* T). Алгебраическая система $\mathfrak{A}^{cs}$ сигнатуры Σ^{cs} называется *полной скулемизацией системы* $\mathfrak{A}$ сигнатуры Σ, если $\mathfrak{A}^{cS} \restriction \Sigma = \mathfrak{A}$ и $\mathfrak{A}^{cS}$ — модель $(\mathrm{Th}(\mathfrak{A}))^{cs}$.

Предложение 2. а) *Любая алгебраическая система $\mathfrak{A}$ имеет некоторую полную скулемизацию $\mathfrak{A}^{cs}$.*

б) *Пусть T — непротиворечивая теория сигнатуры Σ. Тогда теория T^{cs} является универсально аксиоматизируе-*

мым моделью полным расширением T и для любой модели $\mathfrak{A}$ теории T существует модель $\mathfrak{A}_1$ теории T^{cs} такая, что $\mathfrak{A}_1 \restriction \Sigma \parallel \mathfrak{A}$.

Доказательство. а) В силу предложения 1 б) существуют такие системы $\mathfrak{A}^{ns}$, $n \in \omega$, что $\mathfrak{A}^{0s} = \mathfrak{A}$ и $\mathfrak{A}^{(n+1)s}$ является скулемизацией $\mathfrak{A}^{ns}$. Пусть $\mathfrak{A}^{cs} = \langle A, \nu^{\mathfrak{A}^{cS}} \rangle$ — система сигнатуры Σ^{cs}, где $\nu^{\mathfrak{A}^{cS}}$ совпадает с $\nu^{\mathfrak{A}^{nS}}$ на символах из Σ^{ns}. Ясно, что $\mathfrak{A}^{cs}$ будет полной скулемизацией $\mathfrak{A}$.

б) Пусть $\mathfrak{A}$ — модель T^{cs} сигнатуры Σ^{cs} и $\mathfrak{B} \subseteq \mathfrak{A}$. Из предложения 1 а) получаем, что $\mathfrak{B} \restriction \Sigma^{nS} \prec \mathfrak{A} \restriction \Sigma^{nS}$ для любого $n \in \omega$. Так как $\Sigma^{cS} = \bigcup\limits_{n \in \omega} \Sigma^{nS}$, то получаем $\mathfrak{B} \prec \mathfrak{A}$. Следовательно, T^{cs} модельно полна и в силу теоремы 5 класс $K_{\Sigma^{cS}}(T^{cS})$ является $\forall$-аксиоматизируемым, т. е. $K_{\Sigma^{cS}}(T^{cS}) = K_{\Sigma^{cS}}(Z)$, где Z — множество $\forall$-предложений сигнатуры Σ^{cs}. Тогда Z — система аксиом для T^{cs}. Второе утверждение в б) следует из а). □

Упражнение

1. Показать, что для того чтобы все скулемизации системы $\mathfrak{A}$ были элементарно эквивалентными, необходимо и достаточно, чтобы A было одноэлементно. (Указание. Рассмотреть различные значения $\nu^{\mathfrak{A}^S}(f_\Phi)$ для $\Phi = \exists v_0 (v_0 \approx v_0 \wedge v_1 \approx v_1)$.)

§ 27. Механизм совместности

Механизм совместности имеет в основном методическое значение. Он позволяет выделить общую часть в многих теоремах, доказательство которых связано с построением моделей. В этом параграфе мы докажем несколько таких теорем. Всюду в дальнейшем предполагается, что сигнатура Σ имеет конечную или счетную мощность.

Определение. Для формулы Φ сигнатуры Σ определим формулу $\Phi\neg$ следующим образом:

1) если Φ — атомарная формула, то $\Phi\neg = \neg\Phi$,

2) $(\neg\Psi)\neg = \Psi$,

3) $(\Psi_1 \to \Psi_2)\neg = \Psi_1 \wedge \neg\Psi_2$,

4) $(\Psi_1 \wedge \Psi_2)\neg = \neg\Psi_1 \vee \neg\Psi_2$,

5) $(\Psi_1 \vee \Psi_2) \neg = \neg \Psi_1 \wedge \neg \Psi_2$,

6) $(\exists x \Psi) \neg = \forall x \neg \Psi$,

7) $(\forall x \Psi) \neg = \exists x \neg \Psi$.

Из определения $\Phi \neg$ видно, что $\Phi \neg \equiv \neg \Phi$. Обозначим через Σ^C сигнатуру, полученную из сигнатуры $\Sigma = \langle R, F, \mu \rangle$ добавлением счетного множества C новых констант. Константу сигнатуры Σ^C и терм вида $f(c_1, \ldots, c_n)$, где $c_1, \ldots, c_n \in C$ и $f \in F$, будем называть *базисным термом сигнатуры* Σ^C.

Определение. Множество S конечных или счетных множеств предложений сигнатуры Σ^C называется *механизмом совместности сигнатуры* Σ, если для каждого $s \in S$ выполняются следующие условия:

(C1) включение $\{\Phi, \neg \Phi\} \subseteq s$ не имеет места ни для какого предложения Φ;

(C2) $\neg \Phi \in s \Rightarrow (s \cup \{\Phi \neg\} \subseteq s_1$ для некоторого $s_1 \in S)$;

(C3) $\Phi \to \Psi \in s \Rightarrow (s \cup \{\Psi\} \subseteq s_1$ или $s \cup \{\neg \Phi\} \subseteq s_1$ для некоторого $s_1 \in S)$;

(C4) $\Phi \wedge \Psi \in s \Rightarrow (s \cup \{\Phi\} \subseteq s_1$ и $s \cup \{\Psi\} \subseteq s_2$ для некоторых $s_1, s_2 \in S)$;

(C5) $\Phi \vee \Psi \in s \Rightarrow (s \cup \{\Phi\} \subseteq s_1$ или $s \cup \{\Psi\} \subseteq s_1$ для некоторого $s_1 \in S)$;

(C6) $\forall x \Phi \in s \Rightarrow$ (для любого $c \in C$ существует такое $s_1 \in S$, что $s \cup \{(\Phi)^x_c\} \subseteq s_1)$;

(C7) $\exists x \Phi \in s \Rightarrow (s \cup \{(\Phi)^x_c\} \subseteq s_1$ для некоторого $c \in C$ и некоторого $s_1 \in S)$;

(C8) $(c_1, c_2 \in C$ и $c_1 \approx c_2 \in s) \Rightarrow (s \cup \{c_2 \approx c_1\} \subseteq s_1$ для некоторого $s_1 \in S)$;

(C9) если $c \in C$ и t — базисный терм сигнатуры Σ^C, то выполняются два условия:

а) $s \cup \{d \approx t\} \subseteq s_1$ для некоторого $d \in C$ и некоторого $s_1 \in S$,

б) $\{c \approx t, (\Phi)^x_t\} \subseteq s \Rightarrow (s \cup \{(\Phi)^x_c\} \subseteq s_1$ для некоторого $s_1 \in S)$.

Множество S будем называть *механизмом совместности*, если оно является механизмом совместности некоторой сигнатуры Σ.

Предложение 1. *Пусть T — теория сигнатуры Σ. Тогда множество S таких конечных множеств s предложений сигнатуры Σ^C, что $T \cup s$ совместно, является механизмом совместности.*

Доказательство. Проверим условие (C7). Проверку остальных условий оставляем читателю в качестве легкого упражнения. Пусть множество $T \cup s \cup \{(\Phi)^x_c\}$ несовместно для константы $c \in C$, не входящей в элементы $s \cup \{\Phi\}$, и D — доказательство секвенции $\Psi_1, \ldots, \Psi_n, (\Phi)^x_c \vdash$, где $\{\Psi_1, \ldots, \Psi_n\} \subseteq T \cup s$. Используем обычный прием: заменяя константу c во всех секвенциях из D на переменную y, не встречающуюся в элементах D, получаем доказательство D_1 секвенции $\Psi_1, \ldots, \Psi_n, (\Phi)^x_y \vdash$. Применяя правило 16, получаем доказуемость $\Psi_1, \ldots, \Psi_n, \exists y\, (\Phi)^x_y \vdash$. Так как $\exists x \Phi$ и $\exists y\, (\Phi)^x_y$ конгруэнтны, то множество $T \cup s$ несовместно, если $\exists x \Phi \in s$. □

Предложение 2. *Пусть S — механизм совместности и $s \in S$.*

а) $\{\Phi, \Phi \to \Psi\} \subseteq s \Rightarrow (s \cup \{\Psi\} \subseteq s_1$ *для некоторого* $s_1 \in S)$.

б) *Для любого $c \in C$ существует такое $s_1 \in S$, что $s \cup \{c \approx c\} \subseteq s_1$.*

в) $(c, d, e \in C$ *и* $\{c \approx d, d \approx e\} \subseteq s) \Rightarrow (s \cup \{c \approx e\} \subseteq s_1$ *для некоторого* $s_1 \in S)$.

г) $S' = \{s' \mid s' \subseteq s \in S\}$ — *механизм совместности.*

Доказательство. г) очевидно, а) следует из (С3) и (С1), в) следует из (С9) б), если в качестве Φ взять $x \approx e$, а в качестве t — константу d. Докажем б). В силу (С9) а) имеем $s \cup \{d \approx c\} \subseteq s_1$ для некоторой константы $d \in C$ и $s_1 \in S$. Из (С8) получаем $s \cup \{d \approx c, c \approx d\} \subseteq s_1$ для некоторого $s_1 \in S$. Теперь применяем в) и получаем $s \cup \{d \approx c, c \approx d, c \approx c\} \subseteq s_1$ для некоторого $s_1 \in S$. □

Алгебраическую систему $\mathfrak{A}$ сигнатуры Σ^c назовем *канонической*, если $\nu^{\mathfrak{A}}(C) = A$, т. е. любой элемент $a \in A$ является значением некоторой константы $c \in C$.

Теорема 9. *Если S — механизм совместности сигнатуры Σ и $s^* \in S$, то s^* имеет каноническую модель $\mathfrak{A}$ сигнатуры Σ^c.*

Доказательство. Рассмотрим класс $S' = \{s' \subseteq s \mid s \in S\}$, который по предложению 2 г) является механизмом совместности. Пусть

$$\Phi_0, \Phi_1, \ldots, \Phi_n, \ldots \quad (n \in \omega)$$

— нумерация всех предложений сигнатуры Σ^c и

$$t_0, t_1, \ldots, t_n, \ldots \quad (n \in \omega)$$

— нумерация всех базисных термов сигнатуры Σ^c. Индукцией по $n \in \omega$ будем строить последовательность

$$s_0 \subseteq s_1 \subseteq \ldots \subseteq s_n \subseteq \ldots$$

элементов S'. Полагаем $s_0 = s^*$. Если $n = 3k$, то по (С9) а) находим такую константу $c \in C$, что $s_n \cup \{c \approx t_k\} \in S'$, и полагаем $s_{n+1} = s_n \cup \{c \approx t_k\}$. При $n = 3k+1$ полагаем $s_{n+1} = s_n \cup \{\Phi_k\}$, если $s_n \cup \{\Phi_k\} \in S'$ и $s_{n+1} = s_n$ в противном случае. Пусть $n = 3k+2$. Если $\Phi_k = \exists x\Psi$ и $\Phi_k \in s_n$, то полагаем $s_{n+1} = s_n \cup \{(\Psi)^x_c\} \in S'$ для некоторой $c \in C$. В противном случае полагаем $s_{n+1} = s_n$. Рассмотрим множество $s_\omega = \bigcup\limits_{n \in \omega} s_n$. Из построения s_ω вытекает следующий факт:

(*) одноэлементное множество $\{s_\omega\}$ является механизмом совместности.

На множестве C определим отношение $\sim$:

$$c \sim d \Leftrightarrow c \approx d \in s_\omega.$$

В силу (С8) и предложения 2 б), в) отношение $\sim$ является эквивалентностью на множестве C. На множестве $A = \{\tilde{c} \mid \tilde{c}$ — класс эквивалентности по отношению $\sim$, содержащий $c \in C\}$ определяем интерпретацию $\nu^{\mathfrak{A}}$ сигнатуры $\Sigma^c = \langle R, F^c, \mu^c \rangle$ следующим образом:

$$\nu^{\mathfrak{A}}(f)(\tilde{c}_1, \ldots, \tilde{c}_n) = \tilde{c} \Leftrightarrow c \approx f(c_1, \ldots, c_n) \in s_\omega,$$

$$\langle \tilde{c}_1, \ldots, \tilde{c}_n \rangle \in \nu^{\mathfrak{A}}(r) \Leftrightarrow r(c_1, \ldots, c_n) \in s_\omega,$$

где $f \in F^c$, $r \in R$, $\mu^c(f) = \mu^c(r) = n$. Из (*) и (С9) б) следует, что эти определения корректны. Пусть, например, $c_1 \approx f(c_2, c_3)$, $c_4 \approx f(c_5, c_6)$, $c_2 \approx c_5$ и $c_3 \approx c_6$ принадлежат s_ω. Применяя (*) и (С9) б), получаем $c_4 \approx \approx f(c_2, c_6) \in s_\omega$. Еще два раза применяя (*) и (С9) б), получаем $c_4 \approx f(c_2, c_3) \in s_\omega$ и $c_4 \approx c_1 \in s_\omega$.

Так как $\nu^{\mathfrak{A}}(c) = \tilde{c}$ для $c \in C$, то $\mathfrak{A} = \langle A, \nu^{\mathfrak{A}} \rangle$ является канонической системой. Покажем теперь, что для любого предложения Φ сигнатуры Σ^c имеет место

$$\Phi \in s_\omega \Rightarrow \mathfrak{A} \models \Phi. \tag{1}$$

Отсюда будет вытекать, что $\mathfrak{A}$ — модель s^*. Если $\Phi = = c \approx t$ для базисного терма t, $c \in C$, $\Phi = r(c_1, \ldots, c_n)$ для $r \in R$, $c_1, \ldots, c_n \in C$, или Φ есть отрицание таких формул, то (1) следует из определения $\nu^{\mathfrak{A}}$, (*) и (С1). Если $t \approx c \in s_\omega$, где t — базисный терм, $c \in C$, то из (*) и (С9) а) получаем $d \approx t \in s_\omega$ для некоторого $d \in C$.

Тогда по $(*)$ и (С9) б) имеем $d \approx c \in s_\omega$. Следовательно, $\mathfrak{A} \models t \approx c$. Пусть $\neg t \approx c \in s_\omega$, где t — базисный терм, $c \in C$. Если в $\mathfrak{A}$ ложно $\neg t \approx c$, то по определению $\mathfrak{A}$ $c \approx t \in s_\omega$. Из $(*)$ и (С9) б) получаем $\neg c \approx c \in s_\omega$. В силу $(*)$ и предложения 2 б) это противоречит (С1). Таким образом, мы показали истинность (1), если Φ — атомарное предложение или отрицание атомарного и число $n(\Phi)$ символов сигнатуры Σ, входящих в Φ, не больше 1. Пусть $\Phi \in s_\omega$ — атомарное предложение или отрицание атомарного и $n(\Phi) > 1$. Тогда существует базисный терм $t \notin C$, входящий в Φ. По свойствам $(*)$ и (С9) а) имеем $d \approx t \in s_\omega$ для некоторого $d \in C$. Из $(*)$ и (С9) б) следует, что формула Φ_1, полученная из Φ заменой t на d, принадлежит s_ω. Так как $n(\Phi_1) < n(\Phi)$, то по индукционному предположению Φ истинно в $\mathfrak{A}$. Для остальных предложений Φ сигнатуры Σ^c утверждение (1) получается непосредственно из $(*)$ и (С2) — (С7) индукцией по длине Φ. □

Определение. Множество S конечных или счетных множеств предложений сигнатуры Σ^c называется *механизмом совместности сигнатуры Σ без равенства*, если S удовлетворяет условиям (С1) — (С7) и предложения, входящие в элементы S, не содержат равенства.

Теорема 9′. *Пусть сигнатура Σ не содержит символов функций и констант, S — механизм совместности сигнатуры Σ без равенства. Тогда любое $s^* \in S$ имеет каноническую модель сигнатуры Σ^c.*

Доказательство. Рассмотрим множество $X = \{c \approx c \mid c \in C\}$ и класс $S' = \{s \cup X \mid s \in S\}$. Очевидно, что S' является механизмом совместности сигнатуры Σ. По теореме 9 $s^* \cup X$ имеет каноническую модель сигнатуры Σ^c. □

Следующая теорема является обобщением теоремы 9, которое нам понадобится в дальнейшем.

Теорема 10. *Пусть S — механизм совместности сигнатуры Σ, X_i, $i \in \omega$, — конечные или счетные множества предложений сигнатуры Σ^c и T — непротиворечивая теория сигнатуры Σ. Пусть для любых $s \in S$, $\Phi \in T$ и $i \in \omega$ существуют такие $\Psi \in X_i$ и $s_1 \in S$, что $s \cup \{\Phi, \Psi\} \subseteq s_1$. Тогда для любого $s^* \in S$ существует такое множество X предложений сигнатуры Σ, что $s^* \cup X \cup T$ имеет каноническую модель $\mathfrak{A}$ и $X \cap X_i \neq \varnothing$ для любого $i \in \omega$.*

Доказательство. Рассмотрим класс $S' = \{s \cup T \mid s \in S\}$. Легко проверяется, что S' — механизм совместности. Например, пусть $\exists x\Phi \in s \cup T$ и $s \in S$. Если $\exists x\Phi \in s$, то в силу (C7) $s \cup \{(\Phi)_c^x\} \cup T \subseteq s_1 \cup T$ для некоторого $s_1 \in S$. Если $\exists x\Phi \in T$, то по условию теоремы существует такое $s_1 \in S$, что $s \cup \{\exists x\Phi\} \subseteq s_1$. Опять по (C7) имеем $s_1 \cup \{(\Phi)_c^x\} \subseteq s_2$ для некоторых $c \in C$ и $s_2 \in S$. Следовательно, $s \cup T \cup \{(\Phi)_c^x\} \subseteq s_2 \cup T$. Пусть $\Phi_0, \Phi_1, \ldots, \Phi_n, \ldots$ $(n \in \omega)$ и $t_0, t_1, \ldots, t_n, \ldots$ $(n \in \omega)$ — нумерации всех предложений сигнатуры Σ^C и всех базисных термов сигнатуры Σ^C.

По S' строим множество $s_\omega = \bigcup\limits_{n\in\omega} s_n$ следующим образом. Множество s_0 равно $s^* \cup T$, и s_{n+1} для n, равных $4k$, $4k+1$ или $4k+2$, определяем по S' так же, как по S в теореме 9 строятся s_{n+1} для n, равных $3k$, $3k+1$ или $3k+2$ соответственно. Для $n = 4k+3$ поступаем следующим образом: если $s_n = s'_n \cup T$, $s'_n \in S$, то по условию теоремы существуют такие $\Psi \in X_k$ и $s'_n \in S$, что $s'_n \cup \cup \{\Psi\} \subseteq s'$; полагаем $s_{n+1} = s' \cup T$. Построение модели $\mathfrak{A}$ то же самое, что и в теореме 9. В качестве X берем множество s_ω. □

Из теоремы 9 можно получить в качестве следствия теорему о существовании модели из § 22.

Т е о р е м а 21.5. *Если множество* Γ *формул сигнатуры* Σ *непротиворечиво, то* Γ *имеет модель.*

Д о к а з а т е л ь с т в о. В силу теоремы компактности достаточно доказать теорему для конечного множества $\Gamma = \{\Phi_1, \ldots, \Phi_k\}$. Выполнимость и совместность Γ равносильна соответственно выполнимости и совместности предложения $\Psi = \exists x_1 \ldots \exists x_n (\Phi_1 \wedge \ldots \wedge \Phi_k)$, где $x_1, \ldots, x_n$ — все свободные переменные, входящие в $\Phi_1, \ldots, \Phi_k$. Если $\{\Psi\}$ непротиворечиво, то из предложения 1 получаем, что существует механизм совместности S, для которого $\{\Psi\} \in S$. Теперь применяем теорему 9 для $s^* = \{\Psi\}$. □

О п р е д е л е н и е. Множество Z формул сигнатуры Σ, свободные переменные которых содержатся в множестве $\{v_1, \ldots, v_n\}$, называется *n-типом сигнатуры* Σ. Если T — непротиворечивая теория сигнатуры Σ, то n-тип Z сигнатуры Σ называется *главным в* T, если существует такая формула $\Phi(v_1, \ldots, v_n)$ сигнатуры Σ, что $T \cup \{\exists v_1 \ldots \exists v_n \Phi\}$ совместно и $T \rhd \Phi \to \Psi$ для любой $\Psi \in Z$. Будем говорить, что n-тип Z сигнатуры Σ *реализуется в алгебраической системе* $\mathfrak{A}$ сигнатуры Σ, если существуют такие элементы $a_1, \ldots, a_n \in A$, что $\mathfrak{A} \models \Psi(a_1, \ldots, a_n)$ для любой формулы $\Psi(v_1, \ldots, v_n) \in Z$. Если n-тип Z сигнатуры Σ не реализуется в системе $\mathfrak{A}$ сигнатуры Σ, то говорим, что Z *опускается в* $\mathfrak{A}$.

Следующая теорема называется *теоремой об опускании типов*.

Теорема 11. *Если T — непротиворечивая теория сигнатуры Σ и Z_i, $i \in \omega$,— неглавные в T n_i-типы сигнатуры Σ, то существует модель T сигнатуры Σ, опускающая все типы Z_i, $i \in \omega$.*

Доказательство. Рассмотрим совокупность S таких конечных множеств s предложений сигнатуры Σ^c, что $s \cup T$ совместно. По предложению 1 S является механизмом совместности. Пусть f_i, $i \in \omega$,— разнозначные отображения ω на C^{n_i} и g — разнозначное отображение ω на ω^2. Определим множества X_k, $k \in \omega$, следующим образом: если $g(k) = \langle i, j \rangle$ и $f_i(j) = \langle c_1, \ldots, c_{n_i} \rangle$, то полагаем $X_k = \left\{ \neg (\Phi)^{v_1, \ldots, v_{n_i}}_{c_1, \ldots, c_{n_i}} \,\middle|\, \Phi \in Z_i \right\}$. Предположим, что условие теоремы 10 не выполнено. Тогда существуют такие $s_0 \in S$ и $k_0 \in \omega$, что $s_0 \cup T \cup \{\Psi\}$ несовместно для любого $\Psi \in X_{k_0}$. Пусть $g(k_0) = \langle i_0, l \rangle$, $f_{i_0}(l) = \langle c_1, \ldots, c_{n_{i_0}} \rangle$ и Φ_0 — конъюнкция всех элементов s_0. Тогда $\{\Phi_0\} \cup T$ совместно и $T \rhd \Phi_0 \to (\Phi)^{v_1, \ldots, v_{n_{i_0}}}_{c_1, \ldots, c_{n_{i_0}}}$ для всех $\Phi(v_1, \ldots, v_{n_{i_0}}) \in Z_{i_0}$. Пусть $c_{n_{i_0}+1}, \ldots, c_m$ — все элементы C, отличные от $c_1, \ldots, c_{n_{i_0}}$ и содержащиеся в Φ_0. Пусть Φ_1 — предложение, конгруэнтное предложению Φ_0, не содержащее переменных $v_1, \ldots, v_m$, и пусть Φ_2 — формула сигнатуры Σ, для которой $(\Phi_2)^{v_1, \ldots, v_m}_{c_1, \ldots, c_m} = \Phi_1$. Покажем, что $T \rhd \exists v_{n_{i_0}+1} \ldots \exists v_m \Phi_2 \to \Phi$ для всех $\Phi \in Z_{i_0}$. В самом деле, пусть $\mathfrak{A} \models \Phi_2[\gamma]$ для некоторой модели $\mathfrak{A}$ теории T, имеющей сигнатуру Σ, и интерпретации γ: $\{v_1, \ldots, v_m\} \to A$. Рассмотрим такое обогащение $\mathfrak{A}'$ системы $\mathfrak{A}$ до сигнатуры Σ^c, что $\nu^{\mathfrak{A}'}(c_1) = \gamma(v_1), \ldots, \nu^{\mathfrak{A}'}(c_m) = \gamma(v_m)$. Тогда $\mathfrak{A}' \models \Phi_1$ и из эквивалентности $\Phi_1 \equiv \Phi_0$ получаем $\mathfrak{A}' \models \Phi_0$. Так как $\mathfrak{A}'$ — модель T и $T \rhd \Phi_0 \to (\Phi)^{v_1, \ldots, v_{n_{i_0}}}_{c_1, \ldots, c_{n_{i_0}}}$, то $\mathfrak{A} \models \Phi[\gamma]$. Таким образом, $\mathfrak{A} \models (\exists v_{n_{i_0}+1} \ldots \exists v_m \Phi_2 \to \Phi)[\gamma]$ для любой модели $\mathfrak{A}$ теории T, любой формулы $\Phi = Z_{i_0}$

и любой интерпретации $\gamma: \{v_1, \ldots, v_{n_{i_0}}\} \to A$. Из следствия 22.4 тогда следует, что $T \triangleright \exists v_{n_{i_0}+1} \ldots \exists v_m \Phi_2 \to \Phi$ для любого $\Phi \in Z_{i_0}$. Так как $s_0 \cup T$ совместно, то $T \cup \{\exists v_1 \ldots \exists v_m \Phi_2\}$ также совместно. Это противоречит тому, что Z_{i_0} — неглавный n_{i_0}-тип. Таким образом, условия теоремы 10 выполнены, значит, существует такое множество X предложений сигнатуры Σ^c, что $X \cap X_i \neq \varnothing$, $i \in \omega$, и существует система $\mathfrak{A}$ сигнатуры Σ^c, являющаяся моделью $T \cup X$, у которой любой элемент $a \in A$ является значением некоторой константы $c \in C$. Так как для любого $i \in \omega$ и любого кортежа $\langle c_1, \ldots, c_{n_i}\rangle \in C^{n_i}$ существует такое $k \in \omega$, что $X_k = \left\{ \neg (\Phi)^{v_1, \ldots, v_{n_i}}_{c_1, \ldots, c_{n_i}} \middle| \Phi \in Z_i \right\}$, то $\mathfrak{A} \restriction \Sigma$ опускает все типы Z_i, $i \in \omega$. □

Теорема об опускании типов является очень важным методом построения моделей. Она дополняет теорему компактности, которая применяется в основном тогда, когда нужно реализовывать совместные типы. Применения теоремы 11 будут даны в § 29.

Вхождение символа q в формулу Φ, не содержащую связки $\to$, назовем *положительным* (*отрицательным*), если число различных подформул формулы Φ вида $\neg \Psi$, содержащих это вхождение, является четным (нечетным). Обозначим через $\Sigma^+(\Phi)$ и $\Sigma^-(\Phi)$ множества символов отношений сигнатуры Σ, имеющих соответственно положительные и отрицательные вхождения в Φ. Например, если

$$\Phi = \forall v_1 (\neg (\exists v_2 r(t_1, v_2) \vee \neg s(v_2)) \wedge \neg(\neg r(v_3, t_2) \wedge v_1 \approx t_1)),$$

где t_1, t_2 — термы, то $\Sigma^+(\Phi) = \{r, s\}$, $\Sigma^-(\Phi) = \{r\}$.

Следующая теорема называется *интерполяционной теоремой Крейга — Линдона.*

Теорема 12. *Пусть Φ, Ψ — предложения сигнатуры Σ, не содержащие связки $\to$, и $\Phi \triangleright \Psi$. Тогда*

а) *существует такое предложение X сигнатуры Σ, не содержащее связки $\to$, что $\Phi \triangleright X$, $X \triangleright \Psi$, $\Sigma^+(X) \subseteq \Sigma^+(\Phi) \cap \Sigma^+(\Psi)$ и $\Sigma^-(X) \subseteq \Sigma^-(\Phi) \cap \Sigma^-(\Psi)$;*

б) *если Σ не содержит символов функций и констант, Φ, Ψ не содержат равенства, а $\neg\Phi$ и Ψ обе недоказуемы, то в* а) *можно потребовать, чтобы X не содержало равенства.*

Доказательство. Предложение X, удовлетворяющее условиям утверждения а), назовем интерполирующим для пары $\langle \Phi, \Psi \rangle$.

а) Пусть S — множество конечных множеств s предложений сигнатуры Σ^c, не содержащих символа импликации, которые удовлетворяют следующему условию: существуют такие $s_1 \neq \varnothing$ и $s_2 \neq \varnothing$, что $s = s_1 \cup s_2$ и не существует интерполирующего предложения для пары $\langle \bigwedge s_1, \neg (\bigwedge s_2) \rangle$. (Через $\bigwedge s$ мы обозначаем конъюнкцию элементов s.) Множество s_1 при этом будем называть началом, а s_2 — концом s *). Проверим условия (C1) — (C9) механизма совместности. Так как импликация не входит в элементы $s \in S$, то (C3) тривиально выполнено. Если предложение Θ_1 сигнатуры Σ^c эквивалентно предложению $\Theta_2 \in s \in S$ и $\Sigma^\tau(\Theta_1) = \Sigma^\tau(\Theta_2)$, $\tau \in \{+, -\}$, то очевидно, что $s \cup \{\Theta_1\} \in S$. Отсюда получаем условия (C2) и (C8). Пусть $s \in S$, s_1 — начало s, а s_2 — конец s.

(C1) Пусть $\{\Theta, \neg \Theta\} \subseteq s$. Если $\{\Theta, \neg \Theta\}$ содержится в начале (конце) s, то предложение $\forall v_1 \neg v_1 \approx v_1$ (предложение $\forall v_1 v_1 \approx v_1$) будет интерполирующим для $\langle \bigwedge s_1, \neg (\bigwedge s_2) \rangle$, что противоречит условию. Если $\Theta \in s_1$ и $\neg \Theta \in s_2$ ($\neg \Theta \in s_1$ и $\Theta \in s_2$), то интерполирующим для $\langle \bigwedge s_1, \neg (\bigwedge s_2) \rangle$ будет предложение Θ (предложение $\neg \Theta$).

(C4) Пусть $\Theta_1 \bigwedge \Theta_2 \in s_1$, и предположим, что существует интерполирующее предложение X для $\langle (\bigwedge s_1) \bigwedge \Theta_1, \neg (\bigwedge s_2) \rangle$ или для $\langle (\bigwedge s_1) \bigwedge \Theta_2, \neg (\bigwedge s_2) \rangle$. Тогда из $\bigwedge s_1 \rhd \Theta_1$ и $\bigwedge s_1 \rhd \Theta_2$ получаем, что X будет интерполирующим предложением для $\langle \bigwedge s_1, \neg (\bigwedge s_2) \rangle$, что невозможно. Если $\Theta_1 \bigwedge \Theta_2 \in s_2$ и X — интерполирующее предложение для $\langle \bigwedge s_1, \neg ((\bigwedge s_2) \bigwedge \Theta_1) \rangle$ или для $\langle \bigwedge s_1, \neg ((\bigwedge s_2) \bigwedge \Theta_2) \rangle$, то в силу $\neg (\bigwedge s_2 \bigwedge \Theta_1) \rhd \neg (\bigwedge s_2)$ и $\neg (\bigwedge s_2 \bigwedge \Theta_2) \rhd \neg (\bigwedge s_2)$ X будет интерполирующим предложением для $\langle \bigwedge s_1, \neg (\bigwedge s_2) \rangle$. Полученные противоречия с условием показывают, что $s \cup \{\Theta_1\} \in S$ и $s \cup \{\Theta_2\} \in S$.

(C5) Пусть $\Theta_1 \bigvee \Theta_2 \in s_1$ и X_1, X_2 — интерполирующие предложения для $\langle (\bigwedge s_1) \bigwedge \Theta_1, \neg (\bigwedge s_2) \rangle$, $\langle (\bigwedge s_1) \bigwedge \Theta_2, \neg (\bigwedge s_2) \rangle$ соответственно. Тогда $X_1 \bigvee X_2$ будет интерполирующим предложением для $\langle \bigwedge s_1, \neg (\bigwedge s_2) \rangle$. Если $\Theta_1 \bigvee \Theta_2 \in s_2$ и X_1, X_2 — интерполирующие предложения для $\langle \bigwedge s_1, \neg ((\bigwedge s_2) \bigwedge \Theta_1) \rangle$, $\langle \bigwedge s_1, \neg ((\bigwedge s_2) \bigwedge \Theta_2) \rangle$ соответ-

*) Отметим, что начало и конец s определяются по s неоднозначно.

ственно, то $X_1 \wedge X_2$ будет интерполирующим предложением для $\langle \bigwedge s_1, \neg(\bigwedge s_2)\rangle$.

(C6) Пусть $\forall x\Theta \in s_2$, $c \in C$ и X — интерполирующее предложение для $\langle \bigwedge s_1, \neg((\bigwedge s_2) \wedge (\Theta)^x_c)\rangle$. Так как $\neg((\bigwedge s_2) \wedge (\Theta)^x_c) \rhd \neg(\bigwedge s_2)$, то X является интерполирующим предложением для $\langle \bigwedge s_1, \neg(\bigwedge s_2)\rangle$, что невозможно. В случае $\forall x\Theta \in s_1$ аналогично получаем, что в качестве начала $s \cup \{(\Theta)^x_c\}$ можно взять $s_1 \cup \{(\Theta)^x_c\}$, а в качестве конца s_2.

(C7) Пусть $c_0 \in C$ не содержится в элементах s. Если $\exists x\Theta \in s_1$ и X — интерполирующее предложение для $\langle(\bigwedge s_1) \wedge (\Theta)^x_{c_0}, \neg(\bigwedge s_2)\rangle$, от из аксиомы 12 и правила 3 $\text{ИП}_1^{\Sigma C}$ получаем, что $\exists y X_1$ будет интерполирующим предложением для $\langle \bigwedge s_1, \neg(\bigwedge s_2)\rangle$, где X_1 не содержит константу c_0, $(X_1)^y_{c_0} = X$ и y — переменная, не входящая в элементы $s \cup \{X\}$. В случае, когда $\exists x\Theta \in s_2$ и X — интерполирующее предложение для $\langle \bigwedge s_1, \neg((\bigwedge s_2) \wedge (\Theta)^x_{c_0})\rangle$, предложение $\forall y X_1$ будет интерполирующим для $\langle \bigwedge s_1, \neg(\bigwedge s_2)\rangle$. В самом деле, $\bigwedge s_1 \rhd \forall y X_1$ следует из $\bigwedge s_1 \rhd X$, так как c_0 не входит в $\bigwedge s_1$. Из $X \rhd \neg((\bigwedge s_2) \wedge (\Theta)^x_{c_0})$ получаем $\forall y X_1 \rhd \neg(\bigwedge s_2) \vee \forall y \neg(\Theta)^x_y$. Если $\forall y X_1 \rhd \neg(\bigwedge s_2)$ не имеет места, то существует модель $\mathfrak{A}$ множества $\{\forall y X_1, \bigwedge s_2\}$. Из предыдущего получаем, что в $\mathfrak{A}$ истинно $\forall y \neg(\Theta)^x_y$. Это противоречит $\mathfrak{A} \models \bigwedge s_2$ и $\exists x\Theta \in s_2$.

(C9). Пусть $c' \in C$ не входит в элементы s. Если X является интерполирующим предложением для $\langle(\bigwedge s_1) \wedge \wedge c' \approx f(c_1, \ldots, c_n), \neg(\bigwedge s_2)\rangle$, то X будет интерполирующим предложением для $\langle \bigwedge s_1, \neg(\bigwedge s_2)\rangle$. Пусть $\{c_0 \approx \approx f(c_1, \ldots, c_n), (\Theta)^x_{f(c_1,\ldots,c_n)}\} \subseteq s$. Если $(\Theta)^x_{f(c_1,\ldots,c_n)} \in s_1$ и X — интерполирующее предложение для $\langle(\bigwedge s_1) \wedge \wedge(\Theta)^x_{c_0}, \neg(\bigwedge s_2)\rangle$, то интерполирующим для $\langle(\bigwedge s_1), \neg(\bigwedge s_2)\rangle$ будет предложение X в случае $c_0 \approx f(c_1, \ldots, c_n) \in s_1$ и предложение $\neg c_0 \approx f(c_1, \ldots, c_n) \vee X$ в случае $c_0 \approx f(c_1, \ldots, c_n) \in s_2$. Если $(\Theta)^x_{f(c_1,\ldots,c_n)} \in s_2$ и X — интерполирующее предложение для $\langle \bigwedge s_1, \neg((\bigwedge s_2) \wedge \wedge(\Theta)^x_{c_0})\rangle$, то интерполирующим для $\langle \bigwedge s_1, \neg(\bigwedge s_2)\rangle$ будет предложение X в случае $c_0 \approx f(c_1, \ldots, c_n) \in s_2$ и предложение $c_0 \approx f(c_1, \ldots, c_n) \wedge X$ в случае $c_0 \approx f(c_1, \ldots, c_n) \in s_1$.

Итак, мы показали, что S — механизм совместности. Если бы а) не имело места, то множество $\{\Phi, \neg \Psi\}$ принадлежало бы S. По теореме 9 множество $\{\Phi, \neg \Psi\}$ имело бы модель, что в силу следствия 22.4 противоречило бы условию $\Phi \rhd \Psi$.

Чтобы доказать б), нужно в определении S заменить слова «предложение» на «предложение без равенства» и потребовать, чтобы не имело места ни $\rhd \neg (\bigwedge s_1)$, ни $\rhd \neg (\bigwedge s_2)$. Тогда при проверке (C1) случаи $\{\Theta, \neg \Theta\} \subseteq s_1$ и $\{\Theta, \neg \Theta\} \subseteq s_2$ невозможны. Остальная проверка условий (C1)—(C7) та же, что и в а). Следовательно, S — механизм совместности без равенства. Затем применяем теорему 9′ вместо теоремы 9. □

Если в Φ или в Ψ входит равенство, то в теореме 12 б) потребовать, чтобы равенство входило в X только тогда, когда оно входит в Φ и Ψ, нельзя (см. упражнение 1). В оставшейся части параграфа мы применим теорему 12 для характеризации предложений, сохраняющих свою истинность при переходе к гомоморфным образам.

Определение. Если $\mathfrak{A}$ — алгебраическая система сигнатуры Σ, то отношение E на множестве A назовем *конгруэнтностью* на $\mathfrak{A}$, если оно является эквивалентностью на A и для любых $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$, $r \in R$, $f \in F$, $\mu(r) = \mu(f) = n$ из $\langle a_1, b_1\rangle \in E, \ldots, \langle a_n, b_n\rangle \in E$, $\langle a_1, \ldots, a_n\rangle \in \nu^{\mathfrak{A}}(r)$ следует $\langle b_1, \ldots, b_n\rangle \in \nu^{\mathfrak{A}}(r)$ и из $\langle a_1, b_1\rangle \in E, \ldots, \langle a_n, b_n\rangle \in E$ следует $\langle \nu^{\mathfrak{A}}(f)(a_1, \ldots, a_n), \nu^{\mathfrak{A}}(f)(b_1, \ldots, b_n)\rangle \in E$. Если E — конгруэнтность на системе $\mathfrak{A}$ сигнатуры Σ, то определим новую систему $\mathfrak{A}/E$ сигнатуры Σ, которую назовем *факторсистемой системы* $\mathfrak{A}$ *по* E. Носитель $\mathfrak{A}/E$ состоит из классов эквивалентности $aE = \{b \mid \langle b, a\rangle \in E\}$. Интерпретация $\nu^{\mathfrak{A}/E}$ определяется так:

$$\langle a_1E, \ldots, a_nE\rangle \in \nu^{\mathfrak{A}/E}(r) \Leftrightarrow \langle a_1, \ldots, a_n\rangle \in \nu^{\mathfrak{A}}(r) \quad (r \in R),$$

$$\nu^{\mathfrak{A}/E}(f)(a_1E, \ldots, a_nE) = \nu^{\mathfrak{A}}(f)(a_1, \ldots, a_n)E \quad (f \in F).$$

Проверку корректности этого определения, а также доказательство следующего простого предложения мы оставляем читателю в качестве упражнения.

Предложение 3. а) *Пусть* Φ — *предложение сигнатуры* Σ, *а* Φ' *получается из* Φ *заменой подформул* $t_1 \approx t_2$ *на* $E(t_1, t_2)$, *где* E — *символ отношения, не входящий в* R. *Если* $\mathfrak{A}$ — *система сигнатуры* $\Sigma' \supseteq \Sigma$, $E \in R'$ *и* $\nu^{\mathfrak{A}}(E)$ — *конгруэнтность на* $\mathfrak{A} \upharpoonright \Sigma$, *то*

$$\mathfrak{A} \models \Phi' \Leftrightarrow \mathfrak{A}/\nu^{\mathfrak{A}}(E) \models \Phi.$$

б) *Если* E — *конгруэнтность на системе* $\mathfrak{A}$, *то отображение, сопоставляющее элементу* $a \in A$ *элемент* aE, *будет гомоморфизмом* $\mathfrak{A}$ *на* $\mathfrak{A}/E$. □

Формулу Φ назовем *положительной*, если она не содержит импликации и все вхождения в Φ символов отношений и равенства являются положительными. Будем говорить, что предложение Φ сигнатуры Σ сохраняется *при гомоморфизмах относительно предложения* Ψ сигнатуры Σ, если из истинности $\Phi \wedge \Psi$ на системе $\mathfrak{A}$ сигнатуры Σ следует истинность $\Psi \to \Phi$ на любом ее гомоморфном образе.

Теорема 13. *Пусть* Φ *и* Ψ — *предложения сигнатуры* Σ *и предложение* $\Psi \to \neg\Phi$ *недоказуемо. Для того чтобы* Φ *сохранялось при гомоморфизмах относительно предложения* Ψ, *необходимо и достаточно, чтобы* Φ *было эквивалентно относительно* Ψ *положительному предложению* X (*т. е.* $\Psi \rhd (\Phi \to X) \wedge (X \to \Phi)$).

Доказательство. Необходимость. Так как Φ и Ψ содержат конечное число символов, то можно считать сигнатуру $\Sigma = \langle R, F, \mu \rangle$ конечной. Предположим сначала, что $F = \varnothing$. Обозначим через Θ конъюнкцию предложений

$$\forall v_1 \ldots \forall v_n (\neg r(v_1, \ldots, v_n) \vee r'(v_1, \ldots, v_n)), \; r \in R, \; \mu(r) = n,$$

и предложения

$$\forall v_1 \forall v_2 (\neg E(v_1, v_2) \vee E'(v_1, v_2)),$$

где r' $(r \in R)$, E и E' — попарно различные символы, не принадлежащие R. Обозначим через Δ предложение сигнатуры, содержащей лишь символы из $R \cup \{E\}$ и не содержащее импликации, истинность которого на системе $\mathfrak{A}$ равносильна тому, что $\nu^{\mathfrak{A}}(E)$ — конгруэнтность на $\mathfrak{A} \upharpoonright \Sigma$. Пусть Φ_0 и Ψ_0 получаются соответственно из Φ и Ψ заменой всех подформул вида $x \approx y$ на $E(x, y)$. Пусть Φ_0', Φ_0' и Δ' получаются соответственно из Φ_0, Ψ_0 и Δ заменой всех предикатных символов на штрихованные. Если на системе $\mathfrak{A}$ истинно предложение $\Theta \wedge \Delta \wedge \Delta'$, то

$\nu^{\mathfrak{A}}(r) \subseteq \nu^{\mathfrak{A}}(r')$ для $r \in R$ и $\nu^{\mathfrak{A}}(E) \subseteq \nu^{\mathfrak{A}}(E')$, поэтому отображение, сопоставляющее элементу aE элемент aE', будет гомоморфизмом $(\mathfrak{A} \upharpoonright \Sigma)/\nu^{\mathfrak{A}}(E)$ на $\mathfrak{A}_1/\nu^{\mathfrak{A}}(E')$, где $\mathfrak{A}_1 = \langle A, \nu^{\mathfrak{A}_1}\rangle$ — система сигнатуры Σ, для которой $\nu^{\mathfrak{A}_1}(r) = \nu^{\mathfrak{A}}(r')\,(r \in R)$. Отсюда, используя следствие 22.4, предложение 3 а) и условие теоремы, получаем, что имеет место

$$\Psi_0 \wedge \Phi_0 \wedge \Delta \rhd \neg\, \Psi_0' \vee \neg\Theta \vee \neg\, \Delta' \vee \Phi_0'.$$

Предположим, что $\rhd \neg\, \Psi_0' \vee \neg\Theta \vee \neg\Delta' \vee \Phi_0'$. Заменив в доказательстве символы r' на r для $r \in R$ и E' на E, получаем

$$\rhd \neg\, \Psi_0 \vee \neg\, \Theta_1 \vee \neg\Delta \vee \Phi_0,$$

где Θ_1 получается из Θ заменой r' на r для $r \in R$ и E' на E. Ясно, что $\rhd\Theta_1$, следовательно, $\neg\Psi_0 \vee \neg\Delta \vee \Phi_0$ — тождественно истинное предложение. Отсюда, используя тот факт, что Δ истинно на системах $\mathfrak{A}$, у которых отношение $\nu^{\mathfrak{A}}(E)$ является равенством, получаем, что $\Psi \rightarrow \Phi$ также тождественно истинно. Поэтому в качестве X можно взять предложение $\forall v_1 v_1 \approx v_1$. Пусть теперь $\neg\, \Psi_0' \vee \neg\,\Theta \vee \neg\Delta' \vee \Phi_0'$ не доказуемо. Предложение $\neg\, (\Psi_0 \wedge \Phi_0 \wedge \Delta)$ также не доказуемо, так как в противном случае в силу того, что Δ истинно на системах $\mathfrak{A}$, у которых $\nu^{\mathfrak{A}}(E)$ является равенством, предложение $\Psi \rightarrow \neg\,\Phi$ также было бы тождественно истинным, что противоречит условию о его недоказуемости. Тогда по теореме 12 б) существует интерполирующее предложение X_0, не содержащее равенства, для которого имеют место условия $\Psi_0 \wedge \Phi_0 \wedge \Delta \rhd X_0$, $X_0 \rhd \neg\, \Psi_0' \vee \neg\,\Theta \vee \neg\, \Delta' \vee \Phi_0'$, $\Sigma^+(X_0) \subseteq R \cup \{E\}$, а также $\Sigma^-(X_0) \subseteq \Sigma^-(\Psi_0 \wedge \Phi_0 \wedge \Delta) \cap \Sigma^-(\neg\, \Psi_0' \vee \neg\Theta \vee \neg\Delta' \vee \Phi_0') = \varnothing$. Следовательно, X_0 — положительное предложение сигнатуры Σ_1, которая кроме символов Σ имеет лишь символ E. Заменяя в выводе символы r' на r для $r \in R$ и E' на E, получаем $X_0 \rhd \neg\Psi_0 \vee \neg\,\Theta_1 \vee \neg\Delta \vee \Phi_0$. Так как $\rhd\, \Theta_1$, то $X_0 \rhd \neg\, \Psi_0 \vee \neg\, \Delta \vee \Phi_0$. Таким образом, мы получили $\Psi_0, \Delta \rhd (\Phi_0 \rightarrow X_0) \wedge (X_0 \rightarrow \Phi_0)$. Так как Δ истинно на системах $\mathfrak{A}$, у которых отношение $\nu^{\mathfrak{A}}(E)$ является равенством, то $\Psi \rhd (\Phi \rightarrow X) \wedge (X \rightarrow \Phi)$ для положительного предложения X, полученного из X_0 заменой подформул вида $E(x, y)$ на $x \approx y$.

Пусть теперь $\Sigma = \langle R, \{f_1, \ldots, f_m\}, \mu\rangle$. Рассмотрим сигнатуру $\Sigma' = \langle R \cup \{F_1, \ldots, F_m\}, \varnothing, \mu'\rangle$, где $F_1, \ldots, F_m$ — попарно различные символы, не принадлежащие R, $\mu'(r) = \mu(r)$ $(r \in R)$ и $\mu'(F_i) = \mu(f_i) + 1$, $i \in \{1, \ldots, m\}$. Пусть Ψ_0 — предложение, выражающее в системах сигнатуры Σ', что отношения $F_1, \ldots, F_m$ являются функциями*). Пусть Φ_1, Ψ_1 — предложения сигнатуры Σ, находящиеся в приведенной н. ф., эквивалентные соответственно предложениям Φ, Ψ. Пусть Φ_2, Ψ_2 получаются соответственно из Φ_1, Ψ_1 заменой атомных подформул вида $y \approx f_i(x_1, \ldots, x_n)$, $f_i(x_1, \ldots, x_n) \approx y$ на $F_i(x_1, \ldots, x_n, y)$. Ясно, что если Φ сохраняется при гомоморфизмах относительно Ψ, то Φ_2 сохраняется при гомоморфизмах относительно $\Psi_0 \wedge \Psi_2$. Так как Σ' не содержит символов функций, то по только что доказанному существует положительное предложение X_1 сигнатуры Σ', для которого имеет место

$$\Psi_0 \wedge \Psi_2 \rhd (\Phi_2 \to X_1) \wedge (X_1 \to \Phi_2).$$

Используя следствие 22.4, получаем, что тогда справедливо

$$\Psi \rhd (\Phi \to X) \wedge (X \to \Phi),$$

где X — положительное предложение сигнатуры Σ, полученное из X_1 заменой $F_i(x_1, \ldots, x_{n+1})$ на $x_{n+1} \approx \approx f(x_1, \ldots, x_n)$.

Достаточность условия теоремы получается из следующих двух фактов, которые проверяются непосредственно индукцией по длине X. 1) Если h — гомоморфизм $\mathfrak{A}$ на $\mathfrak{B}$ и $X(x_1, \ldots, x_n)$ — формула, не содержащая отрицания и импликации, то

$$\mathfrak{A} \vDash X(a_1, \ldots, a_n) \Rightarrow \mathfrak{B} \vDash X(ha_1, \ldots, ha_n).$$

2) Положительная формула X эквивалентна формуле X_1, не содержащей отрицания и импликации. □

Упражнения

1. Используя теорему 11, доказать, что для любого счетного линейного порядка $\mathfrak{B}$ без последнего элемента существует такое собственное элементарное расширение $\mathfrak{B}$ (т. е. $\mathfrak{A} \prec \mathfrak{B}$ и $A \neq B$),

---

*) То есть Ψ_0 является конъюнкцией предложений $\forall x_1 \ldots \forall x_{n_i} \forall y \forall z \left(\left(F_i(x_1, \ldots, x_{n_i}, y) \wedge F_i(x_1, \ldots, x_{n_i}, z)\right) \to y \approx z\right) \wedge \wedge \forall x_1 \ldots \forall x_{n_i} \exists y F_i(x_1, \ldots, x_{n_i}, y)$, $i \in \{1, \ldots, m\}$, $n_i = \mu(f_i)$.

что $\mathfrak{A}$ является начальным отрезком $\mathfrak{B}$ (т. е. из $\langle b, a\rangle \in \nu^{\mathfrak{B}}(\leqslant)$ и $a \in A$ следует $b \in A$). (Указание. Добавить в сигнатуру константы $\{c\} \cup \{c_a | a \in A\}$, рассмотреть теорию T с множеством аксиом $D^*(\mathfrak{A}) \cup \{\neg c \approx c_a \,|\, a \in A\}$ и типы $Z_b = \{v_1 \leqslant c_b\} \cup \{\neg v_1 \approx \approx c_a \,|\, a \in A\}$ и применить теорему об опускании типов.)

2. Показать, что если в Φ или в Ψ входит равенство, то в теореме 12 б) нельзя потребовать чтобы равенство входило в X только тогда, когда оно входит в Φ и Ψ. (Указание. Рассмотреть примеры $c_1 \approx c_2 \rhd r(c_1) \vee \neg r(c_2)$, $r(c_1) \wedge \neg r(c_2) \rhd \neg c_1 \approx c_2$.)

3. Формулу Ψ назовем отрицательной, если у формулы Ψ_1, полученной из Ψ заменой всех ее подформул вида $\Psi_1 \to \Psi_2$ на $\neg \Psi_1 \vee \Psi_2$, каждое вхождение символа отношения и равенства является отрицательным. Показать, что доказуемые формулы не могут быть отрицательными. (Указание. Отрицательная формула ложна в E_Σ.)

4. Из упражнения 3 вывести, что в теореме 13 условие недоказуемости $\Psi \to \neg \Phi$ опустить нельзя.

§ 28. Счетная однородность и универсальность

Пусть T — теория сигнатуры Σ. Обозначим через $F_n(\Sigma)$ множество формул сигнатуры Σ со свободными переменными из множества $\{v_1, \ldots, v_n\}$. Если $\Phi \in \in F_n(\Sigma)$, то через $\|\Phi\|_T$ или просто через $\|\Phi\|$ обозначаем множество $\{\Psi \in F_n(\Sigma) \,|\, T \rhd (\Phi \to \Psi) \wedge (\Psi \to \Phi)\}$. Обозначим через $\mathfrak{B}_n(T)$ булеву алгебру с носителем $B_n(T) = \{\|\Psi\| \,|\, \Psi \in F_n(\Sigma)\}$ и следующими операциями:

а) $\|\Phi\| \cup \|\Psi\| = \|\Phi \vee \Psi\|$;

б) $\|\Phi\| \cap \|\Psi\| = \|\Phi \wedge \Psi\|$;

в) $\overline{\|\Phi\|} = \|\neg \Phi\|$.

Корректность определения операций, а также проверку аксиом 1) — 10) булевых алгебр оставляем читателю в качестве упражнения.

Пусть в этом параграфе все рассматриваемые алгебраические системы и теории, если не оговорено противное, имеют сигнатуру Σ, а мощность Σ конечна или счетна. Под моделью теории T мы будем понимать модель T сигнатуры Σ. Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры Σ и $a_1, \ldots, a_n \in A$. *Типом набора* $\langle a_1, \ldots, a_n\rangle$ в $\mathfrak{A}$ назовем следующий n-тип:

$$T(\mathfrak{A}, a_1, \ldots, a_n) = \\ = \{\Phi(v_1, \ldots, v_n) \,|\, \mathfrak{A} \models \Phi(a_1, \ldots, a_n),\quad \Phi \in F_n(\Sigma)\}.$$

Если $\mathfrak{A}$, $\mathfrak{B}$ — системы сигнатуры Σ, $a_1, \ldots, a_n \in A$, $b_1, \ldots \ldots, b_n \in B$, то равенство $T(\mathfrak{A}, a_1, \ldots, a_n) = T(\mathfrak{B}, b_1, \ldots$

$\ldots, b_n)$ будем обозначать также через

$$\langle \mathfrak{A}, a_1, \ldots, a_n \rangle \equiv \langle \mathfrak{B}, b_1, \ldots, b_n \rangle.$$

Определение. Счетная алгебраическая система $\mathfrak{A}$ называется *однородной*, если для любых $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ и любого элемента $a \in A$ из

$$\langle \mathfrak{A}, a_1, \ldots, a_n \rangle \equiv \langle \mathfrak{A}, b_1, \ldots, b_n \rangle \quad (1)$$

следует

$$\langle \mathfrak{A}, a_1, \ldots, a_n, a \rangle \equiv \langle \mathfrak{A}, b_1, \ldots, b_n, b \rangle \quad (2)$$

для некоторого $b \in A$.

Ясно, что если $\mathfrak{A}$ — однородная система и $X \subseteq A$ — конечное множество, то система $\mathfrak{A}_X$ также является однородной.

Предложение 1. *Для любой счетной системы $\mathfrak{A}$ существует счетное элементарное однородное расширение $\mathfrak{B} \succ \mathfrak{A}$.*

Доказательство. Покажем сначала, что для любой счетной системы $\mathfrak{A}$ существует такое счетное элементарное расширение $\mathfrak{A}^{(1)} \succ \mathfrak{A}$, что для любых $a_1, \ldots, a_n, b_1, \ldots, b_n, a \in A$ из (1) следует

$$\langle \mathfrak{A}^{(1)}, a_1, \ldots, a_n, a \rangle \equiv \langle \mathfrak{A}^{(1)}, b_1, \ldots, b_n, b \rangle \quad (3)$$

для некоторого $b \in A^{(1)}$. Для каждого $X = \{a_1, \ldots, a_n\} \subseteq A$ определяем множество

$$R(X) = \{\gamma\colon X \to A \mid \langle \mathfrak{A}, a_1, \ldots, a_n \rangle \equiv \langle \mathfrak{A}, \gamma a_1, \ldots, \gamma a_n \rangle\}.$$

Обозначим через R объединение всех $R(X)$, где X — конечное подмножество A. Ясно, что R имеет счетную мощность. Расширим сигнатуру Σ_A до Σ_1, добавив новые символы одноместных операций f_γ для каждого $\gamma \in R$. Рассмотрим следующее множество предложений сигнатуры Σ_1:

$$Z = D^*(\mathfrak{A}) \cup \{\forall x(\Phi(x, c_{a_1}, \ldots, c_{a_n}) \to \Phi(f_\gamma(x), c_{\gamma a_1}, \ldots, c_{\gamma a_n}))$$
$$\mid \gamma \in R,\ a_1, \ldots, a_n \in \operatorname{dom}\gamma,\quad \Phi(x, y_1, \ldots, y_n) \in F(\Sigma)\}.$$

Из определения множества R следует, что каждое конечное множество $Z_1 \subseteq Z$ выполняется в некотором обогащении системы $\mathfrak{A}$. Пусть $\mathfrak{A}_1$ — счетная модель Z и $\mathfrak{A}^{(1)} = \mathfrak{A}_1 \restriction \Sigma$. Так как $\mathfrak{A}$ — модель $D^*(\mathfrak{A})$, то по предложению 24.4 а) можно считать, что $\mathfrak{A} \prec \mathfrak{A}^{(1)}$. Если выполняется (1), то из истинности на $\mathfrak{A}_1$ предложений из Z

следует выполнимость (3) для $b = f_\gamma^{\mathfrak{A}_1}(a)$, где $\gamma(a_1) = b_1, \ldots, \gamma(a_n) = b_n$.

Определим последовательность систем $\{\mathfrak{A}_i \mid i \in \omega\}$ следующим образом: $\mathfrak{A}_0 = \mathfrak{A}$, $\mathfrak{A}_{i+1} = \mathfrak{A}_i^{(1)}$, $i \in \omega$. По предложению 24.3 получаем $\mathfrak{A}_k \prec \mathfrak{B} = \bigcup\limits_{i \in \omega} \mathfrak{A}_i$, $k \in \omega$, в частности, $\mathfrak{A} \prec \mathfrak{B}$. Так как $\mathfrak{B} = \bigcup \mathfrak{A}_i$, то $\mathfrak{B}$ — счетная система. Если $a_1, \ldots, a_n, b_1, \ldots, b_n, a \in B$ и

$$\langle \mathfrak{B}, a_1, \ldots, a_n \rangle \equiv \langle \mathfrak{B}, b_1, \ldots, b_n \rangle,$$

то $a_1, \ldots, a_n, b_1, \ldots, b_n, a \in A_i$ для некоторого $i \in \omega$. Так как $\mathfrak{A}_i \prec \mathfrak{B}$, то имеем

$$\langle \mathfrak{A}_i, a_1, \ldots, a_n \rangle \equiv \langle \mathfrak{A}_i, b_1, \ldots, b_n \rangle.$$

Из определения $\mathfrak{A}_i^{(1)} = \mathfrak{A}_{i+1}$ получаем

$$\langle \mathfrak{A}_{i+1}, a_1, \ldots, a_n, a \rangle \equiv \langle \mathfrak{A}_{i+1}, b_1, \ldots, b_n, b \rangle$$

для некоторого $b \in A_{i+1}$. Так как $\mathfrak{A}_{i+1} \prec \mathfrak{B}$, то

$$\langle \mathfrak{B}, a_1, \ldots, a_n, a \rangle \equiv \langle \mathfrak{B}, b_1, \ldots, b_n, b \rangle.$$

Таким образом, $\mathfrak{B} \succ \mathfrak{A}$ — счетная однородная система. □

Предложение 2. *Пусть $\mathfrak{A}$, $\mathfrak{B}$ — счетные однородные системы сигнатуры Σ. Тогда следующие условия эквивалентны:*

1) $\mathfrak{A} \simeq \mathfrak{B}$,

2) *в $\mathfrak{A}$ и $\mathfrak{B}$ реализуются одни и те же n-типы сигнатуры Σ, $n \in \omega$.*

Доказательство. 1) ⇒ 2) очевидно. Пусть выполняется 2). Занумеруем A и B: $A = \{a_i \mid i \in \omega\}$, $B = \{b_i \mid i \in \omega\}$. Индукцией по $n \in \omega$ построим конечные отображения $f_n\colon A_n \to B$, $A_n \subseteq A$, со следующими свойствами:

а$_n$) если $n \neq 0$, то $f_{n-1} \subseteq f_n$;

б$_n$) если $n = 2k + 1$, то $a_k \in A_n$;

в$_n$) если $n = 2(k+1)$, то $b_k \in f_n(A_n)$;

г$_n$) если $A_n = \{e_1, \ldots, e_m\}$, то

$$\langle \mathfrak{A}, e_1, \ldots, e_m \rangle \equiv \langle \mathfrak{B}, f_n e_1, \ldots, f_n e_m \rangle.$$

Для $f_0 = \varnothing$ условия а$_0$) — в$_0$) тривиально выполнены. Условие г$_0$) следует из 2), так как $\mathrm{Th}(\mathfrak{A})$ является 0-типом. Пусть $n = 2k + 1$ и $A_{n-1} = \{e_1, \ldots, e_m\}$. По индукционному предположению имеем

$$\langle \mathfrak{A}, e_1, \ldots, e_m \rangle \equiv \langle \mathfrak{B}, f_{n-1} e_1, \ldots, f_{n-1} e_m \rangle. \qquad (1)$$

Из условия 2) получаем, что тип $T(\mathfrak{A}, e_1, \ldots, e_m, a_k)$ реализуется в $\mathfrak{B}$, поэтому

$$\langle\mathfrak{A}, e_1, \ldots, e_m, a_k\rangle \equiv \langle\mathfrak{B}, d_1, \ldots, d_{m+1}\rangle \tag{2}$$

для некоторых $d_1, \ldots, d_{m+1} \in B$. Из (1) и (2) получаем

$$\langle\mathfrak{B}, d_1, \ldots, d_m\rangle \equiv \langle\mathfrak{B}, f_{n-1}e_1, \ldots, f_{n-1}e_m\rangle;$$

поэтому в силу однородности $\mathfrak{B}$ существует такой $b \in B$, что

$$\langle\mathfrak{B}, d_1, \ldots, d_{m+1}\rangle \equiv \langle\mathfrak{B}, f_{n-1}e_1, \ldots, f_{n-1}e_m, b\rangle.$$

В силу (2) тогда имеем

$$\langle\mathfrak{A}, e_1, \ldots, e_m, a_k\rangle \equiv \langle\mathfrak{B}, f_{n-1}e_1, \ldots, f_{n-1}e_m, b\rangle,$$

следовательно, отображение $f_n = f_{n-1} \cup \{\langle a_k, b\rangle\}$ будет удовлетворять условиям а$_n$) — г$_n$). Случай $n = 2(k+1)$ рассматривается аналогично. Из условий а$_n$) — г$_n$), $n \in \omega$, получаем, что $f = \bigcup\limits_{n\in\omega} f_n$ будет изоморфизмом $\mathfrak{A}$ на $\mathfrak{B}$. □

Определение. Счетная алгебраическая система $\mathfrak{A}$ сигнатуры Σ называется *универсальной*, если для любого $n \in \omega$ в ней реализуются все совместные с $\mathrm{Th}(\mathfrak{A})$ n-типы сигнатуры Σ. Счетная алгебраическая система $\mathfrak{A}$ сигнатуры Σ называется *насыщенной*, если для любого конечного $X \subseteq A$ в $\mathfrak{A}_X$ реализуются все совместные с $\mathrm{Th}(\mathfrak{A}_X)$ 1-типы сигнатуры Σ_X.

Ясно, что совместность n-типа Z с $\mathrm{Th}(\mathfrak{A})$ равносильна локальной выполнимости Z в $\mathfrak{A}$. Очевидно, что счетное элементарное расширение универсальной системы является универсальной системой. Ясно также, что если система $\mathfrak{A}$ насыщена, то система $\mathfrak{A}_X$ также насыщена для любого конечного $X \subseteq A$.

Предложение 3. *Для счетной алгебраической системы $\mathfrak{A}$ следующие условия эквивалентны:*

1) *$\mathfrak{A}$ насыщена,*

2) *$\mathfrak{A}$ универсальна и однородна.*

Доказательство. 1) ⇒ 2). Пусть $\mathfrak{A}$ насыщена. Индукцией по $n \in \omega$ покажем, что в $\mathfrak{A}$ выполняется любой совместный с $\mathrm{Th}(\mathfrak{A})$ n-тип Z_0 сигнатуры Σ. Если $n = 1$, то выполнимость Z_0 в $\mathfrak{A}$ следует из определения насыщенности. Пусть $n > 1$. Рассмотрим $(n-1)$-тип $Z_1 = \{\exists v_n(\Phi_1 \wedge \ldots \wedge \Phi_k) \mid \Phi_1, \ldots, \Phi_k \in Z_0\}$. Так как Z_1 локально выполним в $\mathfrak{A}$, то по индукционному предположению тип Z_1 реализуется в $\mathfrak{A}$ элементами $a_1, \ldots, a_{n-1}$. Будем считать, что v_1 не входит связано в элементы Z_0.

В силу предложения 19.4 б) достаточно рассмотреть только такие n-типы Z_0. Рассмотрим 1-тип

$$Z_2 = \left\{(\Phi)^{v_1, \ldots, v_{n-1}, v_n}_{c_{a_1}, \ldots, c_{a_{n-1}}, v_1} \,\middle|\, \Phi \in Z_0\right\}.$$

Ясно, что 1-тип Z_2 локально выполним в $\mathfrak{A}_{\{a_1, \ldots, a_{n-1}\}}$. В силу насыщенности $\mathfrak{A}$ существует элемент $a \in A$, реализующий в $\mathfrak{A}_{\{a_1, \ldots, a_{n-1}\}}$ тип Z_2. Тогда n-тип Z_0 реализуется в $\mathfrak{A}$ элементами $a_1, \ldots, a_{n-1}, a$.

Покажем однородность $\mathfrak{A}$. Пусть $a_1, \ldots, a_n, b_1, \ldots, b_n, a \in A$ и

$$\langle \mathfrak{A}, a_1, \ldots, a_n\rangle \equiv \langle \mathfrak{A}, b_1, \ldots, b_n\rangle. \qquad (*)$$

Рассмотрим 1-тип

$$Z_0 = \{\Phi(v_1) \mid \mathfrak{A}_{\{a_1, \ldots, a_n\}} \models \Phi(a),\ \Phi \in F_1(\Sigma_{\{a_1, \ldots, a_n\}})\}.$$

Из $(*)$ следует, что 1-тип

$$Z_1 = \left\{(\Phi_1)^{x_1, \ldots, x_n}_{c_{b_1}, \ldots, c_{b_n}} \,\middle|\, (\Phi_1)^{x_1, \ldots, x_n}_{c_{a_1}, \ldots, c_{a_n}} \in Z_0,\right.$$
$$\left.\Phi_1(x_1, \ldots, x_n, v_1) \in F(\Sigma)\right\}$$

локально выполним в $\mathfrak{A}_{\{b_1, \ldots, b_n\}}$. Так как $\mathfrak{A}$ насыщена, то Z_1 реализуется в $\mathfrak{A}_{\{b_1, \ldots, b_n\}}$ элементом $b \in A$. Ясно, что тогда имеет место

$$\langle \mathfrak{A}, a_1, \ldots, a_n, a\rangle \equiv \langle \mathfrak{A}, b_1, \ldots, b_n, b\rangle.$$

2) $\Rightarrow$ 1). Пусть $\mathfrak{A}$ универсальна и однородна, $a_1, \ldots, a_n \in A$ и Z_0 — локально выполнимый в $\mathfrak{A}_{\{a_1, \ldots, a_n\}}$ 1-тип сигнатуры $\Sigma_{\{a_1, \ldots, a_n\}}$. Без ограничения общности можно считать, что все связанные переменные в элементах Z_0 отличны от $v_1, \ldots, v_{n+1}$. Рассмотрим n-тип $Z_1 = T(\mathfrak{A}, a_1, \ldots, a_n)$ и $(n+1)$-тип

$$Z_2 = Z_1 \cup \left\{\Phi \mid (\Phi)^{v_1, \ldots, v_n, v_{n+1}}_{c_{a_1}, \ldots, c_{a_n}, v_1} \in Z_0,\right.$$
$$\left.\Phi(v_1, \ldots, v_{n+1}) \in F(\Sigma)\right\}$$

Из локальной выполнимости Z_0 в $\mathfrak{A}_{\{a_1, \ldots, a_n\}}$ следует локальная выполнимость Z_2 в $\mathfrak{A}$. В силу универсальности $\mathfrak{A}$ следует выполнимость Z_2 в $\mathfrak{A}$ некоторыми $b_1, \ldots, b_{n+1} \in A$. Так как $Z_1 \subseteq Z_2$, то

$$\langle \mathfrak{A}, a_1, \ldots, a_n\rangle \equiv \langle \mathfrak{A}, b_1, \ldots, b_n\rangle.$$

Из однородности $\mathfrak{A}$ получаем

$$\langle \mathfrak{A}, a_1, \ldots, a_n, a \rangle \equiv \langle \mathfrak{A}, b_1, \ldots, b_{n+1} \rangle$$

для некоторого $a \in A$. Очевидно, что a реализует Z_0 в $\mathfrak{A}_{\{a_1,\ldots,a_n\}}$. □

Предложение 4. *Если $\mathfrak{A}$ и $\mathfrak{B}$ — счетные насыщенные элементарно эквивалентные системы, то $\mathfrak{A} \simeq \mathfrak{B}$.*

Доказательство. Непосредственное следствие предложений 3 и 2, так как в $\mathfrak{A}$ и $\mathfrak{B}$ реализуются все совместные с $\mathrm{Th}(\mathfrak{A}) = \mathrm{Th}(\mathfrak{B})$ n-типы. □

Таким образом, между полными теориями T, имеющими счетные насыщенные модели, и счетными насыщенными моделями T существует взаимно однозначное с точностью до изоморфизма соответствие. В силу предложения 1 любая теория T имеет счетную однородную модель. Однако не все теории T имеют счетную насыщенную модель (см. упражнение 2). Следующее предложение характеризует полные теории T, имеющие насыщенные модели.

Предложение 5. *Для полной теории T, имеющей бесконечные модели, следующие условия эквивалентны:*

1) *T имеет счетную универсальную модель;*

2) *T имеет счетную насыщенную модель;*

3) *для любого $n \in \omega$ булева алгебра $\mathfrak{B}_n(T)$ имеет счетное число ультрафильтров.*

Доказательство. 1) $\Rightarrow$ 2). Пусть $\mathfrak{A}$ — счетная универсальная модель T. По предложению 1 существует счетная однородная модель $\mathfrak{B} \succ \mathfrak{A}$. Из предложения 3 получаем, что $\mathfrak{B}$ — насыщенная модель T.

2) $\Rightarrow$ 3). Пусть $\mathfrak{A}$ — счетная насыщенная модель T, $n \in \omega$, и U — ультрафильтр алгебры $\mathfrak{B}_n(T)$. Рассмотрим n-тип

$$T(U) = \{\Phi \mid \|\Phi\| \in U, \quad \Phi \in F_n(\Sigma)\}.$$

Ясно, что $T(U)$ — совместный с T n-тип. Так как $\mathfrak{A}$ универсальна, то существует набор $\bar{a}(U) = \langle a_1, \ldots, a_n \rangle$, который реализует тип $T(U)$ в $\mathfrak{A}$. Если U_1, U_2 — два различных ультрафильтра $\mathfrak{B}_n(T)$, то для некоторой $\Phi \in F_n(\Sigma)$ имеем $\|\Phi\| \in U_1$ и $\|\neg\Phi\| \in U_2$. Следовательно, $\bar{a}(U_1) \neq \bar{a}(U_2)$. Таким образом, существует разнозначное отображение множества всех ультрафильтров алгебры $\mathfrak{B}_n(T)$ в счетное множество A^n. Это дает условие 3).

3) $\Rightarrow$ 1). Пусть $\{U_i^n \mid i \in \omega\}$ — множество всех ультрафильтров $\mathfrak{B}_n(T)$ и сигнатура Σ_1 получается добавлением

к Σ новых попарно различных констант $\{c_j^{n,i} \mid n,\ i \in \omega,\ 1 \leqslant j \leqslant n\}$. Тогда счетное множество предложений сигнатуры Σ

$$X = T \cup \left\{ (\Phi)^{v_1, \ldots, v_n}_{c_1^{n,i}, \ldots, c_n^{n,i}} \,\middle|\, n,\ i \in \omega;\ \Phi \in T\left(U_i^n\right) \right\}$$

совместно. Пусть $\mathfrak{A}$ — счетная модель X. Тогда $\mathfrak{A} \restriction \Sigma$ будет универсальной моделью T. В самом деле, пусть Z_0 — совместный с T n-тип сигнатуры Σ. Тогда множество $Y = \{\|\Phi\| \mid \Phi \in Z_0\}$ будет центрированным множеством алгебры $\mathfrak{B}_n(T)$. По предложению 12.1 существует ультрафильтр $U_i^n \supseteq Y$ алгебры $\mathfrak{B}_n(T)$. Так как $Z_0 \subseteq T\left(U_i^n\right)$, то Z_0 будет реализовываться в $\mathfrak{A} \restriction \Sigma$ элементами $\nu^{\mathfrak{A}}\left(c_1^{n,i}\right), \ldots$ $\ldots, \nu^{\mathfrak{A}}\left(c_n^{n,i}\right)$. □

Понятия однородной, универсальной и насыщенной счетной системы легко обобщаются на другие мощности. В частности, алгебраическая система $\mathfrak{A}$ сигнатуры Σ называется *$\varkappa$-насыщенной*, где $\varkappa$ — кардинал, если для любого множества $X \subseteq A$ мощности $< \varkappa$ в $\mathfrak{A}_X$ реализуется любой совместный с $\mathrm{Th}(\mathfrak{A}_X)$ 1-тип сигнатуры Σ_X. В заключение этого параграфа мы приведем теорему, доказанную независимо Ю. Л. Ершовым и Г. Дж. Кейслером.

Фильтр D на множестве I называется *счетно полным*, если для любого множества $\{X_i \mid i \in \omega\} \subseteq D$ имеет место $\bigcap\limits_{i \in \omega} X_i \in D$. Обозначим через ω_1 первый несчетный кардинал.

Предложение 6. *Если $\mathfrak{A}_i$, $i \in I$,— алгебраические системы сигнатуры Σ, а D — ультрафильтр на I, не являющийся счетно полным, то система D-$\mathrm{prod}\,\mathfrak{A}_i$ является ω_1-насыщенной.*

Доказательство. Пусть $\{X_i \mid i \in \omega\} \subseteq D$ и $\bigcap\limits_{i \in \omega} X_i \notin D$. Рассмотрим семейство $\{W_i \mid i \in \omega\}$, где $W_0 = I \setminus X_0$, $W_1 = \bigcap\limits_{i \in \omega} X_i$ и $W_i = (X_0 \cap \ldots \cap X_{i-2}) \setminus (X_0 \cap \ldots \cap X_{i-1})$ для $i \geqslant 2$. Ясно, что $W_i \notin D$ для $i \in \omega$, $\bigcup\limits_{i \in \omega} W_i = I$ и $W_i \cap W_j = \varnothing$ для $i \neq j$. Пусть $\mathfrak{A}_i$, $i \in I$,— алгебраические системы сигнатуры Σ, $X \subseteq D$-$\mathrm{prod}\,A_i$, $|X| \leqslant \omega$, $Z = \{\Phi_i(v_1) \mid i \in \omega\}$ — совместный с $\mathrm{Th}((D\text{-}\mathrm{prod}\,\mathfrak{A}_i)_X)$ 1-тип сигнатуры Σ_X и Φ_0 — тождественно истинная формула.

Пусть $\mathfrak{B} = (D\text{-}\mathrm{prod}\,\mathfrak{A}_i)_X$ и $X = \{Df^k \mid k \in \omega\}$. Рассмотрим обогащения $\mathfrak{B}_i$ систем $\mathfrak{A}_i$ сигнатуры Σ_X, для которых

$c_{Df}^{\mathfrak{B}_i k} = f^k(i)$. Ясно, что $\mathfrak{B} = D\text{-prod}\,\mathfrak{B}_i$ и для всех $k \in \omega$

$$\{i \in I \mid \mathfrak{B}_i \models \exists v_1 (\Phi_0 \wedge \ldots \wedge \Phi_k)\} \in D. \tag{1}$$

Возьмем такое $f \in I\text{-prod}\,B_i$, чтобы для любых $k,\ n \in \omega$, $k \in W_n$ было $\mathfrak{B}_k \models \Phi_0(fk) \wedge \ldots \wedge \Phi_{m(k)}(fk)$, где $m(k)$ — наибольшее число из множества $\{0, 1, \ldots, n\}$, для которого $\mathfrak{B}_k \models \exists v_1 (\Phi_0 \wedge \ldots \wedge \Phi_{m(k)})$. Так как $W_i \cap W_j = \varnothing$ для $i \neq j$ и Φ_0 тождественно истинна, то такое f можно выбрать.

Покажем, что для любого $k_0 \in \omega$, $k_0 \geqslant 1$

$$\{i \in I \mid \mathfrak{B}_i \models \Phi_{k_0}(fi)\} \in D, \tag{2}$$

и предложение тем самым будет доказано. Рассмотрим множество

$$G = \{i \in I \mid \mathfrak{B}_i \models \exists v_1 (\Phi_1 \wedge \ldots \wedge \Phi_{k_0})\} \setminus (W_0 \cup \ldots \cup W_{k_0 - 1}).$$

Из (1) и из того, что $W_0 \notin D, \ldots, W_{k_0-1} \notin D$, получаем $G \in D$. Так как $m(i) \geqslant k_0$ для любого $i \in G$, то из построения f вытекает $G \subseteq \{i \in I \mid \mathfrak{B}_i \models \Phi_k(fi)\}$, откуда получаем (2). □

Упражнения

1. Показать, что в $\mathfrak{B}_n(T)$ истинны аксиомы булевых алгебр.

2. Пусть сигнатура Σ_0 состоит из счетного множества $\{r_i \mid i \in \omega\}$ одноместных предикатов и теория T_0 определяется множеством аксиом

$$\{\exists v_1 (s_1(v_1) \wedge \ldots \wedge s_n(v_1)) \mid n \in \omega,\ s_1 \in \{r_1, \neg r_1\}, \ldots, s_n \in \{r_n, \neg r_n\}\}.$$

Показать, что T_0 — полная теория, не имеющая универсальной счетной модели. (Указание. Полнота T_0 следует из того, что $\mathfrak{A} \restriction \Sigma_1 \simeq \mathfrak{B} \restriction \Sigma_1$ для любой конечной $\Sigma_1 \subseteq \Sigma_0$ и любых счетных моделей $\mathfrak{A}$, $\mathfrak{B}$ теории T; отсутствие универсальной модели T следует из того, что все 1-типы $\{s_i(v_1) \mid i \in \omega,\ s_i \in \{r_i, \neg r_i\}\}$ совместны с T_0.)

§ 29. Категоричность

Теорема 24.3 показывает, что $\mathrm{Th}(\mathfrak{A})$ для бесконечной системы $\mathfrak{A}$ не определяет $\mathfrak{A}$ (с точностью до изоморфизма). Однако существует интересный класс систем $\mathfrak{A}$, теория которых определяет $\mathfrak{A}$ с точностью до изоморфизма среди систем той же мощности. В этом параграфе мы рассмотрим некоторые свойства теорий таких систем. Сигнатуры в этом параграфе имеют счетную или конечную мощность.

Определение. Класс K алгебраических систем сигнатуры Σ называется *категоричным в мощности* $\varkappa$ или $\varkappa$-*категоричным*, если все системы из K мощности $\varkappa$ изоморфны между собой. Теория T сигнатуры Σ называется *категоричной в* $\varkappa$, если класс $K_\Sigma(T)$ является $\varkappa$-категоричным.

Если класс K не имеет систем мощности $\varkappa$, то по определению он категоричен в $\varkappa$. Если K — класс алгебраических систем (T — теория) сигнатуры Σ, то через K_∞ (через T_∞) обозначаем класс бесконечных алгебраических систем из K (теорию $T \cup \left\{\exists v_1 \ldots \exists v_n \left(\bigwedge\limits_{i<j\leqslant n} \neg v_i \approx \approx v_j\right) \,\middle|\, n \in \omega\right\}$). Ясно, что $K_\Sigma(T_\infty) = (K_\Sigma(T))_\infty$.

Предложение 1. *Если теория T сигнатуры Σ категорична в некоторой бесконечной мощности $\varkappa$ и T_∞ совместна, то T_∞ полна.*

Доказательство. Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — две бесконечные модели T. Достаточно показать, что $\mathfrak{A} \equiv \mathfrak{B}$. По теореме 24.2 существуют счетные элементарные подсистемы $\mathfrak{A}_1 \prec \mathfrak{A}$ и $\mathfrak{B}_1 \prec \mathfrak{B}$. По теореме 24.3 существуют элементарные расширения $\mathfrak{A}_2 \succ \mathfrak{A}_1$ и $\mathfrak{B}_2 \succ \mathfrak{B}_1$ мощности $\varkappa$. Так как $\mathfrak{A}_2$ изоморфна $\mathfrak{B}_2$, то $\mathfrak{A}_2 \equiv \mathfrak{B}_2$. Следовательно, $\mathfrak{A} \equiv \mathfrak{B}$. □

Если T полна и имеет конечные модели, то по следствию 24.2 все модели T изоморфны некоторой конечной системе. До конца этого параграфа пусть T обозначает полную теорию сигнатуры Σ, имеющую бесконечные модели. Заметим, что из полноты теории T следует выполнимость любого главного совместного n-типа в любой модели T.

Теорема 14 (К. Рыль-Нардзевский). *Для того чтобы теория T была категорична в счетной мощности, необходимо и достаточно, чтобы для любого $n \in \omega$ алгебры $\mathfrak{B}_n(T)$ были конечны.*

Доказательство. Необходимость. Пусть $\mathfrak{B}_{n_0}(T)$ — бесконечная булева алгебра. Так как T полна, то $|\mathfrak{B}_0(T)| = 2$, следовательно, $n_0 > 0$. По предложению 12.3 существует неглавный ультрафильтр U на $\mathfrak{B}_{n_0}(T)$. Ясно, что n_0-тип $Z = \{\Phi \in F_n(\Sigma) \mid \|\Phi\| \in U\}$ является неглавным n_0-типом в T. По теореме 11 существует счетная модель $\mathfrak{A}$ теории T, в которой он опускается. Так как $T \cup Z$ совместно, то по теореме о существовании модели существует модель $\mathfrak{B}$, в которой Z реализуется. Так как можно считать $\mathfrak{B}$ счетной, то T не является счетно категоричной.

Достаточность. Пусть $\mathfrak{B}_n(T)$ конечны для всех $n \in \omega$. Тогда любой n-тип Z является главным в T. В силу предложения 28.4 достаточно показать, что любая счетная модель $\mathfrak{A}$ теории T насыщена, для чего в свою очередь достаточно показать, что любой 1-тип сигнатуры $\Sigma^{\{a_1,\ldots,a_n\}}$, где $a_1, \ldots, a_n \in A$, является главным в $T_1 = \mathrm{Th}\left(\mathfrak{A}_{\{a_1,\ldots,a_n\}}\right)$. Последнее следует из того, что отображение h, переводящее $\Phi(v_1, \ldots, v_{n+1})$ в $\Phi\left(v_1, c_{a_1}, \ldots, c_{a_n}\right)$, сохраняет отношение $\|\Phi\| \leqslant \|\Psi\|$ (т. е. $T \rhd \Phi \to \Psi \Rightarrow T_1 \rhd h\Phi \to h\Psi$) и любой $(n+1)$-тип сигнатуры Σ является главным в T. □

Следующее предложение доказано П. Линдстрёмом.

Предложение 2. *Если* $\forall\exists$*-аксиоматизируемая непротиворечивая теория* T *сигнатуры* Σ *категорична в счетной мощности, то* T *модельно полна.*

Доказательство. Будем говорить, что формула $\Phi(x_1, \ldots, x_n)$ сигнатуры Σ сохраняется при переходе к подмоделям (надмоделям) теории T, если для любых моделей $\mathfrak{A} \subseteq \mathfrak{B}$ теории T и любых $a_1, \ldots, a_n \in A$ из истинности $\Phi(a_1, \ldots, a_n)$ в $\mathfrak{B}$ (в $\mathfrak{A}$) следует истинность $\Phi(a_1, \ldots, a_n)$ в $\mathfrak{A}$ (в $\mathfrak{B}$). Рассмотрим множество G формул сигнатуры Σ, находящихся в пренексной н. ф. и не сохраняющихся при переходе к подмоделям T. Ясно, что модельная полнота T равносильна тому, что $G = \varnothing$. Предположим, что T не модельно полна. Возьмем $\Phi_0(x_1, \ldots, x_n) \in G$, кванторная приставка которой имеет наименьшую длину r_0. Очевидно, что $r_0 > 0$. Пусть $\Phi_0 = \mathsf{Q}y\Psi_0(y, x_1, \ldots, x_n)$. Из минимальности r_0 следует, что Ψ_0 сохраняется при переходе к подсистемам, поэтому $\mathsf{Q} = \exists$. Так как $\neg\Psi_0$ эквивалентна формуле с кванторной приставкой длины $r_0 - 1$, то из минимальности r_0 получаем, что Ψ_0 сохраняется при переходе к надсистемам.

Возьмем такое $\varphi\colon \omega \to \omega^n$, что для любого $a \in \omega^n$ множество $\{k \mid \varphi k = a\}$ бесконечно. Строим последовательность $\mathfrak{A}_m$, $m \in \omega$, счетных моделей теории T со следующими свойствами:

1) $A_m \subseteq \omega$ и множество $\omega \setminus A_m$ бесконечно;

2) $\mathfrak{A}_m \subseteq \mathfrak{A}_s$ для $m \leqslant s$;

3) если $\varphi m \in (A_m)^n$ и существует счетная модель $\mathfrak{B} \supseteq \mathfrak{A}_m$ теории T, для которой $\mathfrak{B} \models \Phi_0\left(\pi_1^n(\varphi m), \ldots, \pi_n^n(\varphi m)\right)$,

то в качестве $\mathfrak{A}_{m+1}$ берем модель T, удовлетворяющую условию 1) при $k=m+1$, для которой $\mathfrak{A}_m \subseteq \mathfrak{A}_{m+1}$ и $\mathfrak{A}_{m+1} \models \Phi_0(\pi_1^n(\varphi m), \ldots, \pi_n^n(\varphi m))$.

Рассмотрим систему $\mathfrak{A}_\omega = \bigcup\limits_{m\in\omega} \mathfrak{A}_m$, которая в силу $\forall\exists$-аксиоматизируемости T является моделью T (предложение 25.4 б)). Так как $\Phi_0 \in G$, то существуют модели $\mathfrak{A} \subseteq \mathfrak{B}$, и для $a_1, \ldots, a_n \in A$ имеем $\mathfrak{B} \models \Phi_0(a_1, \ldots, a_n)$ и $\mathfrak{A} \models \neg\,\Phi_0(a_1, \ldots, a_n)$. Взяв соответствующие счетные элементарные подсистемы, можно считать, что $\mathfrak{A}$ и $\mathfrak{B}$ счетны, а в силу категоричности T в счетной мощности можно считать, что $\mathfrak{A} = \mathfrak{A}_\omega$. Так как $A_\omega \subseteq \omega$, то из условия на φ следует, что $\varphi m_0 = \langle a_1, \ldots, a_n\rangle \in (A_{m_0})^n$ для некоторого $m_0 \in \omega$. Так как $\mathfrak{A}_{m_0} \subseteq \mathfrak{A}_\omega \subseteq \mathfrak{B}$, то из свойства 3) получаем $\mathfrak{A}_{m_0+1} \models \Phi_0(a_1, \ldots, a_n)$, следовательно, имеем $\mathfrak{A}_{m_0+1} \models \Psi_0(b, a_1, \ldots, a_n)$ для некоторого $b \in \omega$. Это противоречит тому, что $\mathfrak{A}_\omega \models \neg\,\exists y \Psi_0(y, a_1, \ldots, a_n)$ и Ψ_0 сохраняется при переходе к надсистемам. □

Отметим, что условие $\forall\exists$-аксиоматизируемости теории T в предыдущем предложении является также необходимым для модельной полноты T. А именно, можно доказать обращение предложения 25.4 б): если аксиоматизируемый класс K замкнут относительно объединений систем, то K $\forall\exists$-аксиоматизируем. Поэтому любая модельно полная теория $\forall\exists$-аксиоматизируема.

Теория плотно упорядоченных множеств без первого и последнего элемента является категоричной в счетной мощности (предложение 15.4) и некатегорична ни в какой бесконечной несчетной мощности (упражнение 1). Теория алгебраически замкнутых полей характеристики 0 категорична во всех бесконечных несчетных мощностях и некатегорична в счетной мощности. Легко строятся примеры полных теорий, категоричных во всех бесконечных мощностях, и теорий, некатегоричных во всех бесконечных мощностях. Как показал М. Морли, других случаев «распределения» категоричности для полных теорий счетной сигнатуры с бесконечными моделями не существует.

Оставшуюся часть параграфа мы посвятим следующей теореме, доказанной Е. А. Палютиным. В ее доказательстве находят применение многие результаты данной главы, а также иллюстрируется важный метод теории моделей — метод минимальных множеств.

Теорема 15. *Если квазимногообразие K категорично в счетной мощности, то оно категорично во всех неединичных мощностях.*

Класс неодноэлементных систем из K обозначим через K_+. Пусть в дальнейшем K — счетно категоричное квазимногообразие сигнатуры Σ, для которого K_+ не пуст. Элементы классов K, K_+ и K_∞ будут называться соответственно K-системами, K_+-системами и K_∞-системами. Под формулой мы будем понимать, если не оговорено противное, формулу сигнатуры Σ. В дальнейшем, если не оговорено противное, буквами $\mathfrak{A}$, $\mathfrak{B}$ будут обозначаться K-системы. Через $\overline{w}$ обозначаем упорядоченный набор $\langle w_1, \ldots, w_n\rangle$, при этом пишем $\overline{w} \in A$, если $w_1, \ldots, w_n \in A$, и $\Phi(\overline{w})$ вместо $\Phi(w_1, \ldots, w_n)$. Если $\Phi(y, \overline{x})$ — формула, $\overline{a} \in A$, то через $\Phi(\mathfrak{A}, \overline{a})$ обозначается множество $\{b \in A \mid \mathfrak{A} \models \Phi(b, \overline{a})\}$. Если $t(y_1, \ldots, y_m, \overline{x})$ — терм, $\overline{a} \in A$ и $X_1 \subseteq A, \ldots, X_m \subseteq A$, то через $t^{\mathfrak{A}}(X_1, \ldots, X_m, \overline{a})$ обозначается множество

$$\{b_0 \in A \mid \text{существуют } b_1 \in X_1, \ldots, b_m \in X_m \text{ такие, что } b_0 = t^{\mathfrak{A}}(b_1, \ldots, b_m, \overline{a})\}.$$

Если $X_1 = \ldots = X_m = X$, то вместо $t^{\mathfrak{A}}(X_1, \ldots, X_m, \overline{a})$ пишем $t^{\mathfrak{A}}(\overline{X}, \overline{a})$. Для сокращения записи мы будем часто опускать кванторы всеобщности в записи квазитождеств, т. е. обозначать квазитождество $\forall x_1 \ldots \forall x_n \Phi(x_1, \ldots, x_n)$ через $\Phi(x_1, \ldots, x_n)$. Для простоты обозначений мы будем также отождествлять «диагональные» элементы $f_a \in A^I$, которые тождественно равны $a \in A$ на I, с элементом $a \in A$. Поэтому система $\mathfrak{A}$ будет считаться подсистемой своей декартовой степени $\mathfrak{A}^I$. Это возможно в силу того, что отображение, сопоставляющее элементу $a \in A$ элемент $f_a \in A^I$, является изоморфизмом $\mathfrak{A}$ на подсистему диагональных элементов $\mathfrak{A}^I$.

В силу предложений 1 и 2 теория $\mathrm{Th}(K_\infty)$ является полной и модельно полной. Из предложений 25.4 а) и 25.5 а) получаем, что класс K замкнут относительно подсистем и декартовых произведений. В частности, из $K_+ \neq \varnothing$ следует $K_\infty \neq \varnothing$.

Лемма 1. а) *Если предложение Φ условно фильтруется вместе со своим отрицанием $\neg\Phi$ и истинно на некоторой K_+-системе $\mathfrak{A}$, то оно истинно на любой K_+-системе. Фильтрующееся предложение и квазитождество условно фильтруются вместе со своими отрицаниями.*

б) *Для любой K-системы $\mathfrak{A}$ и любого конечного множества $X \subseteq A$ система $\mathfrak{A}(X)$ конечна.*

Доказательство. а) Если предложение Φ ложно в K_+-системе $\mathfrak{B}$, то из условной фильтруемости Φ и $\neg\Phi$ следует, что Φ истинно в $\mathfrak{A}^\omega$ и ложно в $\mathfrak{B}^\omega$. Это противоречит полноте $\mathrm{Th}(K_\infty)$. Если Φ — фильтрующаяся формула, то условная фильтруемость $\neg\Phi$ очевидна. Условная фильтруемость квазитождества показана в доказательстве предложения 25.5 а). Отрицание квазитождества Φ эквивалентно предложению $\exists x_1 \ldots \exists x_n (\Phi_1 \wedge \wedge \neg \Phi_2)$, где Φ_1, Φ_2 — фильтрующиеся формулы. По лемме 17.2 $\neg\Phi$ условно фильтруется.

б) Пусть $\mathfrak{A}(a_1, \ldots, a_n)$ бесконечна. Для каждого $a \in A(a_1, \ldots, a_n)$ существует такой терм $t_a(v_1, \ldots, v_n)$, что $t_a^{\mathfrak{A}}(a_1, \ldots, a_n) = a$. Тогда формулы $v_{n+1} \approx t_a(v_1, \ldots, v_n)$, $a \in A(a_1, \ldots, a_n)$ будут попарно неэквивалентными в $\mathrm{Th}(\mathfrak{A}(a_1, \ldots, a_n)) = \mathrm{Th}(K_\infty)$. Так как $\mathrm{Th}(K_\infty)$ ω-категорична, то это противоречит теореме 14. □

Лемма 2. *Пусть $\Phi(y, \bar{x})$ — фильтрующаяся формула, $\mathfrak{A} \in K_+$, $\bar{a} = \langle a_1, \ldots, a_n\rangle \in A$ и $\Phi(\mathfrak{A}, \bar{a})$ содержит не менее двух элементов. Тогда*

а) *существует такой терм $t(\bar{y}, \bar{x})$, что $t^{\mathfrak{A}}(\overline{\Phi(\mathfrak{A}, \bar{a})}, \bar{a}) = A$;*

б) *для любой $\mathfrak{B} \in K_+$ и $\bar{b} = \langle b_1, \ldots, b_n\rangle \in B$ множество $\Phi(\mathfrak{B}, \bar{b})$ содержит не менее двух элементов или пусто.*

Доказательство. а) Докажем сначала, что если $\Phi(\mathfrak{A}, \bar{a})$ бесконечно, то множество $X = \Phi(\mathfrak{A}, \bar{a}) \cup \{a_1, \ldots \ldots, a_n\}$ порождает $\mathfrak{A}$. Пусть $\{t_i(v_1, \ldots, v_i) \mid 0 < i < \omega\}$ — нумерация всех термов. Для каждого $i \in \omega$, $i > n$, рассмотрим формулу

$$\Psi_i(v_0, v_1, \ldots, v_n) = \exists v_{n+1} \exists v_{n+2} \ldots \\ \ldots \exists v_i \Big(\bigvee_{j \leqslant i} v_0 \approx t_j \wedge \bigwedge_{n < k \leqslant i} \Phi(v_k, v_1, \ldots, v_n)\Big),$$

истинность которой на системе $\mathfrak{B}$ при интерпретации $\gamma\colon \{v_0, \ldots, v_n\} \to B$ равносильна тому, что $\gamma(v_0)$ есть значение терма $t_j^{\mathfrak{B}}(\gamma(v_1), \ldots, \gamma(v_n), b_{n+1}, \ldots, b_j)$, где $j \leqslant i$ и $b_{n+1}, \ldots, b_j \in \Phi(\mathfrak{B}, \gamma(v_1), \ldots, \gamma(v_n))$. Ясно, что для любого $b \in A(X)$ существует $i \in \omega$, $i \geqslant n$, для которого $\mathfrak{A}(X) \models \Psi_i(b, \bar{a})$. По теореме 14 существует такое конечное множество $\{i_1, \ldots, i_k\}$, что для любого $i \in \omega$

$\mathrm{Th}(K_\infty) \rhd \Psi_i \to (\Psi_{i_1} \vee \ldots \vee \Psi_{i_k})$. Тогда в $\mathfrak{A}(X)$ истинно $\forall v_0 (\Psi_{i_1}(v_0, \bar{a}) \vee \ldots \vee \Psi_{i_k}(v_0, \bar{a}))$. Так как $\mathfrak{A}(X) \prec \mathfrak{A}$, то эта формула истинна в $\mathfrak{A}$, откуда получаем, что $\mathfrak{A}$ порождается множеством X. Предположим, что а) ложно. Тогда существуют такие $b_i \in A$, $n \leqslant i \in \omega$, что $t_i^{\mathfrak{A}}(\bar{a}, a_{n+1}, \ldots, a_i) \neq b_i$ для любых $a_{n+1}, \ldots, a_i \in \Phi(\mathfrak{A}, \bar{a})$. Тогда множество $Y = \Phi(\mathfrak{A}^\omega, \bar{a}) = (\Phi(\mathfrak{A}, \bar{a}))^\omega$ бесконечно и $g \notin A^\omega(Y \cup \{a_1, \ldots, a_n\})$, где $gi = b_i$, $i \in \omega$. Это противоречит предыдущему.

б) Предположим, что существуют такие $\mathfrak{B} \in K_+$ и $\bar{b} \in B$, что $\Phi(\mathfrak{B}, \bar{b}) = \{d_0\}$. В силу фильтруемости Φ множество $\Phi(\mathfrak{A} \times \mathfrak{B}, \bar{a} \times \bar{b})$ равно $\Phi(\mathfrak{A}, \bar{a}) \times \{d_0\}$, где $\bar{a} \times \bar{b} = \langle\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle\rangle$. Пусть $a_0 \in A$; $d_1, d_2 \in B$, $d_1 \neq d_2$, тогда по а) имеем

$$t(\langle c_1, d_0\rangle, \ldots, \langle c_m, d_0\rangle, \bar{a} \times \bar{b}) = \langle a_0, d_1\rangle,$$
$$t(\langle c_1', d_0\rangle, \ldots, \langle c_m', d_0\rangle, \bar{a} \times \bar{b}) = \langle a_0, d_2\rangle$$

для некоторого терма $t(y_1, \ldots, y_m, \bar{x})$ и некоторых $c_1, \ldots, c_m, c_1', \ldots, c_m' \in \Phi(\mathfrak{A}, \bar{a})$. Из определения операций на $\mathfrak{A} \times \mathfrak{B}$ получаем $t(d_0, \ldots, d_0, \bar{b}) = d_1$ из первого равенства и $t(d_0, \ldots, d_0, \bar{b}) = d_2$ из второго равенства, что противоречит условию $d_1 \neq d_2$. □

Рассмотрим максимальное совместное с $\mathrm{Th}(K)$ множество

$$X^* = \{\neg\, v_1 \approx v_2\} \cup \{\Phi_i(v_1, v_2) \mid i \in \omega\},$$

где $\Phi_i(v_1, v_2)$, $i \in \omega$,— атомарные формулы. Пусть сигнатура Σ^* получается из Σ добавлением двух новых констант c_1, c_2. Рассмотрим квазимногообразие K^* сигнатуры Σ^*, множество аксиом которого состоит из аксиом K, а также квазитождеств $v_1 \approx v_1 \to \Phi(c_1, c_2)$ для атомарных формул $\Phi(v_1, v_2) \in X^*$ и квазитождеств $\Phi(c_1, c_2) \to v_1 \approx v_2$ для атомарных $\Phi(v_1, v_2) \notin X^*$.

Лемма 3. а) *Для любой K_+-системы $\mathfrak{A}$ существует такая K^*-система $\mathfrak{A}^*$, что $\mathfrak{A}^* \upharpoonright \Sigma = \mathfrak{A}$.*

б) *Квазимногообразие K^* категорично в счетной мощности.*

Доказательство. а) В силу максимальности X^* достаточно показать, что X^* выполняется в любой K_+-системе $\mathfrak{A}$. Из теоремы 14 следует существование такого $n_0 \in \omega$, что $\mathrm{Th}(K_\infty) \rhd (\Phi_0 \wedge \ldots \wedge \Phi_{n_0}) \to \Phi_i$ для всех

$i \in \omega$. Так как $K_\infty \neq \varnothing$, то по лемме 1 а) $\mathfrak{A} \models (\Phi_0 \wedge \ldots \ldots \wedge \Phi_{n_0}) \to \Phi_i$ для всех $i \in \omega$. Поэтому достаточно показать, что в $\mathfrak{A}$ истинно предложение $\exists v_1 \exists v_2 \Psi(v_1, v_2)$, где $\Psi(v_1, v_2)$ равна $\neg v_1 \approx v_2 \wedge \Phi_0 \wedge \ldots \wedge \Phi_{n_0}$. Пусть X^* выполняется в K-системе $\mathfrak{B}$. Тогда $|B| > 1$ и $\exists v_1 \exists v_2 \Psi(v_1, v_2)$ истинно в K_∞-системе $\mathfrak{B}^\omega$. В силу полноты $\mathrm{Th}(K_\infty)$ имеем $\mathfrak{A}^\omega \models \Psi(f_1, f_2)$ для некоторых $f_1, f_2 \in A^\omega$. Так как $\mathfrak{A}^\omega \models \neg f_1 \approx f_2$, то $f_1 i_0 \neq f_2 i_0$ для некоторого $i_0 \in \omega$. Из фильтруемости $\Phi_0 \wedge \ldots \wedge \Phi_{n_0}$ получаем, что $\mathfrak{A} \models \Psi(f_1 i_0, f_2 i_0)$.

б) Как было показано в доказательстве теоремы 14, каждая счетная K_∞-система является насыщенной. Так как любая K_∞^*-система $\mathfrak{A}^*$ является обогащением некоторой K_∞-системы $\mathfrak{A}$ на две константы, то $\mathfrak{A}^*$ является насыщенной. Поэтому в силу предложения 28.4 достаточно показать, что любые K_∞^*-системы $\mathfrak{A}$, $\mathfrak{B}$ элементарно эквивалентны. Пусть $\nu^{\mathfrak{A}}(c_1) = a_1$, $\nu^{\mathfrak{A}}(c_2) = a_2$, $\nu^{\mathfrak{B}}(c_1) = b_1$ и $\nu^{\mathfrak{B}}(c_2) = b_2$. Так как квазитождества $\Phi(c_1, c_2) \to v_1 \approx v_2$ эквивалентны в $\mathrm{Th}(K_+^*)$ предложению $\neg \Phi(c_1, c_2)$, то из аксиом K^* следует, что отображение, сопоставляющее элементам a_1, a_2 соответственно элементы b_1, b_2, продолжается до изоморфизма $f\colon \mathfrak{A}_0 \simeq \mathfrak{B}_0$, где $\mathfrak{A}_0 = \mathfrak{A}(a_1, a_2) \restriction \Sigma$ и $\mathfrak{B}_0 = \mathfrak{B}(b_1, b_2) \restriction \Sigma$. Тогда f продолжается до изоморфизма K_∞-систем $\mathfrak{A}_0^\omega \subseteq \mathfrak{A}^\omega \restriction \Sigma$ и $\mathfrak{B}_0^\omega \subseteq \mathfrak{B}^\omega \restriction \Sigma$. Следовательно, $\langle \mathfrak{A}_0^\omega, a_1, a_2 \rangle \equiv \langle \mathfrak{B}_0^\omega, b_1, b_2 \rangle$ и в силу модельной полноты $\mathrm{Th}(K_\infty)$ получаем $\langle \mathfrak{A}^\omega \restriction \Sigma, a_1, a_2 \rangle \equiv \langle \mathfrak{B}^\omega \restriction \Sigma, b_1, b_2 \rangle$. Снова из модельной полноты $\mathrm{Th}(K_\infty)$ получаем $\langle \mathfrak{A} \restriction \Sigma, a_1, a_2 \rangle \equiv \langle \mathfrak{B} \restriction \Sigma, b_1, b_2 \rangle$, следовательно, имеет место $\mathfrak{A} \equiv \mathfrak{B}$. □

В дальнейшем будем предполагать, что сигнатура Σ содержит константы c_1, c_2 и предложение $\neg c_1 \approx c_2$ истинно в любой K_+-системе. Такое предположение для доказательства теоремы 15 можно сделать в силу леммы 3. Тогда для любой K_+-системы определена K_+-система $\mathfrak{A}(\varnothing)$, носитель которой состоит из значений в $\mathfrak{A}$ константных термов. Из леммы 1 а) следует, что $\mathfrak{A}(\varnothing) \simeq \mathfrak{B}(\varnothing)$ для любых K_+-систем $\mathfrak{A}$ и $\mathfrak{B}$. Множество $X \subseteq A$ назовем атомно минимальным в K-системе $\mathfrak{A}$, если $|X| > 1$ и для любой атомарной формулы $\Phi(y, \bar{x})$, любого $\bar{a} \in A$ множество $X \cap \Phi(\mathfrak{A}, \bar{a})$ пусто, одноэлементно или равно X.

Лемма 4. *Существует такая фильтрующаяся формула $\Phi^*(v_1)$, что для любой K_+-системы $\mathfrak{A}$ множество $\Phi^*(\mathfrak{A})$ атомно минимально в $\mathfrak{A}$.*

Доказательство. Пусть $\mathfrak{B} \in K_+$. По лемме 1 б) K_+-система $\mathfrak{B}_0 = \mathfrak{B}(\varnothing)$ конечна. Рассмотрим такую конъюнкцию $\Phi^*(v_1)$ атомарных формул, что $|\Phi^*(\mathfrak{B}_0)| > 1$ и для любой атомарной формулы $\Phi(v_1)$ множество $\Phi^*(\mathfrak{B}_0) \cap \Phi(\mathfrak{B}_0)$ пусто, одноэлементно или равно $\Phi^*(\mathfrak{B}_0)$. Пусть $\Phi(y, \bar{x})$ — атомарная формула. Так как любой элемент $b \in B_0$ является значением в $\mathfrak{B}_0$ константного терма, то множество $\Phi^*(\mathfrak{B}_0) \cap \Phi(\mathfrak{B}_0, \bar{b})$ пусто, одноэлементно или равно $\Phi^*(\mathfrak{B}_0)$ для любого $\bar{b} \in B_0$. В силу леммы 2 б) не существует таких $\bar{a}, \bar{b} \in B_0$, что $\Phi^*(\mathfrak{B}_0) \subseteq \Phi(\mathfrak{B}_0, \bar{b})$ и $\Phi^*(\mathfrak{B}_0) \cap \Phi(\mathfrak{B}_0, \bar{a})$ одноэлементно. Таким образом, в $\mathfrak{B}_0$ истинно одно из следующих квазитождеств:

а) $(\Phi^*(v_1) \wedge \Phi(v_1, \bar{x}) \wedge \Phi^*(v_2) \wedge \Phi(v_2, \bar{x})) \to v_1 \approx v_2$;

б) $(\Phi^*(v_1) \wedge \Phi(v_1, \bar{x}) \wedge \Phi^*(v_2)) \to \Phi(v_2, \bar{x})$.

По лемме 1 а) одно из этих квазитождеств истинно в любой K_+-системе $\mathfrak{A}$. Так как $\Phi^*(\mathfrak{A}) \supseteq \Phi^*(\mathfrak{A}(\varnothing))$ и $\mathfrak{A}(\varnothing) \simeq \mathfrak{B}_0$, то $|\Phi^*(\mathfrak{A})| > 1$. Следовательно, $\Phi^*(\mathfrak{A})$ атомно минимально в $\mathfrak{A}$. □

Пусть $\mathfrak{A} \in K_+$. Множество $X \subseteq \Phi^*(\mathfrak{A})$ назовем базисом для $\mathfrak{A}$, если выполняются следующие условия:

1) $\mathfrak{A}(X) = \mathfrak{A}$;

2) если $a_1, \ldots, a_n$ — попарно различные элементы X и $\mathfrak{A} \models \Phi(a_1, \ldots, a_n)$ для некоторой атомарной формулы $\Phi(v_1, \ldots, v_n)$, то в любой K_+-системе истинно квазитождество $(\Phi^*(v_1) \wedge \ldots \wedge \Phi^*(v_n)) \to \Phi(v_1, \ldots, v_n)$.

Лемма 5. а) *Если $\Phi(y, \bar{x})$ — фильтрующаяся формула и $\Phi(\mathfrak{A}, \bar{a}) = \{b\}$ для K_+-системы $\mathfrak{A}$ и $\bar{a} \in A$, то $t^{\mathfrak{A}}(\bar{a}) = b$ для некоторого терма $t(\bar{x})$.*

б) *Каждая K_+-система $\mathfrak{A}$ имеет базис.*

Доказательство. а) Пусть $\mathfrak{A}_0 = \mathfrak{A}(\bar{a})$. Если а) не выполняется, что предложение $\exists y \Phi(y, \bar{a})$ в K_∞-системе $\mathfrak{A}_0^\omega$ ложно, а в $\mathfrak{A}^\omega \supseteq \mathfrak{A}_0^\omega$ истинно. Это противоречит модельной полноте $\mathrm{Th}(K_\infty)$.

б) Пусть $X \subseteq \Phi^*(\mathfrak{A})$ — максимальное множество, удовлетворяющее условию 2). В силу леммы 2 а) достаточно показать, что $\mathfrak{A}(X)$ содержит $\Phi^*(\mathfrak{A})$. Предположим, что существует $a_0 \in \Phi^*(\mathfrak{A}) \setminus A(X)$. Пусть $\mathfrak{A} \not\models \Phi(a_0, a_1, \ldots, a_n)$ для атомарной $\Phi(v_0, v_1, \ldots, v_n)$ и попарно различных $a_1, \ldots, a_n \in X$. В силу а) и атомной минимальности $\Phi^*(\mathfrak{A})$ имеем $\Phi^*(\mathfrak{A}) \subseteq \Phi(\mathfrak{A}, a_1, \ldots, a_n)$. Так как $\Phi^*(\mathfrak{A}(\varnothing)) \neq \varnothing$, то $\mathfrak{A} \models \Phi^*(t_0) \wedge \Phi(t_0, a_1, \ldots, a_n)$ для некоторого константного терма t_0. Так как X удовлетворяет условию 2) и $\Phi^*(t_0) \in \mathrm{Th}(K_+)$ (лемма 1 а)), то множество $\Phi^*(\mathfrak{B}) \wedge \Phi(\mathfrak{B}, b_1, \ldots, b_n)$ не пусто для любой K_+-системы $\mathfrak{B}$ и любых $b_1, \ldots, b_n \in \Phi^*(\mathfrak{B})$. Поэтому в силу леммы 2 б) из $|\Phi(\mathfrak{A}, a_1, \ldots, a_n) \cap \Phi^*(\mathfrak{A})| > 1$ и атомной минимальности $\Phi^*(\mathfrak{B})$ получаем истинность $\Phi(b_0, b_1, \ldots, b_n)$ в любой K_+-системе $\mathfrak{B}$ для любых $b_0, b_1, \ldots, b_n \in \Phi^*(\mathfrak{B})$. Следовательно, $X \cup \{a_0\}$ удовлетворяет условию 2), что противоречит максимальности X. $\square$

Доказательство теоремы 15. Пусть $\mathfrak{A}$, $\mathfrak{B}$ — две K_+-системы одной мощности $\varkappa$ и X, Y — их базисы. Из определения базиса следует, что любое разнозначное отображение $f\colon X \to Y$ продолжается единственным образом до изоморфизма $\mathfrak{A}$ на $\mathfrak{B}(f(X))$. Поэтому в силу свойства 1) базиса достаточно заметить, что $|X| = |Y|$. Если $\varkappa \geqslant \omega$, то из леммы 1 б) получаем $|X| = |Y| = \varkappa$. Если $\varkappa < \omega$ и $|X| \leqslant |Y|$, то $\mathfrak{A}$ изоморфна подсистеме $\mathfrak{B}_1 \subseteq \mathfrak{B}$. Так как $|B_1| = |A| = |B|$, то $\mathfrak{B}_1 = \mathfrak{B}$. $\square$

Упражнения

1. Показать, что теория T_0 плотных линейных порядков без первого и последнего элемента не категорична ни в какой бесконечной несчетной мощности. (Указание. Пусть $\mathfrak{A}$ — модель T_0 мощности $\varkappa > \omega$ и $\mathfrak{A}_0$ — счетная модель T_0, для которой $A_0 \cap A = \varnothing$; рассмотрим модель $\mathfrak{A}_1$ с носителем A^2 и отношением $\langle a, b\rangle \leqslant^{\mathfrak{A}_1} (c, d) \Leftrightarrow \left(a <^{\mathfrak{A}} c \text{ или } \left(a = c \text{ и } b \leqslant^{\mathfrak{A}} d\right)\right)$ и модель $\mathfrak{A}_2$ с носителем $A \cup A_0$ и отношением

$$a \leqslant^{\mathfrak{A}_2} b \Leftrightarrow \Big(\left(a \in A \text{ и } b \in A_0\right) \text{ или } \left(a, b \in A \text{ и } a \leqslant^{\mathfrak{A}} b\right) \text{ или } \left(a, b \in A_0 \text{ и } a \leqslant^{\mathfrak{A}_0} b\right)\Big);$$

тогда $\mathfrak{A}_1$ и $\mathfrak{A}_2$ неизоморфны.)

2. Показать, что многообразие булевых алгебр категорично во всех конечных мощностях и некатегорично во всех бесконечных.

3. Доказать, что многообразие M с аксиомами (кванторы всеобщности опущены)

1) $f(g_1(x), g_2(x)) \approx x$,
2) $f(x, y) \approx f(g_1(x), g_2(y))$,
3) $g_1(f(g_1(x), g_1(y))) \approx g_1(x)$,
4) $g_2(f(g_1(x), g_1(y))) \approx g_1(y)$,
5) $g_i(g_k(x)) \approx g_k(x)$, $i, k \in \{1, 2\}$,

категорично во всех мощностях. (Указание. Показать, что $\nu^{\mathfrak{A}}(f)$ для любой $\mathfrak{A} \in M$ разнозначно отображает $\left(g_1^{\mathfrak{A}}[A]\right)^2$ на A

и любое разнозначное отображение $h\colon g_1^{\mathfrak{A}}[A] \to g_1^{\mathfrak{B}}[B]$ для $\mathfrak{A}, \mathfrak{B} \in M$ продолжается до изоморфизма системы $\mathfrak{A}$ на $\mathfrak{B}\left(h\left(g_1^{\mathfrak{A}}[A]\right)\right)$, переводящего a в $f^{\mathfrak{B}}\left(hg_1^{\mathfrak{A}}(a),\ hg_2^{\mathfrak{A}}(a)\right)$.)

4. Построить пример, показывающий, что в теореме 15 нельзя утверждать, что K категорично также в мощности 1.

5. Обобщить предложение 2 на теории, категоричные в бесконечной мощности $\varkappa$, и получить тем самым теорему Линдстрёма в полном объеме. (Указание. Применить метод предложения 2 с заменой ω на $\varkappa$ и показать, что если формула Φ не сохраняется при переходе к подмоделям теории T, то Φ не сохраняется при переходе к подмоделям мощности $\varkappa$.)

Глава 6

ТЕОРИЯ ДОКАЗАТЕЛЬСТВ

§ 30. Генценовская система G

Изученные ранее исчисления представляют собой естественные формализации правил логики. Однако для более глубокого изучения самого понятия доказательства более удобными являются другие формы исчислений. В настоящем параграфе мы изучим одно из таких исчислений G, близкое к исчислению, предложенному Генценом.

Алфавит исчисления G отличается от алфавита исчисления предикатов, изученного в главе 4, отсутствием знаков импликации и равенства. Понятие *формулы исчисления* G отличается от соответствующего понятия главы 4: 1) отсутствием правил образования формул вида $(\Phi \to \Psi)$, $t_1 \approx t_2$ и 2) выполнением *условия несмешанности переменных*, которое означает отсутствие переменных, имеющих как свободные, так и связанные вхождения в формулу. *Секвенции* G — это выражения вида $\Gamma \vdash \Theta$, где Γ и Θ — конечные последовательности формул исчисления G такие, что для $\Gamma \vdash \Theta$ выполнено условие несмешанности переменных, определяемое для секвенций так же, как и для формул. Соглашения о сокращенной записи формул и некоторые обозначения, используемые ниже, имеют тот же смысл, что и в главе 4.

Определение. *Аксиомами исчисления* G являются секвенции вида $\Phi, \Gamma \vdash \Theta, \Phi$, где Φ — атомарная формула, Γ и Θ — последовательности (быть может, пустые) атомарных формул.

Определение. *Правилами вывода исчисления* G будут следующие:

1. $\dfrac{\Gamma \vdash \Theta, \Phi; \; \Gamma \vdash \Theta, \Psi}{\Gamma \vdash \Theta, \Phi \wedge \Psi}$,   2. $\dfrac{\Phi, \Psi, \Gamma \vdash \Theta}{\Phi \wedge \Psi, \Gamma \vdash \Theta}$,

3. $\dfrac{\Gamma \vdash \Theta, \Phi, \Psi}{\Gamma \vdash \Theta, \Phi \vee \Psi}$,   4. $\dfrac{\Phi, \Gamma \vdash \Theta; \; \Psi, \Gamma \vdash \Theta}{\Phi \vee \Psi, \Gamma \vdash \Theta}$,

5. $\dfrac{\Phi, \Gamma \vdash \Theta}{\Gamma \vdash \Theta, \neg \Phi}$,   6. $\dfrac{\Gamma \vdash \Theta, \Phi}{\neg \Phi, \Gamma \vdash \Theta}$,

7. $\dfrac{\Gamma \vdash \Theta, (\Phi)^x_t}{\Gamma \vdash \Theta, \exists x \Phi}$,

8. $\dfrac{[\Phi]^x_y, \Gamma \vdash \Theta}{\exists x \Phi, \Gamma \vdash \Theta}$, где y не входит свободно в формулы из Γ и Θ,

9. $\dfrac{\Gamma \vdash \Theta, [\Phi]^x_y}{\Gamma \vdash \Theta, \forall x \Phi}$, где y не входит свободно в формулы из Γ и Θ,

10. $\dfrac{(\Phi)^x_t, \Gamma \vdash \Theta}{\forall x \Phi, \Gamma \vdash \Theta}$,

11. $\dfrac{\Gamma \vdash \Delta, \Phi, \Psi, \Delta}{\Gamma \vdash \Delta, \Psi, \Phi, \Theta}$,

12. $\dfrac{\Gamma, \Phi, \Psi, \Delta \vdash \Theta}{\Gamma, \Psi, \Phi, \Delta \vdash \Theta}$,

13. $\dfrac{\Gamma \vdash \Theta, \Phi, \Phi}{\Gamma \vdash \Theta, \Phi}$,

14. $\dfrac{\Phi, \Phi, \Gamma \vdash \Theta}{\Phi, \Gamma \vdash \Theta}$.

Правила 1—10 называются *основными*, а правила 11—14 — *структурными*. Понятие доказательства (линейного и в виде дерева) определяется так же, как для исчисления предикатов.

Отметим ряд особенностей этого исчисления. Во-первых, это большая симметричность правых и левых частей секвенции $\Gamma \vdash \Theta$ (называемых *заключением* или *сукцедентом* (Θ) и *посылкой* или *антецедентом* (Γ) соответственно). Во-вторых, каждое основное (в отличие от структурных) правило под чертой содержит более сложную формулу, получаемую из формул посылки (эту формулу будем называть *главной формулой правила*). Третья особенность — свойство подформульности — требует введения новых понятий.

На вхождениях I секвенций в доказательство D в виде дерева определим операцию l следующим образом: если I — заключительное вхождение в D, то $l(I)=I$; если I содержится в переходе P над чертой, то $l(I)$ есть вхождение секвенции из перехода P под чертой. На вхождениях J формул в дерево D определим операцию S следующим образом: если J содержится во вхождении I некоторой секвенции, то $S(J)$ входит в секвенцию $l(I)$; если J входит в последовательность Γ или Θ (или Δ) в секвенции I, то $S(J)$ равно тому же вхождению формулы в Γ или Θ (или Δ), но уже в секвенции $l(I)$; для основных правил, если J не входит в Γ и Θ, то $S(J)$ есть главная формула перехода; для структурных правил, если J не входит в Γ, Θ или Δ, то в обозначениях правил 11—14 имеем $S(\Phi)=\Phi$, $S(\Psi)=\Psi$. Если для некоторого положительного n имеем $l^n(I_1)=I_2$, то говорим, что *вхождение* I_1 *в дереве* D *расположено выше вхождения* I_2. (Здесь через $l^n(I)$ обозначается значение $l\ldots$ $\ldots l(I)$, где l повторено n раз.) Если для некоторого положительного n имеем $S^n(J_1)=J_2$, то говорим, что J_1 является *предком* J_2, а J_2 является *потомком* J_1.

Если Φ — формула исчисления G, x — переменная, t — терм, то будем говорить, что *терм* t *свободен для переменной* x *в формуле* Φ, если Φ не имеет свободных вхождений переменной x или если ни одна переменная терма t не имеет связанных вхождений в Φ.

Расширим понятие подформулы, считая *обобщенными подформулами* формул $\exists x\Phi$, $\forall x\Phi$ и формулы $(\Phi)_t^x$, где терм t свободен для x в Φ.

З а м е ч а н и е. Если Ψ есть обобщенная подформула формулы Φ и переменная v имеет связанное вхождение в Ψ, то она имеет связанное вхождение и в Φ.

Справедливо следующее свойство подформульности.

Л е м м а 1. *Отношение предок — потомок удовлетворяет следующим условиям: если вхождение секвенции* C_0 *находится выше вхождения секвенции* C_1, *то для любого вхождения формулы в* C_0 *существует единственный ее потомок в* C_1; *для любого вхождения формулы в* C_1 *существует по крайней мере один его предок в* C_0. *Любой предок является обобщенной подформулой потомка.*

Справедливость леммы легко устанавливается индукцией. □

Хотя в определении понятий формулы и секвенции G предполагалось условие несмешанности переменных, этого не предполагается в определении доказательства (в виде дерева). Тем не менее можно даже требовать большего. Будем говорить, что доказательство (в виде дерева) D обладает *свойством чистоты переменных*, если для дерева D выполнено условие несмешанности переменных и для любого перехода в D по правилам 8 или 9 соответствующая переменная y встречается только в секвенциях, находящихся выше заключительной секвенции этого перехода.

Л е м м а 2. *Для любой доказуемой в* G *секвенции существует доказательство этой секвенции со свойством чистоты переменных.*

Пусть D — доказательство секвенции C в G. Скажем, что переменная y *исчезает в переходе* P дерева D, если y имеет по крайней мере одно свободное вхождение в секвенцию над чертой и не имеет свободных вхождений в секвенцию под чертой в этом переходе. Заметим, что переменная может исчезать лишь в переходах, соответствующих одному из правил 7—10. Скажем, что переменная *y исчезает правильно*, если y исчезает в некотором переходе и имеет вхождения в D только в секвенции, находящиеся выше нижней секвенции этого перехода. Заметим, что если переменная y исчезает правильно, то она имеет только свободные вхождения в дереве D. Если все исчезающие переменные в D исчезают правильно, то D имеет свойство чистоты переменных. Если D имеет неправильно исчезающие переменные, то найдем переход P, в котором некоторая переменная y исчезает неправильно; пусть D' — *поддерево* D, соответствующее нижней секвенции этого перехода, т. е. дерево, состоящее из этой секвенции и секвенций и переходов, находящихся выше нее в D. Выберем переменную z, отличную от всех переменных в D, и заменим в D поддерево D' на дерево $[D']^y_z$, которое получается из D' заменой каждого вхождения формулы Ψ на $[\Psi]^y_z$. Легко проверить, что получившееся дерево D^* остается доказательством и это доказательство таково, что переменная z исчезает в D^* правильно. Ясно, что за конечное число таких преобразований (D на D^*) мы получим доказательство, в котором все исчезновения переменных правильные. □

Следующая лемма позволит ввести в исчисление G полезное допустимое правило (правило утончения).

Лемма 3. *Пусть* $\Gamma \vdash \Theta$ — *доказуемая секвенция и* Φ — *формула такая, что* $\Phi, \Gamma \vdash \Theta$ *является секвенцией* G, *тогда секвенции* $\Phi, \Gamma \vdash \Theta$ *и* $\Gamma \vdash \Theta, \Phi$ *доказуемы в* G.

Доказательство. Пусть $x_0, \ldots, x_n$ — все свободные переменные формулы Φ. Пусть D — доказательство секвенции $\Gamma \vdash \Theta$ со свойством чистоты переменных. Как видно из доказательства леммы 2, можно предполагать, что все исчезающие переменные в D отличны от $x_0, \ldots, x_n$.

Докажем лемму индукцией по построению формулы Φ. Если Φ атомарна, а (D, Φ) — дерево, полученное заменой каждого вхождения секвенции $\Delta \vdash \Lambda$ на вхождения секвенции $\Delta, \Phi \vdash \Lambda$, то (при сформулированных выше предположениях относительно D) дерево (D, Φ) есть доказательство секвенции $\Gamma, \Phi \vdash \Theta$. Применяя структурное правило перестановки 12 несколько раз, получим доказательство секвенции $\Phi, \Gamma \vdash \Theta$. Аналогично определяется дерево (Φ, D) ($\Delta \vdash \Lambda$ заменяется на $\Delta \vdash \Phi, \Lambda$), которое есть доказательство секвенции $\Gamma \vdash \Phi, \Theta$; использование правила 11 завершает доказательство секвенции $\Gamma \vdash \Theta, \Phi$.

Пусть $\Phi = \Phi_0 \vee \Phi_1$. По индукции из доказуемости $\Gamma \vdash \Theta$ следует доказуемость секвенций $\Phi_0, \Gamma \vdash \Theta$; $\Phi_1, \Gamma \vdash \Theta$; $\Gamma \vdash \Theta, \Phi_0$; $\Gamma \vdash \Theta, \Phi_0, \Phi_1$, тогда квазивыводы

$$\frac{\Phi_0, \Gamma \vdash \Theta;\ \Phi_1, \Gamma \vdash \Theta}{\Phi_0 \vee \Phi_1, \Gamma \vdash \Theta}, \quad \frac{\Gamma \vdash \Theta, \Phi_0, \Phi_1}{\Gamma \vdash \Theta, \Phi_0 \vee \Phi_1}$$

показывают доказуемость секвенций $\Phi_0 \vee \Phi_1, \Gamma \vdash \Theta$ и $\Gamma \vdash \Theta, \Phi_0 \vee \Phi_1$. Аналогично проверяется утверждение для $\Phi = \Phi_0 \wedge \Phi_1$ и $\Phi = \neg \Phi_0$. Для формул вида $\exists x\Phi$, $\forall x\Phi$ выбираем переменную y, не имеющую вхождений в $\exists x\Phi$, Γ, Θ, и применяем индукционное предположение к формуле $[\Phi]^x_y$. Тогда, например, из доказуемости $\Gamma \vdash \Theta$ следует доказуемость $[\Phi]^x_y, \Gamma \vdash \Theta$, и квазивывод

$$\frac{[\Phi]^x_y, \Gamma \vdash \Theta}{\exists x\Phi, \Gamma \vdash \Theta}$$

показывает, что $\exists x\Phi \vdash \Theta$ тоже доказуема. □

В заключение отметим ряд простых свойств, которыми в дальнейшем будем пользоваться без явного на них указания.

1. *Если* $\dfrac{\Gamma \vdash \Theta;\ \Lambda \vdash \Delta}{\Gamma' \vdash \Theta'}$ *есть переход, соответствующий одному из правил вывода, то для любой формулы* Φ *такой, что* $\Gamma \vdash \Theta, \Phi$ *и* $\Lambda \vdash \Phi, \Delta$ *являются секвенциями* G,

$$\frac{\Gamma \vdash \Phi, \Theta;\ \Lambda \vdash \Phi, \Delta}{\Gamma' \vdash \Phi, \Theta'}, \quad \frac{\Gamma, \Phi \vdash \Theta;\ \Lambda, \Phi \vdash \Delta}{\Gamma', \Phi \vdash \Theta'}$$

суть переходы, соответствующие тому же правилу вывода.

2. *Если* $\dfrac{\Gamma \vdash \Theta}{\Gamma' \vdash \Theta'}$ — *переход, соответствующий одному из правил вывода,* Φ — *формула такая, что* $\Gamma, \Phi \vdash \Theta$ — *секвенция* G *и переменные* x *и* y *не свободны в* Φ *в случае, когда этот переход соответствует правилу* 8 *или* 9, *то*

$$\frac{\Gamma \vdash \Phi, \Theta}{\Gamma' \vdash \Phi, \Theta'}, \quad \frac{\Gamma, \Phi \vdash \Theta}{\Gamma', \Phi \vdash \Theta'}$$

— *переходы, соответствующие тому же правилу вывода.*

3. *Если* $\dfrac{\Gamma \vdash \Theta \quad (\Lambda \vdash \Delta)}{\Gamma' \vdash \Theta'}$ — *переход, соответствующий одному из правил вывода, и* Φ *входит в* Γ' (Θ'), *то*

переход

$$\frac{\Gamma^* \vdash \Theta \quad (\Lambda^* \vdash \Delta)}{\Gamma'^* \vdash \Theta'} \quad \left(\frac{\Gamma \vdash \Theta^* \quad (\Lambda \vdash \Delta^*)}{\Gamma' \vdash \Theta'^*}\right),$$

где Γ^*, Λ^* (Θ^*, Δ^*) *получены вычеркиванием из* Γ, Λ (Θ, Δ) *предков фиксированного вхождения* Φ *в* Γ' (Θ'), *а* Γ'^* (Θ'^*) *получено из* Γ' (Θ') *вычеркиванием этого вхождения* Φ, *является либо переходом, соответствующим тому же правилу вывода, либо тривиальным переходом (т. е. секвенции над чертой совпадают с нижней секвенцией этого перехода).*

Упражнения

1. Показать, что для любой формулы Φ исчисления предикатов ИП$^\Sigma$ существует эквивалентная ей формула Ψ, удовлетворяющая условию несмешанности переменных.

2. Проверить, что любая формула ИП$^\Sigma$, находящаяся в пренексной нормальной форме, удовлетворяет условию несмешанности переменных.

3. Расширим язык исчисления G, допуская формулы и секвенции и без условия несмешанности переменных. Установить, что тождественно истинная секвенция $P(x) \vdash \exists y \forall x P(y)$ не доказуема в получившемся исчислении G^*.

§ 31. Обратимость правил

Большинство правил вывода исчисления G обладают еще одним примечательным свойством, которое можно использовать при поиске вывода в исчислении. Свойство это — обратимость, выражающаяся (несколько огрубленно) в том, что секвенция, стоящая под чертой в правиле, доказуема тогда и только тогда, когда доказуемы секвенции (секвенция), стоящие над чертой.

Сформулируем и докажем это свойство сначала для пропозициональных правил.

Предложение 1. 1) *Если доказуема секвенция* $\Gamma \vdash \Theta, \Phi \wedge \Psi$, *то доказуемы и секвенции* $\Gamma \vdash \Theta, \Phi$ *и* $\Gamma \vdash \Theta, \Psi$; 2) *если доказуема секвенция* $\Phi \wedge \Psi, \Gamma \vdash \Theta$, *то доказуема и секвенция* $\Phi, \Psi, \Gamma \vdash \Theta$; 3) *если доказуема секвенция* $\Gamma \vdash \Theta, \Phi \vee \Psi$, *то доказуема и секвенция* $\Gamma \vdash \Theta, \Phi, \Psi$; 4) *если доказуема секвенция* $\Phi \vee \Psi, \Gamma \vdash \Theta$, *то доказуемы и секвенции* $\Phi, \Gamma \vdash \Theta$ *и* $\Psi, \Gamma \vdash \Theta$; 5) *если доказуема секвенция* $\Gamma \vdash \Theta, \neg\Phi$, *то доказуема и секвенция* $\Phi, \Gamma \vdash \Theta$; 6) *если доказуема секвенция* $\neg\Phi, \Gamma \vdash \Theta$, *то доказуема и секвенция* $\Gamma \vdash \Theta, \Phi$.

Доказательство. Проверка всех утверждений предложения утомительна и однообразна. Поэтому докажем типичные случаи, например, утверждения 1) и 6). Проверку будем вести индукцией по высоте доказательства (см. также доказательство леммы 9.2).

Утверждение 1) будем доказывать в чуть более общей форме и только для формулы Φ: если секвенция $\Gamma \vdash \Theta,\ \Phi \wedge \Psi, \Lambda$ доказуема, то доказуема и секвенция $\Gamma \vdash \Theta,\ \Phi,\ \Lambda$, причем существует доказательство с меньшим числом переходов, чем в доказательстве исходной.

Пусть доказательство D секвенции $\Gamma \vdash \Theta, \Phi \wedge \Psi,\ \Lambda$ имеет вид $\dfrac{D_0;\ D_1}{C}$.

Если $\Phi \wedge \Psi$ — главная формула последнего перехода, то D_0 — доказательство секвенции $\Gamma \vdash \Theta,\ \Phi,\ \Lambda$ (в этом случае Λ — пустая последовательность формул) и D_0 имеет меньше переходов, чем D.

Если $\Phi \wedge \Psi$ — не главная формула последнего перехода, то заключительные секвенции C_0 и C_1 доказательств D_0 и D_1 имеют вид $\Gamma_0 \vdash \Theta_0, \Phi \wedge \Psi,\ \Lambda_0$ и $\Gamma_1 \vdash \Theta_1,\ \Phi \wedge \Psi,\ \Lambda_1$ соответственно, где выделенные вхождения $\Phi \wedge \Psi$ в C_0 и C_1 — это предки рассматриваемого вхождения формулы $\Phi \wedge \Psi$ в секвенцию C. По индукционному предположению существуют доказательства D_0' и D_1' секвенций $\Gamma_0 \vdash \Theta_0,\ \Phi,\ \Lambda_0$ и $\Gamma_1 \vdash \Theta_1,\ \Phi,\ \Lambda_1$ соответственно. Тогда дерево секвенций

$$\frac{D_0';\ D_1'}{\Gamma \vdash \Theta,\ \Phi,\ \Lambda}$$

будет доказательством. (Так как $\Phi \wedge \Psi$ не была главной формулой перехода

$$\frac{\Gamma_0 \vdash \Theta_0,\ \Phi \wedge \Psi,\ \Lambda_0;\ \Gamma_1 \vdash \Theta_1,\ \Phi \wedge \Psi,\ \Lambda_1}{\Gamma \vdash \Theta,\ \Phi \wedge \Psi,\ \Lambda},$$

то переход

$$\frac{\Gamma_0 \vdash \Theta_0,\ \Phi,\ \Lambda_0;\ \Gamma_1 \vdash \Theta_1,\ \Phi,\ \Lambda_1}{\Gamma \vdash \Theta,\ \Phi,\ \Lambda}$$

осуществляется по тому же правилу, что и первый.)

Пусть доказательство секвенции C имеет вид

$$\frac{D_0}{C}.$$

Если последний переход осуществляется не по правилу 13, примененному к $\Phi \wedge \Psi$, а $C_0 = \Gamma_0 \vdash \Theta_0,\ \Phi \wedge \Psi,$

Λ_0 — заключительная секвенция доказательства D_0, то по индукционному предположению существует доказательство D_0' секвенции $\Gamma_0 \vdash \Theta_0, \Phi, \Lambda_0$ и дерево

$$\frac{D_0'}{\Gamma \vdash \Theta, \Phi, \Lambda}$$

есть доказательство.

Пусть последний переход в дереве D есть

$$\frac{\Gamma \vdash \Theta, \Phi \wedge \Psi, \Phi \wedge \Psi}{\Gamma \vdash \Theta, \Phi \wedge \Psi}.$$

По индукционному предположению существует доказательство D_0' секвенции $\Gamma \vdash \Theta, \Phi \wedge \Psi, \Phi$, причем число переходов доказательства D_0' меньше числа переходов D_0. Снова по индукционному предположению существует доказательство D_0'' секвенции $\Gamma \vdash \Theta, \Phi, \Phi$. Тогда

$$\frac{D_0''}{\Gamma \vdash \Theta, \Phi}$$

есть нужное доказательство.

Докажем теперь утверждение 6). Пусть D — доказательство секвенции $C_0 = \neg \Phi, \Gamma \vdash \Theta$; по лемме 2 предыдущего параграфа можно считать, что доказательство D обладает свойством чистоты переменных. Перейдем от дерева D к дереву D', сделав следующие преобразования: заменяем каждое вхождение секвенции $C = \Lambda \vdash \Delta$ на вхождение секвенции $C' = \Lambda' \vdash \Phi, \Delta'$, где Λ' и Δ' получаются из Λ и Δ вычеркиванием всех предков формулы $\neg \Phi$ заключительного вхождения секвенции C_0, имеющих вид Φ или $\neg \Phi$. (З а м е ч а н и е. Легко с помощью индукции проверить, что предок формулы $\neg \Phi$ вида $\neg \Phi$ может быть только в левой части секвенции, а предок вида Φ — только в правой части.) Проверим, что D' — квазивывод секвенции $\Gamma \vdash \Phi, \Theta$. Это, очевидно, достаточно для доказуемости секвенции $\Gamma \vdash \Theta, \Phi$. Если $C = \Lambda \vdash \Delta$ — аксиома, то $\Lambda' = \Lambda$; если последняя формула из Δ есть предок $\neg \Phi$ вида Φ, то $\Lambda' \vdash \Phi, \Delta'$ получается из аксиомы $\Lambda \vdash \Delta$ применением только правила перестановки; если последняя формула из Δ не есть предок $\neg \Phi$ вида Φ, то $\Lambda' \vdash \Delta'$ — аксиома и $\Lambda' \vdash \Phi, \Delta'$ получается из нее правилом утончения (лемма 3 § 30) и перестановками.

Посмотрим теперь на переходы дерева D'. Легко проверяется, что если в переходе дерева D ни один предок формулы $\neg\Phi$ вида Φ или $\neg\Phi$ не является главной формулой, то соответствующий переход в D' будет осуществляться по тому же правилу вывода. Рассмотрим теперь случаи, когда предок $\neg\Phi$ вида Φ или $\neg\Phi$ является главной формулой перехода. Тогда этот переход может быть только по правилам 1, 3, 5, 6, 7, 9 или по структурным правилам 11—14.

Разбор всех случаев вряд ли поучителен. Рассмотрим случаи применения правил 1, 5, 6, 9, 13.

Пусть переход в D имеет вид

$$\frac{\Delta \vdash \Lambda, \Psi;\ \Delta \vdash \Lambda, X}{\Delta \vdash \Lambda, \Psi \wedge X}$$

и $\Phi = \Psi \wedge X$ есть предок $\neg\Phi$, тогда переход в D' будет

$$\frac{\Delta' \vdash \Phi, \Lambda', \Psi;\ \Delta' \vdash \Phi, \Lambda', X}{\Delta' \vdash \Phi, \Lambda'}$$

и нижняя секвенция может быть получена из верхних правилами введения конъюнкции (1), перестановки (11) и сокращения (13).

Пусть переход в D имеет вид

$$\frac{\Psi, \Delta \vdash \Lambda}{\Delta \vdash \Lambda, \neg\Psi}$$

и $\Phi = \neg\Psi$ есть предок $\neg\Phi$, тогда переход в D' будет

$$\frac{\Psi, \Delta' \vdash \Phi, \Lambda'}{\Delta' \vdash \Phi, \Lambda'},$$

но так как $\Phi = \neg\Psi$, то нижняя секвенция получается из верхней применением правил введения отрицания (5), перестановки (11) и сокращения (13).

Пусть переход в D имеет вид

$$\frac{\Delta \vdash \Lambda, \Phi}{\neg\Phi, \Delta \vdash \Lambda},$$

а Φ и $\neg\Phi$ — предки формулы $\neg\Phi$ (из заключительной секвенции), тогда соответствующий переход в D' будет

$$\frac{\Delta' \vdash \Phi, \Lambda'}{\Delta' \vdash \Phi, \Lambda'},$$

т. е. тривиален.

Пусть переход в D имеет вид

$$\frac{\Delta \vdash \Lambda, [\Psi]^x_y}{\Delta \vdash \Lambda, \forall x \Psi}$$

и $\Phi = \forall x\Psi$ — предок $\neg\,\Phi$, тогда соответствующий переход в D' будет

$$\frac{\Delta' \vdash \Phi,\ \Lambda',\ [\Psi]_y^x}{\Delta' \vdash \Phi,\ \Lambda'}$$

и нижняя секвенция получается из верхней применением правил 9 (это применение законно, так как Δ' и Λ' являются частями Δ и Λ и y отлично от всех свободных переменных формулы Φ по свойству чистоты переменных в D), 11 и 13.

Пусть, наконец, переход в D таков:

$$\frac{\Delta \vdash \Delta,\ \Phi,\ \Phi}{\Delta \vdash \Lambda,\ \Phi}$$

и Φ — предок $\neg\,\Phi$, тогда в D' соответствующий переход

$$\frac{\Delta' \vdash \Phi,\ \Lambda'}{\Delta' \vdash \Phi,\ \Lambda'}$$

будет тривиальным. □

Обратимся теперь к кванторным правилам.

Предложение 2. 1) *Если в G доказуема секвенция* $\exists x\Phi,\ \Gamma \vdash \Theta$, *то для любого терма t такого, что* $(\Phi)_t^x,\ \Gamma \vdash \Theta$ — *секвенция G, эта секвенция доказуема в G*; 2) *если доказуема секвенция* $\Gamma \vdash \Theta,\ \forall x\Phi$, *то для любого терма t такого, что* $\Gamma \vdash \Theta,\ (\Phi)_t^x$ — *секвенция G, эта секвенция доказуема в G.*

Доказательства этих утверждений аналогичны, поэтому приведем только доказательство утверждения 2).

Пусть $y_0, \ldots, y_k$ — все свободные переменные терма t и пусть D — доказательство секвенции $\Gamma \vdash \Theta,\ \forall x\Phi$, обладающее свойством чистоты переменных и такое, что любая переменная, исчезающая в этом доказательстве, отлична от переменных $y_0, \ldots, y_k$. Пусть $[\Phi]_{z_0}^x, \ldots$ $\ldots, [\Phi]_{z_s}^x$ — все предки вида $[\Phi]_y^x$ вхождения формулы $\forall x\Phi$ в заключительную секвенцию. Построим дерево секвенций D' следующим образом. Каждое вхождение секвенции C в D заменяем на вхождение секвенции C', полученной из C заменой всех предков формулы $\forall x\Phi$ вида $\forall x\Phi$ на $(\Phi)_t^x$ и подстановкой терма t вместо всех вхождений переменных $z_0, \ldots, z_s$. Легко проверяется, что все начальные секвенции дерева D' являются аксиомами, а все переходы D' либо совершаются по тем же правилам, что и в соответствующем переходе D, либо являются тривиальными переходами. Последнее случается, когда в D соответствующий переход есть

$$\frac{\Delta \vdash \Lambda,\ [\Phi]^x_{z_i}}{\Delta \vdash \Lambda,\ \forall x\Phi}$$

и $\forall x\Phi$ — предок формулы $\forall x\Phi$ заключительной секвенции. Таким образом, D' есть квазивывод секвенции $\Gamma \vdash \Theta$, $(\Phi)^x_t$. □

Следствие. *Пусть переменная y не имеет вхождений ни в одну из формул секвенции $\Gamma \vdash \Theta$, $\forall x\Phi$; эта секвенция (секвенция $\exists x\Phi$, $\Gamma \vdash \Theta$) доказуема тогда и только тогда, когда доказуема секвенция $\Gamma \vdash \Theta$, $[\Phi]^x_y$ (секвенция $[\Phi]^x_y$, $\Gamma \vdash \Theta$).* □

Для правил 7 и 10 хорошей формулировки свойства обратимости нет (см. упражнение 1), хотя оно справедливо в некотором «распределенном по всему доказательству» виде (ср. доказательство теоремы об устранении сечения в следующем параграфе).

Упражнения

1. Доказать, что не существует термов $t_0, \ldots, t_k$ таких, что секвенция $\exists xP(x) \vdash (P)^x_{t_0}, \ldots, (P)^x_{t_k}$ доказуема, хотя секвенция $\exists xP(x) \vdash \exists xP(x)$ доказуема.

2. Доказать в G секвенцию $\exists zP(z) \vdash \exists y\forall xP(y)$.

3. Показать, что в исчислении G^* (см. упражнение 3 § 30) предложение 2 несправедливо. (Указание. Воспользоваться упражнением 2 и упражнением 3 из § 30.)

§ 32. Сравнение исчислений $ИП^{\Sigma}$ и G

В этом параграфе докажем, что секвенция исчисления $ИП^{\Sigma}$, которая является и секвенцией исчисления G (т. е. не содержит знаков импликации $\to$ и равенства $\approx$ и удовлетворяет условию несмешанности переменных), доказуема в $ИП^{\Sigma}$ тогда и только тогда, когда она доказуема в G.

В основе доказательства этого утверждения лежит следующая важная теорема об исчислении G.

Теорема 1 (об устранении сечения). *Пусть $\Gamma \vdash \Theta, \Phi$ и $\Phi, \Lambda \vdash \Delta$ — доказуемые секвенции исчисления G. Если $\Gamma, \Lambda \vdash \Delta, \Theta$ — секвенция исчисления G, то она доказуема.*

Доказательство. Докажем теорему сначала для атомарной формулы Φ индукцией по числу существенных переходов в доказательстве секвенции $\Gamma \vdash \Theta$, Φ, понимая под существенными переходами те переходы, которые осуществляются по правилам, отличным от правил перестановки 11 и 12. Если $\Gamma \vdash \Theta, \Phi$ имеет доказательство без существенных переходов, то $\Gamma \vdash \Theta, \Phi$ отличается от аксиом только перестановкой формул. Рассмотрим два возможных случая.

1. $\Phi \in \Gamma$; тогда секвенция $\Gamma, \Lambda \vdash \Delta, \Theta$ может быть получена из (доказуемой) секвенции $\Phi, \Lambda \vdash \Delta$ применением производного правила утончения (лемма 3 § 30) и правил перестановки.

2. Существует формула Ψ такая, что $\Psi \in \Gamma$ и $\Psi \in \Theta$; тогда секвенция $\Gamma \vdash \Theta$ доказуема (перестановка аксиомы) и секвенция $\Gamma, \Lambda \vdash \Delta, \Theta$ получается из нее утончениями и перестановками.

Предположим, что для секвенций $\Gamma \vdash \Theta, \Phi$, имеющих доказательство с менее чем $n > 0$ существенными переходами, теорема справедлива. Пусть D — доказательство секвенции $\Gamma \vdash \Theta, \Phi$, имеющее n существенных переходов; будем предполагать, что доказательство D обладает свойством чистоты переменных.

Рассмотрим самый нижний существенный переход в доказательстве D. Возможны следующие случаи:

1. Переход имеет вид

$$\frac{\Gamma_0 \vdash \Theta_0', \Phi, \Theta_0''; \ \Gamma_1 \vdash \Theta_1', \Phi, \Theta_1''}{\Gamma' \vdash \Theta', \Phi, \Theta''}. \qquad (*)$$

Здесь Γ' — перестановка Γ; Θ', Θ'' — перестановка Θ; указанные вхождения формулы Φ являются предками вхождения Φ в заключительную секвенцию $\Gamma \vdash \Theta, \Phi$. Секвенции $\Gamma_0 \vdash \Theta_0', \Theta_0'', \Phi$ и $\Gamma_1 \vdash \Theta_1', \Theta_1'', \Phi$ имеют доказательство с числом существенных переходов $<n$ (так как они получаются перестановкой из секвенций $\Gamma_0 \vdash \Theta_0'$, Φ, Θ_0'' и $\Gamma_1 \vdash \Theta_1', \Phi, \Theta_1''$). Поэтому доказуемы секвенции $\Gamma_0, \Lambda \vdash \Delta, \Theta_0', \Theta_0''$ и $\Gamma_1, \Lambda \vdash \Delta, \Theta_1', \Theta_1''$. Дерево секвенций

$$\frac{\dfrac{\Gamma_0, \Lambda \vdash \Delta, \Theta_0', \Theta_0''; \ \Gamma_1, \Lambda \vdash \Delta, \Theta_1', \Theta_1''}{\Gamma', \Lambda \vdash \Delta, \Theta', \Theta''}}{\Gamma, \Lambda \vdash \Delta, \Theta}$$

является квазивыводом, так как атомарная формула Φ не является главной формулой перехода (*).

2. Переход имеет вид

$$\frac{\Gamma' \vdash \Theta', \Phi, \Phi}{\Gamma' \vdash \Theta', \Phi}.$$

Здесь Γ' — перестановка Γ, Θ' — перестановка Θ, а указанные вхождения Φ являются предками вхождения Φ в заключительную секвенцию. Если D' — поддерево дерева D, определенное вхождением в D секвенции $\Gamma' \vdash \Theta', \Phi, \Phi$, то пусть D'' получается из D' вычеркиванием в каждой секвенции всех предков правого вхождения формулы Φ заключительной секвенции $\Gamma' \vdash \Theta', \Phi, \Phi$. На вершинах дерева D'' будут секвенции, отличающиеся от аксиом только перестановкой. Переходы будут либо тривиальны, либо происходить в соответствии с теми же правилами, что и в D'. Простой перестройкой из D'' можно получить доказательство секвенции $\Gamma' \vdash \Theta', \Phi$ (а следовательно, и доказательство секвенции $\Gamma \vdash \Theta, \Phi$) с числом существенных переходов, равным числу существенных переходов в D'. Так как число существенных переходов в D' меньше чем в D, то по индукционному предположению секвенция $\Gamma, \Lambda \vdash \Delta, \Theta$ доказуема.

3. Переход имеет вид

$$\frac{\Gamma_0 \vdash \Theta_0', \Phi, \Theta_0''}{\Gamma' \vdash \Theta', \Phi, \Theta''}.$$

Здесь Γ' — перестановка Γ; Θ', Θ'' — перестановка Θ; указанные вхождения Φ являются предками Φ из заключительной секвенции дерева D и Φ не является главной формулой этого перехода.

Секвенция $\Gamma_0 \vdash \Theta_0', \Theta_0'', \Phi$ получается из $\Gamma_0 \vdash \Theta_0'$, Φ, Θ_0'' перестановкой, поэтому эта секвенция имеет доказательство с числом существенных переходов $n-1$. Тогда по индукционному предположению секвенция Γ_0, $\Lambda \vdash \Delta, \Theta_0', \Theta_0''$ доказуема. Дерево секвенций

$$\cfrac{\cfrac{\Gamma_0, \Lambda \vdash \Delta, \Theta_0', \Theta_0''}{\Gamma', \Lambda \vdash \Delta, \Theta', \Theta''}}{\Gamma, \Lambda \vdash \Delta, \Theta}$$

есть квазивывод.

Итак, для секвенций $\Gamma \vdash \Theta, \Phi$ с атомарной формулой Φ теорема установлена.

Продолжим доказательство теоремы, применяя индукцию по построению формулы Φ. Предполагая, что для собственных (т. е. не равных Φ) обобщенных подформул формулы Φ и любых $\Gamma, \Lambda, \Theta, \Delta$ теорема справедлива, установим ее справедливость и для Φ.

Пусть $\Phi = \Psi \wedge X$; $\Gamma \vdash \Theta, \Phi$ и $\Phi, \Lambda \vdash \Delta$ — доказуемые секвенции, а $\Gamma, \Lambda \vdash \Theta, \Phi$ — секвенция исчисления G. По свойству обратимости (предложение 31.1) доказуемы и секвенции $\Gamma \vdash \Theta, \Psi$; $\Gamma \vdash \Theta, X$; $\Psi, X, \Lambda \vdash \Delta$. Используя индукционное предположение, получаем, что доказуемы и секвенции $\Gamma, X, \Lambda \vdash \Delta, \Theta$; $X, \Gamma, \Lambda \vdash \Delta, \Theta$; $\Gamma, \Gamma, \Lambda \vdash \Delta, \Theta, \Theta$ и, наконец, доказуема секвенция $\Gamma, \Lambda \vdash \Delta, \Theta$.

Случаи $\Phi = \Psi \vee X$, $\Phi = \neg \Psi$ разбираются аналогично.

Пусть теперь $\Phi = \forall x \Psi$; $\Gamma \vdash \Theta, \Phi$ и $\Phi, \Lambda \vdash \Delta$ — доказуемые секвенции, $\Gamma, \Lambda \vdash \Delta, \Theta$ — секвенция исчисления G. Пусть D — доказательство секвенции $\Phi, \Lambda \vdash \Delta$. Будем предполагать, что D обладает свойством чистоты переменных и что любая переменная y, которая исчезает в D, отлична от всех переменных формул списка Γ, Θ. Установим индукцией по глубине вхождения в дерево D, что для любого вхождения $\Lambda' \vdash \Delta'$ секвенции в D секвенция $\Lambda^*, \Gamma \vdash \Theta, \Delta'$ доказуема, где Λ^* получается из Λ' вычеркиванием всех предков формулы Φ заключительной секвенции вида Φ.

Ясно, что для самых верхних вхождений ($\Lambda' \vdash \Delta'$ — аксиома) соответствующая секвенция $\Lambda', \Gamma \vdash \Theta, \Delta'$ доказуема (получается применениями правила утончения). Рассмотрим переход в D

$$\frac{\Lambda_0 \vdash \Delta_0;\ \Lambda_1 \vdash \Delta_1}{\Lambda' \vdash \Delta'}$$

и предположим, что соответствующие верхним вхождениям секвенции $\Lambda_0^*, \Gamma \vdash \Theta, \Delta_0$ и $\Lambda_1^*, \Gamma \vdash \Theta, \Delta_1$ доказуемы, тогда

$$\frac{\Lambda_0^*, \Gamma \vdash \Theta, \Lambda_0;\ \Lambda_1^*, \Gamma \vdash \Theta, \Delta_1}{\Lambda^*, \Gamma \vdash \Theta, \Delta'},$$

как нетрудно проверить, будет переходом по тому же правилу вывода и, следовательно, квазивыводом. Аналогично обстоит дело для однопосылочных переходов, за исключением переходов вида

$$\frac{(\Psi)_t^x, \Lambda_0 \vdash \Delta_0}{\forall x\Psi, \Lambda_0 \vdash \Delta_0},$$

где вхождение $\Phi = \forall x \Psi$ в нижнюю секвенцию есть предок формулы Φ заключительной секвенции дерева D. Вхождениям в этот переход соответствуют секвенции $(\Psi)_t^x, \Lambda_0^*, \Gamma \vdash \Theta, \Delta_0$ и $\Lambda_0^*, \Gamma \vdash \Theta, \Delta_0$. Предположим, что секвенция $(\Psi)^x_t, \Lambda^*_0, \Gamma \vdash \Theta, \Delta_0$ доказуема. По условию теоремы $\Gamma \vdash \Theta, \forall x \Psi$ — доказуемая секвенция, тогда по предложению 31.2 будет доказуема и секвенция $\Gamma \vdash \Theta, (\Psi)^x_t$. Так как $(\Psi)^x_t$ является собственной обобщенной подформулой формулы $\Phi = \forall x \Psi$, то, применяя индукционное предположение о справедливости теоремы для собственных обобщенных подформул формулы Φ к доказуемым секвенциям $(\Psi)^x_t, \Lambda^*_0, \Gamma \vdash \Theta, \Delta_0$ и $\Gamma \vdash \Theta, (\Psi)^x_t$, получаем, что секвенция $\Gamma, \Lambda^*_0, \Gamma \vdash \Theta, \Delta_0, \Theta$ доказуема. Используя правила перестановок и сокращения из доказуемости последней секвенции, получаем доказуемость секвенции $\Lambda^*_0, \Gamma \vdash \Theta, \Delta_0$.

Итак, для каждого вхождения секвенции $\Lambda' \vdash \Delta'$ в D соответствующая секвенция $\Lambda^*, \Gamma \vdash \Theta, \Delta'$ доказуема. Заключительной секвенции дерева D будет соответствовать доказуемая секвенция $\Lambda, \Gamma \vdash \Theta, \Delta$. Используя правила перестановки, отсюда получаем доказуемость секвенции $\Gamma, \Lambda \vdash \Delta, \Theta$.

Случай, когда Φ имеет вид $\exists x \Psi$, рассматривается аналогично. □

Замечание. Можно считать, что теорема 1 устанавливает допустимость следующего правила — правила сечения

$$\frac{\Gamma \vdash \Theta, \Phi;\ \Phi, \Lambda \vdash \Delta}{\Gamma, \Lambda \vdash \Delta, \Theta}.$$

Приступим к доказательству основного утверждения. Если $\Theta = \Phi_1, \ldots, \Phi_n$ — список формул, то через $\neg\Theta$ будем обозначать список $\neg\Phi_1, \ldots, \neg\Phi_n$.

Предложение 1. *Если секвенция $C = \Gamma \vdash \Theta$ доказуема в G, то секвенция $C' = \Gamma, \neg\Theta \vdash$ доказуема в $ИП^\Sigma$.*

Доказательство. Доказывать будем индукцией по высоте доказательства в исчислении G. Если $\Phi, \Gamma \vdash \Theta, \Phi$ — аксиома, то секвенция $\Phi, \Gamma, \neg\Theta \vdash \Phi$ доказуема в $ИП^\Sigma$ с использованием аксиомы $\Phi \vdash \Phi$ и правила добавления лишней посылки; наконец,

$$\frac{\Phi, \Gamma, \neg\Theta \vdash \Phi;\quad \neg\Phi \vdash \neg\Phi}{\Phi, \Gamma, \neg\Theta, \neg\Phi \vdash}$$

есть квазивывод нужной секвенции в $ИП^\Sigma$.

Теперь для каждого правила вывода исчисления G нужно проверить, что если секвенции C_0 (и C_1), стоящие над чертой в правиле, таковы, что C_0' (и C_1') доказуемы в $ИП^\Sigma$, то и секвенция C', соответствующая секвенции C под чертой, тоже доказуема в ИП$^{\Sigma}$. Проверка всех правил достаточно утомительна, поэтому проверим это только для правил 2, 3, 5, 7, 8, 10.

2) Пусть секвенция $\Phi, \Psi, \Gamma, \neg\Theta \vdash$ доказуема в ИП$^{\Sigma}$, тогда следующее дерево секвенций есть квазивывод в ИП$^{\Sigma}$:

$$\dfrac{\dfrac{\Phi \wedge \Psi \vdash \Phi \wedge \Psi}{\Phi \wedge \Psi \vdash \Psi;} \qquad \dfrac{\dfrac{\dfrac{\Phi \wedge \Psi \vdash \Phi \wedge \Psi}{\Phi \wedge \Psi \vdash \Phi;} \quad \dfrac{\Phi, \Psi, \Gamma, \neg\Theta \vdash}{\Psi, \Gamma, \neg\Theta \vdash \neg\Phi}}{\Phi \wedge \Psi, \Psi, \Gamma, \neg\Theta \vdash}}{\Phi \wedge \Psi, \Gamma, \neg\Theta \vdash \neg\Psi}}{\Phi \wedge \Psi, \Gamma, \neg\Theta \vdash}.$$

3) Пусть секвенция $\Gamma, \neg\Theta, \neg\Phi, \neg\Psi \vdash$ доказуема в ИП$^{\Sigma}$, тогда следующее дерево секвенций есть квазивывод в ИП$^{\Sigma}$:

$$\dfrac{\dfrac{\vdash \Phi \vee \neg\Phi; \quad \dfrac{\Phi \vdash \Phi}{\Phi \vdash \Phi \vee \Psi;} \quad \dfrac{\dfrac{\Gamma, \neg\Theta, \neg\Phi, \neg\Psi \vdash}{\Gamma, \neg\Theta, \neg\Phi \vdash \Psi}}{\Gamma, \neg\Theta, \neg\Phi\Phi \vdash \vee\Psi}}{\Gamma, \neg\Theta \vdash \Phi \vee \Psi;} \qquad \neg(\Phi \vee \Psi) \vdash \neg(\Phi \vee \Psi)}{\Gamma, \neg\Theta, \neg(\Phi \vee \Psi) \vdash}.$$

5) Пусть секвенция $\Phi, \Gamma, \neg\Theta \vdash$ доказуема в ИП$^{\Sigma}$, тогда

$$\dfrac{\dfrac{\Phi, \Gamma, \neg\Theta}{\Gamma, \neg\Theta \vdash \neg\Phi;} \quad \neg\neg\Phi \vdash \neg\neg\Phi}{\Gamma, \neg\Theta, \neg\neg\Phi \vdash}$$

есть квазивывод в ИП$^{\Sigma}$.

7) Пусть секвенция $\Gamma, \neg\Theta, \neg(\Phi)^x_t \vdash$ доказуема в ИП$^{\Sigma}$, тогда

$$\dfrac{\dfrac{\dfrac{\Gamma, \neg\Theta, \neg(\Phi)^x_t \vdash}{\Gamma, \neg\Theta \vdash (\Phi)^x_t}}{\Gamma, \neg\Theta \vdash \exists x\Phi;} \quad \neg\exists x\Phi \vdash \neg\exists x\Phi}{\Gamma, \neg\Theta, \neg\exists x\Phi \vdash}$$

есть квазивывод в ИП$^{\Sigma}$.

8) Пусть секвенция $[\Phi]^x_y, \Gamma, \neg\Theta \vdash$ доказуема в ИП$^{\Sigma}$, переменная y не имеет свободных вхождений в $\Gamma, \neg\Theta$, тогда

$$\dfrac{\exists x\Phi \vdash \exists y\,[\Phi]^x_y; \quad \dfrac{\dfrac{[\Phi]^x_y, \Gamma, \neg\Theta \vdash}{\exists y\,[\Phi]^x_y, \Gamma, \neg\Theta \vdash}}{\Gamma, \neg\Theta \vdash \neg\exists y\,[\Phi]^x_y}}{\exists x\Phi, \Gamma, \neg\Theta \vdash}$$

есть квазивывод в ИП$^{\Sigma}$.

10) Пусть секвенция $(\Phi)_t^x, \Gamma, \neg\Theta \vdash$ доказуема в ИП$^\Sigma$, тогда

$$\frac{(\Phi)_t^x, \Gamma, \neg\Theta \vdash}{\forall x\Phi, \Gamma, \neg\Theta \vdash}$$

есть квазивывод в ИП$^\Sigma$.

Проверка оставшихся правил вполне аналогична уже рассмотренным. Индукция по высоте доказательства в G завершает доказательство предложения. □

Предложение 2. *Если секвенция C исчисления G доказуема в ИП$^\Sigma$, то она доказуема и в исчислении G.*

Доказательство. Установим сначала доказуемость в G аксиом $\Phi \vdash \Phi$ исчисления ИП$^\Sigma$ индукцией по построению формулы Φ. Если Φ — атомарная формула, то $\Phi \vdash \Phi$ — аксиома исчисления G. Пусть для формул Φ и Ψ в G доказуемы секвенции $\Phi \vdash \Phi$ и $\Psi \vdash \Psi$. Рассмотрим следующие квазивыводы в G:

$$\frac{\dfrac{\dfrac{\Phi \vdash \Phi}{\Phi, \Psi \vdash \Phi}}{\Phi \wedge \Psi \vdash \Phi;} \quad \dfrac{\dfrac{\Psi \vdash \Psi}{\Phi, \Psi \vdash \Psi}}{\Phi \wedge \Psi \vdash \Psi}}{\Phi \wedge \Psi \vdash \Phi \wedge \Psi}, \qquad \frac{\dfrac{\dfrac{\Phi \vdash \Phi}{\Phi \vdash \Phi, \Psi}}{\Phi \vdash \Phi \vee \Psi;} \quad \dfrac{\dfrac{\Psi \vdash \Psi}{\Psi \vdash \Phi, \Psi}}{\Psi \vdash \Phi \vee \Psi}}{\Phi \vee \Psi \vdash \Phi \vee \Psi},$$

$$\dfrac{\dfrac{\dfrac{\Phi \vdash \Phi}{\vdash \Phi, \neg\Phi}}{\vdash \neg\Phi, \Phi}}{\neg\Phi \vdash \neg\Phi}, \qquad \dfrac{\dfrac{[\Phi]_y^x \vdash [\Phi]_y^x}{[\Phi]_y^x \vdash \exists x\Phi}}{\exists x\Phi \vdash \exists x\Phi}, \qquad \dfrac{\dfrac{[\Phi]_y^x \vdash [\Phi]_y^x}{\forall x\Phi \vdash [\Phi]_y^x}}{\forall x\Phi \vdash \forall x\Phi}.$$

В двух последних квазивыводах переменная y выбрана так, что она не имеет никаких вхождений в Φ. Эти квазивыводы показывают, что можно завершить индукционное доказательство того, что все секвенции вида $\Phi \vdash \Phi$, где Φ — формула исчисления G, доказуемы в G.

Теперь необходимо для каждого правила вывода исчисления ИП$^\Sigma$ (за исключением правил, касающихся импликации) проверить, что если секвенции, стоящие над чертой, доказуемы в G, то и секвенция, стоящая под чертой, также доказуема в G. Правила 1, 11, 13—16 исчисления ИП$^\Sigma$ являются частными случаями правил вывода G. Для правил 2 и 3

$$\frac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Phi}, \qquad \frac{\Gamma \vdash \Phi \wedge \Psi}{\Gamma \vdash \Psi}$$

необходимое утверждение следует из соответствующего свойства обратимости (предложение 31.2). Для правила 4 (5)

$$\frac{\Gamma \vdash \Phi}{\Gamma \vdash \Phi \vee \Psi} \qquad \left(\frac{\Gamma \vdash \Psi}{\Gamma \vdash \Phi \vee \Psi}\right)$$

квазивывод в G

$$\cfrac{\cfrac{\Gamma \vdash \Phi}{\Gamma \vdash \Phi, \Psi}}{\Gamma \vdash \Phi \vee \Psi} \qquad \left(\cfrac{\cfrac{\cfrac{\Gamma \vdash \Psi}{\Gamma \vdash \Psi, \Phi}}{\Gamma \vdash \Phi, \Psi}}{\Gamma \vdash \Phi \vee \Psi}\right)$$

устанавливает необходимое свойство. Рассмотрим теперь правило 6

$$\frac{\Gamma \vdash \Phi \vee \Psi; \quad \Gamma, \Phi \vdash \mathrm{X}; \quad \Gamma, \Psi \vdash \mathrm{X}}{\Gamma \vdash \mathrm{X}}.$$

Если секвенции, стоящие над чертой, доказуемы в G, то следующее дерево, использующее допустимое правило сечения (см. замечание после доказательства теоремы 1), есть квазивывод в G:

$$\cfrac{\cfrac{\Gamma \vdash \Phi \vee \Psi; \quad \cfrac{\cfrac{\Gamma, \Phi \vdash \mathrm{X}}{\Phi, \Gamma \vdash \mathrm{X};} \quad \cfrac{\Gamma, \Psi \vdash \mathrm{X}}{\Psi, \Gamma \vdash \mathrm{X}}}{\Phi \vee \Psi, \Gamma \vdash \mathrm{X}}}{\Gamma, \Gamma \vdash \mathrm{X}}}{\Gamma \vdash \mathrm{X}}.$$

Правилу 9 соответствует утверждение об обратимости правила введения отрицания.

Для правила 10, если $\Gamma \vdash \Phi$ и $\Gamma \vdash \neg \Phi$ доказуемы в G, то (по обратимости) доказуема в G секвенция $\Phi, \Gamma \vdash$, а по теореме 1 доказуема секвенция $\Gamma, \Gamma \vdash$, а следовательно, и секвенция $\Gamma \vdash$. Допустимость правила 12 в G установлена ранее.

Индукция по высоте доказательства секвенции C в исчислении ИП^{Σ} и завершает доказательство. □

Следствием предложений 1 и 2 и является основное утверждение этого параграфа.

Теорема 2. *Секвенция исчисления ИП^{Σ}, являющаяся и секвенцией исчисления G, доказуема в ИП^{Σ} тогда и только тогда, когда она доказуема в исчислении G.* □

Упражнение

1. Показать, что в исчислении G^* (см. упражнение 3 § 30) теорема 1 несправедлива. (Указание. Воспользоваться результатами упражнения 2 § 31 и упражнением 3 § 30.)

§ 33. Теорема Эрбрана

В этом параграфе мы установим весьма важную теорему Эрбрана, которая, в частности, является теоретической основой современных машинных методов поиска доказательства в исчислении предикатов. Один из таких методов основан на исчислении резольвент, которое будет рассмотрено в следующем параграфе. Теорема Эрбрана обосновывает обнаружение этим методом доказуемости любой доказуемой формулы ИП$^\Sigma$; последнее свойство называется полнотой метода. Теорема эта также придает определенный конструктивный смысл произвольным предложениям исчисления предикатов.

Начнем параграф с изучения некоторых синтаксических связей.

С каждым термом t и переменной x свяжем некоторое множество $F_x(t)$ функциональных символов:

а) если x не входит в t или $x = t$, то $F_x(t) = \varnothing$;

б) если x входит в t и $t \neq x$, то $t = h(t_1, \ldots, t_n)$ для некоторых функционального символа h и термов $t_1, \ldots, t_n$; полагаем тогда $F_x(t) = \{h\} \cup \bigcup\limits_{i=1}^{n} F_x(t_i)$.

Лемма 1. *Если $x \neq y$ и x не входит в t', то для любого терма t имеет место равенство*

$$F_x\left((t)^y_{t'}\right) = F_x(t).$$

Доказательство проводится индукцией по построению терма t. □

Предложение 1. *Если $\mathsf{Q}x\Psi$ ($\mathsf{Q} \in \{\forall, \exists\}$) — обобщенная подформула формулы Φ, то для любого терма t_0 формулы Ψ найдется такой терм t_1 формулы Φ, что*

$$F_x(t_0) = F_x(t_1)$$

и t_1 находится в области действия квантора $\mathsf{Q}x$.

Доказательство. Так как $\mathsf{Q}x\Psi$ является обобщенной подформулой формулы Φ, то существует такая последовательность формул $\Phi_0 = \Phi, \Phi_1, \ldots, \Phi_n = \mathsf{Q}x\Psi$, что для любого $i < n$ выполнено одно из условий:

(1) $\Phi_i = \neg\, \Phi_{i+1}$;

(2) $\Phi_i = \Phi_{i+1}\tau\Psi_{i+1}$ ($\Phi_i = \Psi_{i+1}\tau\Phi_{i+1}$) для подходящей формулы Ψ_{i+1} и $\tau \in \{\bigvee, \bigwedge\}$;

(3) $\Phi_i = \mathsf{Q}'y\mathrm{X}_i$, $\Phi_{i+1} = (\mathrm{X}_i)^y_t$ для подходящих формулы X_i, переменной y, терма t, свободного для y в X_i, и $\mathsf{Q}' \in \{\forall, \exists\}$.

Предположим теперь справедливость предложения для $n-1$. Если в качестве Φ взять формулу Φ_1 последовательности $\Phi_0 = \Phi, \Phi_1, \ldots, \Phi_n = \mathrm{Q}x\Psi$, то по индукционному предположению для любого терма t_0 формулы Ψ в Φ_1 можно указать терм t такой, что $F_x(t_0) = F_x(t)$ и t входит в область действия квантора $\mathrm{Q}x$. Если переход от Φ_0 к Φ_1 удовлетворяет условию (1) или (2), то Φ_1 является подформулой (а не только обобщенной подформулой) формулы $\Phi = \Phi_0$, поэтому в качестве искомого t_1 нужно взять соответствующий терм t. Если выполнено условие (3), то рассмотрим три возможных подслучая.

Подслучай (3а): $y = x$. Тогда $\Phi = \mathrm{Q}'x\mathrm{X}$, $\Phi_1 = (\mathrm{X})_t^x$ для подходящей формулы X. Так как Φ_1 (и, следовательно, X) имеет (по индукционному предположению) несвязанные вхождения переменной x, то по свойству несмешанности переменных x не имеет свободных вхождений в X и $\Phi_1 = \mathrm{X}$, $\Phi = \mathrm{Q}'x\mathrm{X}$; Φ_1 есть подформула Φ.

Подслучай (3б): $y \neq x$ и x входит в t. Тогда $\Phi_1 = (\mathrm{X})_t^y$, $\Phi = \mathrm{Q}'y\mathrm{X}$ для некоторой формулы X. Формула Φ_1 имеет связанные вхождения переменной x; если бы X имела свободные вхождения y, то нарушалось бы условие свободы терма t для переменной y в формуле X. Итак, y не имеет свободных вхождений в X и $\Phi_1 = (\mathrm{X})_t^y = \mathrm{X}$; $\Phi = \mathrm{Q}'y\Phi_1$; Φ_1 есть подформула Φ.

Подслучай (3в): $y \neq x$ и x не входит в t. Пусть X — такая формула, что $\Phi_1 = (\mathrm{X})_t^y$, $\Phi = \mathrm{Q}'y\mathrm{X}$. Для любого терма t_2 формулы Φ_1 существует соответствующий терм t_1 формулы X такой, что $t_2 = (t_1)_t^y$, причем если t_2 входит в область действия какого-либо квантора в Φ_1, то t_1 входит в область действия такого же квантора по той же переменной. По лемме 1 имеем $F_x(t_2) = F_x\left((t_1)_t^y\right) = F_x(t_1)$; если t_2 выбран в Φ_1 для t_0 в соответствии с заключением предложения, то соответствующий терм t_1 будет удовлетворять заключению предложения для формулы Φ.

Предложение доказано. □

Будем говорить, что функциональный символ g имеет связанное вхождение в формулу Φ, если Φ содержит подформулу вида $\mathrm{Q}x\Psi$ и Ψ имеет вхождение терма t такого, что $g \in F_x(t)$.

Укажем два следствия предложения 1.

Следствие 1. *Если Ψ — обобщенная подформула формулы Φ и функциональный символ g имеет связанное* *вхождение в* Ψ, *то* g *имеет связанное вхождение и в* Φ. □

Следствие 2. *Если* D — *доказательство секвенции* C *в исчислении* G *и функциональный символ* g *не имеет связанных вхождений ни в одну из формул секвенции* C, *то* g *не имеет связанных вхождений ни в одну из формул дерева* D.

По свойству подформульности и следствию 1. □

Зафиксируем терм t_0, начинающийся с функционального символа g, и переменную x_0. Определим теперь преобразование s (существенно зависящее от выбора пары $\langle t_0, x_0\rangle$) термов так:

а) если t — переменная или константа (отличная от g), то $s(t)=t$;

б) если $t=f(t_1, \ldots, t_n)$ и $t\neq t_0$, то $s(t)=f(s(t_1), \ldots, s(t_n))$;

в) если $t=t_0$, то $s(t)=x_0$.

Замечание. Если терм t не имеет вхождений терма t_0, то $s(t)=t$.

Следующая лемма показывает взаимоотношения преобразования s с подстановкой.

Лемма 2. *Если* $x\neq x_0$ *и* $g\notin F_x(t)$, *то для любого терма* t' *имеет место равенство*

$$s\left((t)^x_{t'}\right)=(s\,(t))^x_{s(t')}.$$

Доказательство. Доказывать это равенство будем индукцией по построению терма t. Если x не входит в t, то x не входит и в $s(t)$, поэтому $s\left((t)^x_{t'}\right)=s\,(t)=(s(t))^x_{s(t')}$. Пусть x входит в t, тогда $t\neq t_0$, так как если $t=t_0=g\,(t_1, \ldots, t_k)$, то $g\in F_x(t)$. Если $t=x$, то $s\left((x)^x_{t'}\right)=s\,(t')=(x)^x_{s(t')}=(s\,(x))^x_{s(t')}$. Если $t=h(t_1, \ldots, t_n)$, то $(t)^x_{t'}=h\left((t_1)^x_{t'}, \ldots, (t_n)^x_{t'}\right)$ и $s\left((t)^x_{t'}\right)=s\left(h\left((t_1)^x_{t'}, \ldots, (t_n)^x_{t'}\right)\right)=h\left(s\left((t_1)^x_{t'}\right), \ldots, s\left((t_n)^x_{t'}\right)\right)$, так как $h\in F_x(t)$, $g\notin F_x(t)$ и, следовательно, $h\left((t_1)^x_{t'}, \ldots, (t_n)^x_{t'}\right)\neq t_0$. Из индукционного предположения получаем $h\left(s((t_1)^x_{t'}), \ldots, s\left((t_n)^x_{t'}\right)\right)=h\left((s\,(t_1))^x_{s(t')}, \ldots, (s\,(t_n))^x_{s(t')}\right)=(s\,(t))^x_{s(t')}$. □

Замечание. В условиях леммы $s(t)=t$ в соответствии с замечанием после определения преобразования s.

Преобразование термов s можно распространить естественным образом и на формулы, секвенции и деревья секвенций, полагая, например, для формул а) $s(\Phi)=P(s(t_1), \ldots, s(t_n))$ для атомарной формулы $\Phi=P(t_1, \ldots, t_n)$;

б) $s(\Phi)=\neg s(\Psi)$ для $\Phi=\neg\Psi$;

в) $s(\Phi)=s(\Phi_0)\tau s(\Phi_1)$ для $\Phi=\Phi_0\tau\Phi_1$, $\tau\in\{\vee, \wedge\}$;

г) $s(\Phi)=\mathrm{Q}xs(\Psi)$ для $\Phi=\mathrm{Q}x\Psi$, $\mathrm{Q}\in\{\forall, \exists\}$.

Следствием предыдущей леммы будет

Предложение 2. *Пусть переменная x_0 не имеет связанных вхождений в Φ; $x\neq x_0$ — такая переменная, что $g\notin F_x(t)$ для любого терма t формулы Φ. Тогда для любого терма t', свободного для x в Φ, имеет место равенство*

$$s\left((\Phi)^x_{t'}\right)=(s(\Phi))^x_{s(t')}$$

(это соотношение включает в себя и утверждение, что $s(t')$ свободен для x в $s(\Phi)$). □

Очевидно, справедливо следующее

Предложение 2′. *Пусть переменная x_0 не имеет связанных вхождений в Φ; $x_1, \ldots, x_n$ — такие переменные, отличные от x_0, что $g\notin F_{x_i}(t)$, $i=1, \ldots, n$, для любого терма t формулы Φ. Тогда для любых термов $t'_1, \ldots, t'_n$, свободных для $x_1, \ldots, x_n$ в Φ соответственно, имеет место равенство*

$$s\left((\Phi)^{x_1, \ldots, x_n}_{t'_1, \ldots, t'_n}\right)=(s(\Phi))^{x_1, \ldots, x_n}_{s(t'_1), \ldots, s(t'_n)}. \square$$

Установим следующее важное свойство преобразования s, действующего на доказательствах.

Предложение 3. *Если D — доказательство в исчислении G, переменная x_0 не встречается в D и g не имеет связанных вхождений в заключительную секвенцию D, то дерево sD является доказательством в G.*

Доказательство. Если $C=\Phi$, $\Gamma\vdash\Theta$, Φ — аксиома, то $sC=s\Phi$, $s\Gamma\vdash s\Theta$, $s\Phi$ — также аксиома.

Для каждого перехода, соответствующего пропозициональному или структурному правилу, легко проверить, что соответствующий s-переход (т. е. переход в sD) осуществляется по тому же правилу вывода. Например, пусть в D переход таков:

$$\frac{\Gamma\vdash\Theta, \Phi;\ \Gamma\vdash\Theta, \Psi}{\Gamma\vdash\Theta, \Phi\wedge\Psi},$$

тогда в sD соответствующий переход есть

$$\frac{s\Gamma\vdash s\Theta,\ s\Phi;\ s\Gamma\vdash s\Theta,\ s\Psi}{s\Gamma\vdash s\Theta,\ s(\Phi\wedge\Psi)}.$$

Но $s(\Phi \wedge \Psi) = s(\Phi) \wedge s(\Psi)$, следовательно, это переход по тому же правилу (введение конъюнкции в заключение).

Рассмотрим теперь переходы, соответствующие кванторным правилам. Пусть переход в D таков:

$$\frac{\Gamma \vdash \Theta,\ (\Phi)_t^x}{\Gamma \vdash \Theta,\ \exists x\Phi}.$$

Тогда в sD соответствующий переход будет

$$\frac{s\Gamma \vdash s\Theta,\ s\left((\Phi)_t^x\right)}{s\Gamma \vdash s\Theta,\ s(\exists x\Phi)}.$$

По следствию 2 предложения 1 g не имеет связанных вхождений в формулу $\exists x\Phi$; следовательно, для любого терма t' формулы Φ имеем $g \notin F_x(t')$. Тогда по предложению 2 $s\left((\Phi)_t^x\right) = (s\Phi)_{s(t)}^x$. Итак, в дереве sD переходом будет

$$\frac{s\Gamma \vdash s\Theta,\ (s\Phi)_{s(t)}^x}{s\Gamma \vdash s\Theta,\ \exists x(s\Phi)},$$

но это переход по правилу введения квантора существования в заключение.

Рассмотрим теперь переход в D по правилу 8:

$$\frac{[\Phi]_y^x,\ \Gamma \vdash \Theta}{\exists x\Phi,\ \Gamma \vdash \Theta},$$

где y не имеет свободных вхождений в Γ, Θ. Соответствующим переходом в sD будет

$$\frac{s[\Phi]_y^x,\ s\Gamma \vdash s\Theta}{s(\exists x\Phi),\ s\Gamma \vdash s\Theta}.$$

Как и выше, устанавливается, что $s[\Phi]_y^x = (s\Phi)_{s(y)}^x = (s\Phi)_y^x = [s\Phi]_y^x$ и что переменная y не встречается свободно в $s\Gamma$, $s\Theta$. Последнее утверждение вытекает из того, что для любой формулы Φ формула $s\Phi$ может содержать только одну новую свободную переменную, а именно, x_0, которая в D не встречается, в частности, $x_0 \neq y$. Тогда в sD переход имеет вид

$$\frac{[s\Phi]_y^x,\ s\Gamma \vdash s\Theta}{\exists x(s\Phi),\ s\Gamma \vdash s\Theta},$$

где y не входит свободно в $s\Gamma$, $s\Theta$. Следовательно, это переход по правилу 8.

Аналогично рассматриваются правила 9 и 10. □

Приступим теперь к рассмотрению основного утверждения настоящего параграфа. Для сокращения записи последовательность термов $t_1, \ldots, t_n$ будет обозначаться $\bar{t}$; $\exists\bar{x}$ означает $\exists x_1 \ldots \exists x_n$; $\bar{z}$ — последовательность $z_1, \ldots \ldots, z_n$.

Теорема 3. *Пусть секвенция* $C = \Gamma \vdash \Theta$, Φ *такова, что* $\Phi = \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z})$ *и* n*-местный функциональный символ* g *не имеет вхождений в* C. *Секвенция* C *доказуема в* G *тогда и только тогда, когда в* G *доказуема секвенция* $C^* = \Gamma \vdash \Theta, \exists\bar{x}\Psi(\bar{x}, g(\bar{x}), \bar{z})$.

Необходимость. Отмеченной формулой назовем всякую формулу Φ_0 исчисления G вида

$$(\exists x_{s+1} \ldots \exists x_n \forall y \Psi(\bar{x}, y, \bar{z}))^{x_1, \ldots, x_s}_{t_1, \ldots, t_s}, \qquad 0 \leqslant s \leqslant n,$$

являющуюся обобщенной подформулой формулы Φ. Если Φ_0 — отмеченная формула, то через Φ_0^* обозначим формулу

$$(\exists x_{s+1} \ldots \exists x_n \Psi(\bar{x}, g(\bar{x}), \bar{z}))^{x_1, \ldots, x_s}_{t_1, \ldots, t_s}.$$

Пусть D — доказательство секвенции C со свойством чистоты переменных. Пусть дерево секвенций D^* получено из D заменой каждого вхождения каждой отмеченной формулы Φ_0, являющегося предком вхождения Φ в заключительную секвенцию C, на формулу Φ_0^*. Заметим, что заключительной секвенцией дерева D^* будет C^*. Покажем, что D^* является квазивыводом.

На вершинах дерева D^* будут стоять те же аксиомы, что и в D, так как отмеченные формулы не являются атомарными (содержат квантор $\forall y$).

Всем переходам дерева D будут соответствовать переходы дерева D^* по тем же правилам вывода, за исключением переходов вида

$$\frac{\Lambda \vdash \Delta, \left[(\Psi(\bar{x}, y, \bar{z}))^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}\right]^y_u}{\Lambda \vdash \Delta, (\forall y \Psi(\bar{x}, y, \bar{z}))^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}}, \tag{*}$$

где главная формула перехода является отмеченной и предком формулы Φ.

Этому переходу в D^* соответствует переход

$$\frac{\Lambda' \vdash \Delta', \left[(\Psi(\bar{x}, y, \bar{z}))^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}\right]^y_u}{\Lambda' \vdash \Delta', (\Psi(\bar{x}, g(\bar{x}), \bar{z}))^{\bar{x}}_{\bar{t}}}. \tag{**}$$

Воспользуемся индукцией по глубине вывода и будем предполагать, что секвенция, стоящая над чертой в переходе (**), является доказуемой. Так как u не имеет вхождений в Λ, Δ и Λ', Δ' имеет те же переменные, что и Λ, Δ, то u не имеет вхождений в Λ', Δ'; следовательно, доказуема секвенция $\Lambda' \vdash \Delta',\ \forall y (\Psi(\bar{x}, y, \bar{z}))_{\bar{t}}^{\bar{x}}$. По предложению 31.2 тогда доказуема и секвенция

$$\Lambda' \vdash \Delta',\ \left((\Psi(\bar{x}, y, \bar{z}))_{\bar{t}}^{\bar{x}}\right)_{g(\bar{t})}^{y},$$

но $\left((\Psi(\bar{x}, y, \bar{z}))_{\bar{t}}^{\bar{x}}\right)_{g(\bar{t})}^{y} = (\Psi(\bar{x}, g(\bar{x}), \bar{z}))_{\bar{t}}^{\bar{x}}$, следовательно, секвенция, стоящая под чертой в переходе (**), доказуема.

Необходимость установлена.

Достаточность. Отмеченной назовем всякую формулу вида $(\exists x_{s+1} \ldots \exists x_n \Psi(\bar{x}, g(\bar{x}), \bar{z}))_{t_1, \ldots, t_s}^{x_1, \ldots, x_s}$, $0 \leqslant s \leqslant n$. Пусть D — доказательство секвенции C^*. Образуем дерево секвенций D^*, которое получается заменой каждого вхождения секвенции $C' = \Gamma' \vdash \Theta'$ на секвенцию $C^+ = \Gamma' \vdash \Theta^+$, где список формул Θ^+ определяется так. Пусть Θ_0 — список всех формул из Θ', не являющихся одновременно отмеченными формулами и предками формулы $\exists \bar{x} \Psi(\bar{x}, \neg g(\bar{x}), \bar{z})$ из заключительной секвенции C^*. Пусть $\bar{t}^1, \ldots, \bar{t}^l$, $l \geqslant 0$,— это все n-наборы термов такие, что термы $g(\bar{t}^i)$ имеют вхождение в секвенцию C'; тогда полагаем $\Theta_1 \leftrightharpoons \Phi (= \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}))$, $\Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots$ $\ldots, \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})$ и $\Theta^+ \leftrightharpoons \Theta_0, \Theta_1$.

Установим индукцией по глубине вывода, что все секвенции дерева D^* являются доказуемыми (заметим, что заключительной секвенцией дерева D^* является секвенция C).

На вершине дерева D^* стоят секвенции, которые могут быть получены из аксиом утончениями и перестановками.

Если в D переход осуществляется по одному из правил 1 — 6, то соответствующий переход в D^* может быть получен несколькими утончениями, перестановками и применением того же правила. Это легко следует из того, что отмеченная формула, являющаяся предком формулы $\exists \bar{x} \Psi(\bar{x}, g(\bar{x}), \bar{z})$ заключительной секвенции, может быть главной формулой перехода по одному из правил 1 — 6 только в случае, когда $s=1$, и тогда эта формула обязательно попадает в список Θ_1.

Если переход в D осуществляется по структурному правилу (11 — 14), то соответствующий переход в D^* получается также применением структурных правил.

Рассмотрим случай, когда в D переход осуществляется по правилу 8:

$$\frac{[\Phi_0]_v^u,\ \Gamma_0 \vdash \Theta_0,\ \Psi_1,\ \ldots,\ \Psi_k}{\exists u\Phi_0,\ \Gamma_0 \vdash \Theta_0,\ \Psi_1,\ \ldots,\ \Psi_k}, \qquad (*)$$

где $\Psi_1, \ldots, \Psi_k$ — это список всех отмеченных формул этих секвенций, являющихся предками формулы $\exists\bar{x}\Psi(\bar{x}, g(\bar{x}), \bar{z})$ заключительной секвенции C^*.

Тогда в D^* переход будет

$$\frac{[\Phi_0]_v^u,\ \Gamma_0 \vdash \Theta_0,\ \Phi,\ \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}),\ \ldots,\ \Psi(\bar{t}^s, g(\bar{t}^s), \bar{z})}{\exists u\Phi_0,\ \Gamma_0 \vdash \Theta_0,\ \Phi,\ \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}),\ \ldots,\ \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})}, \quad l \leqslant s. \qquad (**)$$

Покажем, что переменная v не входит ни в один из термов $g(\bar{t}^i)$, $i=1, \ldots, k$. Предположим противное; пусть v входит в $g(\bar{t}^i)$, тогда $g(\bar{t}^i)$ должен входить в одну из формул секвенции $[\Phi_0]_v^u$, $\Gamma_0 \vdash \Theta_0$, $\Psi_1, \ldots, \Psi_k$. Если $g(\bar{t}^i)$ входит в одну из формул секвенции $\Gamma_0 \vdash \Theta_0$, $\Psi_1, \ldots, \Psi_k$, то v имеет свободное вхождение в эту секвенцию, так как в противном случае g имело бы связанное вхождение в D, что противоречит следствию 2 предложения 1. Но тогда невозможен переход $(*)$ по правилу 8. Если же $g(\bar{t}^i)$ входит в $[\Phi_0]_v^u$, то формула $\exists u\Phi_0$ имеет связанное вхождение символа g, что невозможно. Следовательно, переменная v не имеет свободных вхождений в секвенцию $\Gamma_0 \vdash \Theta_0$, Φ, $\Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots, \Psi(\bar{t}^s, g(\bar{t}^s), \bar{z})$; кроме того, секвенции $[\Phi_0]_v^u$, $\Gamma_0 \vdash \Theta_0$, $\Psi_1, \ldots, \Psi_k$ и $\exists u\Phi_0$, $\Gamma_0 \vdash \Theta_0$, $\Psi_1, \ldots, \Psi_k$ имеют одни и те же вхождения термов вида $g(\bar{t})$. Но тогда $l=s$ и переход $(**)$ осуществляется по правилу 8.

Аналогично рассматривается случай перехода по правилу 9.

Рассмотрим теперь случай перехода по правилу 7. Пусть в D имеется переход

$$\frac{\Gamma_0 \vdash \Theta_0,\ \Psi_1,\ \ldots,\ \Psi_k,\ (\Phi_0)_t^x}{\Gamma_0 \vdash \Theta_0,\ \Psi_1,\ \ldots,\ \Psi_k,\ \exists x\Phi_0}, \qquad (*)$$

где $\Psi_1, \ldots, \Psi_k$ — это отмеченные формулы, являющиеся предками формулы $\exists \bar{x} \Psi(\bar{x}, g(\bar{x}), \bar{z})$ заключительной секвенции, а список Θ_0 таких формул не содержит.

Возможны два случая: 1) формула $\exists x \Phi_0$ не является отмеченной или предком формулы $\exists \bar{x} \Psi(\bar{x}, g(\bar{x}), \bar{z})$; 2) формула $\exists x \Phi_0$ является таковой. Рассмотрим случай 1). Всякий терм вида $g(\bar{t})$ нижней секвенции в переходе (*) является и термом верхней секвенции. Поэтому в D^* соответствующий переходу (*) переход будет

$$\frac{\Gamma_0 \vdash \Theta_0,\ (\Phi_0)^x_t,\ \Phi,\ \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}),\ \ldots,\ \Psi(\bar{t}^s, g(\bar{t}^s), \bar{z})}{\Gamma_0 \vdash \Theta_0,\ \exists x \Phi_0,\ \Phi,\ \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}),\ \ldots,\ \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})}, \quad l \leqslant s. \tag{**}$$

Вместо перехода (**) рассмотрим дерево секвенций

$$\cfrac{\cfrac{\Gamma_0 \vdash \Theta_0,\ (\Phi_0)^x_t,\ \Phi,\ \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}),\ \ldots,\ \Psi(\bar{t}^s, g(\bar{t}^s), \bar{z})}{\Gamma_0 \vdash \Theta_0,\ \exists x \Phi_0,\ \Phi,\ \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}),\ \ldots,\ \Psi(\bar{t}^s, g(\bar{t}^s), \bar{z})}}{\Gamma_0 \vdash \Theta_0,\ \exists x \Phi_0,\ \Phi,\ \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}),\ \ldots,\ \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})}.$$

В этом дереве верхний переход соответствует (с точностью до перестановки) применению правила 7. Для рассмотрения нижнего перехода докажем следующую лемму.

Лемма 3. *Если в G доказуема секвенция*

$$\Gamma \vdash \Theta,\ \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}),\ \Psi(\bar{t}, g(\bar{t}), \bar{z}),$$

символ g не имеет связанных вхождений в эту секвенцию и $g(\bar{t})$ не имеет вхождений в $\Gamma \vdash \Theta, \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z})$, то в G доказуема секвенция

$$\Gamma \vdash \Theta,\ \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}).$$

Доказательство. Пусть D — доказательство секвенции $\Gamma \vdash \Theta, \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}),\ \Psi(\bar{t}, g(\bar{t}), \bar{z})$; x_0 — переменная, не встречающаяся в D. Если s — синтаксическое преобразование, определенное парой $\langle x_0, g(\bar{t}) \rangle$, то по предложению 3 дерево sD является доказательством (секвенции $\Gamma \vdash \Theta, \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}),\ \Psi(\bar{t}, x_0, \bar{z})$ по предложению 2). Следовательно, секвенция $\Gamma \vdash \Theta, \exists \bar{x} \forall y \Psi(\bar{x}, y, \bar{z}),$ $(\Psi(x_1, \ldots, x_n, x_0, \bar{z}))^{\bar{x}}_{\bar{t}}$ доказуема. Легко утверждать, что дерево секвенций

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash \Theta,\ \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}), \left[(\Psi(\bar{x}, y, \bar{z}))^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}\right]^{y}_{x_0}}{\Gamma \vdash \Theta,\ \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}),\ (\forall y\Psi(\bar{x}, y, \bar{z}))^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}}}{\Gamma \vdash \Theta,\ \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}),\ (\exists x_n\forall y\Psi(\bar{x}, y, \bar{z}))^{x_1, \ldots, x_{n-1}}_{t_1, \ldots, t_{n-1}}}}{\vdots}$$

$$\dfrac{\overline{\Gamma \vdash \Theta,\ \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}),\ \exists\bar{x}, \forall y\Psi(\bar{x}, y\ \bar{z})}}{\Gamma \vdash \Theta,\ \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z})}$$

является квазивыводом. □

Следствие. *Если в G доказуема секвенция*

$$\Gamma \vdash \Theta,\ \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z}),\ \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}),\ \ldots,\ \Psi(\bar{t}^s, g(\bar{t}^s), \bar{z}),$$

символ g не имеет связанных вхождений в эту секвенцию и $g(\bar{t}^i)$ не имеет вхождений в $\Gamma \vdash \Theta,\ \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z})$, то в G доказуема секвенция $\Gamma \vdash \Theta,\ \exists\bar{x}\forall y\Psi(\bar{x}, y, \bar{z})$.

Для доказательства нужно расположить термы $g(\bar{t}^1), \ldots$ $\ldots, g(\bar{t}^s)$ в порядке неубывания длины применить индукционное предположение по s и лемму 3. □

Возвращаемся к рассматриваемому случаю: так как термы $g(\bar{t}^1), \ldots, g(\bar{t}^l)$ встречаются в секвенции $\Gamma_0 \vdash \Theta_0$, $\exists x\Phi_0$, а термы $g(\bar{t}^{l+1}), \ldots, g(\bar{t}^s)$ не встречаются в этой секвенции, то эти термы $g(\bar{t}^{l+1}), \ldots, g(\bar{t}^s)$ не встречаются и в секвенции $\Gamma_0 \vdash \Theta_0,\ \exists x\Phi_0,\ \Phi,\ \Psi(\bar{t}^1, g(\bar{t}^1), \bar{z}), \ldots$ $\ldots, \Psi(\bar{t}^l, g(\bar{t}^l), \bar{z})$. Поэтому для установления доказуемости последней секвенции достаточно воспользоваться следствием леммы 3.

Случай 2), когда $\exists x\Phi_0$ является отмеченным предком формулы $\exists\bar{x}\Psi(\bar{x}, g(\bar{x}), \bar{z})$, рассматривается аналогично (даже проще).

Случай, когда переход в дереве D осуществляется по правилу 10, рассматривается аналогично случаю, соответствующему правилу 7. □

С каждой формулой Φ, находящейся в пренексной нормальной форме, свяжем некоторую $\exists$-формулу Φ_H, которую назовем эрбрановой формой формулы Φ, по следующему правилу. Если Φ есть $\exists$-формула, то $\Phi_H = \Phi$; если Φ имеет вид $\exists x_1 \ldots \exists x_n\forall y\Psi(\bar{x}, y, \bar{z})$ и g — n-местный функциональный символ, не встречающийся в Φ, то

$\Phi_H = (\exists x_1 \ldots \exists x_n \Psi(\bar{x}, g(\bar{x}), \bar{z}))_H$. Индукцией по числу кванторов всеобщности устанавливается, что это определение корректно.

Теорема Эрбрана. *Пусть Φ — формула в пренексной нормальной форме, $\Phi_H = \exists x_1 \ldots \exists x_n \Psi(\bar{x}, \bar{z})$ — эрбранова форма формулы Φ, где Ψ — бескванторная формула. Формула Φ доказуема тогда и только тогда, когда существуют такие последовательности термов $\bar{t}^1 = t_1^1, \ldots, t_n^1; \ldots; \bar{t}^k = t_1^k, \ldots, t_n^k$, что доказуема формула $\Psi(\bar{t}^1, \bar{z}) \vee \ldots \vee \Psi(\bar{t}^k, \bar{z})$.*

Доказательство. Используя индукцию (по числу кванторов всеобщности) и предыдущую теорему, получаем, что формула Φ доказуема тогда и только тогда, когда доказуема формула Φ_H. Для завершения доказательства теоремы установим следующее

Предложение 4. *Формула $\Phi = \exists x_1 \ldots \exists x_n \Psi(\bar{x}, \bar{z})$, где Ψ — бескванторная формула, доказуема тогда и только тогда, когда существует такая последовательность n-наборов термов $\bar{t}^1, \ldots, \bar{t}^k$, что доказуема формула $\Psi(\bar{t}^1, \bar{z}) \vee \ldots \vee \Psi(\bar{t}^k, \bar{z})$.*

Доказательство. По свойству обратимости (предложение 31.1) формула $\Psi(\bar{t}^1, \bar{z}) \vee \ldots \vee \Psi(\bar{t}^k, \bar{z})$ доказуема тогда и только тогда, когда доказуема секвенция $\vdash \Psi(\bar{t}^1, \bar{z}), \ldots, \Psi(\bar{t}^k, \bar{z})$.

Пусть эта секвенция доказуема, тогда, многократно применяя правило введения квантора существования в заключение, получаем доказуемую секвенцию $\vdash \exists \bar{x} \Psi(\bar{x}, \bar{z}), \ldots, \exists \bar{x} \Psi(\bar{x}, \bar{z})$. Из этой секвенции с помощью правил сокращения получаем секвенцию $\vdash \exists \bar{x} \Psi(\bar{x}, \bar{z})$. Так устанавливается достаточность.

Необходимость. Пусть D — доказательство формулы Φ в исчислении G со свойством чистоты переменных. Пусть $\bar{t}^1, \ldots, \bar{t}^k$ — это все наборы n-термов $\bar{t}$ таких, что в D встречается формула $\Psi(\bar{t}, \bar{z})$. Заметим, что все формулы дерева D, являются предками формулы Φ. Пусть дерево D^* получается из D заменой каждого вхождения секвенции $\Gamma_0 \vdash \Delta_0$ на секвенцию $\Gamma_0 \vdash \Psi(\bar{t}^1, \bar{z}), \ldots, \Psi(\bar{t}^k, \bar{z}), \Delta_1$, где Δ_1 получается из Δ_0 вычеркиванием всех формул вида $(\exists x_{s+1} \ldots \exists x_n \Psi(\bar{x}, \bar{z}))_{t_1, \ldots, t_s}^{x_1, \ldots, x_s}$, $0 \leqslant s \leqslant n$. Без труда проверяется, что полученное дерево D^* будет квазивыводом (секвенции $\vdash \Psi(\bar{t}^1, \bar{z}), \ldots, \Psi(\bar{t}^k, \bar{z})$). Действительно, на вершинах стоят секвенции, полученные из аксиом утончениями. Переходу, соответствующему пропозициональным правилам, соответствуют переходы по тому же правилу (быть может, с сокращением и перестановками). Кванторные правила, за исключением правила 7, в дереве D не используются; переходам по правилу 7 соответствуют тривиальные переходы в D^*. Переходам по структурным правилам соответствуют переходы, полученные применением структурных правил. Итак, D^* — квазивывод секвенции $\vdash \Psi(\bar{t}^1, \bar{z}), \ldots, \Psi(\bar{t}^k, \bar{z})$ и необходимость установлена. □

Сила теоремы Эрбрана в том, что вопрос о доказуемости произвольной формулы сводится к вопросу о доказуемости формулы из некоторой эффективно порождаемой последовательности бескванторных формул. А для обнаружения доказуемости бескванторной формулы требуются только пропозициональные (и структурные) правила.

Более точно, пусть Φ — бескванторная формула, а $\Psi_0, \ldots, \Psi_n$ — все различные атомарные подформулы формулы Φ; тогда пропозициональной формой формулы Φ назовем формулу Φ_P исчисления высказываний, которая получается из Φ подстановкой всюду вместо подформулы Ψ_i пропозициональной переменной P_i, $i = 0, \ldots, n$.

Предложение 5. *Бескванторная формула Φ доказуема в исчислении G тогда и только тогда, когда ее пропозициональная форма Φ_P доказуема в исчислении высказываний.*

Доказательство. Прямо вытекает из свойства подформульности. □

§ 34. Исчисления резольвент

Исчисления резольвент используются для поиска вывода в исчислениях высказываний и предикатов. Начнем с пропозиционального варианта.

Формулами пропозициональных исчислений резольвент будут пропозициональные переменные или их отрицания.

Если Φ — формула, то Φ^* есть $\neg\Phi$, когда Φ — пропозициональная переменная, и есть P, когда $\Phi = \neg P$.

Основным синтаксическим понятием будет *список формул*. Пустой список будем обозначать символом $\varnothing$. Исчисления резольвент будут иметь одни и те же правила вывода и различаться только аксиомами. Если Γ_0; ...

...; Γ_n — списки формул, то через $R_P(\Gamma_0; \ldots; \Gamma_n)$ будем обозначать (*пропозициональное*) *исчисление резольвент*, аксиомами которого являются списки $\Gamma_0; \ldots; \Gamma_n$.

Правилами вывода исчислений резольвент будут:

$$1.\ \frac{\Gamma, \Phi;\quad \Theta, \Phi^*}{\Gamma, \Theta}, \quad 2.\ \frac{\Gamma, \Phi, \Psi, \Theta}{\Gamma, \Psi, \Phi, \Theta}, \quad 3.\ \frac{\Gamma, \Phi, \Phi}{\Gamma, \Phi}.$$

Понятие *доказательства* (в виде дерева) определяется обычным образом. Если Γ — непустой список формул, то через $\bigwedge \Gamma$ будем обозначать конъюнкцию формул из Γ. $\bigwedge \Gamma$ — формула исчисления высказываний, но, вообще говоря, не является формулой исчисления резольвент.

Лемма 1. *Если D — доказательсво списка Γ в $R_P(\Gamma_0; \ldots; \Gamma_n)$ и Γ_n встречается на вершине D, то для любого списка Γ' в $R_P(\Gamma_0; \ldots; \Gamma_{n-1}; \Gamma', \Gamma_n)$ доказуем список Γ', Γ.*

Доказательство проводится индукцией по числу списков дерева D. Если $D = \Gamma_n$, то $\Gamma = \Gamma_n$ и Γ', Γ — доказательство в $R_P(\Gamma_0; \ldots; \Gamma_{n-1}; \Gamma', \Gamma_n)$.

Пусть $D = \dfrac{D_0; D_1}{\Gamma}$ и последний переход есть $\dfrac{\Gamma^0, \Phi; \Gamma^1, \Phi^*}{\Gamma^0, \Gamma^1}$, тогда по индукционному предположению существуют доказательства D_0', D_1' в $R_P(\Gamma_0; \ldots; \Gamma_{n-1}; \Gamma', \Gamma_n)$ списков Γ', Γ^0, Φ (или Γ^0, Φ, если Γ_n не встречается на вершине D_0) и $\Gamma', \Gamma^1, \Phi^*$ (или Γ^1, Φ^*, если Γ_n не встречается в D_1) соответственно. Так как Γ_n встречается на вершине D_0 или на вершине D_1, то по крайней мере одно из деревьев

$$\frac{D_0'; D_1'}{\Gamma', \Gamma^0, \Gamma', \Gamma^1}, \quad \frac{D_0'; D_1'}{\Gamma', \Gamma^0, \Gamma^1}, \quad \frac{D_0'; D_1'}{\Gamma^0, \Gamma', \Gamma^1}$$

есть доказательство в $R_P(\Gamma_0; \ldots; \Gamma_{n-1}; \Gamma', \Gamma_n)$. Из заключительного списка структурными правилами легко получается список Γ', Γ.

Если последний переход дерева D осуществляется по правилам 2 и 3, то индукционный шаг очевиден. □

Докажем теперь утверждение, связывающее исчисление резольвент с доказуемостью в исчислении высказываний.

Предложение 1. *Если $\Gamma_0; \ldots; \Gamma_n$ — непустые списки формул (исчисления резольвент), то формула $\bigvee_{i=0}^{n} (\bigwedge \Gamma_i)$ доказуема в исчислении высказываний тогда и* *только тогда, когда в исчислении $R_P(\Gamma_0; \ldots; \Gamma_n)$ доказуем пустой список формул $\varnothing$.*

Доказательство. Пусть D — такое дерево списков формул, что на вершинах стоят непустые списки формул $\Theta_0; \ldots; \Theta_k$, каждый переход есть переход по одному из правил вывода исчисления резольвент, а Θ — заключительный (быть может, пустой) список формул. Докажем, что тогда в исчислении высказываний доказуема секвенция $\Theta \vdash \bigvee_{i=0}^{k} (\bigwedge \Theta_i)$. Доказывать будем индукцией по числу списков формул в дереве D.

Пусть D состоит из единственного (непустого) списка Θ, тогда секвенция $\Theta \vdash \bigwedge \Theta$, очевидно, доказуема в исчислении высказываний.

Пусть дерево D имеет вид $\dfrac{D_0;\ D_1}{\Theta}$; $\Theta_0^0; \ldots; \Theta_{k_0}^0$ — списки, стоящие на вершинах дерева D_0; $\Theta_0^1; \ldots; \Theta_{k_1}^1$ — списки, стоящие на вершинах дерева D_1. Пусть заключительный переход есть

$$\frac{\Theta_0, \Phi;\quad \Theta_1, \Phi^*}{\Theta}$$

(тогда $\Theta = \Theta_0, \Theta_1$). По индукционному предположению в исчислении высказываний доказуемы секвенции $\Theta_0, \Phi \vdash \Phi^0$ и $\Theta_1, \Phi^* \vdash \Phi^1$, где $\Phi^0 = \bigvee_{i=0}^{k_0} (\bigwedge \Theta_i^0)$ и $\Phi^1 = \bigvee_{i=0}^{k_1} (\bigwedge \Theta_i^1)$. Тогда дерево

$$\frac{\vdash \Phi \vee \Phi^*;\quad \dfrac{\Theta_0, \Phi \vdash \Phi^0}{\Theta_0, \Phi \vdash \Phi^0 \vee \Phi^1};\quad \dfrac{\Theta_1, \Phi^* \vdash \Phi^1}{\Theta_1, \Phi^* \vdash \Phi^0 \vee \Phi^1}}{\Theta_0, \Theta_1 \vdash \Phi^0 \vee \Phi^1}$$

есть квазивывод нужной секвенции для дерева D. Случаи, когда последний переход в дереве D соответствует структурным правилам 2 или 3, очевиден. Из доказанного утверждения вытекает, что если в $R_P(\Gamma_0; \ldots; \Gamma_n)$ доказуем пустой список формул, то формула $\bigvee_{i=0}^{n} (\bigwedge \Gamma_i)$ доказуема в исчислении высказываний.

Для доказательства обратного утверждения будем использовать пропозициональный вариант G_P исчисления G. Индукцией по числу символов конъюнкций в секвенции

$$\vdash \bigwedge \Theta_0, \ldots, \bigwedge \Theta_k \qquad (*)$$

покажем, что если эта секвенция доказуема в G_P, то в $R_P(\Theta_0; \ldots; \Theta_k)$ доказуем пустой список.

Пусть секвенция $(*)$ не содержит знака конъюнкции. Тогда она имеет вид $\vdash \Phi_0, \ldots; \Phi_k$, где Φ_i — пропозициональные переменные или их отрицания. Такая секвенция доказуема в G_P в том и только в том случае, когда существуют $i, j \leqslant k$ такие, что $\Phi_i = \Phi_j^*$, тогда

$$\frac{\Phi_j; \Phi_j^*}{\varnothing}$$

есть доказательство в $R_P(\Phi_0; \ldots; \Phi_k)$.

Пусть для секвенций вида $(*)$ с числом знаков $\bigwedge$, меньшим n, утверждение справедливо. Пусть секвенция $(*)$ имеет n знаков $\bigwedge$ и $\Theta_k = \Theta_k^0, \Theta_k^1$, где Θ_k^0 и Θ_k^1 — непустые списки формул. По свойству обратимости, если секвенция $(*)$ доказуема, то доказуемы и секвенции $\vdash \bigwedge \Theta_0, \ldots, \bigwedge \Theta_{k-1}, \bigwedge \Theta_k^0$ и $\vdash \bigwedge \Theta_0, \ldots, \bigwedge \Theta_{k-1}, \bigwedge \Theta_k^1$. По индукционному предположению в $R_P(\Theta_0; \ldots; \Theta_{k-1}; \Theta_k^0)$ и $R_P(\Theta_0; \ldots; \Theta_{k-1}; \Theta_k^1)$ доказуем пустой список $\varnothing$. Пусть D_0 и D_1 — соответствующие доказательства. Если Θ_k^1 не встречается на вершинах дерева D_1, то D_1 — доказательство (списка $\varnothing$) в $R_P(\Theta_0; \ldots; \Theta_{k-1})$ и тем более в $R_P(\Theta_0; \ldots; \Theta_{k-1}; \Theta_k)$. Если же Θ_k^1 встречается на вершинах дерева D_1, то по лемме 1 в $R_P(\Theta_0; \ldots; \Theta_{k-1}; \Theta_k = \Theta_k^0, \Theta_k^1)$ существует доказательство D_0' списка Θ_k^0. Подставляя в D_0 на место всех вершин вида Θ_k^0 дерево D_0', получим доказательство пустого списка в $R_P(\Theta_0; \ldots; \Theta_k)$.

Возвращаемся к доказательству нужного утверждения. По свойству обратимости формула $\bigvee_{i=0}^{n} (\bigwedge \Gamma_i)$ доказуема в G_P тогда и только тогда, когда доказуема секвенция $\vdash \bigwedge \Gamma_0, \ldots, \bigwedge \Gamma_n$. По только что доказанному утверждению из доказуемости секвенции $\vdash \bigwedge \Gamma_0, \ldots, \bigwedge \Gamma_n$ следует, что в $R_P(\Gamma_0; \ldots; \Gamma_n)$ доказуем пустой список формул $\varnothing$. □

Перейдем теперь к изучению *исчислений резольвент* для исчисления предикатов.

Формулами исчисления резольвент будут атомарные формулы исчисления G или их отрицания. Для формулы Φ обозначение Φ^* определяется, как выше. *Правилами вывода* будут правила 1, 2, 3 и правило

$$4.\ \frac{\Gamma}{(\Gamma)^{\bar{x}}_{\bar{t}}},$$

где $\bar{x} = x_1, \ldots, x_k$ — список различных переменных, а $\bar{t} = t_1, \ldots, t_k$ — список термов.

Исчисления резольвент различаются аксиомами. Исчисление резольвент с аксиомами (списками) $\Gamma_0; \ldots; \Gamma_n$ обозначается $R(\Gamma_0; \ldots; \Gamma_n)$. Связь исчисления резольвент с доказуемостью в исчислении предикатов устанавливается следующим утверждением.

Предложение 2. *Предположим, что* $\Phi = \exists x_1 \ldots \ldots \exists x_m \left(\bigvee_{i=0}^{n} (\bigwedge \Gamma_i) \right)$ — *замкнутая формула исчисления предикатов, а* Γ_i, $i = 0, \ldots, n$,— *непустые списки атомарных формул или их отрицаний. Формула* Φ *доказуема в исчислении предикатов тогда и только тогда, когда в исчислении резольвент* $R(\Gamma_0; \ldots; \Gamma_n)$ *доказуем пустой список формул.*

Доказательство. Пусть Φ — доказуемая в G формула, тогда по предложению 33.4 существуют такие наборы термов $\bar{t}^1 = t_1^1, \ldots, t_m^1; \ldots; \bar{t}^k = t_1^k, \ldots, t_m^k$, что доказуема секвенция

$$\vdash \left(\bigvee_{i=0}^{n} (\bigwedge \Gamma_i) \right)^{\bar{x}}_{\bar{t}^1}, \ldots, \left(\bigvee_{i=0}^{n} (\bigwedge \Gamma_i) \right)^{\bar{x}}_{\bar{t}^k}.$$

Доказуемость этой секвенции равносильна доказуемости формулы

$$\Phi' = \bigvee_{\substack{0 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant k}} (\bigwedge \Gamma_i)^{\bar{x}}_{\bar{t}^j}.$$

По предложению 33.5 Φ' доказуема тогда и только тогда, когда доказуема пропозициональная формула Φ'_P. Используя предложение 1, из доказуемости формулы Φ'_P в исчислении высказываний получаем, что в исчислении резольвент $R\left(\ldots; (\Gamma_i)^{\bar{x}}_{\bar{t}^j}; \ldots\right)$ доказуем пустой список с использованием только правил 1—3. (Для этого в доказательстве пустого списка в пропозициональном исчислении резольвент, связанном с формулой Φ'_P, нужно сделать обратную замену пропозициональных переменных на соответствующие элементарные формулы.) Но так как списки $(\Gamma_i)^{\bar{x}}_{\bar{t}^j}$ получаются из списков Γ_i по правилу 4, то получаем, что в $R(\Gamma_0; \ldots; \Gamma_n)$ доказуем пустой список.

Для доказательства обратного утверждения, как в предложении 1, будем доказывать такое утверждение: если D — доказательство списка Θ в $R(\Gamma_0; \ldots; \Gamma_n)$ и $\bar{x} = x_1, \ldots, x_m$ — список всех переменных из формул списков $\Gamma_0; \ldots; \Gamma_n$, то существуют такие наборы термов $\bar{t}^i = \bar{t}^i_1, \ldots, t^i_m$, $i = 1, \ldots, k$, что в исчислении G доказуема секвенция $\Theta \vdash \bigvee\limits_{i=1}^{k} \left(\bigvee\limits_{j=0}^{n} \left(\bigwedge (\Gamma_j)^{\bar{x}}_{\bar{t}^i} \right) \right)$.

Доказательство проводится индукцией по числу списков в доказательстве D. В случае, когда D есть просто список Γ_i, следующее дерево будет квазивыводом нужной секвенции:

$$\frac{\Gamma_i \vdash \bigwedge \Gamma_i}{\Gamma_i \vdash \bigvee\limits_{j=1}^{k} (\bigwedge \Gamma_j)}.$$

Пусть доказательство D имеет вид $\dfrac{D'}{\Theta}$, а последний переход есть $\dfrac{\Theta'}{\Theta}$, где $\Theta = (\Theta')^{\bar{u}}_{\bar{t}}$. По индукционному предположению для некоторых наборов термов $\bar{t}^1, \ldots, \bar{t}^k$ в исчислении предикатов доказуема секвенция

$$C = \Theta' \vdash \bigvee_{i=1}^{k} \left(\bigvee_{j=0}^{n} \left(\bigwedge (\Gamma_j)^{\bar{x}}_{\bar{t}^i} \right) \right).$$

Очевидно, что из доказуемости секвенции C следует и доказуемость секвенции $C' = (C)^{\bar{u}}_{\bar{t}}$ (нужно взять доказательство D секвенции C в G и сделать подстановку $(D)^{\bar{u}}_{\bar{t}}$), но тогда доказуема секвенция $C' = \Theta \vdash \bigvee\limits_{i=1}^{k} \left(\bigvee\limits_{j=0}^{n} \left(\bigwedge (\Gamma_j)^{\bar{x}}_{\bar{t}'^j} \right) \right)$, где $\bar{t}'^j = (\bar{t}^j)^{\bar{u}}_{\bar{t}}$.

Рассмотрение случаев, когда последний переход в доказательстве D осуществляется по правилу 1, 2 или 3,— как в предложении 1. Итак, если в $R(\Gamma_0; \ldots; \Gamma_n)$ доказуем пустой список $\varnothing$, то существуют такие наборы термов $\bar{t}^1; \ldots; \bar{t}^k$, что доказуема секвенция $\vdash \bigvee_{i=1}^{k}\left(\bigvee_{j=0}^{n}\left(\bigwedge (\Gamma_j)_{\bar{t}^i}^{\bar{x}}\right)\right)$.

Тогда доказуема секвенция $\vdash \left(\bigvee_{j=0}^{n}(\bigwedge \Gamma_j)\right)_{\bar{t}^1}^{\bar{x}}, \ldots$

$\ldots, \left(\bigvee_{j=0}^{n}(\bigwedge \Gamma_j)\right)_{\bar{t}^k}^{\bar{x}}$. Из доказуемости такой секвенции легко выводится, что доказуема и секвенция

$$\vdash \exists x_1 \ldots \exists x_m\left(\bigvee_{j=0}^{n}(\bigwedge \Gamma_j)\right). \ \square$$

Укажем теперь, как свести вопрос о доказуемости в G произвольной формулы Φ исчисления G к вопросу о доказуемости пустого списка в подходящем исчислении резольвент.

Если Φ содержит свободные переменные $z_0, \ldots, z_n$, то, используя следствие предложения 31,2, легко проверить, что Φ доказуема тогда и только тогда, когда доказуемо универсальное замыкание $\Phi^0 = \forall z_0 \ldots \forall z_n \Phi$ формулы Φ.

Пусть Φ^0 — замкнутая формула, тогда для нее эффективно находится ей эквивалентная формула Φ^1, находящаяся в пренексной нормальной форме. По теореме Эрбрана доказуемость формулы Φ^1 (а следовательно, также формул Φ^0 и Φ) равносильна доказуемости эрбрановой формы Φ_H^1 формулы Φ^1. Матрица формулы Φ_H^1 находится в дизъюнктивной нормальной форме, т. е. имеет вид $\bigvee_{i=0}^{n}(\bigwedge \Gamma_i)$, где Γ_i — некоторые списки атомарных формул или их отрицаний. Но тогда Φ_H^1 есть замкнутая $\exists$-формула и, следовательно, ее доказуемость по предложению 2 равносильна выводимости пустого списка $\varnothing$ в исчислении резольвент $R(\Gamma_0, \ldots, \Gamma_n)$.

Из только что доказанного, теоремы 23.11 и теоремы 32.2 получаем сводимость вопроса о доказуемости произвольной формулы Φ в исчислении предикатов к вопросу о доказуемости пустого списка в подходящем исчислении резольвент.

Для машинной реализации поиска доказуемости пустого списка в исчислении резольвент используются различные детерминированные (иногда и недетерминированные) способы последовательного преобразования списков так, чтобы все доказуемые списки были получены при таких преобразованиях. Такие способы носят названия *стратегий* поиска. Обсуждение каких-либо стратегий выходит за рамки нашего учебника.

Чтобы хоть немного почувствовать возникающие здесь проблемы, предлагается доказать следующее утверждение.

Предложение 3. *Существует алгоритм, который по двум формулам Ф и Ψ исчисления резольвент узнает, существуют ли такие наборы термов* $\bar{t} = t_1, \ldots, t_n$, *что формулы* $(\Phi)_{\bar{t}}^{\bar{x}}$ *и* $(\Psi)_{\bar{t}}^{\bar{x}}$ *совпадают, и если такие наборы существуют, то находит универсальный такой набор* t.

Универсальность означает, что для любого набора $\bar{t}'$ такого, что $(\Phi)_{\bar{t}'}^{\bar{x}} = (\Psi)_{\bar{t}'}^{\bar{x}}$, существует такой набор термов $\bar{t}'' = t_0'', \ldots, t_k''$, соответствующий списку $\bar{u} = u_0, \ldots, u_k$ свободных переменных термов из $\bar{t}$, что $\bar{t}' = (\bar{t})_{\bar{t}''}^{\bar{u}}$. □

Глава 7

АЛГОРИТМЫ И РЕКУРСИВНЫЕ ФУНКЦИИ

§ 35. Нормальные алгорифмы и машины Тьюринга

В предыдущих главах мы неоднократно говорили об алгоритме $\mathfrak{A}$, действующем на некотором множестве объектов X, понимая под этим точное предписание, определяющее по любому объекту $a \in X$ некоторую вполне определенную последовательность простейших действий, осуществляя которые, мы либо никогда не закончим этот процесс (вычисления), либо этот процесс заканчивается и мы получаем объект $\mathfrak{A}(a)$, называемый *значением* $\mathfrak{A}$ *на* a, либо процесс обрывается без получения значения. Если процесс, определяемый алгоритмом $\mathfrak{A}$ по элементу a, не заканчивается или обрывается без получения значения, то говорят, что $\mathfrak{A}$ *не применим к* a. Примерами алгоритмов могут служить правила сложения, умножения и деления, действующие на множестве пар натуральных чисел. Заметим, что алгоритм деления не применим к паре натуральных чисел $\langle n, m \rangle$, если n не делится нацело на m. Другим примером является описанный в § 20 алгоритм нахождения по формуле исчисления предикатов эквивалентной ей формулы, находящейся в пренексной нормальной форме. Количество простейших действий, необходимых для получения значения алгоритма, может быть весьма большим. Однако мы отвлекаемся (абстрагируемся) на данном уровне изучения от реальных возможностей осуществления алгоритмов и будем исходить из предположения, что при осуществлении процесса вычисления, определенного алгоритмом, мы имеем неограниченный запас времени и материалов. Такое предположение носит название *принципа потенциальной осуществимости*.

Как правило, интуитивного понимания бывает достаточно для установления того, является ли данное предписание алгоритмом или нет. Однако без точного определения алгоритма невозможно обойтись, если пытаться доказывать, что для решения определенного класса задач не существует единой эффективной процедуры (алгоритма). Но возможно ли найти такое математическое определение понятия алгоритма, чтобы и охватить все разнообразие уже существующих алгоритмов и эффективных процедур, накопленных математической и вычислительной практикой, и быть уверенным, что любой предложенный в будущем интуитивно приемлемый алгоритм подпадает под это определение? Поставленный столь широко вопрос вряд ли имеет положительное решение. Однако реальное развитие математики привело к удовлетворительному решению (точнее было бы сказать снятию) этой проблемы. А именно, было предложено несколько формализаций понятия алгоритма, различающихся возможными областями действия, набором допустимых простейших действий и возможностями составления предписаний (программ) для вычисления. Изучение этих формализаций показало, что они обладают свойствами замкнутости относительно всевозможных комбинаций (суперпозиции, итерации и т. п.), большими возможностями воспроизводить с достаточной степенью похожести (адекватности) все известные алгоритмические процедуры и приемы. Наиболее существенным для оправдания определений оказалось совпадение классов вычислимых функций для всех этих понятий. Поэтому по крайней мере понятие (алгоритмически) вычислимой функции (с натуральными аргументами и значениями) оказалось инвариантно определенным и для теоретических целей этого вполне достаточно. Существование ряда различных определений (уточнений) понятия алгоритма имеет и свои преимущества, так как для решения различных задач бывает удобно использовать различные, наиболее подходящие для этого случая, определения. Аналогию этому явлению можно найти в программировании — существующее многообразие языков программирования во многом объясняется разнообразием задач, стоящих перед вычислителями и программистами. В этом параграфе будут даны определения для двух различных классов алгоритмов — *нормальные алгорифмы* (слово «алгорифм» есть вариант написания слова «алгоритм», и этот вариант традиционно используется при изложении теории нормальных алгоритмов) и *машины Тьюринга*. Сколько-нибудь подробного изучения этих понятий здесь не будет, мы ограничимся точными определениями, примерами и формулировками основного утверждения о связи этих понятий. В последующих параграфах будет более подробно изучен класс вычислимых функций и ему будет дано еще одно (уже третье) определение.

Прежде чем перейти к точным определениям, разберем один пример.

Пример 1. Построим алгоритм $\mathfrak{A}$, действующий на множестве слов алфавита ИВ и вычисляющий характеристическую функцию множества формул ИВ, т. е. такой алгоритм $\mathfrak{A}$, что $\mathfrak{A}(\alpha)=1$, если α — формула ИВ, и $\mathfrak{A}(\alpha)=0$ в противном случае.

Пусть φ — буква, отличная от всех букв алфавита ИВ. Над каждым словом α в алфавите ИВ будем производить следующие преобразования:

1. Заменим каждое вхождение пропозициональной переменной в слове α на букву φ; пусть полученное слово есть α_1.

2. Строим последовательность слов $\alpha_1, \alpha_2, \ldots, \alpha_n$ такую, что каждое слово α_{i+1}, $0<i<n$, получается из слова α_i заменой одного подслова вида $\neg\varphi, (\varphi\wedge\varphi)$, $(\varphi\vee\varphi)$ или $(\varphi\to\varphi)$ на φ, а слово α_n не содержит ни одного подслова указанного вида.

3. Если α_n совпадает с φ, то полагаем $\mathfrak{A}(\alpha)=1$, если же α_n отлично от φ, то полагаем $\mathfrak{A}(\alpha)=0$.

Оставляя читателю возможность убедиться в применимости этого алгоритма к любому слову и в правильности этого алгоритма, отметим, что простейшими действиями в этом алгоритме являются последовательные замены вхождений подслов специального вида на другие слова. Важной особенностью этого алгоритма является возможная неоднозначность (недетерминированность) в процессе вычисления — последовательность слов $\alpha_1, \alpha_2, \ldots$ $\ldots, \alpha_n$ определяется по α не единственным образом (хотя число n, как легко проверить, определено однозначно). Определяемые ниже понятия нормального алгорифма и машины Тьюринга в качестве простейших действий также будут иметь замены подслов словами, но последовательность этих операций будет однозначно определена.

Каждый из определяемых ниже алгоритмов будет действовать на множестве всех слов некоторого алфавита B. Часть букв этого алфавита будет играть вспомогательную техническую роль, поэтому, чтобы подчеркнуть существенную часть A алфавита B $(A \subseteq B)$, о всяком алгоритме $\mathfrak{A}$, действующем на множестве слов алфавита B, говорят, что $\mathfrak{A}$ есть *алгоритм над* A.

Алгоритмы $\mathfrak{B}$ и $\mathfrak{C}$ над алфавитом A будем называть *эквивалентными относительно* A, если для любого слова α алфавита A выполняются два условия:

а) если $\mathfrak{B}$ применим к слову α алфавита A, то $\mathfrak{C}$ применим к α и $\mathfrak{B}(\alpha)=\mathfrak{C}(\alpha)$;

б) условие, полученное из а) перестановкой $\mathfrak{B}$ и $\mathfrak{C}$.

Перейдем к формулировке понятия нормального алгорифма, предложенного А. А. Марковым. Пусть в дальнейшем A — конечный алфавит.

Определение. *Схемой S в алфавите A* называется упорядоченный набор троек

$$\langle\langle\alpha_1,\ \beta_1,\ \delta_1\rangle,\ \ldots,\ \langle\alpha_n,\ \beta_n,\ \delta_n\rangle\rangle,$$

у которых первые два элемента α_i, β_i являются словами алфавита A, а третий элемент δ_i принадлежит множеству $\{0, 1\}$. *Нормальным алгорифмом* в алфавите A называется пара $\langle A, S\rangle$, состоящая из алфавита A и схемы S в алфавите A.

Пусть α — слово в алфавите A, $\mathfrak{A}=\langle A, S\rangle$ — нормальный алгорифм, $S=\langle\langle\alpha_1, \beta_1, \delta_1\rangle, \ldots, \langle\alpha_n, \beta_n, \delta_n\rangle\rangle$. Если ни одно из слов $\alpha_1, \ldots, \alpha_n$ не является подсловом слова α, то будем говорить, что слово α *не поддается алгорифму* $\mathfrak{A}$. Если i_0 — наименьшее число, для которого α_{i_0} является подсловом α, и β — результат замены первого вхождения α_{i_0} в α на слово β_{i_0}, то будем говорить, что $\mathfrak{A}$ *просто переводит α в β, если* $\delta_{i_0}=0$ (обозначаем $\mathfrak{A}$: $\alpha\vdash\beta$), и $\mathfrak{A}$ *заключительно переводит* α в β, если $\delta_{i_0}=1$ (обозначаем $\mathfrak{A}$: $\alpha\vdash\cdot\beta$). При этом предполагается, конечно, что знаки $\vdash$ и $\cdot$ не принадлежат алфавиту A. Если нормальный алгорифм $\mathfrak{A}$ просто или заключительно переводит α в β, то говорим, что $\mathfrak{A}$ *переводит* α в β. Будем говорить, что нормальный алгорифм $\mathfrak{A}$ *преобразует слово α в слово* β (обозначаем $\mathfrak{A}(\alpha)=\beta$), если существует такая последовательность $\gamma_0, \ldots, \gamma_k$ слов алфавита A, что выполняются следующие условия:

а) $\gamma_0=\alpha$ и $\gamma_k=\beta$;

б) если $k=0$, то α не поддается $\mathfrak{A}$;

в) $\mathfrak{A}$ просто переводит γ_i в γ_{i+1} для $i<k-1$;

г) если $k>0$ и не имеет места $\mathfrak{A}$: $\gamma_{k-1}\vdash\cdot\gamma_k$, то $\mathfrak{A}$: $\gamma_{k-1}\vdash\gamma_k$ и γ_k не поддается $\mathfrak{A}$.

Если последовательность $\gamma_0, \ldots, \gamma_k$ удовлетворяет условиям а)—в) и условию $\mathfrak{A}$: $\gamma_{k-1}\vdash\gamma_k$ ($\mathfrak{A}$: $\gamma_{k-1}\vdash\cdot\gamma_k$), то будем в этом случае писать $\mathfrak{A}$: $\alpha\models\beta$ ($\mathfrak{A}$: $\alpha\models\cdot\beta$).

Из определения следует, что если нормальный алгорифм $\mathfrak{A}$ переводит слово α в слово β, то β однозначно определяется по $\mathfrak{A}$ и α. Если алгорифм $\mathfrak{A}$ заключительно переводит α в β, то $\mathfrak{A}$ не может просто переводить α в β. Ясно также, что если α не поддается $\mathfrak{A}$, то $\mathfrak{A}$ не переводит α ни в какое слово. Из этих свойств получаем, что если нормальный алгорифм $\mathfrak{A}$ преобразует слово α в слово β, то β однозначно определяется по $\mathfrak{A}$ и α (это оправдывает обозначение $\mathfrak{A}(\alpha)=\beta$). Если нормальный алгорифм не преобразует слово α ни в какое слово, то говорим, что алгоритм $\mathfrak{A}$ *не применим к слову* α. Заметим, что если нормальный алгорифм $\mathfrak{A}=\langle A, S\rangle$ не применим к слову α алфавита A, то существует бесконечная последовательность слов $\gamma_0=\alpha, \gamma_1, \gamma_2, \ldots, \gamma_n, \ldots$, для которой $\mathfrak{A}$: $\gamma_i\vdash\gamma_{i+1}$, $i\in\omega$.

В дальнейшем тройку $\langle\alpha, \beta, \delta\rangle$, принадлежащую схеме S в алфавите A, будем изображать более наглядно: $\alpha\to\beta$, если $\delta=0$, и $\alpha\to\cdot\beta$, если $\delta=1$, предполагая, конечно, что символы $\to$ и $\cdot$ не принадлежат алфавиту A. При этом схему S будем задавать через нумерацию таких слов.

Пример 2. Пусть $A=\{Q_0, Q_1, \wedge, \vee, \neg, (,), a\}$. Рассмотрим нормальный алгорифм $\mathfrak{A}=\langle A, S\rangle$ со следующей схемой:

1) $aQ_0\to Q_0a$,	6) $a(\to(a$,
2) $aQ_1\to Q_1a$,	7) $a)\to)a$,
3) $a\wedge\to\wedge a$,	8) $a\to\cdot\vee Q_0)$,
4) $a\vee\to\vee a$,	9) $\Lambda\to(a$.
5) $a\neg\to\neg a$,	

Предлагаем читателю проверить, что если Φ — формула ИВ в алфавите $A\setminus\{a\}$, то $\mathfrak{A}(\Phi)=(\Phi\vee Q_0)$. Для иллюстрации его работы выпишем ряд последовательных подстановок, осуществляемых алгорифмом $\mathfrak{A}$, начинающим с формулы $(Q_0\wedge\neg Q_1)$. При этом часть слова, которая заменяется на данном этапе, выделим скобкой $\underbracket{\quad}$:

$$\underbracket{\quad}(Q_0 \wedge \neg Q_1) \to (\underbracket{a\,(}Q_0 \wedge \neg Q_1) \to ((\underbracket{aQ_0} \wedge \neg Q_1) \to$$

$$\to ((Q_0\underbracket{a \wedge} \neg Q_1) \to ((Q_0 \wedge \underbracket{a\, \neg}\, Q_1) \to ((Q_0 \wedge \neg\, \underbracket{aQ_1)} \to$$

$$\to ((Q_0 \wedge \neg\, \underbracket{Q_1 a)} \to ((Q_0 \wedge \neg Q_1)\, \underbracket{a} \to \cdot\, ((Q_0 \wedge \neg Q_1) \vee Q_0).$$

Сформулируем теперь основное принципиальное положение об «универсальности» нормальных алгорифмов.

Принцип нормализации. *Любой алгоритм над конечным алфавитом A эквивалентен относительно A некоторому нормальному алгорифму над A.*

Основания к справедливости этого принципа, не являющегося математическим утверждением, обсуждались по ходу изложения с самого начала параграфа.

Может показаться, что требование конечности алфавита не позволяет рассматривать нормальные алгорифмы как адекватное отображение понятия алгоритма в математике. Однако, это не является существенным ограничением. Дело в том, что если некоторый алгоритм $\mathfrak{B}$ действует на множестве M, то элементы множества M и элементы $\mathfrak{B}(m)$ должны задаваться эффективно, следовательно, элементы M и $\mathfrak{B}(m)$ имеют конечное число целочисленных инвариантов, причем вычисление этих инвариантов и восстановление по ним объекта можно осуществить с помощью некоторых алгоритмов «кодирования» и «декодирования». Таким образом, достаточно ограничиться алгоритмами, действующими на последовательностях натуральных чисел и выдающих в качестве значений также последовательности натуральных чисел. Последовательности же натуральных чисел можно закодировать самими натуральными числами (например, сопоставив последовательности $n_0, \ldots, n_k$ число $2^{n_0+1} \cdot 3^{n_1+1} \cdot \ldots \cdot p_k^{n_k+1}$, где $p_0, p_1, \ldots, p_k$ — простые числа, выписанные в порядке возрастания). Поэтому вопрос об уточнении понятия алгоритма сводится к вопросу об описании класса функций $f\colon X \to \omega$, где $X \subseteq \omega^n$, для которых существует алгоритм вычисления в упомянутом в начале параграфа интуитивном смысле.

Всюду в дальнейшем под *частичной функцией* будем понимать отображение $f\colon X \to \omega$, где $X \subseteq \omega^n$ для некоторого $n \in \omega$. О частичной функции $f\colon X \to \omega$, $X \subseteq \omega^n$, будем говорить как о *вычислимой*, если существует алгоритм $\mathfrak{B}$, действующий на ω^n, не применимый к n-кам $\bar{a} \notin X$, для которого $\mathfrak{B}(\bar{a}) = f(\bar{a})$, $\bar{a} \in X$. Для изображения натурального числа m мы будем использовать не обычную десятичную запись, а более простую запись $11 \ldots 1$, где число единиц равно $m+1$. Такое слово будем далее называть *записью числа* m и обозначать через $\boldsymbol{m}$. Набор чисел $\langle m_1, \ldots, m_n \rangle$ будем изображать словом $\alpha = \boldsymbol{m}_1 0 \boldsymbol{m}_2 0, \ldots, 0 \boldsymbol{m}_n$ и называть это слово *записью n-ки* $\alpha = \langle m_1, \ldots, m_n \rangle$.

Определение. Частичная функция $f \colon X \to \omega$, $X \subseteq \omega^n$ называется *нормально вычислимой*, если существует такой нормальный алгорифм $\mathfrak{A} = \langle A, S \rangle$, что $0, 1 \in A$, для любой n-ки $\langle m_1, \ldots, m_n \rangle \in \omega$ имеем
$\langle m_1, \ldots, m_n \rangle \in X \Leftrightarrow \mathfrak{A}$ применим к записи $\langle m_1, \ldots, m_n \rangle$ и $\mathfrak{A}(\alpha) = f(\alpha)$ для $\alpha \in X$. Такой алгорифм $\mathfrak{A}$ будем называть *нормальным алгорифмом, вычисляющим функцию* f.

Принцип нормализации для частичных функций будет теперь гласить: *класс вычислимых частичных функций совпадает с классом нормально вычисимых частичных функций.*

Пример 3. Построим нормальный алгорифм $\mathfrak{A}$, вычисляющий функцию x^2. Пусть $\mathfrak{A} = \langle A, S \rangle$, где $A = \{0, 1, a, b, c, d, e\}$, а члены S располагаются в следующем порядке:

1) $c1 \to 0ac$,	7) $ad \to d$,
2) $a0 \to 0a$,	8) $0d \to d$,
3) $ea \to ae$,	9) $bc \to \cdot 1$,
4) $0a \to ae0$,	10) $bd \to \cdot 1$,
5) $0c \to d$,	11) $1 \to bc$.
6) $ed \to d1$,	

Проиллюстрируем работу данного алгоритма на записи числа 2:

$$\underline{1}11 \to b\underline{c1}1 \to b0a\underline{c1} \to b0\underline{a0}ac \to b0\underline{0a}ac \to b\underline{0a}e0ac \to$$
$$\to bae0e\underline{0a}c \to bae0\underline{ea}e0c \to bae\underline{0a}ee0c \to bae\underline{ea}0ee0c \to$$
$$\to baaee0ee\underline{0c} \to baaee0e\underline{ed} \to baaee0\underline{ed}1 \to baaee\underline{0d}11 \to$$
$$\to baae\underline{ed}11 \to baa\underline{ed}111 \to ba\underline{ad}1111 \to b\underline{ad}1111 \to$$
$$\to \underline{bd}1111 \to \cdot 11111.$$

Перейдем к описанию класса алгоритмов, который был введен А. М. Тьюрингом и Э. Постом в 1936 г.

Пусть заданы два конечных множества A и Q, не содержащих букв L и R. Множество четверок $P = \{\langle x_i, y_i, u_i, v_i\rangle \mid i \leqslant m\}$ называется *программой* с внешним алфавитом A и с внутренним алфавитом Q, если $x_i \in Q$, $y_i \in A$, $u_i \in Q$ и $v_i \in A \cup \{L, R\}$ для любого $i \leqslant m$. В дальнейшем элементы программы $\langle x, y, u, v\rangle$ будем называть *командами* и обозначать через $xy \to uv$.

Определение. *Машиной Тьюринга* называется шестерка $\langle A, Q, a_0, q_0, q_1, P\rangle$, удовлетворяющая следующим условиям:

1) множества A, Q конечны, не пересекаются и не содержат букв L, R;

2) $a_0 \in A$; $q_0, q_1 \in Q$;

3) P — такая программа с внешним алфавитом A и внутренним алфавитом Q, что

а) не существует двух различных четверок в P, у которых первые и соответственно вторые члены совпадают,

б) q_0 не является первым членом ни одной четверки из P.

Машинным словом с внешним алфавитом A и внутренним алфавитом Q (или просто *машинным словом в* $\langle A, Q\rangle$) называется такое слово α в алфавите $A \cup Q$, что α является словом в алфавите $A \cup \{q\}$ для некоторого $q \in Q$ и α содержит ровно одно вхождение символа q.

Пусть α — слово в алфавите B и $a \in B$. Слово $a\alpha a$ будем обозначать через α^a. Если $\alpha = b\alpha_1 c$, где $b, c \in B$, то через α_a будем обозначать

а) слово α_1, если $b = c = a$;

б) слово $\alpha_1 c$, если $b = a$ и $c \neq a$;

в) слово $b\alpha_1$, если $c = a$ и $b \neq a$;

г) слово α, если $b \neq a$ и $c \neq a$.

Пусть α и β — машинные слова в $\langle A, Q\rangle$ и элемент $q \in Q$ входит в α. Будем говорить, что машина Тьюринга $M = \langle A, Q, a_0, q_0, q_1, P\rangle$ *переводит слово α в слово* β (обозначаем $\alpha \xrightarrow{M} \beta$), если выполняются следующие три условия:

1) если $\alpha^{a_0} = \alpha_1 qa\alpha_2$ и $qa \to rb \in P$, $b \in A$, то $\beta = (\alpha_1 rb\alpha_2)_{a_0}$;

2) если $\alpha^{a_0} = \alpha_1 aqb\alpha_2$ и $qb \to rL \in P$, то $\beta = (\alpha_1 rab\alpha_2)_{a_0}$;

3) если $\alpha^{a_0} = \alpha_1 qa\alpha_2$ и $qa \to rR \in P$, то $\beta = (\alpha_1 ar\alpha_2)_{a_0}$.

Отметим, что машина M может переводить слово α только в одно слово. Это следует из условия 3 а) определения машины Тьюринга. Если машинное слово α в $\langle A, Q\rangle$ не переводится машиной Тьюринга $M=\langle A, Q, a_0, q_0, q_1, P\rangle$ ни в какое слово β, то будем говорить, что α — *тупиковое слово для* M. Заметим, что из условия 3 б) определения машины Тьюринга следует, что если машинное слово α содержит символ q_0, то оно является тупиковым для M.

Пусть α — машинное слово в алфавите B. Слово, полученное из α заменой всех вхождений символа b на пустое слово, будем обозначать через α/b.

Определение. Пусть $M=\langle A, Q, a_0, q_0, q_1, P\rangle$ — машина Тьюринга и α, β — слова в алфавите $A\setminus\{a_0\}$. Будем говорить, что машина M *преобразует слово* α *в слово* β (обозначаем $M(\alpha)=\beta$), если существует последовательность $\gamma_0, \ldots, \gamma_n$ машинных слов в $\langle A, Q\rangle$, удовлетворяющих следующим условиям:

1) $\gamma_0=q_1\alpha$;

2) $\beta=(\gamma_n/q_0)/a_0$;

3) $\gamma_i \xrightarrow{M} \gamma_{i+1}$, $i<n$.

Заметим, что если для последовательности $\gamma_0, \ldots, \gamma_n$ выполнены условия 1)—3), то слово γ_n содержит вхождение q_0, так как β — слово в алфавите $A\setminus\{a_0\}$.

Ясно, что машина M может преобразовывать слово α только в одно слово. Если машина M не преобразовывает слово α ни в какое слово, то будем говорить, что машина M не применима к слову α или что значение $M(\alpha)$ не определено. В этом случае или существует бесконечная последовательность $\gamma_0, \ldots, \gamma_n, \ldots, n\in\omega$, для которой $\gamma_0=q_1\alpha$ и $\gamma_i \xrightarrow{M} \gamma_{i+1}, i\in\omega$, или существует конечная последовательность машинных слов $\gamma_0, \ldots, \gamma_n$, удовлетворяющая условиям 1) и 3), а γ_n — тупиковое слово, не содержащее q_0.

Определение. Частичная функция $f\colon X\to\omega$, $X\subseteq\omega^n$, называется *вычислимой по Тьюрингу*, если существует машина Тьюринга $M=\langle A, Q, a_0, q_0, q_1, P\rangle$, для которой выполняются условия:

а) $0, 1\in A$, $a_0\neq 0$, $a_0\neq 1$;

б) машина M применима к записи n-ки $a \Leftrightarrow a\in X$;

в) $M(a)=e$ для $a\in X$ и $f(a)=e$.

Такую машину M будем называть *машиной Тьюринга, вычисляющей функцию* f.

Очевидно, что все вычислимые по Тьюрингу частичные функции вычислимы.

Пример 4. Построим машину Тьюринга M, вычисляющую функцию $f(n)=2n$. Пусть $M=\langle A, Q, a, q_0, q_1, P\rangle$, где $A=\{0, 1, a\}$, $Q=\{q_0, q_1, q_2, q_3, q_4\}$, а P состоит из следующих четверок:

$$q_11\to q_30,\quad q_30\to q_3R,\quad q_31\to q_20,$$
$$q_20\to q_2L,\quad q_2a\to q_30,\quad q_3a\to q_4L,$$
$$q_40\to q_41,\quad q_41\to q_4L,\quad q_4a\to q_0a.$$

Предоставляем читателю самому убедиться, что эта машина действительно вычисляет функцию $f(n)=2n$. Для иллюстрации ее работы выпишем «процесс вычисления» $f(2)$:

$$q_1111 \xrightarrow{M} q_3011 \xrightarrow{M} 0q_311 \xrightarrow{M} 0q_201 \xrightarrow{M} q_2001 \xrightarrow{M}$$
$$\xrightarrow{M} q_2a001 \xrightarrow{M} q_30001 \xrightarrow{M} 0q_3001 \xrightarrow{M} 00q_301 \xrightarrow{M} 000q_31 \xrightarrow{M}$$
$$\xrightarrow{M} 000q_20 \xrightarrow{M} 00q_200 \xrightarrow{M} 0q_2000 \xrightarrow{M} q_20000 \xrightarrow{M} q_2a0000 \xrightarrow{M}$$
$$\xrightarrow{M} q_300000 \xrightarrow{M} 0q_30000 \xrightarrow{M} 00q_3000 \xrightarrow{M} 000q_300 \xrightarrow{M}$$
$$\xrightarrow{M} 0000q_30 \xrightarrow{M} 00000q_3 \xrightarrow{M} 0000q_40 \xrightarrow{M} 0000q_41 \xrightarrow{M}$$
$$\xrightarrow{M} 000q_401 \xrightarrow{M} 000q_411 \xrightarrow{M} 00q_4011 \xrightarrow{M} 00q_4111 \xrightarrow{M}$$
$$\xrightarrow{M} 0q_40111 \xrightarrow{M} 0q_41111 \xrightarrow{M} q_401111 \xrightarrow{M} q_411111 \xrightarrow{M}$$
$$\xrightarrow{M} q_4a11111 \xrightarrow{M} q_0a11111.$$

Имеет место следующая

Теорема 1. *Класс частичных функций, вычислимых по Тьюрингу, совпадает с классом нормально вычислимых частичных функций.*

Доказательство того, что вычислимые по Тьюрингу функции нормально вычислимы, мы предоставляем читателю в качестве упражнения. Доказательство другой части теоремы довольно громоздкое и состоит по существу из выписывания большого количества программ, поэтому мы его опускаем.

В силу теоремы 1 следующий тезис равносилен принципу нормализации для частичных функций: *любая вычислимая частичная функция вычислима по Тьюрингу* (тезис Тьюринга).

Упражнения

1. Построить нормальный алгорифм, эквивалентный относительно алфавита $\{Q_0, Q_1, \wedge, \vee, \neg, \to, (,)\}$ алгоритму, описанному в примере 1.

2. Построить нормальный алгорифм $\mathfrak{A}$ над алфавитом A такой, что для любого слова α в алфавите A $\mathfrak{A}(\alpha) = \alpha\alpha$.

3. Доказать, что класс функций, вычислимых по Тьюрингу, замкнут относительно суперпозиции.

§ 36. Рекурсивные функции

В настоящем параграфе мы приведем способ уточнения понятия вычислимой функции, который можно назвать алгебраическим, так как определяемый класс функций будет порождаться из некоторых простейших функций с помощью некоторых операций.

Напомним, что под частичной функцией мы понимаем здесь всякое отображение $f\colon X \to \omega$, где $X \subseteq \omega^n$ для некоторого $n \in \omega$. Число n в этом случае называется местностью частичной функции f и обозначается через $\nu(f)$. Если $f\colon X \to \omega$ — частичная функция, то будем называть f *нигде не определенной* при $X = \varnothing$ и *всюду определенной* при $X = \omega^{\nu(f)}$ *). Всюду определенную частичную функцию в дальнейшем будем называть просто функцией. Частичную функцию местности n будем называть n-местной частичной функцией. Мы допускаем случай, когда $n = 0$. Тогда 0-местная функция $f\colon \omega^0 \to \omega$ будет состоять из одной пары $\langle \varnothing, n\rangle$ для некоторого $n \in \omega$ и часто будет отождествляться с числом n. Всюду в дальнейшем буквы m, k, n, i и j, возможно с индексами, будут обозначать натуральные числа.

Пусть $f\colon X \to \omega$ — n-местная частичная функция. Если $\langle m_1, \ldots, m_n\rangle \in X$, то $f(m_1, \ldots, m_n)$ — это значение функции f на n-ке $\langle m_1, \ldots, m_n\rangle$. Если $\langle m_1, \ldots, m_n\rangle \notin X$,

*) Отметим, что если f — частичная функция, то ее местность определена по f однозначно в случае, когда f не является нигде не определенной. Нигде не определенные функции местности n и m для любых n, $m \in \omega$ равны.

то будем говорить, что $f(m_1, \ldots, m_n)$ не определено или что f не определена на n-ке $\langle m_1, \ldots, m_n\rangle$.

Ясно, что для задания частичной n-местной функции f достаточно для любой n-ки $\langle m_1, \ldots, m_n\rangle$ сказать, определено ли $f(m_1, \ldots, m_n)$, и если определено, то указать число $k = f(m_1, \ldots, m_n)$. Если f и g — частичные функции, то будем писать

$$f(m_1, \ldots, m_n) = g(m_1, \ldots, m_n),$$

когда обе части равенства определены и равны, либо обе части равенства не определены.

Пусть $\mathscr{F}_n$ — семейство всех n-местных частичных функций, а $\mathscr{F} = \bigcup\limits_{n\in\omega} \mathscr{F}_n$ — семейство всех частичных функций.

Определим на семействе $\mathscr{F}$ всех частичных функций операторы S, R, M, которые сохраняют вычислимость функций.

Пусть n, $k \in \omega$, f — $(n+1)$-местная частичная функция, $g_0, \ldots, g_n$ — k-местные частичные функции. Определим k-местную частичную функцию h следующим образом: $h(m_1, \ldots, m_k)$ не определено, если хотя бы одна из частичных функций $g_0, \ldots, g_n$ не определена на $\langle m_1, \ldots, m_k\rangle$, и если все $g_0, \ldots, g_n$ определены на $\langle m_1, \ldots, m_k\rangle$, то

$$h(m_1, \ldots, m_k) = f(g_0(m_1, \ldots, m_k), \ldots, g_n(m_1, \ldots, m_k)).$$

Будем говорить, что h *получена регулярной суперпозицией из* $f, g_0, \ldots, g_n$ и обозначать это следующим образом: $h = S^{k,n}(f, g_0, \ldots, g_n)$. Оператор (*регулярной суперпозиции*) $S^{k,n}$ является всюду определенным отображением из $\mathscr{F}_{n+1} \times \mathscr{F}_k^{n+1}$ в $\mathscr{F}_k$ и сохраняет вычислимость, т. е. если частичные функции $f \in \mathscr{F}_{n+1}$; $g_0, \ldots, g_n \in \mathscr{F}_k$ вычислимы, то и частичная функция $S^{k,n}(f, g_0, \ldots, g_n)$ вычислима. Верхние индексы у оператора S будут опускаться и вместо $S(f, g_0, \ldots, g_n)$ будет, как правило, использоваться более привычное, но менее точное обозначение $f(g_0, \ldots, g_n)$.

Пусть $n \in \omega, f \in \mathscr{F}_n$, $g \in \mathscr{F}_{n+2}$. Определим по f и g $(n+1)$-местную частичную функцию h так, что для любых $m_1, \ldots, m_n \in \omega$

$$h(m_1, \ldots, m_n, 0) = f(m_1, \ldots, m_n);$$

$h(m_1, \ldots, m_n, k+1)$ не определено, если $h(m_1, \ldots, m_n, k)$

не определено и $h(m_1, \ldots, m_n, k+1) = g(m_1, \ldots, m_n, k, h(m_1, \ldots, m_n, k))$, если $h(m_1, \ldots, m_n, k)$ определено. Очевидно, что h однозначно определена по f и g и вычислима, если вычислимы f и g. Указанное определение h по f и g задает оператор R^{n+1}: $\mathcal{F}_n \times \mathcal{F}_{n+2} \to \mathcal{F}_{n+1}$, который назовем *оператором примитивной рекурсии*. Про функцию $h = R^{n+1}(f, g)$ будем говорить, что она *получена примитивной рекурсией из функций f и g*. Верхний индекс у оператора R^{n+1} будем опускать.

Пусть $n \in \omega$, $f \in \mathcal{F}_{n+1}$. Определим по f такую n-местную частичную функцию g, что для любых $k, m_1, \ldots, m_n \in \omega$ $g(m_1, \ldots, m_n) = k$ тогда и только тогда, когда $f(m_1, \ldots, m_n, 0) = 0$ и $k = 0$ или $k > 0$ и $f(m_1, \ldots, m_n, 0), \ldots, f(m_1, \ldots, m_n, k-1)$ определены и не равны нулю, а $f(m_1, \ldots, m_n, k) = 0$. Ясно, что такая функция g существует и однозначно определена по f; кроме того, если f — вычислимая функция, то из определения g видно, как вычислять g. Таким образом, задан оператор M^n — *оператор минимизации* — из $\mathcal{F}_{n+1}$ в $\mathcal{F}_n$; если $g = M^n(f)$, то будем говорить, что g *получена минимизацией из f*.

Базисными функциями называются функции o, s, I_m^n $(1 \leqslant m \leqslant n)$, где o — одноместная функция, которая на любом n принимает значение 0, s — одноместная функция, принимающая на числе n значение $n+1$, а I_m^n — n-местная функция, принимающая на наборе $\langle k_1, \ldots, k_n \rangle$ значение k_m. Очевидно, что базисные функции вычислимы.

Определение. Частичная функция f называется *частично рекурсивной*, если существует такая конечная последовательность частичных функций $g_0, \ldots, g_k$, что $g_k = f$ и каждая g_i, $i \leqslant k$, либо базисная, либо получается из некоторых предыдущих регулярной суперпозицией, примитивной рекурсией или минимизацией. Эта последовательность $g_0, \ldots, g_k$ называется *определяющей последовательностью для f*. Если для всюду определенной частично рекурсивной функции f существует определяющая последовательность, состоящая только из всюду определенных функций, то f называется *рекурсивной*.

В следующем параграфе будет доказано, что любая всюду определенная частично рекурсивная функция является рекурсивной.

Из данного определения и приведенных выше замечаний о сохранении вычислимости операторами S, R, M легко следует, что всякая частично рекурсивная функция является вычислимой.

Обратное утверждение носит название *тезиса Чёрча*: *Любая вычислимая частичная функция частично рекурсивна.*

Исторически именно это утверждение было первым точным математическим определением понятия (алгоритмически) вычислимой функции.

Имеет место следующая теорема, доказательство которой мы опустим из-за его громоздкости.

Теорема 2. *Класс частично рекурсивных функций совпадает с классом функций, вычислимых по Тьюрингу.*

Таким образом, тезис Тьюринга эквивалентен тезису Чёрча.

Пусть k, $n \in \omega$, α — некоторое отображение множества $\{1, \ldots, k\}$ в множество $\{1, \ldots, n\}$, f — k-местная частичная функция. Будем говорить, что n-местная частичная функция g *получена из f подстановкой α*, если для любых $m_1, \ldots, m_n \in \omega$ имеет место соотношение

$$g(m_1, \ldots, m_n) = f(m_{\alpha 1}, \ldots, m_{\alpha k}).$$

Будем использовать в этом случае обозначение $g = f^\alpha$.

Предложение 1. *Если f — частично рекурсивная функция и g получена из f подстановкой α, то g частично рекурсивна.*

Доказательство. Легко проверить, что если $g = f^\alpha$, то

$$g = S^{n,k-1}\left(f, I^n_{\alpha 1}, \ldots, I^n_{\alpha k}\right). \ \square$$

Предложение 2. *Следующие функции рекурсивны:*

1) *нульместные функции n, $n \in \omega$;*

2) *двухместная функция сложения $+$;*

3) *двухместная функция умножения $\cdot$;*

4) *двухместная функция усеченной разности $\dot{-}$, определенная следующим образом:*

$$m \dot{-} n = \begin{cases} m - n, & \text{если } n \leqslant m, \\ 0 & \text{в противном случае;} \end{cases}$$

5) *одноместные функции* sg *и* $\overline{\mathrm{sg}}$, *определенные следующим образом*:

$$\mathrm{sg}(n) = \begin{cases} 0, & \text{если } n = 0, \\ 1 & \text{в противном случае;} \end{cases}$$

$$\overline{\mathrm{sg}}(n) = \begin{cases} 1, & \text{если } n = 0, \\ 0 & \text{в противном случае;} \end{cases}$$

6) *двухместная функция идентификации* δ, *определенная следующим образом*:

$$\delta(n, m) = \begin{cases} 0, & \text{если } n = m, \\ 1 & \text{в противном случае.} \end{cases}$$

Доказательство. Покажем рекурсивность нульместной функции $\{\langle\varnothing, n\rangle\}$ индукцией по n. Функция $\{\langle\varnothing, 0\rangle\}$ равна $M(o)$. Если функция $\{\langle\varnothing, n\rangle\}$ рекурсивна, то рекурсивна функция $s(\{\langle\varnothing, n\rangle\}) = \{\langle\varnothing, n+1\rangle\}$. Так как $n+0=n$ и $n+(m+1)=(n+m)+1$, то функция $+$ равна $R(I_1^1, s(I_3^3))$. Из равенств $n\cdot 0=0$ и $n\cdot(m+1)=n\cdot m+n$ следует, что функция $\cdot$ равна $R(o, I_1^3+I_3^3)$.

Для того чтобы показать рекурсивность усеченной разности $\dot{-}$, рассмотрим одноместную функцию $\dot{-}1$, определенную так:

$$n \dot{-} 1 = \begin{cases} 0, & \text{если } n = 0, \\ n-1, & \text{если } n \neq 0. \end{cases}$$

Она равна $R(0, I_1^2)$, поэтому рекурсивна. Так как $n\dot{-}(m+1)=(n\dot{-}m)\dot{-}1$, то функция $\dot{-}$ равна $R(I_1^1, I_3^3 \dot{-} 1)$, следовательно, также является рекурсивной.

Рекурсивность функций 5) следует из равенств $\mathrm{sg} = R(0, s(o(I_1^2)))$ и $\overline{\mathrm{sg}} = R(1, o(I_1^2))$.

Пусть α: $\{1, 2\} \to \{1, 2\}$ таково, что $\alpha(1)=2$, $\alpha(2)=1$, а f — функция, полученная из функции $\dot{-}$ подстановкой α. Тогда для функции δ справедливо равенство $\delta = S(\mathrm{sg}, S(+, \dot{-}, f))$. Из рекурсивности функций sg, $\dot{-}$ и предложения 1 получаем, что функция идентификации δ является рекурсивной. □

Для задания рекурсивных функций и изучения их свойств удобно пользоваться специальным формальным языком R_Σ, который похож на язык, описанный в § 16. Пусть $V = \{v_i \mid i \in \omega\}$ — множество переменных, элементы которого будем обозначать буквами x, y, z, w, u, возможно с индексами.

Пусть $\Sigma=(R, F, \mu)$ — некоторая конечная сигнатура такая, что $F\supseteq F_0=\{0, s, +, \cdot\}$, где 0 — символ нульместной функции, s — символ одноместной функции, $+$, $\cdot$ — символы двухместных функций; $R\supseteq R_0=\{<\}$, где $<$ — символ двухместного предиката.

Определение выражений (синтаксис) языка R_Σ будет зависеть еще и от семантики этого языка. Поэтому определение синтаксиса и семантики будет вестись одновременно, но прежде всего зададимся фиксированной алгебраической системой Ω_Σ сигнатуры Σ с основным множеством ω и такой, что значения символов сигнатуры $\Sigma_0=(R_0, F_0, \mu_0)$ совпадают с функциями и предикатом, обозначенными этими символами ранее (например, символу $\cdot$ соответствует операция умножения натуральных чисел).

Итак, будем одновременной индукцией определять понятие *Σ-терма*, *Σ-формулы* (более точно было бы говорить об Ω_Σ-термах и Ω_Σ-формулах), множества свободных переменных $FV(t)$ и $FV(\varphi)$ Σ-терма t и Σ-формулы φ соответственно, натуральное число $t[\eta]$ и истинностное значение $\varphi[\eta]\in\{u, л\}$ для всякой интерпретации $\eta\colon X\to\omega$, где $X\subseteq V$, $FV(t)\subseteq X$, $FV(\varphi)\subseteq X$:

а) символ 0 является Σ-термом, $FV(0)=\varnothing$ и $0[\eta]=0$;

б) переменная $x\in V$ является Σ-термом, $FV(x)=\{x\}$, $x[\eta]=\eta(x)$;

в) если $f\in F$ — n-местный функциональный символ, $t_1, \ldots, t_n$ — Σ-термы, то $f(t_1, \ldots, t_n)$ — Σ-терм; $FV(f(t_1, \ldots, t_n))=FV(t_1)\cup\ldots\cup FV(t_n)$; $f(t_1, \ldots, t_n)[\eta]=f^{\Omega_\Sigma}(t_1[\eta], \ldots, t_n[\eta])$, здесь f^{Ω_Σ} — n-местная операция алгебраической системы Ω_Σ, соответствующая сигнатурному символу f;

г) если Q — n-местный предикатный символ из R, а $t_1, \ldots, t_n$ — Σ-термы, то $Q(t_1, \ldots, t_n)$ — Σ-формула, $FV(Q(t_1, \ldots, t_n))=FV(t_1)\cup\ldots\cup FV(t_n)$; $Q(t_1, \ldots, t_n)[\eta]=u\Leftrightarrow\langle t_1[\eta], \ldots, t_n[\eta]\rangle\in Q^{\Omega_\Sigma}$, здесь Q^{Ω_Σ} — n-местный предикат, соответствующий в алгебраической системе Ω_Σ предикатному символу Q;

д) если t_1, t_2 — Σ-термы, то $t_1\approx t_2$ — Σ-формула, $FV(t_1\approx t_2)=FV(t_1)\cup FV(t_2)$, $(t_1\approx t_2)[\eta]=u\Leftrightarrow t_1[\eta]=t_2[\eta]$;

е) если φ и ψ — Σ-формулы, то $\neg\varphi$, $(\varphi\tau\psi)$ для $\tau \in \{\wedge, \vee, \to\}$ — также Σ-формулы, $FV(\neg\varphi) = FV(\varphi)$, $FV(\varphi\tau\psi) = FV(\varphi) \cup FV(\psi)$ и $(\neg\varphi)[\eta] = \neg(\varphi[\eta])$, $(\varphi\tau\psi)[\eta] = \varphi[\eta]\tau\psi[\eta]$, где операции $\neg$, $\wedge$, $\vee$, $\to$ определены на множестве $\{и, л\}$ таблицей (1) из § 6 с заменой «0» на «$л$» и «1» на «$и$»;

ж) пусть φ — Σ-формула, $x \in V$ и для любой интерпретации η_1: $X \to \omega$, для которой $x \notin X$ и $FV(\varphi) \subseteq X \cup \{x\}$, существует такое $n \in \omega$, что $\varphi[\eta] = и$ для $\eta = \eta_1 \cup \{\langle x, n\rangle\}$; тогда $\mu x\varphi$ — Σ-терм, $FV(\mu x\varphi) = FV(\varphi) \setminus \{x\}$ и $(\mu x\varphi)[\eta]$ — наименьшее $n_0 \in \omega$, для которого $\varphi[\eta'] = и$, где $\eta' = (\eta \setminus \{\langle x, \eta x\rangle\}) \cup \{\langle x, n_0\rangle\}$.

Индукцией по построению Σ-терма (Σ-формулы) Θ легко устанавливается, что *для любых интерпретаций* η_0: $X_0 \to \omega$, η_1: $X_1 \to \omega$ *таких, что* $FV(\Theta) \subseteq X_0 \cap X_1$ *и для всех* $x \in FV(\Theta)$ $\eta_0(x) = \eta_1(x)$, *выполняется равенство* $\Theta[\eta_0] = \Theta[\eta_1]$.

Как обычно, вместо $+(t_1, t_2)$ $(\cdot(t_1, t_2))$ будем писать $(t_1 + t_2)$ $((t_1 \cdot t_2))$ и $(t_1 < t_2)$ вместо $<(t_1, t_2)$. Кроме того, будем пользоваться обычными сокращениями для термов и формул, принятыми в арифметике и исчислении высказываний (например, вместо $(x + ((z \cdot z) + (x \cdot y)))$ и $((\varphi \wedge \psi) \to \varphi)$ будем писать соответственно $x + z^2 + xy$ и $(\varphi \wedge \psi) \to \varphi$).

Для Σ-формулы φ и интерпретации η: $X \to \omega$, $FV(\varphi) \subseteq X$, часто вместо «$\varphi[\eta] = и$» будем писать «$\varphi[\eta]$ истинно» или просто «$\varphi[\eta]$», а вместо «$\varphi[\eta] = л$» будем писать «$\varphi[\eta]$ ложно» или «$\neg\varphi[\eta]$».

Пусть Θ — Σ-терм или Σ-формула. Вхождение переменной x в Θ называется *свободным*, если оно не находится в подслове вида $\mu x\varphi$, являющемся Σ-термом. Если вхождение переменной в Θ не является свободным, то оно называется *связанным*. Легко проверить, что множество $FV(\Theta)$ состоит в точности из переменных, имеющих свободные вхождения в Θ.

Пусть Θ — Σ-терм (Σ-формула), $x_1, \ldots, x_n \in V$ — различные переменные, $t_1, \ldots, t_n$ — Σ-термы такие, что для любого $i \in \{1, \ldots, n\}$ и любого $y \in FV(t_i)$ ни одно свободное вхождение в Θ переменной x_i не содержится в терме вида $\mu y\varphi$, являющемся подсловом Θ. Тогда $(\Theta)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$ будет обозначать результат замены всех свободных вхождений переменных $x_1, \ldots, x_n$ на Σ-термы $t_1, \ldots, t_n$ соответственно.

Индукцией по построению Σ-терма и Σ-формулы без труда устанавливается следующее

Предложение 3. *Если Θ — Σ-терм (Σ-формула), $x_1, \ldots, x_n \in V$ — различные переменные, $t_1, \ldots, t_n$ — Σ-термы такие, что для Θ, $x_1, \ldots, x_n$, $t_1, \ldots, t_n$ выполнены сформулированные выше условия, то*

1) $\Theta_1 = (\Theta)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$ *является Σ-термом (Σ-формулой),*

$FV(\Theta_1) \subseteq (FV(\Theta) \setminus \{x_1, \ldots, x_n\}) \cup FV(t_1) \cup \ldots \cup FV(t_n)$;

2) *для любой интерпретации η: $X \to \omega$ такой, что $(FV(\Theta) \setminus \{x_1, \ldots, x_n\}) \cup FV(t_1) \cup \ldots \cup FV(t_n) \subseteq X$, выполняется равенство $\Theta_1[\eta] = \Theta[\eta']$, где $\eta' = \{\langle y, \eta(y)\rangle \mid y \in FV(\Theta),\ y \notin \{x_1, \ldots, x_n\}\} \cup \{\langle x_i, t_i[\eta]\rangle \mid i = 1, \ldots, n\}$.* □

Про Σ-терм (Σ-формулу) $\Theta_1 = (\Theta)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$ будем говорить, что Θ_1 получен из Θ *подстановкой* Σ-термов $t_1, \ldots, t_n$ вместо переменных $x_1, \ldots, x_n$.

К сожалению, условия для возможности подстановки Σ-термов вместо переменных не всегда выполнены. Чтобы всегда иметь возможность для подстановки, введем следующие понятия. Будем говорить, что Σ-терм (Σ-формула) Θ получается из Σ-терма (Σ-формулы) Θ_1 *заменой связанной переменной*, если Θ получается из Θ_1 заменой вхождения Σ-терма $\mu x \varphi$ на $\mu y (\varphi)^x_y$, где $y \notin FV(\varphi)$. Σ-термы (Σ-формулы) Θ и Θ' называются *конгруэнтными*, если существует такая последовательность $\Theta_0, \ldots, \Theta_n$, что $\Theta_0 = \Theta$, $\Theta_n = \Theta'$, а Θ_{i+1}, $i < n$, получается из Θ_i заменой связанной переменной.

Очевидно, что отношение конгруэнтности является эквивалентностью на множестве Σ-термов и Σ-формул.

Предложение 4. *Если Θ и Θ' — конгруэнтные Σ-термы или Σ-формулы, то $FV(\Theta) = FV(\Theta')$ и для любой интерпретации η: $FV(\Theta) \to \omega$ имеем $\Theta[\eta] = \Theta'[\eta]$.*

Доказательство. Индукцией по длине Θ легко показать, что если Θ' получается из Θ заменой связанной переменной, то утверждение предложения истинно. Далее индукция по длине последовательности $\Theta_0, \ldots, \Theta_n$ из предыдущего определения. □

Отметим, что для любого Σ-терма (Σ-формулы) Θ, любого набора попарно различных переменных $x_1, \ldots, x_n$ и любых Σ-термов $t_1, \ldots, t_n$ существует Σ-терм (Σ-формула) Θ' такой (такая), что Θ' конгруэнтен (конгруэнтна) Θ и для Θ' выполнены условия для подстановки

$(\Theta')^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$. Пользуясь этим свойством и предложением 4, будем впредь использовать запись $(\Theta)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$, не заботясь о выполнении условий на связанные переменные, считая, что если эти условия не выполнены, то $(\Theta)^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$ есть $(\Theta')^{x_1,\ldots,x_n}_{t_1,\ldots,t_n}$ для Σ-терма (Σ-формулы) Θ', конгруэнтного (конгруэнтной) Θ, причем для Θ' все условия для подстановки уже выполнены.

Напомним, что подмножество $X \subseteq A^n$ называется n-местным предикатом на A. В дальнейшем под предикатами будем понимать предикаты на ω. Если X — n-местный предикат, то n-местная функция π_X, определенная следующим образом: для любых $m_1, \ldots, m_n \in \omega$

$$\pi_X(m_1, \ldots, m_n) = \begin{cases} 0, & \text{если } \langle m_1, \ldots, m_n \rangle \in X, \\ 1 & \text{в противном случае,} \end{cases}$$

называется *представляющей* функцией для X.

Наряду с представляющей функцией π_X предиката X часто используют *характеристическую* функцию χ_X предиката X, которая связана с функцией π_X соотношением $\chi_X = \overline{\mathrm{sg}}(\pi_X)$.

Предикат X называется *рекурсивным*, если его представляющая функция π_X рекурсивна.

Алгебраическая система Ω_Σ называется *рекурсивной*, если все функции и предикаты, соответствующие символам сигнатуры Σ, являются рекурсивными.

В дальнейшем, говоря о Σ-формулах и Σ-термах (определение которых зависит от фиксированной алгебраической системы Ω_Σ), *будем всегда предполагать, что* Ω_Σ — *рекурсивная алгебраическая система.*

Заметим, что предикаты $\approx$, $<$ являются рекурсивными, так как представляющей функцией для $\approx$ является функция идентификации δ, а представляющей функцией для $<$ будет рекурсивная функция $\mathrm{sg}(\mathrm{s}(I_1^2) \dot{-} I_2^2)$.

С каждым Σ-термом (Σ-формулой) можно связать семейство функций (предикатов), которые *реализуются* этим Σ-термом (Σ-формулой). Для обозначения этих функций (предикатов) будем использовать расширение языка R_Σ, добавив новую пару символов [,] квадратных скобок.

Перейдем к точным определениям.

Если t — Σ-терм и $FV(t) \subseteq \{x_1, \ldots, x_n\} \subseteq V$, $x_i \neq x_j$ для $i \neq j$, то через $t[x_1, \ldots, x_n]$ будем обозначать n-местную функцию, принимающую на n-ке $\langle m_1, \ldots, m_n \rangle \in \omega^n$ значение $t[\eta]$, где $\eta = \{\langle x_i, m_i \rangle | i = 1, \ldots, n\}$. Если φ — Σ-формула и $FV(\varphi) \subseteq \{x_1, \ldots, x_n\} \subseteq V$, $x_i \neq x_j$ для $i \neq j$, то через $\varphi\ [x_1, \ldots, x_n]$ будем обозначать предикат $\{\langle m_1, \ldots, m_n \rangle | \varphi[\eta] = u$ для $\eta = \{\langle x_i, m_i \rangle | i = 1, \ldots, n\}\}$.

Заметим, что один и тот же Σ-терм t реализует много функций; например, если $FV(t) \subseteq \{x, y\}$, то $t[x, y]$, $t[y, x]$ и $t[x, y, z]$,— вообще говоря, различные функции. Символ $[x_1, \ldots, x_n]$ играет роль, аналогичную кванторам, он *связывает* переменные $x_1, \ldots, x_n$; так, например, если $FV(t) \subseteq \{x_1, \ldots, x_n\}$ и $y_1, \ldots, y_n$ — попарно различные переменные, то имеет место равенство

$$t[x_1, \ldots, x_n] = (t)^{x_1, \ldots, x_n}_{y_1, \ldots, y_n}[y_1, \ldots, y_n].$$

Предложение 5. *Всякая функция и всякий предикат, реализуемые Σ-термом и Σ-формулой соответственно, являются рекурсивными.*

Доказательство. Пусть Θ — Σ-терм или Σ-формула и $FV(\Theta) \subseteq \{x_1, \ldots, x_k\}$; индукцией по построению Θ будем доказывать рекурсивность $\Theta[x_1, \ldots, x_k]$.

а) Если $\Theta = 0$, то $\Theta[x_1, \ldots, x_k] = M\left(o\left(I^k_1\right)\right)$.

б) Если $\Theta = x \in V$, то $x = x_{i_0}$ для некоторого $i_0 \in \{1, \ldots, k\}$; тогда $\Theta[x_1, \ldots, x_k] = I^k_{i_0}$.

в) Пусть $\Theta = f(t_1, \ldots, t_n)$, где f — n-местный функциональный символ, $t_1, \ldots, t_n$ — Σ-термы; имеем $FV(\Theta) = FV(t_1) \cup \ldots \cup FV(t_n) \subseteq \{x_1, \ldots, x_k\}$; по индукционному предположению k-местные функции $g_1 = t_1[x_1, \ldots, x_k], \ldots, g_n = t_n[x_1, \ldots, x_k]$ являются рекурсивными. Если f^{Ω_Σ} — n-местная рекурсивная функция, соответствующая в модели Ω_Σ функциональному символу f, то, очевидно, имеет место равенство $\Theta[x_1, \ldots, x_k] = S\left(f^{\Omega_\Sigma}, g_1, \ldots, g_n\right) = f^{\Omega_\Sigma}(g_1, \ldots, g_n)$.

г) Пусть $\Theta = Q(t_1, \ldots, t_n)$, где Q — n-местный предикатный символ, $t_1, \ldots, t_n$ — Σ-термы. Имеем $FV(\Theta) = FV(t_1) \cup \ldots \cup FV(t_n) \subseteq \{x_1, \ldots, x_k\}$; по индукционному предположению k-местные функции $g_1 = t_1[x_1, \ldots, x_k], \ldots, g_n = t_n[x_1, \ldots, x_k]$ являются рекурсивными. Если Q^{Ω_Σ} — n-местный предикат, соответствующий в модели Ω_Σ предикатному символу Q, то по нашему соглашению Q^{Ω_Σ} — рекурсивный предикат; следовательно,

π_Q — представляющая функция предиката Q^{Ω_Σ} — является рекурсивной. Легко проверить, что k-местная рекурсивная функция $S(\pi_Q, g_1, \ldots, g_n)$ является представляющей для предиката $\Theta[x_1, \ldots, x_k]$; следовательно, этот предикат является рекурсивным.

д) Пусть $\Theta = t_1 \approx t_2$, где t_1, t_2 — Σ-термы; представляющей функцией для предиката $\Theta[x_1, \ldots, x_k]$ будет рекурсивная функция $S(\delta, t_1[x_1, \ldots, x_k], t_2[x_1, \ldots, x_k])$.

е) Случай, когда Θ имеет вид $\neg\varphi$ или $(\varphi\tau\psi)$ для $\tau \in \{\wedge, \vee, \to\}$ и для Σ-формул φ и ψ, совсем очевиден и оставляется для разбора читателю.

ж) Пусть $\Theta = \mu x\varphi$, где φ — Σ-формула и выполнены условия п. ж) определения Σ-термов и Σ-формул, тогда $FV(\varphi) \subseteq \{x_1, \ldots, x_k, x\}$. Будем предполагать, что x отлично от всех переменных $x_1, \ldots, x_k$; если это не так, то выбираем $y \in V$ так, что y отлично от $x_1, \ldots, x_k$ и не имеет вхождений в φ, и вместо Θ рассматриваем Σ-терм $\Theta' = \mu y(\varphi)^x_y$. По индукционному предположению можно считать, что $(k+1)$-местная функция g, представляющая предикат $\varphi[x_1, \ldots, x_k, x]$, является рекурсивной, тогда, как легко видеть, $\Theta[x_1, \ldots, x_k] = M(g)$, следовательно, функция $\Theta[x_1, \ldots, x_k]$ рекурсивна. □

Нашей основной задачей до конца параграфа будет доказательство того, что *всякая рекурсивная функция и всякий рекурсивный предикат реализуются Σ_0-термом и Σ_0-формулой.*

Важным шагом в доказательстве этого утверждения будет рассмотрение следующей ситуации: сигнатура Σ' получена из сигнатуры Σ добавлением одного k-местного функционального символа f; алгебраическая система Ω_Σ является обеднением алгебраической системы $\Omega_{\Sigma'}$. Заметим, что в этом случае всякий Σ-терм является и Σ'-термом.

Предложение 6. *Если существует такой Σ-терм t_0, что функция $f^{\Omega_{\Sigma'}}$, соответствующая в алгебраической системе $\Omega_{\Sigma'}$ символу f, реализуется термом t_0, то по любому Σ'-терму t', любой Σ'-формуле φ' можно эффективно построить Σ-терм t, Σ-формулу φ такие, что $FV(t) \subseteq FV(t')$, $FV(\varphi) \subseteq FV(\varphi')$ и для любой интерпретации η: $X \to \omega$, $FV(t') \subseteq X$ $(FV(\varphi') \subseteq X)$, имеет место равенство $t'[\eta] = t[\eta]$ или $\varphi'[\eta] = \varphi[\eta]$ соответственно.*

Доказательство. Пусть $f^{\Omega_{\Sigma'}} = t_0[x_1, \ldots, x_k]$. Определим индуктивно для любого Σ'-терма (Σ'-формулы)

Θ слово $r(\Theta)$ так: а) если Θ не содержит символа f, т. е. если Θ — Σ-терм или Σ-формула, то $r(\Theta)=\Theta$;

б) если $g\in F'$ — n-местный функциональный символ, отличный от f, а $t_1, \ldots, t_n$ — Σ'-термы, то $r(g(t_1, \ldots \ldots, t_n))=g(r(t_1), \ldots, r(t_n))$;

в) если $t_1, \ldots, t_k$ — Σ'-термы, то $r(f(t_1, \ldots, t_k)) = (t_0)^{x_1, \ldots, x_k}_{r(t_1),\ldots,r(t_k)}$;

г) если Q — n-местный предикатный символ из $R'=R$, $t_1, \ldots, t_n$ — Σ'-термы, то $r(Q(t_1, \ldots, t_n))=Q(r(t_1), \ldots \ldots, r(t_n))$;

д) $r(t_1\approx t_2)=r(t_1)\approx r(t_2)$, если t_1, t_2 — Σ'-термы;

е) $r(\neg\varphi)=\neg r(\varphi)$, $r(\varphi\tau\psi)=(r(\varphi)\tau r(\psi))$ для $\tau\in\{\wedge, \vee, \rightarrow\}$, если φ, ψ — Σ'-формулы;

ж) $r(\mu x\varphi)=\mu x r(\varphi)$ для Σ'-формулы φ.

Индукцией по построению Σ'-термов и Σ'-формул, используя предложения 3, 4 и определение Σ-термов, нетрудно доказать одновременно следующие утверждения:

1) *для любого Σ'-терма t $r(t)$ является Σ-термом и* $FV(t)\supseteq FV(r(t))$;

2) *для любой Σ'-формулы φ $r(\varphi)$ является Σ-формулой и* $FV(\varphi)\supseteq FV(r(\varphi))$;

3) *если Θ — Σ'-терм или Σ'-формула*, $FV(\Theta)\subseteq X$, η: $X\to\omega$ — *интерпретация, то* $\Theta[\eta]=r(\Theta)[\eta]$.

Ясно, что из этих утверждений вытекает и заключение предложения. □

Совершенно аналогично доказывается эффективная элиминируемость предикатного символа сигнатуры из $R'\setminus R$, когда существует Σ-формула без этого предикатного символа, реализующая соответствующий предикат в алгебраической системе $\Omega_{\Sigma'}$. Поэтому мы будем ссылаться на предложение 6 и для случая предиката.

Если дана Σ-формула φ, то $\mu x\varphi$ не всегда будет Σ-термом, а Σ-формулы с кванторами $\exists x\varphi$ и $\forall x\varphi$ вообще нами не допускались. Поэтому удобно использовать хотя бы «ограниченные» аналоги этих операторов.

Определение. Пусть φ — Σ-формула, t — Σ-терм, $x\in V$ и $x\notin FV(t)$. Введем следующие обозначения:

а) $\mu x\leqslant t\varphi=\mu x(\varphi\vee x\approx s(t))$;

б) $\exists x\leqslant t\varphi=(\mu x\leqslant t\varphi)<s(t)$;

в) $\forall x\leqslant t\varphi=\neg\exists x\leqslant t\neg\varphi$.

Очевидно, что $\mu x\leqslant t\varphi$, $\exists x\leqslant t\varphi$ и $\forall x\leqslant t\varphi$ — Σ-терм и Σ-формулы, $FV(\mu x\leqslant t\varphi)=FV(\exists x\leqslant t\varphi)=FV(\forall x\leqslant t\varphi)=(FV(\varphi)\cup FV(t))\setminus\{x\}$, и для интерпретации η:

$(FV(t) \cup FV(\varphi)) \setminus \{x\} \to \omega$ имеем

$$(\mu x \leqslant t\varphi)[\eta] = \begin{cases} \text{наименьшему } n \leqslant t[\eta], \text{ для которого} \\ \varphi[\eta'], \quad \text{где} \quad \eta' = \eta \cup \{\langle x, n\rangle\}, \\ \text{если такое } n \text{ существует,} \\ t[\eta] + 1 \text{ в противном случае;} \end{cases}$$

$(\exists x \leqslant t\varphi)[\eta] = u \Leftrightarrow$ (существует $n \leqslant t[\eta]$, для которого $\varphi[\eta'] = u$, где $\eta' = \eta \cup \{\langle x, n\rangle\}$);

$(\forall x \leqslant t\varphi)[\eta] = u \Leftrightarrow$ (для всех $n \leqslant t[\eta]$ имеем $\varphi[\eta'] = u$, где $\eta' = \eta \cup \{\langle x, n\rangle\}$).

Введем в рассмотрение ряд рекурсивных функций и предикатов, добавляя соответствующие им символы к сигнатуре Σ_0. Добавим к сигнатуре Σ_0 символы для функций, определенных в предложении 2 и не содержащихся в Σ_0:

1) двухместный функциональный символ $\dot{-}$, совпадающий с обозначением соответствующей функции на ω;

2) два одноместных функциональных символа sg и $\overline{\mathrm{sg}}$;

3) двухместный функциональный символ δ.

Кроме того, будем использовать сокращение n для Σ_0-терма $s(\ldots s(0)\ldots)$, где символ s встречается n раз, $n \in \omega$.

Алгебраическая система Ω_Σ полученной сигнатуры определяется естественным образом. Заметим, что каждый введенный символ удовлетворяет условиям предложения 6:

1) $\dot{-} = \mu z\,((z \approx 0 \wedge (y \approx x \vee x < y)) \vee (y < x \wedge y + z \approx x))[x, y]$;

2) $\overline{\mathrm{sg}} = (1 \dot{-} x)[x]$; $\mathrm{sg} = (1 \dot{-} \overline{\mathrm{sg}}(x))[x]$;

3) $\delta = \mu z\,((x \approx y \wedge z \approx 0) \vee (\neg x \approx y \wedge \neg z \approx 0))[x, y]$

Заметим, что в правой части этих соотношений использовались и новые функциональные символы, для которых ранее было уже дано термальное выражение. Введем еще ряд важных для дальнейшего рекурсивных функций и рекурсивный предикат и соответствующие им символы:

4) $\leqslant$ — двухместный предикат, имеющий на ω свой обычный смысл; сигнатурный символ будет совпадать с этим обозначением;

5) двухместную функцию $[/]$, реализуемую термом так:

$$[/] = \mu z\,((x < (s(z)\cdot y)) \vee (y \approx 0 \wedge z \approx x))\,[x, y],$$

сигнатурный символ будет тем же самым; вместо записи $[/]\ (m, n)$ будем использовать запись $[m/n]$; терм $[/]\ (t_1, t_2)$ также будем записывать в виде $[t_1/t_2]$;

6) одноместную функцию $[\sqrt{\ }]$, реализуемую термом так:

$$[\sqrt{\ }] = \mu y\,(x < s(y)^2)\,[x],$$

сигнатурный символ будет тот же самый; вместо $[\sqrt{\ }](n)$ будем писать $[\sqrt{n}]$, а вместо $[\sqrt{\ }](t)$ будем писать $[\sqrt{t}]$;

7) двухместную функцию rest, реализуемую термом так:

$$\mathrm{rest} = (x \dot{-} ([x/y]\cdot y))\,[x, y],$$

соответствующий сигнатурный символ будет rest;

8) двухместную функцию c, реализуемую термом так:

$$c = [((x+y)^2 + 3x + y)/2]\,[x, y],$$

соответствующий сигнатурный символ будет c;

9) одноместную функцию l, реализуемую термом так:

$$l = (x \dot{-} [([([\sqrt{8x+1}] + 1)/2])\,([([\sqrt{8x+1}] \dot{-} 1)/2])/2])[x],$$

соответствующий сигнатурный символ будет l;

10) одноместную функцию r, реализуемую термом так:

$$r = ([([\sqrt{8x+1}] \dot{-} 1)/2] \dot{-} l(x))\,[x],$$

соответствующий сигнатурный символ будет r;

11) двухместную функцию β, определенную термом так:

$$\beta = \mu z \leqslant r(x)\,(\exists w \leqslant l(x)\,((1 + (c(z, y) + 1)\cdot r(x))\cdot w \approx \\ \approx l(x)))\,[x, y],$$

соответствующий сигнатурный символ будет β.

Обозначим через Σ_1 сигнатуру (R_1, F_1, μ_1), где

$$F_1 = \{0, s, +, \cdot, \dot{-}, \mathrm{sg}, \overline{\mathrm{sg}}, \delta, [/], [\sqrt{\ }], \mathrm{rest}, c, l, r, \beta\},$$

а $R_1 = \{<, \leqslant\}$.

Используя предложение 6, легко показать, что *по любой Σ_1-формуле φ_1 и Σ_1-терму t_1 можно эффективно построить Σ_0-формулу φ_0 и Σ_0-терм t_0 такие, что*

$FV(\varphi_0)=FV(\varphi_1)$, $FV(t_0)=FV(t_1)$, *и если* $FV(\varphi_0)\subseteq \subseteq\{x_1, \ldots, x_n\}$ $(FV(t_0)\subseteq\{x_1, \ldots, x_n\})$, *то* $\varphi_0[x_1, \ldots, x_n] = =\varphi_1[x_1, \ldots, x_n]$ *и* $t_0[x_1, \ldots, x_n]=t_1[x_1, \ldots, x_n]$ *соответственно.*

Отметим теперь некоторые свойства введенных выше функций.

Для любых $m, n\in\omega$, *если* $n\neq 0$, *то* $[m/n]$ — *целая часть дроби* m/n, *если же* $n=0$, *то* $[m/n]=m$.

Для любых $m, n\in\omega$, *если* $n\neq 0$, *то* $\mathrm{rest}(m, n)$ — *это остаток от деления* m *на* n; *если же* $n=0$, *то* $\mathrm{rest}(m, n)=m$.

Для любого $m\in\omega$ $[\sqrt{m}]$ — *это целая часть корня квадратного из числа* m.

Функции c, l, r рассмотрим вместе.

Предложение 7. *Для функций* c, l, r *и любых* $m, n\in\omega$ *выполняются следующие равенства:*

1) $c(l(n), r(n))=n$;
2) $l(c(m, n))=m$;
3) $r(c(m, n))=n$.

В частности, c *взаимно однозначно отображает* ω^2 *на* ω.

Доказательство. Ниже мы будем пользоваться для вычисления c, l и r обычной арифметической записью.

Из равенства $c(n, m)=\dfrac{(n+m)^2+3n+m}{2}$ следует, что

$$8c(n, m)=4(n+m)^2+12n+4m.$$

Правая часть этого равенства допускает два таких представления: $(2n+2m+1)^2+8n-1$ и $(2n+2m+3)^2-8m-9$. Отсюда получаем соотношения:

$$(2n+2m+1)^2\leqslant 8c(n, m)+1<(2n+2m+3)^2,$$

$$2n+2m+1\leqslant[\sqrt{8c(n, m)+1}]<2n+2m+3,$$

$$2n+2m+2\leqslant[\sqrt{8c(n, m)+1}]+1<2n+2m+4,$$

$$n+m+1\leqslant\left[\frac{[\sqrt{8c(n, m)+1}]+1}{2}\right]<n+m+2.$$

Следовательно,

$$n+m+1=\left[\frac{[\sqrt{8c(n, m)+1}]+1}{2}\right],$$

$$n+m=\left[\frac{[\sqrt{8c(n, m)+1}]+1}{2}\right]\dot{-}1=\left[\frac{[\sqrt{8c(n, m)+1}]\dot{-}1}{2}\right].$$

Так как

$$c(n, m) = \frac{(n+m)^2 + 3n + m}{2} = \frac{(n+m)(n+m+1)}{2} + n,$$

то

$$n = $$
$$= c(n, m) \dot{-} \frac{1}{2}\left[\frac{[\sqrt{8c(n, m)+1}]+1}{2}\right] \cdot \left[\frac{[\sqrt{8c(n, m)+1}] \dot{-} 1}{2}\right],$$

$$m = \left[\frac{[\sqrt{8c(n, m)+1}] \dot{-} 1}{2}\right] \dot{-} n.$$

Отсюда получаем $l(c(n, m)) = n$, $r(c(n, m)) = m$.

Если $n = c(i, j)$ для некоторых $i, j \in \omega$, то из равенств $l(c(i, j)) = i$ и $r(c(i, j)) = j$ получаем $c(l(n), r(n)) = n$. Следовательно, для доказательства равенства $c(l(n), r(n)) = n$ для любого $n \in \omega$ достаточно показать, что для любого $n \in \omega$ существуют $i, j \in \omega$, для которых $n = c(i, j)$. Из определения c получаем $c(0, 0) = 0$. Если $c(i, j) = m$ и $j > 0$, то легко проверить, что $c(i+1, j-1) = m+1$. Если $c(i, j) = m$ и $j = 0$, то $c(0, i+1) = m+1$. □

Обратимся теперь к рассмотрению (технически) очень важной функции β.

Предложение 8. *Для любого $k \in \omega$, любых $n_0, \ldots, n_k \in \omega$ существует такое число $m \in \omega$, что*

$$\beta(m, i) = n_i \quad \textit{для всех} \quad i \leqslant k.$$

Доказательство. *Пусть* $c = \max\{c(n_i, i)+1 \mid i \leqslant k\}$ и $a = c!$. Покажем, что для $0 \leqslant j < l \leqslant c$ числа $1+ja$ и $1+la$ взаимно просты. Предположим противное, и пусть простое число p делит числа $1+ja$ и $1+la$, тогда p делит их разность $(1+la)-(1+ja) = (l-j)a$; тогда p делит $l-j$ или a, но так как $l-j \leqslant c$, то $l-j$ делит $a = c!$, так что в любом случае p делит a, но тогда $a = pa'$ и $1+ja = (ja')p+1$, и это число не может делиться на p. Получаем противоречие.

Полагаем

$$s = (1 + (c(n_0, 0)+1)a)\cdot(1+(c(n_1, 1)+1)a)\cdot\ldots$$
$$\ldots\cdot(1+(c(n_k, k)+1)a) = \prod_{i \leqslant k}(1+(c(n_i, i)+1)\cdot a)$$

и $m = c(s, a)$.

Покажем, что это m и удовлетворяет заключению предложения. Пусть $i \leqslant k$, тогда $(1+(c(n_i, i)+1)a)$ делит s $(a=r(m),\ s=l(m))$; предположим, что для некоторого $z \leqslant n_i$ $(1+(c(z, i)+1)a)$ также делит s. Так как $z \leqslant n_i$, то $c(z, i) \leqslant c(n_i, i) < c$. Отсюда и из отмеченной выше взаимной простоты чисел вида $1+ja$ и $1+la$ для $j \neq l \leqslant c$ следует, что $c(z, i)+1$ должно совпадать с некоторым $c(n_j, j)+1$, $j \leqslant k$. Но если $c(z, i)+1 = c(n_j, j)+1$, то $c(z, i) = c(n_j, j)$, $i=j$ и $z=n_i$. Таким образом, n_i является наименьшим z таким, что $(1+(c(z, i)+1)a)$ делит s и $n_i \leqslant c(n_i, i) < c(n_i, i)+1 \leqslant c \leqslant a = c! = r(m)$, поэтому $\beta(m, i) = n_i$. □

В дальнейшем Σ_0-термы и Σ_0-формулы будем называть *рекурсивными* термами и формулами. Следующая теорема дает указанную ранее характеризацию рекурсивных функций.

Теорема 3. *Для того чтобы функция $f: \omega^n \to \omega$ была рекурсивной, необходимо и достаточно, чтобы f реализовывалась некоторым рекурсивным термом t_f.*

Доказательство. Достаточность установлена раньше в предложении 5. Доказательство необходимости проведем индукцией по минимальной длине определяющей последовательности рекурсивных функций для f. В силу отмеченного выше, нужно доказывать только существование Σ_1-термов, реализующих функции. Базисные функции o, s и I_m^n реализуются Σ_0-термами $\mu y(x \approx x)$, $s(x)$ и x_m так:

$$o = \mu y(x \approx x)[x], \quad s = s(x)\ [x], \quad I_m^n = x_m[x_1, \ldots, x_n].$$

Пусть $f = S(h, g_0, \ldots, g_m)$ и Σ_1-термы $t, q_0, \ldots, q_m$ реализуют $h, g_0, \ldots, g_m$ соответственно так: $h = t[x_0, \ldots, x_m]$, $g_0 = q_0[z_1, \ldots, z_k]$, $\ldots$, $g_m = q_m[z_1, \ldots, z_k]$. Тогда Σ_1-терм $t_f = \mu w \exists x_0 \leqslant q_0 \ldots \exists x_m \leqslant q_m (x_0 \approx q_0 \wedge \ldots \wedge x_m \approx q_m \wedge \wedge w \approx t)$, очевидно, реализует f так: $f = t_f[z_1, \ldots, z_k]$.

Если $f = M(g)$ и $g = t_g[x_0, \ldots, x_n]$ для Σ_1-терма t_g, то, как легко проверить, для Σ_1-терма $t_f = \mu x_n (t_g \approx 0)$ $f = t_f[x_0, \ldots, x_{n-1}]$.

Пусть $f = R(g, h)$ и $g = t_g[x_1, \ldots, x_n]$, $h = t_h[x_1, \ldots, x_{n+2}]$ для подходящих Σ_1-термов t_g и t_h. Рассмотрим Σ_1-формулу φ, определенную так:

$$\left(\beta(u, 0) \approx t_g \wedge \forall w \leqslant x_{n+1} \left(\beta(u, s(w)) \approx (t_h)_{w,\ \ \beta(u,w)}^{x_{n+1}, x_{n+2}}\right)\right),$$

где $u \neq w$ — переменные, отличные от переменных из

$\{x_1, \ldots, x_{n+2}\}$ и всех переменных, имеющих вхождения в t_g и t_h. Так как $FV(t_g) \subseteq \{x_1, \ldots, x_n\}$, $FV(t_h) \subseteq \{x_1, \ldots, x_{n+2}\}$, то $FV(\varphi) \subseteq \{u, x_1, \ldots, x_{n+1}\}$. Предыдущее предложение показывает, что для любой интерпретации переменных η: $\{x_1, \ldots, x_n\} \to \omega$ существует такое значение $n \in \omega$ переменной u, что для $\eta' = \eta \cup \{\langle u, n\rangle\}$ $\varphi[\eta']$ истинно. Следовательно, мы можем образовать Σ_1-терм $t_1 = \mu u\varphi$; $FV(t_1) \subseteq \{x_1, \ldots, x_{n+1}\}$. Если положим теперь $t_f = \beta(t_1, x_{n+1})$, то $FV(t_f) \subseteq \{x_1, \ldots, x_{n+1}\}$, и индукцией по значению переменной x_{n+1} без труда устанавливается, что $f = t_f[x_1, \ldots, x_{n+1}]$. □

Следствие. 1. *Для любой конечной сигнатуры Σ и рекурсивной алгебраической системы Ω_Σ существует эффективная процедура переработки каждого Σ-терма или Σ-формулы Θ в рекурсивный терм или рекурсивную формулу Θ_0 так, что $FV(\Theta) \supseteq FV(\Theta_0)$, и если $FV(\Theta) \subseteq \{x_1, \ldots, x_n\}$, то $\Theta[x_1, \ldots, x_n] = \Theta_0[x_1, \ldots, x_n]$.*

Это вытекает из предложения 6 и теоремы 3. □

Упражнения

1. Доказать рекурсивность двухместной функции ex такой, что для $m, n \in \omega$, если $n \neq 0$, то ex $(m, n) = m^n$ и ex $(m, 0) = 1$.

2. Доказать рекурсивность двухместной функции $|-|$ такой, что для любых $n, m \in \omega$ $|n - m|$ — модуль разности этих чисел.

3. Доказать рекурсивность одноместного предиката $\{n \mid n \in \omega$, n — простое число$\}$.

§ 37. Рекурсивно перечислимые предикаты

В предыдущем параграфе было определено понятие рекурсивного предиката как предиката, представляющая функция которого является рекурсивной. Таким образом, рекурсивные предикаты — это в точности такие предикаты $R \subseteq \omega^n$, для которых эффективно решается проблема вхождения, т. е. проблема определения по заданной n-ке чисел $\langle m_1, \ldots, m_n\rangle$, будет ли она принадлежать предикату R.

Однако алгоритмические процедуры можно использовать не только для распознавания принадлежности предикату, но и для процесса порождения самого предиката (множества) $R \subseteq \omega^n$. Таких эффективно порождаемых предикатов, вообще говоря, больше, чем рекурсивных предикатов. В этом параграфе будет определено понятие рекурсивно перечислимого предиката, которое и является подходящим математическим уточнением для понятия эффективно порождаемого предиката, и будут изучены некоторые базисные свойства рекурсивно перечислимых предикатов.

В следующем параграфе мы увидим, что рекурсивно перечислимых предикатов действительно больше, чем рекурсивных.

Расширим класс рекурсивных формул до класса *рекурсивно перечислимых формул* с помощью следующего определения:

1. Если φ — рекурсивная формула, то φ — рекурсивно перечислимая формула.

2. Если φ — рекурсивно перечислимая формула, $x \in V$, то $\exists x\varphi$ — рекурсивно перечислимая формула и $FV(\exists x\varphi) = FV(\varphi)\setminus\{x\}$.

Другими словами, рекурсивно перечислимые формулы получаются из рекурсивных навешиванием нескольких кванторов существования. Для всякой рекурсивно перечислимой формулы φ и интерпретации η: $X \to \omega$, $FV(\varphi) \subseteq X \subseteq V$, естественным образом определяется значение $\varphi[\eta] \in \{u, л\}$; а именно, если φ представима в виде $\exists x_0 \exists x_1 \ldots \exists x_n \varphi_0$, где φ_0 — рекурсивная формула, $FV(\varphi_0) \subseteq FV(\varphi) \cup \{x_0, \ldots, x_n\}$, то $\varphi[\eta] = u$ тогда и только тогда, когда существует такая интерпретация η': $FV(\varphi_0) \to \omega$, что $\eta'(v) = \eta(v)$ для всех $v \in FV(\varphi)$ и $\varphi_0[\eta'] = u$.

Заметим, что согласно следствию 36.1 мы в равной степени вместо рекурсивных термов и формул можем (и будем) пользоваться произвольными Σ_1-термами и Σ_1-формулами.

Со всякой рекурсивно перечислимой формулой φ и последовательностью попарно различных переменных $x_1, \ldots, x_n$ такой, что $FV(\varphi) \subseteq \{x_1, \ldots, x_n\}$, можно связать n-местный предикат, который будем обозначать $\varphi[x_1, \ldots, x_n]$, следующим образом:

$$\varphi[x_1, \ldots, x_n] = \{\langle m_1, \ldots, m_n\rangle \mid \varphi[\eta] = u \quad \text{для } \eta = \{\langle x_i, m_i\rangle \mid i = 1, \ldots, n\}\}.$$

Будем говорить, что предикат $\varphi[x_1, \ldots, x_n]$ *реализуется* рекурсивно перечислимой формулой φ.

Определение. Предикат $R \subseteq \omega^n$ назовем *рекурсивно перечислимым*, если он реализуется некоторой рекурсивно перечислимой формулой.

Из этого определения и полученных ранее результатов видно, что всякий рекурсивный предикат является рекурсивно перечислимым.

Понятие рекурсивно перечислимого предиката позволяет охарактеризовать частично рекурсивные функции, используя понятие графика. *Графиком* частичной n-местной функции f назовем $(n+1)$-местный предикат Γ_f, определенный соотношением: для $m_1, \ldots, m_n, k \in \omega$

$$\langle m_1, \ldots, m_n, k\rangle \in \Gamma_f \Leftrightarrow f(m_1, \ldots, m_n) = k.$$

Теорема 4 (теорема о графике). *Частичная функция f является частично рекурсивной тогда и только тогда, когда ее график Γ_f рекурсивно перечислим.*

Доказательство начнем с одного вспомогательного утверждения.

Лемма. *Для любого n-местного рекурсивно перечислимого предиката R существует рекурсивная формула φ такая, что $FV(\varphi) \subseteq \{x_0, x_1, \ldots, x_n\}$ и $R = (\exists x_0 \varphi)[x_1, \ldots, x_n]$.*

Содержание леммы состоит в том, что можно всегда предполагать, что рекурсивно перечислимая формула, реализующая рекурсивно перечислимый предикат, имеет только один квантор существования. Доказательство леммы получается индукцией по числу кванторов существования рекурсивно перечислимой формулы, используя следующее легко проверяемое свойство:

Для любой рекурсивной формулы φ, $FV(\varphi) \subseteq \{x, y, x_1, \ldots, x_n\}$,

$$(\exists x \exists y \varphi)[x_1, \ldots, x_n] = \left(\exists x \, (\varphi)^{x,\ y}_{l(x), r(x)}\right)[x_1, \ldots, x_n].$$

Заметим, что $(\varphi)^{x,\ y}_{l(x), r(x)}$ — Σ_1-формула. □

Для индуктивного доказательства необходимости установим следующие факты:

1) Графики основных функций рекурсивны:

$$\Gamma_o = (x \approx x \,\&\, y \approx 0)[x, y];$$

$$\Gamma_s = (s(x) \approx y)[x, y];$$

$$\Gamma_{I^n_m} = (x_m \approx y)[x_1, \ldots, x_n, y].$$

2) Пусть $f = S(h, g_0, \ldots, g_n)$, графики $\Gamma_h, \Gamma_{g_0}, \ldots, \Gamma_{g_n}$ соответственно функций $h, g_0, \ldots, g_n$ рекурсивно перечислимы и $\varphi_h, \varphi_{g_0}, \ldots, \varphi_{g_n}$ — такие рекурсивные формулы,

что

$$\Gamma_h = (\exists z\varphi_h)[u_0, \ldots, u_n, y];$$
$$\Gamma_{g_0} = (\exists z_0\varphi_{g_0})[y_1, \ldots, y_k, u_0];$$
$$\vdots$$
$$\Gamma_{g_n} = (\exists z_n\varphi_{g_n})[y_1, \ldots, y_k, u_n],$$

причем переменные $z, z_0, \ldots, z_n, y, y_1, \ldots, y_k, u_0, \ldots, u_n$ попарно различны. Рассмотрим рекурсивную формулу φ:

$$\varphi = \varphi_h \wedge \varphi_{g_0} \wedge \ldots \wedge \varphi_{g_n},$$

тогда проверка показывает, что имеет место равенство

$$\Gamma_f = (\exists z\exists z_0 \ldots \exists z_n\exists u_0 \ldots \exists u_n\varphi)[y_1, \ldots, y_k, y].$$

Следовательно, Γ_f рекурсивно перечислим.

3) Пусть $f = R(h, g)$ и графики Γ_h, Γ_g соответственно функций h, g рекурсивно перечислимы; пусть φ_h и φ_g — такие рекурсивные формулы, что

$$\Gamma_h = (\exists z_0\varphi_h)[x_1, \ldots, x_n, y_0];$$
$$\Gamma_g = (\exists z_1\varphi_g)[x_1, \ldots, x_{n+1}, x_{n+2}, y_1]$$

и переменные $z_0, z_1, x_1, \ldots, x_n, x_{n+1}, x_{n+2}, y_0, y_1$ попарно различны. Образуем следующую Σ_1-формулу φ:

$$\varphi = \forall x \leqslant x_{n+1}\left(\left(\left(x \approx 0 \wedge (\varphi_h)^{y_0\ \ z_0}_{\beta(u,0),\beta(v,0)}\right) \vee \right.\right.$$
$$\left.\left.\vee \left(\neg\, x \approx 0 \wedge (\varphi_g)^{x_{n+1},x_{n+2},\ \ y_1\ \ \ z_1}_{x\dot-1,\ \beta(u,x\dot-1),\beta(u,x),\beta(v,x)}\right)\right) \wedge \right.$$
$$\left. \wedge\, y \approx \beta(u, x_{n+1})\right)$$

здесь переменные u, v, y попарно различны и отличны от всех переменных формул φ_h, φ_g и переменных z_0, z_1, $x_1, \ldots, x_{n+2}$. Тогда $FV(\varphi) \subseteq \{u, v, y, x_1, \ldots, x_{n+1}\}$.

Пусть η: $\{u, v, y, x_1, \ldots, x_{n+1}\} \to \omega$ такова, что $\varphi[\eta]$; покажем, что в этом случае $f(\eta x_1, \ldots, \eta x_{n+1})$ определено и $f(\eta x_1, \ldots, \eta x_{n+1}) = \beta(\eta u, \eta x_{n+1}) = \eta y$. Индукцией по $l \leqslant \eta x_{n+1}$ будем показывать, что $f(\eta x_1, \ldots, \eta x_n, l)$ определено и $f(\eta x_1, \ldots, \eta x_n, l) = \beta(\eta u, l)$.

Пусть $l = 0$, тогда, так как $\varphi[\eta] = u$, придавая x значение 0, видим, что должна быть истинна формула $(\varphi_h)^{y_0\ \ z_0}_{\beta(u,0),\beta(v,0)}[\eta]$. А это означает, что $\langle \eta x_1, \ldots, \eta x_n, \beta(\eta u, 0)\rangle \in \Gamma_h$; следовательно, $h(\eta x_1, \ldots, \eta x_n)$ определено и равно $\beta(\eta u, 0)$. Но и $f(\eta x_1, \ldots, \eta x_n, 0) = h(\eta x_1, \ldots, \eta x_n)$; следовательно, $f(\eta x_1, \ldots, \eta x_n, 0)$ определено и равно $\beta(\eta u, 0)$.

Пусть для $l < \eta x_{n+1}$ уже показано, что $f(\eta x_1, \ldots$ $\ldots, \eta x_n, l)$ определено и равно $\beta(\eta u, l)$. Придавая x значение $l+1 (\leqslant \eta x_{n+1})$, видим, что должна быть истинна формула $(\varphi_g)^{x_{n+1}, x_{n+2}, \ y_1, \ z_1}_{x\dot{-}1, \ \beta(u,x\dot{-}1), \beta(u,x), \beta(v,x)} [\eta']$, где $\eta' = \eta \cup \{\langle x, l+1\rangle\}$. В частности,

$$\langle \eta x_1, \ldots, \eta x_n, l, \beta(\eta u, l), \beta(\eta u, l+1)\rangle \in \Gamma_g,$$

т. е. $g(\eta x_1, \ldots, \eta x_n, l, \beta(\eta u, l))$ определено и равно $\beta(\eta u, l+1)$; но так как по индукционному предположению $\beta(\eta u, l) = f(\eta x_1, \ldots, \eta x_n, l)$, то $f(\eta x_1, \ldots, \eta x_n, l+1) =$ $= g(\eta x_1, \ldots, \eta x_n, l, f(\eta x_1, \ldots, \eta x_n, l))$ определено и равно $\beta(\eta u, l+1)$.

Таким образом, $f(\eta x_1, \ldots, \eta x_n, \eta x_{n+1})$ определено и равно $\beta(\eta u, \eta x_{n+1})$; но так как и $(y \approx \beta(u, x_{n+1}))[\eta]$ истинно, то $\eta y = \beta(\eta u, \eta x_{n+1})$.

Используя свойства функции β, отмеченные в предложении 8 предыдущего параграфа, и реализуемость графиков функций h и g формулами $\exists z_0 \varphi_h$ и $\exists z_1 \varphi_g$ соответственно, легко доказать, что если $m_1, \ldots, m_{n+1} \in \omega$ таковы, что $f(m_1, \ldots, m_{n+1})$ определена и $f(m_1, \ldots, m_{n+1}) =$ $= k$,то существуют такие $l, s \in \omega$, что для интерпретации $\eta = \{\langle x_i, m_i\rangle | i = 1, \ldots, n+1\} \cup \{\langle y, k\}, \langle u, l\rangle, \langle v, s\rangle\}$ $\varphi[\eta]$ истинно.

Тогда из отмеченных выше свойств формулы φ видно, что график f имеет представление $\Gamma_f = (\exists u \exists v \varphi)[x_1, \ldots$ $\ldots, x_{n+1}, y]$, т. е. график f рекурсивно перечислим.

4) Пусть $f = M(g)$ и график Γ_g функции g имеет представление $\Gamma_g = (\exists z \varphi_g)[x_1, \ldots, x_{n+1}, y]$, где φ_g — рекурсивная формула.

Пусть φ —Σ_1-формула, определенная так:

$$\varphi = \forall u \leqslant y \Big((\varphi_g)^{x_{n+1}, z, \quad y}_{u, \quad \beta(v,u), \beta(w,u)} \wedge$$
$$\wedge\, \beta(w, y) \approx 0 \wedge (u < y \to \neg \beta(w, u) \approx 0)\Big);$$

здесь u, v, w — различные переменные, не встречающиеся в φ_g. Поступая, как и в предыдущем случае, нетрудно проверить, что для графика Γ_f функции f справедливо соотношение

$$\Gamma_f = (\exists v \exists w \varphi)[x_1, \ldots, x_n, y],$$

т. е. график f рекурсивно перечислим.

Завершает доказательство необходимости индукция по длине определяющей последовательности с использованием установленных выше фактов 1)—4).

Докажем достаточность. Пусть f — n-местная частичная функция и ее график Γ_f рекурсивно перечислим. Пусть φ — рекурсивная формула такая, что

$$\Gamma_f = (\exists z\varphi)[x_1, \ldots, x_n, y].$$

Рассмотрим рекурсивный предикат $\varphi[x_1, \ldots, x_n, y, z]$. По предложению 36.5 этот предикат является рекурсивным, т. е. его представляющая функция g является рекурсивной. По определению представляющей функции:

для любых $m_1, \ldots, m_n, k, l \in \omega$

$$\langle m_1, \ldots, m_n, k, l\rangle \in \varphi[x_1, \ldots, x_n, y, z] \Leftrightarrow$$
$$\Leftrightarrow g(m_1, \ldots, m_n, k, l) = 0.$$

Рекурсивная $(n+1)$-местная функция $h = g(I_1^{n+1}, \ldots$ $\ldots, I_n^{n+1}, l(I_{n+1}^{n+1}), r(I_{n+1}^{n+1}))$ для любых $m_1, \ldots, m_n, k$ удовлетворяет соотношению

$$h(m_1, \ldots, m_n, k) = g(m_1, \ldots, m_n, l(k), r(k)).$$

Рассмотрим частично рекурсивную функцию $f_0 = l(M(h))$ и покажем, что она совпадает с f.

Пусть $m_1, \ldots, m_n \in \omega$ произвольны. Если $f(m_1, \ldots$ $\ldots, m_n)$ определена: $f(m_1, \ldots, m_n) = t \in \omega$, то $\langle m_1, \ldots$ $\ldots, m_n, t\rangle \in \Gamma_f$; следовательно, существует $s \in \omega$ такое, что $\langle m_1, \ldots, m_n, t, s\rangle \in \varphi[x_1, \ldots, x_n, y, z]$; тогда $g(m_1, \ldots, m_n, t, s) = 0$ и для $k = c(t, s)$

$$h(m_1, \ldots, m_n, k) = g(m_1, \ldots, m_n, l(k), r(k)) =$$
$$= g(m_1, \ldots, m_n, t, s) = 0.$$

Следовательно, $M(h)(m_1, \ldots, m_n)$ определено. Пусть $M(h)(m_1, \ldots, m_n) = k_0$; тогда $h(m_1, \ldots, m_n, k_0) = 0 = g(m_1, \ldots, m_n, l(k_0), r(k_0))$; отсюда $\langle m_1, \ldots, m_n, l(k_0), r(k_0)\rangle \in \varphi[x_1, \ldots, x_n, y, z]$, $\langle m_1, \ldots, m_n, l(k_0)\rangle \in (\exists z\varphi)[x_1, \ldots, x_n, y] = \Gamma_f$ и $f(m_1, \ldots, m_n) = l(k_0) = f_0(m_1, \ldots, m_n)$, так как $f_0(m_1, \ldots, m_n) = l(M(h)(m_1, \ldots$ $\ldots, m_n)) = l(k_0)$. Итак, если $f(m_1, \ldots, m_n)$ определено, то $f_0(m_1, \ldots, m_n)$ определено и $f(m_1, \ldots, m_n) = f_0(m_1, \ldots, m_n)$. Пусть $m_1, \ldots, m_n \in \omega$ и $f_0(m_1, \ldots, m_n)$ определено, тогда и $M(h)(m_1, \ldots, m_n)$ определено и $f_0(m_1, \ldots, m_n) = l(M(h)(m_1, \ldots, m_n))$. Пусть $k \in \omega$ таково, что $M(h)(m_1, \ldots, m_n) = k$, тогда $h(m_1, \ldots, m_n, k) = 0 = g(m_1, \ldots, m_n, l(k), r(k))$; следовательно, $\langle m_1, \ldots, m_n, l(k), r(k)\rangle \in \varphi[x_1, \ldots, x_n, y, z]$; $\langle m_1, \ldots, m_n, l(k)\rangle \in$

$\in(\exists z\varphi)[x_1, \ldots, x_n, y]=\Gamma_f$, следовательно, $f(m_1, \ldots, m_n) = l(k)$.

Поэтому, если $f_0(m_1, \ldots, m_n)$ определено, то и $f(m_1, \ldots, m_n)$ определено и $f_0(m_1, \ldots, m_n) = l(M(h)(m_1, \ldots, m_n)) = l(k) = f(m_1, \ldots, m_n)$. Таким образом, $f = f_0$ и, следовательно, f — частично рекурсивная функция. □

Следствие 1. *Для всякой n-местной частично рекурсивной функции f существует такая $(n+1)$-местная рекурсивная функция h, что для любых $m_1, \ldots, m_n$*

$$f(m_1, \ldots, m_n) = l(M(h)(m_1, \ldots, m_n)).$$

Непосредственно вытекает из доказательства достаточности в теореме. □

Следствие 2. *Частично рекурсивная функция является рекурсивной тогда и только тогда, когда она всюду определена.*

Необходимость очевидна. Достаточность непосредственно вытекает из предыдущего следствия. □

Одноместные предикаты будем называть просто множествами. Соответственно рекурсивные (рекурсивно перечислимые) одноместные предикаты будем называть *рекурсивными* (*рекурсивно перечислимыми*) *множествами*.

Докажем основные структурные свойства рекурсивных и рекурсивно перечислимых множеств.

Предложение 1. а) *Если множество X рекурсивно, то X рекурсивно перечислимо.*

б) *Конечное множество рекурсивно.*

в) *Если множества X, Y рекурсивны (рекурсивно перечислимы), то и множества $X \cup Y$ и $X \cap Y$ также рекурсивны (рекурсивно перечислимы).*

г) *Для рекурсивно перечислимого множества X множество $\omega \setminus X$ рекурсивно перечислимо тогда и только тогда, когда X рекурсивно.*

Доказательство. Утверждение а) было отмечено раньше для предикатов произвольной местности.

б) Если $X = \varnothing$, то представляющей функцией для X будет $\mathrm{sg}(s)$. Если $X = \{n\}$, то функция $\delta(\boldsymbol{n}, x)$ $[x]$ является представляющей для X. Если $X = \{n_0, n_1, \ldots n_k\}$, $k > 0$, то представляющей функцией для X будет функция

$$(\delta(\boldsymbol{n}_0, x) \cdot \delta(\boldsymbol{n}_1, x) \cdot \ldots \cdot \delta(\boldsymbol{n}_k, x))[x].$$

в) Если X и Y рекурсивны и g, h — представляющие функции для X и Y соответственно, то $g \cdot h$ — представляющая функция для $X \cup Y$, а $\mathrm{sg}(g+h)$ — представляющая функция для $X \cap Y$.

Пусть X и Y рекурсивно перечислимы, а φ_0, φ_1 — рекурсивные формулы такие, что $X = (\exists z_0\varphi_0)[x]$, $Y = (\exists z_1\varphi_1)[x]$ и x, z_0, z_1 — попарно различные переменные, тогда

$$X \cup Y = (\exists z_0 \exists z_1 (\varphi_0 \vee \varphi_1))[x];$$
$$X \cap Y = (\exists z_0 \exists z_1 (\varphi_0 \wedge \varphi_1))[x],$$

т. е. $X \cup Y$ и $X \cap Y$ реализуются рекурсивно перечислимыми формулами и, следовательно, рекурсивно перечислимы.

г) Если X — рекурсивное множество, а g — рекурсивная представляющая функция для X, то $\overline{\mathrm{sg}}(g)$ — рекурсивная представляющая функция для $\omega \setminus X$.

Предположим теперь, что X и $\omega \setminus X$ — рекурсивно перечислимые множества, и пусть φ_0, φ_1 — рекурсивные формулы такие, что $X = (\exists z\varphi_0)[x]$ и $\omega \setminus X = (\exists z\varphi_1)[x]$. Не уменьшая общности, будем предполагать, что φ_0 и φ_1 не содержат связанных вхождений переменной x. Рассмотрим рекурсивную формулу $\varphi = (\varphi_0 \vee \varphi_1)$: $FV(\varphi) \subseteq \{x, z\}$. Для любого значения n переменной x существует такое значение m переменной z, что для $\eta = \{\langle x, n\rangle, \langle z, m\rangle\}$ имеем $\varphi[\eta] = u$. Действительно, если $n \in X$, то существует такое значение m для z, что $\varphi_0[\eta] = u$, если же $n \in \omega \setminus X$, то найдется значение m для z такое, что $\varphi_1[\eta] = u$. Следовательно, $\mu z\varphi$ — рекурсивный терм, а $(\varphi_0)^z_{\mu z\varphi}$ — рекурсивная формула. Проверим, что $X = (\varphi_0)^z_{\mu z\varphi}[x]$. Пусть $h = \mu z\varphi[x]$ — рекурсивная функция, тогда по построению для любого $n \in \omega$, для $\eta = \{\langle x, n\rangle, \langle z, h(n)\rangle\}$ $\varphi[\eta] = u$; заметим еще, что для $\eta_0 = \{\langle x, n\rangle\}$ $(\varphi_0)^z_{\mu z\varphi}[\eta_0] = \varphi_0[\eta]$. Если $n \in X$, то $\varphi_1[\eta]$ не может быть истинным, так как в противном случае $n \in \omega \setminus X$; следовательно, $\varphi_0[\eta]$ и $(\varphi_0)^z_{\mu z\varphi}[\eta_0]$ истинны и $n \in (\varphi_0)^z_{\mu z\varphi}[x]$. Если $n \in \omega \setminus X$, то $\varphi_0[\eta]$ не может быть истинным, следовательно, $(\varphi_0)^z_{\mu z\varphi}[\eta_0] = л$ и $n \notin (\varphi_0)^z_{\mu z\varphi}[x]$. Итак, множество X реализуется рекурсивной формулой $(\varphi_0)^z_{\mu z\varphi}$, следовательно, X рекурсивно. □

Дадим теперь характеризацию рекурсивно перечислимых множеств с помощью рекурсивных функций.

Предложение 2. *Непустое множество X рекурсивно перечислимо тогда и только тогда, когда существует одноместная рекурсивная функция f такая, что $X = \{f(n) \mid n \in \omega\}$.*

Доказательство. Пусть X рекурсивно перечислимо и $n_0 \in X$; пусть φ — рекурсивная формула такая, что $X = (\exists y\varphi)[x]$, тогда $FV(\varphi) \subseteq \{x, y\}$. Рассмотрим Σ_1-формулу ψ:

$$\psi = \left(\varphi^{x,\ y}_{l(x), r(x)} \wedge z \approx l(x)\right) \vee \left(\neg\varphi^{x,\ y}_{l(x), r(x)} \wedge z \approx n_0\right);$$

$FV(\psi) \subseteq \{x, z\}$ и для любого значения k переменной x существует значение s переменной z такое, что для $\eta = \{\langle x, k\rangle, \langle z, s\rangle\}$ $\psi[\eta] = u$. Действительно, если для $\eta_0 = \{\langle x, k\rangle\}$ $\varphi^{x,\ y}_{l(x), r(x)}[\eta_0]$, то в качестве s можно взять $l(k)$; если же $\neg\varphi^{x,\ y}_{l(x), r(x)}[\eta_0]$, то в качестве s можно взять n_0. Следовательно, $\mu z\psi$ является Σ_1-термом, а реализуемая им рекурсивная функция $f = \mu z\psi[x]$ удовлетворяет заключению предложения. Действительно, если $k \in X$, то существует такое $s \in \omega$, что для $\eta = \{\langle x, k\rangle, \langle y, s\rangle\}$ $\varphi[\eta]$, следовательно, для $t = c(k, s)$, $\eta_0 = \{\langle x, t\rangle\}$ $\varphi^{x,\ y}_{l(x), r(x)}[\eta_0] = \varphi[\eta] = u$ и, следовательно, $f(t) = l(t) = l(c(k, s)) = k$. Таким образом, $X \subseteq \{f(t) \mid t \in \omega\}$. Наоборот, если $f(t) = k$, то для $\eta = \{\langle x, t\rangle, \langle z, k\rangle\}$ $\psi[\eta]$ и, следовательно, либо $\langle l(t), r(t)\rangle \in \varphi[x, y]$ и тогда $k = l(t) \in X$, либо $\langle l(t), r(t)\rangle \notin \varphi[x, y]$ и тогда $k = n_0 \in X$. Итак, $\{f(t) \mid t \in \omega\} \subseteq X$ и $X = \{f(t) \mid t \in \omega\}$.

Достаточность будет следовать из более общего утверждения:

Область значений всякой одноместной частично рекурсивной функции f, т. е. множество $R_f = \{k \mid$ существует $n \in \omega$, $f(n)$ определено и $f(n) = k\}$, рекурсивно перечислима.

Действительно, пусть φ — рекурсивно перечислимая формула, реализующая график Γ_f функции f: $\Gamma_f = \varphi[x, y]$; тогда, очевидно, $R_f = (\exists x\varphi)[y]$. □

Пусть для n-местной частичной функции f через Δ_f обозначена область определения функции f, т. е. n-местный предикат $\{\langle m_1, \ldots, m_n\rangle \mid m_1, \ldots, m_n \in \omega,\ f(m_1, \ldots, m_n)$ определено$\}$.

Предложение 3. *Для любой n-местной частично рекурсивной функции f ее область определения Δ_f является рекурсивно перечислимым предикатом.*

Доказательство. Пусть φ — рекурсивно перечислимая формула, реализующая график Γ_f функции f: $\Gamma_f = \varphi[x_1, \ldots, x_n, y]$; тогда, очевидно, $\Delta_f = (\exists y\varphi)[x_1, \ldots, x_n]$. □

Предложение 4 (теорема о редукции). *Для любых двух рекурсивно перечислимых множеств R_0 и R_1 существуют такие рекурсивно перечислимые множества R_0' и R_1', что $R_0' \subseteq R_0$, $R_1' \subseteq R_1$, $R_0' \cap R_1' = \varnothing$ и $R_0 \cup R_1 = R_0' \cup R_1'$.*

Доказательство. Пусть φ_0, φ_1 — такие рекурсивные формулы, что $R_0 = (\exists z\varphi_0)[x]$ и $R_1 = (\exists z\varphi_1)[x]$. Рассмотрим рекурсивные формулы:

$$\varphi_0' = \varphi_0 \wedge \forall y \leqslant z\left(y \approx z \vee \neg (\varphi_1)_y^z\right);$$
$$\varphi_1' = \varphi_1 \wedge \forall y \leqslant z \neg (\varphi_0)_y^z.$$

Тогда множества $R_0' = (\exists z\varphi_0')[x]$ и $R_1' = (\exists z\varphi_1')[x]$ будут искомыми. Действительно, включения $R_0' \subseteq R_0$ и $R_1' \subseteq R_1$ очевидны, так как φ_i' влечет φ_i, $i = 0, 1$. Пусть $n \in R_0 \cup R_1$, тогда существует наименьшее s такое, что для $\eta = \{\langle x, n\rangle, \langle z, s\rangle\}$ истинна $(\varphi_0 \vee \varphi_1)[\eta]$. Если $\varphi_0[\eta]$, то очевидно, что и $\varphi_0'[\eta]$, следовательно, $n \in R_0'$; если же $\neg\varphi_0[\eta]$, то истинна $\varphi_1'[\eta]$ и, следовательно, $n \in R_1'$, Итак, $R_0 \cup R_1 = R_0' \cup R_1'$. Предположим теперь, что $k \in R_0' \cap R_1'$ и $s_0, s_1 \in \omega$ таковы, что для $\eta_0 = \{\langle x, k\rangle, \langle z, s_0\rangle\}, \eta_1 = \{\langle x, k\rangle, \langle z, s_1\rangle\}$ справедливы $\varphi_0'[\eta_0]$ и $\varphi_1'[\eta_1]$. Предположим сначала, что $s_1 < s_0$, тогда из истинности $\forall y \leqslant z\left(y \approx z \vee \neg(\varphi_1)_y^z\right)[\eta_0]$ должно следовать $\neg\varphi_1[\eta_1]$ и тем более $\neg\varphi_1'[\eta_1]$; если же $s_0 \leqslant s_1$, то из истинности $\forall y \leqslant z \neg(\varphi_0)_y^z[\eta_1]$ следует, что $\neg\varphi_0[\eta_0]$, тем более $\neg\varphi_0'[\eta_0]$. Полученное противоречие показывает, что $R_0' \cap R_1' = \varnothing$. □

Предложение 5 (теорема об униформизации). *Пусть R — произвольный $(n+1)$-местный рекурсивно перечислимый предикат, тогда существует такая n-местная частично рекурсивная функция f, что $\Gamma_f \subseteq R$ и $\Delta_f = R' = \langle\{m_1, \ldots, m_n\rangle \mid$ существует $m_{n+1} \in \omega$ такое, что $\langle m_1, \ldots, m_n, m_{n+1}\rangle \in R\}$.*

Доказательство. Пусть φ — рекурсивная формула такая, что $R = (\exists y\varphi)[x_1, \ldots, x_n, x_{n+1}]$. Пусть $u \neq z$ — переменные, не встречающиеся в формуле φ, рассмотрим рекурсивную формулу ψ, определенную так:

$$\psi = y \approx l(z) \wedge (\varphi)^{x_{n+1}, y}_{l(z),\ r(z)} \wedge \forall u \leqslant z \left(u \approx z \vee \neg\, (\varphi)^{x_{n+1}, y}_{l(u),\ r(u)}\right),$$

тогда $R_0 = (\exists z \psi)[x_1, \ldots, x_n, y]$ будет графиком Γ_f некоторой (частично рекурсивной) функции f, $\Gamma_f \subseteq R$ и $\Delta_f \subseteq R' = \{\langle m_1, \ldots, m_n\rangle \mid$ существует $m_{n+1} \in \omega$ такое, что $\langle m_1, \ldots, m_{n+1}\rangle \in R\}$. Это легко вытекает из следующих фактов:

1) *Если* $\langle m_1, \ldots, m_n\rangle \in R'$ *и* k — *наименьшее натуральное число такое, что для* $\eta = \{\langle x_1, m_1\rangle, \ldots, \langle x_n, m_n\rangle, \langle x_{n+1}, l(k)\rangle, \langle y, r(k)\rangle\}$ $\varphi[\eta]$, *то* $\psi[\eta_0]$ *для* $\eta_0 = \{\langle x_1, m_1\rangle, \ldots$ $\ldots, \langle x_n, m_n\rangle, \langle z, k\rangle, \langle y, l(k)\rangle\}$;

2) *если* η_0: $\{x_1, \ldots, x_n, z, y\} \to \omega$, η_1: $\{x_1, \ldots, x_n, z, y\} \to \omega$ *таковы, что* $\eta_0(x_i) = \eta_1(x_i)$, $1 \leqslant i \leqslant n$, *и* $\psi[\eta_0]$, $\psi[\eta_1]$ *истинны, то* $\eta_0 = \eta_1$;

3) *если для* η_0: $\{x_1, \ldots, x_n, z, y\} \to \omega$ $\psi[\eta_0]$, *то для* $\eta = \{\langle x_1, \eta_0 x_1\rangle, \ldots, \langle x_n, \eta_0 x_n\rangle, \langle x_{n+1}, \eta_0 y\rangle, \langle y, r(\eta_0 z)\rangle\}$ *будет* $\varphi[\eta]$.

Факты непосредственно проверяются, исходя из определения формулы ψ. □

С каждым $(n+1)$-местным предикатом R, $n > 0$, можно связать семейство n-местных предикатов, получаемых из R сечениями следующим образом:

для любого $k \in \omega$ пусть $R_k = \{\langle m_1, \ldots, m_n\rangle \mid \langle k, m_1, \ldots, m_n\rangle \in R\}$; предикат R_k назовем *k-сечением предиката R*.

Легко проверяется, что если R — рекурсивный или рекурсивно перечислимый предикат, то для любого $k \in \omega$ R_k также является рекурсивным или рекурсивно перечислимым соответственно.

Назовем $(n+1)$-местный рекурсивно перечислимый предикат R *универсальным для n-местных рекурсивно перечислимых предикатов*, если семейство $\{R_k \mid k \in \omega\}$ сечений R совпадает с семейством всех n-местных рекурсивно перечислимых предикатов. В следующем параграфе будет доказано существование универсальных $(n+1)$-местных рекурсивно перечислимых предикатов для любых $n > 0$.

Аналогично, с каждой $(n+1)$-местной частичной функцией f, $n > 0$, можно связать семейство n-местных частичных функций f_k, $k \in \omega$, полагая для $m_1, \ldots, m_n \in \omega$

$$f_k(m_1, \ldots, m_n) = f(k, m_1, \ldots, m_n).$$

Ясно, что если f — частично рекурсивная функция, то и f_k — частично рекурсивна для любого $k \in \omega$.

Назовем $(n+1)$-местную частично рекурсивную функцию f *универсальной для n-местных частично рекурсивных функций*, если $\{f_k | k \in \omega\}$ совпадает с семейством всех n-местных частично рекурсивных функций.

Отметим теперь, что существование универсальных частично рекурсивных функций является следствием существования универсальных рекурсивно перечислимых предикатов.

Предложение 6. *Если R — $(n+2)$-местный рекурсивно перечислимый предикат, универсальный для $(n+1)$-местных рекурсивно перечислимых предикатов, $n > 0$, а f — $(n+1)$-местная частично рекурсивная функция, униформизирующая R, т. е. такая, что $\Gamma_f \subseteq R$ и $\Delta_f = R' = \{\langle m_1, \ldots, m_{n+1}\rangle |$ существует $m_{n+2} \in \omega$ такое, что $\langle m_1, \ldots, m_{n+1}, m_{n+2}\rangle \in R\}$, то f является универсальной для n-местных частично рекурсивных функций.*

Доказательство. Пусть g — n-местная частично рекурсивная функция, тогда график Γ_g функции g — $(n+1)$-местный рекурсивно перечислимый предикат. Следовательно, существует $k \in \omega$ такое, что $\Gamma_g = R_k = \{\langle m_1, \ldots, m_{n+1}\rangle | \langle k, m_1, \ldots, m_{n+1}\rangle \in R\}$. Рассмотрим функцию f_k и покажем, что $g = f_k$.

Пусть $f_k(m_1, \ldots, m_n)$ определено и равно $l \in \omega$, тогда $f(k, m_1, \ldots, m_n) = l$ и $\langle k, m_1, \ldots, m_n, l\rangle \in R$ и, следовательно, $\langle m_1, \ldots, m_n, l\rangle \in R_k = \Gamma_g$; поэтому $g(m_1, \ldots, m_n)$ определено и равно l. Наоборот, пусть $g(m_1, \ldots, m_n)$ определено и равно l, тогда $\langle m_1, \ldots, m_n, l\rangle \in \Gamma_g = R_k$, $\langle k, m_1, \ldots, m_n, l\rangle \in R$, $\langle k, m_1, \ldots, m_n\rangle \in R'$ и, следовательно, $f(k, m_1, \ldots, m_n)$ определено и, как показано выше, $f_k(m_1, \ldots, m_n) = f(k, m_1, \ldots, m_n) = l = g(m_1, \ldots, m_n)$.

Итак, $g = f_k$. В силу произвольности выбора g получаем, что $\{f_k | k \in \omega\}$ состоит из всех n-местных частично рекурсивных функций. □

В заключение параграфа рассмотрим одно понятие, которое можно использовать для некоторого сравнения рекурсивно перечислимых множеств и предикатов по их «алгоритмической» сложности. Это понятие относится к семейству понятий сводимости в теории алгоритмов и является одним из наиболее интуитивно оправданных.

Пусть R — n-местный предикат, $n > 0$, X — множество; будем говорить, что R *m-сводится к X*, если существует n-местная рекурсивная функция f такая, что для любых $m_1, \ldots, m_n \in \omega$

$$\langle m_1, \ldots, m_n \rangle \in R \Leftrightarrow f(m_1, \ldots, m_n) \in X.$$

Всякую рекурсивную функцию f, удовлетворяющую этому условию, будем называть *сводящей для* R *и* X.

Если R m-сводится к X, то обозначать это будем так: $R \leqslant_m X$.

Простейшие свойства этого понятия сформулируем в виде предложения.

Предложение 7. *Пусть* R — *n-местный предикат,* X, X_0, X_1 — *множества,* $R \leqslant_m X$, *тогда*

1) *если* X — *рекурсивное или рекурсивно перечислимое множество, то* R — *рекурсивный или рекурсивно перечислимый предикат соответственно;*

2) $X \leqslant_m X$; *если* $X \leqslant_m X_0$, $X_0 \leqslant_m X_1$, *то* $X \leqslant_m X_1$;

3) *любой рекурсивный предикат* Q *m-сводится к любому множеству* X, *отличному от* $\varnothing$ *и* ω.

Доказательство. 1) Пусть f — сводящая функция (для R и X). Если X рекурсивно и χ_X — характеристическая функция X, то $\chi_X(f)$ — характеристическая (рекурсивная!) функция предиката R. Если X рекурсивно перечислимо, то пусть φ — рекурсивная формула, реализующая X так: $X = (\exists z\varphi)[x]$; пусть t — рекурсивный терм, реализующий функцию f так: $f = t[x_1, \ldots, x_n]$. Тогда, как нетрудно проверить, имеет место соотношение

$$R = (\exists x \exists z\ (t \approx x \wedge \varphi))[x_1, \ldots, x_n],$$

следовательно, R реализуется рекурсивно перечислимой формулой.

Утверждение 2) предложения 7 очевидно.

3) Пусть $n_0 \notin X$, $n_1 \in X$ и f — любая одноместная рекурсивная функция, принимающая в нуле значение n_0, а в единице значение n_1. Если χ_R — (рекурсивная) характеристическая функция предиката R, то $f(\chi_R)$ является сводящей функцией для R и X. □

В следующем параграфе будет показано, что среди рекурсивно перечислимых множеств существуют наибольшие относительно m-сводимости; точнее, такие рекурсивно перечислимые множества X_0, что $X \leqslant_m X_0$ для любого рекурсивно перечислимого множества X; такие множества назовем *m-универсальными рекурсивно перечислимыми множествами.*

Мощностные соображения показывают, что среди всех множеств не может существовать наибольшего относительно m-сводимости, так как к фиксированному множеству может m-сводиться не более счетного семейства множеств (множество рекурсивных функций счетно!).

Упражнения

Для двухместного предиката $R \subseteq \omega^2$ через $c(R)$ будем обозначать множество $\{n \mid n \in \omega, \langle l(n), r(n) \rangle \in R\}$.

1. Доказать, что отображение $R \mapsto c(R)$ является одно-однозначным соответствием между всеми двухместными предикатами и подмножествами ω.

2. Доказать, что $R \subseteq \omega^2$ — рекурсивный предикат тогда и только тогда, когда $c(R)$ — рекурсивное множество.

3. Доказать, что $R \subseteq \omega^2$ — рекурсивно перечислимый предикат тогда и только тогда, когда $c(R)$ — рекурсивно перечислимое множество.

4. Пусть $n_0, \ldots, n_m \in \omega$ попарно различны, $k_0, \ldots, k_m \in \omega$ произвольны; доказать, что существует одноместная рекурсивная функция f такая, что $f(n_i) = k_i$ для всех $i \leqslant m$. (Указание. Воспользоваться теоремой о графике.)

5. Доказать, что не существует $(n+1)$-местного рекурсивного предиката R_n, универсального для семейства всех n-местных рекурсивных предикатов. (Указание. Для $(n+1)$-местного рекурсивного предиката R_n рассмотреть n-местный рекурсивный предикат $\{\langle m_1, \ldots, m_n \rangle \mid \langle m_1, m_1, \ldots, m_n \rangle \notin R_n\}$.)

§ 38. Неразрешимость исчисления предикатов и теорема Гёделя о неполноте

Одним из наиболее важных вопросов при изучении исчисления является вопрос о его разрешимости.

Исчисление I называется *разрешимым*, если существует алгоритм, позволяющий по любому выражению Φ исчисления I узнавать, является ли Φ теоремой I или нет. В противном случае исчисление I называется *неразрешимым*.

Гёделевой нумерацией множества X слов алфавита A назовем такое разнозначное отображение $g\colon X \to \omega$, что существует алгоритм G, вычисляющий по слову $\alpha \in X$ его номер $g(\alpha)$, и существует алгоритм G_1, выписывающий по числу $n \in \omega$ слово α, если $n = g(\alpha)$, и выдающий число 0, если $n \in \omega \setminus \{g(\alpha) \mid \alpha \in X\}$.

Ясно, что в силу тезиса Чёрча вопрос о разрешимости исчисления I, имеющего гёделеву нумерацию g всех выражений I, сводится к вопросу о рекурсивности множества $\{g(\Phi) \mid \Phi$ — теорема $I\}$.

Рассмотрим сигнатуру $\Sigma_0 = \langle <^2;\ +^2,\ \cdot^2,\ s^1,\ 0\rangle$, состоящую из символа $<$ двухместного отношения, символов $+$, $\cdot$ двухместных функций, символа s одноместной функции и символа 0 константы. Индукцией по построению термов и формул определим гёделеву нумерацию $\gamma\colon T(\Sigma_0) \cup F(\Sigma_0) \to \omega$ термов и формул сигнатуры Σ_0:

1) $\gamma(0) = c(0, 1)$,
2) $\gamma(v_i) = c(1, i)$,
3) $\gamma(s(t)) = c(2, \gamma t)$,
4) $\gamma(t + q) = c(3, c(\gamma t, \gamma q))$,
5) $\gamma(t \cdot q) = c(4, c(\gamma t, \gamma q))$,
6) $\gamma(t \approx q) = c(5, c(\gamma t, \gamma q))$,
7) $\gamma(t < q) = c(6, c(\gamma t, \gamma q))$,
8) $\gamma(\Phi \wedge \Psi) = c(7, c(\gamma\Phi, \gamma\Psi))$,
9) $\gamma(\Phi \vee \Psi) = c(8, c(\gamma\Phi, \gamma\Psi))$,
10) $\gamma(\Phi \to \Psi) = c(9, c(\gamma\Phi, \gamma\Psi))$,
11) $\gamma(\neg \Phi) = c(10, \gamma\Phi)$,
12) $\gamma(\exists v_i \Phi) = c(11, c(i, \gamma\Phi))$,
13) $\gamma(\forall v_i \Phi) = c(12, c(i, \gamma\Phi))$.

Так как функции c, r, l вычислимы, то легко проверить, что γ — гёделева нумерация формул и термов сигнатуры Σ_0.

В дальнейшем множество $X \subseteq T(\Sigma_0) \cup F(\Sigma_0)$ будем называть *рекурсивным* (*рекурсивно перечислимым*), если множество $\gamma[X]$ рекурсивно (рекурсивно перечислимо).

Ниже нам придется устанавливать рекурсивность большого числа функций. Поэтому дальнейшее изложение начнем с одного чисто технического результата, который будет постоянно использоваться в дальнейшем.

Для любой $(n+1)$-местной функции f определим $(n+1)$-местную функцию $\bar{f}$ следующим образом: для любых $m_1, \ldots, m_n, m_{n+1} \in \omega$ $\bar{f}(m_1, \ldots, m_n, m_{n+1})$ — это наименьшее число $k \in \omega$ такое, что имеют место равенства $\beta(k, 0) = f(m_1, \ldots, m_n, 0)$, $\beta(k, 1) = f(m_1, \ldots, m_n, 1), \ldots$ $\ldots, \beta(k, m_{n+1}) = f(m_1, \ldots, m_n, m_{n+1})$.

Если f рекурсивна, то и $\bar{f}$ рекурсивна, так как если $f = t[x_1, \ldots, x_n, x_{n+1}]$, где t — рекурсивный терм, то $\bar{f} = q[x_1, \ldots, x_n, x_{n+1}]$, где

$$q = \mu y\left(\forall z \leqslant x_{n+1}\left(\beta(y, z) \approx (t)_z^{x_{n+1}}\right)\right)$$

— рекурсивный терм. Наоборот, если $\bar{f}$ рекурсивна, то f рекурсивна, так как $f(m_1, \ldots, m_n, m_{n+1}) = \beta(\bar{f}(m_1, \ldots$ $\ldots, m_n, m_{n+1}), m_{n+1})$.

Предложение 1. *Пусть даны числа* $k, n_0, \ldots, n_k \in \omega$, *рекурсивные функции* $\overset{n+1}{f}, \overset{n+n_0+1}{f_0}, \ldots, \overset{n+n_k+1}{f_k}$, *местность которых указывает верхний индекс, одноместные рекурсивные функции* $g_{0,1}, \ldots, g_{0,n_0}, \ldots, g_{k,1}, \ldots, g_{k,n_k}$ *и рекурсивные формулы* $\varphi_0, \ldots, \varphi_k$; $FV(\varphi_i) \subseteq \{x_1, \ldots, x_n, y\}$, $i \leqslant k$. *Предположим, что для любой интерпретации* η: $\{x_1, \ldots, x_n, y\} \to \omega$ *и любого* $i \leqslant k$ *выполнены условия*:

а) *если* $\varphi_i[\eta]$, *то* $\neg\,\varphi_j[\eta]$ *для любого* $j \leqslant k$, $j \neq i$;

б) *если* $\varphi_i[\eta]$ *и* $n_i \neq 0$, *то* $g_{i,j}(\eta(y)) < \eta(y)$ *для всех* $j \in \{1, \ldots, n_i\}$.

Тогда существует, единственна и рекурсивна функция h, *удовлетворяющая условию: для любых* $m_1, \ldots, m_n$, $l \in \omega$, *если* $\eta = \{\langle x_i, m_i\rangle \mid 1 \leqslant i \leqslant n\} \cup \{\langle y, l\rangle\}$, *то*

$$h(m_1, \ldots, m_n, l) =$$

$$= \begin{cases} f_0(m_1, \ldots, m_n, l, h(m_1, \ldots, m_n, g_{0,1}(l)), \ldots \\ \qquad \ldots, h(m_1, \ldots, m_n, g_{0,n_0}(l))), \text{ если } \varphi_0[\eta]; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(m_1, \ldots, m_n, l, h(m_1, \ldots, m_n, g_{k,1}(l)), \ldots \\ \qquad \ldots, h(m_1, \ldots, m_n, g_{k,n_k}(l))), \text{ если } \varphi_k[\eta]; \\ f(m_1, \ldots, m_n, l) \text{ в остальных случаях.} \end{cases}$$

Доказательство. Существование и единственность функции h, удовлетворяющей сформулированному в предложении условию, без труда устанавливается индукцией по последнему аргументу с использованием условий на φ_i, $i \leqslant k$, и $g_{i,j}$. Ниже будем доказывать, что функция $\bar{h}$ реализуется некоторым Σ_1-термом. После установления этого факта рекурсивность h будет следовать из отмеченной выше связи между h и $\bar{h}$ и предложения 36.5.

Пусть имеют место следующие соотношения для подходящих рекурсивных термов $q, t_0, \ldots, t_k$, $r_{0,1}, \ldots, r_{k,n_k}$:

$$f = q[x_1, \ldots, x_n, y];$$

$$f_0 = t_0[x_1, \ldots, x_n, y, z_1, \ldots, z_{n_0}];$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$f_k = t_k[x_1, \ldots, x_n, y, z_1, \ldots, z_{n_k}];$$

$$g_{i,j} = r_{i,j}[y],\ i \leqslant k,\ j \in \{1, \ldots, n_i\}.$$

Пусть $s_{i,j} = \beta(z, r_{i,j})$, $i \leqslant k$, $j \in \{1, \ldots, n_i\}$; $s_{i,j}$ — Σ_1-термы и $FV(s_{i,j}) \subseteq \{z, y\}$.

Рассмотрим следующую Σ_1-формулу φ:

$$\left(\bigwedge_{i\leqslant k}\left(\varphi_i \to \beta(z, y) \approx (t_i)^{z_1, \ldots, z_{n_i}}_{s_{i,1}, \ldots, s_{i,n_i}}\right)\right) \wedge$$
$$\wedge \left(\bigwedge_{i\leqslant k} \neg\, \varphi_i \to \beta(z, y) \approx q\right);$$

тогда $FV(\varphi) \subseteq \{x_1, \ldots, x_n, y, z\}$; положим $\psi = \forall w \leqslant y\, (\varphi)^y_w$, $FV(\psi) = FV(\varphi)$. Покажем, что

для интерпретации $\eta = \{\langle x_i, m_i\rangle \mid i = 1, \ldots, n\} \cup \cup \{\langle y, l\rangle\}$ *и для числа* $j \in \omega$ *следующие условия эквивалентны*:

1) $\psi[\eta']$ *истинно, где* $\eta' = \eta \cup \{\langle z, j\rangle\}$;

2) *для любого* $m \leqslant l$ $\beta(j, m) = h(m_1, \ldots, m_n, m)$.

Предположим, что для $l' < l$ эквивалентность условий 1) и 2) доказана (с заменой l на l'). Докажем эту эквивалентность для l.

Пусть выполнено условие 1). Тогда из вида формулы ψ легко видеть, что если $l' < l$, $\eta'' = (\eta' \setminus \{\langle y, l\rangle\}) \cup \cup \{\langle y, l'\rangle\}$, то $\psi[\eta'']$; следовательно, по индукционному предположению можно считать, что $\beta(j, m) = h(m_1, \ldots \ldots, m_n, m)$ для всех $m < l$.

Рассмотрим случай, когда существует $i \leqslant k$ такое, что $\varphi_i[\eta]$ истинно. Тогда из истинности $\psi[\eta']$ и $\varphi[\eta']$ следует, что имеют место равенства

$$\beta(j, l) = \beta(z, y)[\eta'] = (t_i)^{z_1, \ldots, z_{n_i}}_{s_{i,1}, \ldots, s_{i,n_i}}[\eta'] =$$
$$= f_i(m_1, \ldots, m_n, l, s_{i,1}[\eta'], \ldots, s_{i,n_i}[\eta']). \quad (*)$$

Далее, для $j' \in \{1, \ldots, n_i\}$ $s_{i,j'}[\eta'] = \beta(j, r_{i,j'}[\eta']) = \beta(j, g_{i,j'}(l))$; так как истинно $\varphi_i[\eta]$, то по условию, б) предложения 1 $g_{i,j'}(l) < l$ (если $n_i \neq 0$). Тогда $\beta(j, g_{i,j'}(l)) = h(m_1, \ldots, m_n, g_{i,j'}(l))$ и, следовательно,

$$\beta(j, l) = f_i(m_1, \ldots, m_n, l, h(m_1, \ldots, m_n, g_{i,1}(l)), \ldots$$
$$\ldots, h(m_1, \ldots, m_n, g_{i,n_i}(l))) = h(m_1, \ldots, m_n, l).$$

В случае, когда для любого $i \leqslant k$ $\neg\varphi_i[\eta]$, из истинности $\psi[\eta']$ следуют равенства

$$\beta(j, l) = \beta(z, y)[\eta'] = q[\eta'] = f(m_1, \ldots, m_n, l) =$$
$$= h(m_1, \ldots, m_n, l). \quad (**)$$

Итак, в любом случае, если $\psi[\eta']$ истинно, то для любого $m \leqslant l$ $\beta(j, m) = h(m_1, \ldots, m_n, m)$.

Наоборот, пусть $j \in \omega$ таково, что для всех $m \leqslant l$ $\beta(j, m) = h(m_1, \ldots, m_n, m)$, тогда используя эти равенства и соотношения (*) и (**), получим, что $\varphi[\eta']$ истинно. Если же $l' < l$ и $\eta'' = (\eta' \setminus \{\langle y, l\rangle\}) \cup \{\langle y, l'\rangle\}$, то $\varphi[\eta'']$ истинно по индукционному предположению о равносильности условий 1) и 2).

Отсюда получаем, что для $\eta = \{\langle x_i, m_i\rangle \mid i = 1, \ldots \ldots, n\} \cup \{\langle y, l\rangle\}$ $(\mu z\psi)[\eta]$ — это наименьшее $j \in \omega$ такое, что $\beta(j, m) = h(m_1, \ldots, m_n, m)$ для всех $m \leqslant l$. По определению h получаем, что $\bar{h}(m_1, \ldots, m_n, l) = (\mu z\psi)[\eta]$. Следовательно, $\bar{h} = (\mu z\psi)[x_1, \ldots, x_n, y]$. Как было отмечено в начале доказательства, отсюда уже следует рекурсивность h. □

Про функцию h из предыдущего предложения будем говорить, что она определена *возвратной рекурсией по кусочной схеме* или что она определена *кусочно возвратной рекурсией*. Часто вместо формул φ_i в определении по кусочно возвратной рекурсии мы будем писать условия, которые можно легко выразить формулой (например, $3 \leqslant x \leqslant 9$, $x \neq 2$ и т. п.).

Предложение 2. *Рекурсивными являются*:

а) *множество* $T(\Sigma_0)$ *термов сигнатуры* Σ_0;

б) *множество* $F(\Sigma_0)$ *формул сигнатуры* Σ_0;

в) *множество* $A(\Sigma_0)$ *аксиом* $ИП_1^{\Sigma_0}$.

Доказательство. Выпишем определение кусочно возвратной рекурсией для характеристической функции T множества $\gamma(T(\Sigma_0))$:

$$T(n) = \begin{cases} 1, \text{ если } n = c(0, 1) \text{ или } l(n) = 1, \\ T(r(n)), \text{ если } l(n) = 2, \\ T(lr(n)) \cdot T(rr(n)), \text{ если } 3 \leqslant l(n) \leqslant 4, \\ 0 \text{ в остальных случаях.} \end{cases}$$

Заметим, что из определений c, l, r следует $l(n) \leqslant n$, $r(n) \leqslant n$ и $k, m < c(k, m)$ для $k \geqslant 2$.

Для характеристической функции F множества $\gamma(F(\Sigma_0))$ определение кусочно возвратной рекурсией будет следующим:

$$F(n) = \begin{cases} T(lr(n)) \cdot T(rr(n)), \text{ если } 5 \leqslant l(n) \leqslant 6, \\ F(lr(n)) \cdot F(rr(n)), \text{ если } 7 \leqslant l(n) \leqslant 9, \\ F(r(n)), \text{ если } l(n) = 10, \\ F(rr(n)), \text{ если } 11 \leqslant l(n) \leqslant 12, \\ 0 \text{ в остальных случаях.} \end{cases}$$

Рассмотрим функцию Sb, определенную кусочно возвратной рекурсией следующим образом:

$$\mathrm{Sb}(n, m, k) = \begin{cases} k, \text{ если } l(n) = 1 \text{ и } r(n) = m, \\ c(l(n), c(\mathrm{Sb}(lr(n), m, k), \mathrm{Sb}(rr(n), m, k))), \\ \qquad\qquad\qquad \text{если } 3 \leqslant l(n) \leqslant 9, \\ c(l(n), \mathrm{Sb}(r(n), m, k)), \text{ если } l(n) \in \{2, 10\}, \\ c(l(n), c(lr(n), \mathrm{Sb}(rr(n), m, k))), \\ \qquad\qquad\qquad \text{если } 11 \leqslant l(n) \leqslant 12 \text{ и } m \neq lr(n), \\ n \text{ в остальных случаях.} \end{cases}$$

Легко проверить, что если $\theta \in T(\Sigma_0) \cup F(\Sigma_0)$ и $t \in T(\Sigma_0)$, то $\mathrm{Sb}(\gamma\theta, m, \gamma t) = \gamma\theta'$, где θ' получается из θ заменой всех свободных вхождений переменной v_m на терм t.

Определим кусочно возвратной рекурсией двухместную функцию Fr, обладающую следующим свойством: для любой $\theta \in T(\Sigma_0) \cup F(\Sigma_0)$ имеем $\mathrm{Fr}(\gamma\theta, n) = 1$, если v_n входит свободно в θ, и $\mathrm{Fr}(\gamma\theta, n) = 0$ в противном случае.

$$\mathrm{Fr}(n, m) = \begin{cases} \overline{\mathrm{sg}}(\delta(r(n), m)), \text{ если } l(n) = 1, \\ \mathrm{Fr}(r(n), m), \text{ если } l(n) \in \{2, 10\}, \\ \mathrm{sg}(\mathrm{Fr}(lr(n), m) + \mathrm{Fr}(rr(n), m)), \text{ если } 3 \leqslant l(n) \leqslant 9, \\ \mathrm{Fr}(rr(n), m), \text{ если } 11 \leqslant l(n) \leqslant 12 \text{ и } m \neq lr(n), \\ 0 \text{ в остальных случаях.} \end{cases}$$

Рассмотрим функцию P, определенную кусочно возвратной рекурсией следующего вида:

$$P(n, m, k) = \begin{cases} 1, \text{ если } 0 \leqslant l(n) \leqslant 6, \\ P(r(n), m, k), \text{ если } l(n) = 10, \\ P(lr(n), m, k) \cdot P(rr(n), m, k), \text{ если } 7 \leqslant l(n) \leqslant 9, \\ P(rr(n), m, k), \text{ если } 11 \leqslant l(n) \leqslant 12 \text{ и} \\ \qquad\qquad\qquad \mathrm{Fr}(rr(n), m) \cdot \mathrm{Fr}(k, lr(n)) = 0, \\ 0 \text{ в остальных случаях,} \end{cases}$$

Если $\Phi \in F(\Sigma_0)$, $t \in T(\Sigma_0)$, то $P(\gamma\Phi, m, \gamma t) = 1$, когда выполняется условие на запись $(\Phi)_t^{v_m}$ (см. § 18), и $P(\gamma\Phi, m, \gamma t) = 0$ в противном случае.

Имея в распоряжении рекурсивные функции T, F, Sb, Fr и P, легко построить рекурсивную характеристическую функцию A множества аксиом $\text{ИП}_1^{\Sigma_0}$. Достаточно построить характеристическую функцию A_i для множества аксиом, полученных по схеме i для любого $i \in \{1, 2, \ldots, 12\}$. Построим A_1 и A_{11}, оставляя построение A_i для других i читателю в качестве легкого упражнения.

$$A_1(n) = \begin{cases} 1 \text{ если } F(n) = 1,\ l(n) = 9,\ lrr(n) = 9 \\ \qquad\qquad\qquad\qquad \text{и } lr(n) = rrrr(n), \\ 0 \text{ в остальных случаях,} \end{cases}$$

$$A_{11}(n) = \begin{cases} 1, \text{ если } F(n) = 1,\ l(n) = 9,\ llr(n) = 12 \text{ и } \Phi(n), \\ 0 \text{ в остальных случаях;} \end{cases}$$

где

$$\Phi(n) = \exists x \leqslant n\,(T(x) \wedge rr(n) \approx \mathrm{Sb}(rrlr(n), lrlr(n), x) \wedge \\ \wedge P(rrlr(n), lrlr(n), x)). \quad \square$$

Предложение 3. *Множество теорем $\text{ИП}_1^{\Sigma_0}$ рекурсивно перечислимо.*

Доказательство. Пользуясь функциями F и Fr, легко построить определения кусочно возвратной рекурсией трехместной функции Rl_1 и двухместных функций Rl_2, Rl_3, для которых $\mathrm{Rl}_1(n, k, m) = 1$, $\mathrm{Rl}_2(n, m) = 1$ и $\mathrm{Rl}_3(n, m) = 1$ точно тогда, когда $n = \gamma\Phi$, $m = \gamma\Psi$, $k = \gamma\Theta$ для $\Phi, \Psi, \Theta \in F(\Sigma_0)$ и Ψ получается соответственно из Φ, Θ или Φ по правилам 1, 2 или 3. Например,

$$\mathrm{Rl}_2(n, m) = \begin{cases} 1, \text{ если } l(n) = l(m) = 9,\ lrr(m) = 12, \\ \qquad\qquad rr(n) = rrrr(m),\ F(n) = 1, \\ \qquad lr(n) = lr(m) \text{ и } \mathrm{Fr}(lr(n), lrr(m)) = 0, \\ 0 \text{ в остальных случаях.} \end{cases}$$

Для определения следующей очень важной функции рассмотрим сигнатуру Σ, полученную из Σ_0 добавлением функциональных символов l, r, β, A, Rl_1, Rl_2, Rl_3, и соответствующую алгебраическую систему Ω_Σ, где введенным символам соответствуют рекурсивные функции на ω, обозначенные ранее этими символами. Пусть φ — Σ-формула, определенная так:

$$\forall x \leqslant r(u)\,(A(\beta(l(u), x)) \approx$$
$$\approx 1 \vee \exists y \leqslant x \exists z \leqslant x (\neg\, y \approx x \wedge \neg\, z \approx x \wedge$$
$$\wedge\, (\mathrm{Rl}_1(\beta(l(u), y), \beta(l(u), z), \beta(l(u), x)) \vee$$
$$\vee\, \mathrm{Rl}_2(\beta(l(u), y), \beta(l(u), x)) \vee \mathrm{Rl}_3(\beta(l(u), y), \beta(l(u), x)))));$$

$FV(\varphi) = \{u\}$. Определим теперь одноместную рекурсивную функцию Pr так:

для $n \in \omega$

$$\mathrm{Pr}(n) = \begin{cases} \beta(l(n), r(n)), & \text{если } \varphi[\eta] \text{ для } \eta = \{\langle u, n\rangle\}, \\ \gamma(v_0 \approx v_0) & \text{в остальных случаях.} \end{cases}$$

Остается проверить (это мы оставляем читателю), что функция Pr будет перечислять множество теорем $\text{ИП}_1^{\Sigma_0}$. □

Рассмотрим совокупность Γ_0 предложений, являющихся универсальными замыканиями следующих формул сигнатуры Σ_0:

1) $\neg\, s(v_0) \approx 0$,

2) $s(v_0) \approx s(v_1) \to v_0 \approx v_1$,

3) $v_0 + 0 \approx v_0$,

4) $v_0 + s(v_1) \approx s(v_0 + v_1)$,

5) $v_0 \cdot 0 \approx 0$.

6) $v_0 \cdot s(v_1) \approx (v_0 \cdot v_1) + v_0$,

7) $\neg\, v_0 < 0$,

8) $v_0 < s(v_1) \to (v_0 < v_1 \vee v_0 \approx v_1)$,

9) $(v_0 < v_1 \vee v_0 \approx v_1) \to v_0 < s(v_1)$,

10) $\neg\, v_0 \approx v_1 \to (v_0 < v_1 \vee v_1 < v_0)$.

Множество предложений сигнатуры Σ_0, выводимых в $\text{ИП}_1^{\Sigma_0}$ из аксиом Γ_0, назовем *теорией* A_0.Ясно, что $\Omega = \langle\omega;\ +,\ \cdot,\ <,\ 0\rangle$, где $+,\ \cdot,\ <,\ 0$ обозначают соответственно операции сложения, умножения, отношение «меньше» и число 0, будет моделью A_0. В частности, A_0 непротиворечива.

Терм $s(s(\ldots s(0)\ldots))$, где число символов s равно n, будем, как ранее, обозначать через $\boldsymbol{n}^{\cdot}$.

Определение. Функция $f\colon \omega^n \to \omega$ называется *представимой в теории* A_0, если существует такая формула $\Phi(x_1, \ldots, x_n, y)$ сигнатуры Σ_0, что для любых $m_1, \ldots$ $\ldots, m_n, m \in \omega$

$$f(m_1, \ldots, m_n) = m \Rightarrow A_0 \rhd \Phi(\mathbf{m}_1, \ldots, \mathbf{m}_n, \mathbf{m}), \quad (1)$$

$$f(m_1, \ldots, m_n) \neq m \Rightarrow A_0 \rhd \neg\, \Phi(\mathbf{m}_1, \ldots, \mathbf{m}_n, \mathbf{m}). \quad (2)$$

Если для n-местной функции f и формулы $\Phi(x_1, \ldots$ $\ldots, x_n, y)$ выполняется (1) и (2) для всех $m, m_1, \ldots$ $\ldots, m_n \in \omega$, то будем говорить, что $\Phi(x_1, \ldots, x_n, y)$ *представляет в* A_0 *функцию* f. Отметим, что это отношение зависит не только от формулы Φ и функции f, но и от упорядочения переменных $x_1, \ldots, x_n, y$. Будем говорить, что формула Φ представляет n-местную функцию f, если $\Phi(x_1, \ldots, x_n, y)$ представляет f для некоторых переменных $x_1, \ldots, x_n, y$.

Лемма 1. *Пусть* $n, m \in \omega$. *Тогда*

а) $A_0 \rhd x < s(\mathbf{n}) \to (x \approx 0 \vee \ldots \vee x \approx \mathbf{n})$;

б) *если* $n \neq m$, *то* $A_0 \rhd \neg\, \mathbf{n} \approx \mathbf{m}$;

в) *если* $n < m$, *то* $A_0 \rhd \mathbf{n} < \mathbf{m}$;

г) *если* $n \leqslant m$, *то* $A_0 \rhd \neg\, \mathbf{m} < \mathbf{n}$.

Доказательство. Если $n = 0$, то а) следует из аксиом 7) и 8). Для $n = k + 1$ а) следует из истинности а) для k и аксиомы 8). Утверждение б) для $m = 0$ следует из аксиомы 1). Пусть утверждение б) для $m \leqslant k$ доказано, и пусть $n \neq k + 1$. Если $n = 0$, то б) следует из аксиомы 1). Если $n = l + 1$, то $l \neq k$ и по предположению $A_0 \rhd \neg\, \mathbf{l} \approx \mathbf{k}$. Из аксиомы 2) получаем тогда $A_0 \rhd$ $\rhd \neg\, \mathbf{n} \approx s(\mathbf{k})$.

Утверждение в) докажем индукцией по m. Если $m = 0$, то доказывать нечего. Если $m = k + 1$, то $n < k$ или $n = k$ и по индукционному предположению $A_0 \rhd \mathbf{n} < \mathbf{k} \vee \mathbf{n} \approx \mathbf{k}$. Из аксиомы 9) получаем теперь $A_0 \rhd \mathbf{n} < \mathbf{m}$.

Утверждение г) докажем индукцией по n. При $n =$ $= 0$ — это аксиома 7). Если $k + 1 \leqslant m$, то по индукционному предположению и утверждению б) получаем $A_0 \rhd \neg\, \mathbf{m} < \mathbf{k} \wedge \neg\, \mathbf{m} \approx \mathbf{k}$. Из аксиомы 8) получаем тогда $A_0 \rhd \neg\, \mathbf{m} < s(\mathbf{k})$. □

Лемма 2. *Формулы* $v_0 + v_1 \approx v_2$ *и* $v_0 \cdot v_1 \approx v_2$ *представляют в* A_0 *функции сложения и умножения соответственно.*

Доказательство. Условие $A_0 \rhd \mathbf{m} + \mathbf{n} \approx \mathbf{k}$, где $k = m + n$, $m, n \in \omega$, покажем индукцией по n. Для $n = 0$

это — аксиома 3). Индукционный шаг следует из аксиомы 4. Условие (2) следует теперь из леммы 1 б). Проверку для умножения оставляем читателю. □

Теорема 5. *Любая рекурсивная функция представима в* A_0.

Доказательство. В силу теоремы 36.3 достаточно для любой рекурсивной формулы φ, $FV(\varphi) \subseteq \{x_1, \ldots, x_n\}$, и любого рекурсивного терма t, $FV(t) \subseteq \{x_1, \ldots, x_n\}$, построить такие формулы $\Phi_\varphi(x_1, \ldots, x_n)$, $\Psi_t(x_1, \ldots, x_n, y)$ сигнатуры Σ_0, что для любых $m_1, \ldots, m_n, m \in \omega$ выполняются следующие условия:

$$\langle m_1, \ldots, m_n\rangle \in \varphi[x_1, \ldots, x_n] \Rightarrow A_0 \rhd \Phi_\varphi(\mathbf{m}_1, \ldots, \mathbf{m}_n), \quad (3)$$

$$\langle m_1, \ldots, m_n\rangle \notin \varphi[x_1, \ldots, x_n] \Rightarrow A_0 \rhd \neg\, \Phi_\varphi(\mathbf{m}_1, \ldots, \mathbf{m}_n), \quad (4)$$

$$t[x_1, \ldots, x_n](m_1, \ldots, m_n) = m \Rightarrow A_0 \rhd \Psi_t(\mathbf{m}_1, \ldots, \mathbf{m}_n, \mathbf{m}), \quad (5)$$

$$A_0 \rhd (\Psi_t(\mathbf{m}_1, \ldots, \mathbf{m}_n, y) \wedge \Psi_t(\mathbf{m}_1, \ldots, \mathbf{m}_n, z) \to y \approx z). \quad (6)$$

Строим Φ_φ и Ψ_t одновременно индукцией по длине φ и t:

а) $\Psi_0 = y \approx 0$,

б) $\Psi_x = y \approx x$,

в) $\Psi_{s(t)} = \exists z\left((\Psi_t)^y_z \wedge y \approx s(z)\right)$,

г) $\Psi_{t\tau q} = \exists z \exists w\left((\Psi_t)^y_z \wedge (\Psi_q)^y_w \wedge y \approx z\tau w\right)$, $\tau \in \{+, \cdot\}$,

д) $\Phi_{t\tau q} = \exists z \exists w\left((\Psi_t)^y_z \wedge (\Psi_q)^y_w \wedge z\tau w\right)$, $\tau \in \{\approx, <\}$,

е) $\Phi_{\neg\varphi} = \neg\Phi_\varphi$,

ж) $\Phi_{(\varphi\tau\psi)} = (\Phi_\varphi \tau \Phi_\psi)$, $\tau \in \{\wedge, \vee, \to\}$,

з) $\Psi_{\mu x\varphi} = (\Phi_\varphi)^x_y \wedge \forall x (x < y \to \neg\, \Phi_\varphi)$.

Теперь мы должны в каждом из случаев а) — з) определения формул Φ_φ, Ψ_t установить справедливость (3), (4) или (5), (6) соответственно. Случаи а) — в) и д) следуют из индукционного предположения и леммы 1. Случай г) следует из леммы 2 и индукционного предположения. Случаи е) и ж) очевидны. Проверим з). Так как $\mu x\varphi$ — рекурсивный терм, $FV(\mu x\varphi) \subseteq \{x_1, \ldots, x_n\}$, то для любых $m_1, \ldots, m_n \in \omega$ существует $m \in \omega$ такое, что $\varphi[\eta]$ для $\eta = \{\langle x_i, m_i\rangle \mid i = 1, \ldots, n\} \cup \{\langle x, m\rangle\}$. Из аксиомы 10) получаем истинность (6). Из индукционного предположения и леммы 1 а) получаем истинность (5). □

Теорема 6. *Если T — непротиворечивая теория сигнатуры Σ_0 и $A_0 \subseteq T$, то множество $X_T = \{\gamma(\Phi) \mid \Phi \in F(\Sigma_0),\ T \rhd \Phi\}$ нерекурсивно.*

Доказательство. Рассмотрим одноместную функцию Nm, определенную следующей схемой:

$$\mathrm{Nm}(0) = c(0, 1), \quad \mathrm{Nm}(n+1) = c(2, \mathrm{Nm}(n)).$$

Ясно, что функция Nm рекурсивна и для любого n $\mathrm{Nm}(n) = \gamma(\mathbf{n})$. Обозначим через $\mathrm{Sb}_0(x, y)$ функцию $\mathrm{Sb}(x, 0, \mathrm{Nm}(y))$ (функция Sb определена в доказательстве предложения 2). Заметим, что если $\Phi \in F(\Sigma_0)$, $n \in \omega$, то $\mathrm{Sb}_0(\gamma(\Phi), n) = \gamma(\Psi)$, где Ψ получается из Φ заменой всех свободных вхождений переменной v_0 на терм $\mathbf{n}$.

Предположим, что существует рекурсивная характеристическая функция f множества X_T. По предыдущей теореме существует формула $\Phi(x, y, z)$, представляющая в A_0 функцию $f(\mathrm{Sb}_0)$. Заменив, если нужно, формулу Φ на конгруэнтную, можно считать, что Φ не содержит переменную v_0 связанно. Пусть $n_0 = \gamma\left((\neg\,\Phi)^{x,\,y,\,z}_{v_0, v_0, \mathbf{1}}\right)$. Если $f(\mathrm{Sb}_0(n_0, n_0)) = 1$, то $\gamma(\neg\,\Phi(\mathbf{n}_0, \mathbf{n}_0, \mathbf{1})) \in X_T$, следовательно, $T \rhd \neg\,\Phi(\mathbf{n}_0, \mathbf{n}_0, \mathbf{1})$. Однако этого не может быть в силу представимости $f(\mathrm{Sb}_0)$ в $A_0 \subseteq T$ формулой $\Phi(x, y, z)$ и непротиворечивости T. Таким образом, $f(\mathrm{Sb}_0(n_0, n_0)) = 0$. Из того, что $\Phi(x, y, z)$ представляет в A_0 функцию $f(\mathrm{Sb}_0)$, и включения $A_0 \subseteq T$ получаем $T \rhd \neg\,\Phi(\mathbf{n}_0, \mathbf{n}_0, \mathbf{1})$. Следовательно, $\gamma(\neg\,\Phi(\mathbf{n}_0, \mathbf{n}_0, \mathbf{1})) \in X_T$ и $f(\mathrm{Sb}_0(n_0, n_0)) = 1$. Пришли к противоречию. □

Следствие 1 (Чёрч). *Множество теорем исчисления предикатов $И\Pi_1^{\Sigma_0}$ нерекурсивно.*

Доказательство. Пусть Φ_0 — конъюнкция аксиом 1) — 10) теории A_0 и $\Phi_1 = \forall v_0 \forall v_1 \forall v_2 \Phi_0$. Ясно, что для любой формулы Ψ сигнатуры Σ_0 имеем

$$A_0 \rhd \Psi \Leftrightarrow \left(\Phi_1 \to \Psi \text{ — теорема } \mathrm{И\Pi}_1^{\Sigma_0}\right). \tag{7}$$

Предположим, что характеристическая функция f множества $X_0 = \{\gamma(\Phi) \mid \Phi \text{ — теорема } \mathrm{И\Pi}_1^{\Sigma_0}\}$ рекурсивна. Тогда рекурсивна функция $g = f(c(9, c(n_0, x)))$, где $n_0 = \gamma(\Phi_1)$. В силу (7) g — характеристическая функция множества $\{\gamma(\Phi) \mid \Phi \in F(\Sigma_0),\ A_0 \rhd \Phi\}$ и по теореме 6 не может быть рекурсивной. Противоречие. □

Из предложения 3 и следствия 1 получаем

Следствие 2. *Существует рекурсивно перечислимое нерекурсивное множество.* □

Теорию T сигнатуры Σ_0 будем называть *аксиоматизируемой*, если существует рекурсивно перечислимое множество Γ аксиом для T.

Лемма 3. *Если T — аксиоматизируемая теория сигнатуры Σ_0, то множество $X_T = \{\gamma(\Phi) \mid \Phi \in F(\Sigma_0),\ T \rhd \Phi\}$ рекурсивно перечислимо.*

Доказательство. Пусть f — рекурсивная функция, перечисляющая множество $\gamma[\Gamma]$, где Γ — множество аксиом для T. Пусть Pr — функция из предложения 3, перечисляющая теоремы $\text{ИП}_1^{\Sigma_0}$. Рассмотрим функцию g, определенную следующим образом:

$$g(0) = f(0),\ g(n+1) = c(7,\ c(g(n),\ f(n+1))).$$

Пусть $f(i) = \gamma(\Phi_i)$, $i \in \omega$, тогда $g(n) = \gamma(\ldots(\Phi_0 \wedge \Phi_1) \wedge \wedge \ldots \wedge \Phi_n)$ и

$$X_T = \{\Phi \mid \Phi \in F(\Sigma_0),\ \rhd (\Phi_0 \wedge \ldots \wedge \Phi_n) \to \Phi,\ n \in \omega\}.$$

Следовательно, функция Pr_T, определенная схемой

$$\mathrm{Pr}_T(n) = \begin{cases} rr(\mathrm{Pr}(l(n))), & \text{если } l(\mathrm{Pr}(l(n))) = 9 \\ & \text{и } lr(\mathrm{Pr}(l(n))) = g(r(n)), \\ \gamma(v_0 \approx v_0) & \text{в остальных случаях,} \end{cases}$$

будет перечислять множество X_T. □

Напомним, что теория T сигнатуры Σ называется *полной*, если она непротиворечива и для любой замкнутой формулы Φ сигнатуры Σ либо $\Phi \in T$, либо $\neg\Phi \in T$.

Лемма 4. *Если теория T сигнатуры Σ_0 аксиоматизируема и полна, то множество $X_T = \{\gamma(\Phi) \mid \Phi \in F(\Sigma_0),\ T \rhd \Phi\}$ рекурсивно.*

Доказательство. Рассмотрим двухместную функцию f, определенную следующим образом:

$$f(m, 0) = c(12,\ c(0, m)),$$
$$f(m, n+1) = c(12,\ c(n+1,\ f(m, n))).$$

Тогда для $\Phi \in F(\Sigma_0)$ имеем $f(\gamma(\Phi), n) = \gamma(\forall v_n \forall v_{n-1} \ldots \ldots \forall v_0 \Phi)$. Так как $c(k, s) \geqslant k, s$, то индексы переменных, входящих в формулу Φ, не превосходят $\gamma(\Phi)$. Следовательно, формула Ψ, для которой $\gamma(\Psi) = f(\gamma(\Phi), \gamma(\Phi))$, замкнута для любой $\Phi \in F(\Sigma_0)$. Заметим, что для любой $\Phi \in F(\Sigma_0)$ имеем

$$T \rhd \Phi \Leftrightarrow T \rhd \Psi,$$

где $\gamma(\Psi) = f(\gamma(\Phi), \gamma(\Phi))$. Пусть Pr_T — функция из леммы 3, перечисляющая множество X_T. Из полноты T получаем $n \notin X_T \Leftrightarrow (F(n) = 0$ или $c(10, f(n, n)) \in X_T)$, где F — характеристическая функция множества $F(\Sigma_0)$. Поэтому функция g, определенная следующим образом:

$$g(n) = \begin{cases} l(n), \text{ если } \mathrm{Pr}_T(r(n)) = c(10, f(l(n), l(n))) \\ \qquad\qquad\qquad\qquad \text{или } F(l(n)) = 0, \\ \gamma(\neg\, v_0 \approx v_0) \text{ в остальных случаях,} \end{cases}$$

будет перечислять множество $\omega \setminus X_T$. Из предложения 37.1 получаем рекурсивность X_T. □

Теорема 7 (Гёделя о неполноте). *Любая аксиоматизируемая теория T сигнатуры Σ_0, являющаяся расширением A_0, неполна.*

Доказательство. Непосредственно из теоремы 6 и леммы 4. □

Теорема Гёделя о неполноте имеет исключительно важное значение для оснований математики. Если из теоремы 6 и тезиса Чёрча мы получаем, что не существует универсального метода для доказательства теорем арифметики, то из теоремы Гёделя о неполноте и тезиса Чёрча следует, что не существует даже эффективного способа задания аксиом арифметики. (Под арифметикой здесь понимается теория системы $\Omega = \langle \omega;\ +,\ \cdot,\ <,\ 0\rangle$.)

В заключение параграфа докажем, как было обещано в § 37, существование универсальных рекурсивно перечислимых предикатов.

Теорема 8. *Для любого $n \in \omega$, $n \neq 0$, существует $(n+1)$-местный рекурсивно перечислимый предикат, универсальный для семейства всех n-местных рекурсивно перечислимых предикатов.*

Доказательство. Рассмотрим $(n+1)$-местный предикат R, определенный так: для любых $m_0, m_1, \ldots, m_n \in \omega$

$$\langle m_0, m_1, \ldots, m_n\rangle \in R \Leftrightarrow m_0 \text{ — гёделев номер некоторой формулы } \Phi \text{ сигнатуры } \Sigma_0 \text{ и } A_0 \rhd (\Phi)^{v_0, \ldots, v_{n-1}}_{m_1, \ldots, m_n}.$$

Используя построенные выше функции, легко определить $(n+1)$-местную рекурсивную функцию f такую, что для любых $m_0, \ldots, m_n \in \omega$

а) если $F(m_0)=0$, т. е. m_0 не является гёделевым номером некоторой формулы, то $f(m_0, \ldots, m_n)=\gamma(\neg 0 \approx 0)$;

б) если $F(m_0)=1$ и Φ — такая формула, что $\gamma(\Phi)=m_0$, то

$$f(m_0, m_1, \ldots, m_n) = \gamma\left(\Phi_1 \to (\Phi)^{v_0, \ldots, v_{n-1}}_{m_1, \ldots, m_n}\right);$$

здесь Φ_1 — предложение, определенное в доказательстве следствия 1 к теореме 6.

Если X_0 — множество гёделевых номеров теорем $\text{ИП}_1^{\Sigma_0}$, то из определения функции f видно, что справедливо следующее соотношение: для любых $m_0, m_1, \ldots, m_n \in \omega$

$$\langle m_0, m_1, \ldots, m_n\rangle \in R \Leftrightarrow f(m_0, m_1, \ldots, m_n) \in X_0.$$

Таким образом предикат R m-сводится к множеству X_0. По предложению 3 X_0 рекурсивно перечислимо, следовательно, по предложению 37.7 предикат R также рекурсивно перечислим.

Покажем, что R и является универсальным для семейства всех n-местных рекурсивно перечислимых предикатов.

Пусть R^0 — n-местный рекурсивно перечислимый предикат, а φ — такая рекурсивная формула, что $FV(\varphi) \subseteq \{v_0, \ldots, v_n\}$ и

$$R^0 = (\exists v_n \varphi)[v_0, \ldots, v_{n-1}].$$

Пусть $\Phi_\varphi(v_0, \ldots, v_n)$ — формула из доказательства теоремы 5, тогда для любых $m_0, \ldots, m_{n-1}, m_n \in \omega$ выполнено следующее:

$$\langle m_0, \ldots, m_{n-1}, m_n\rangle \in \varphi[v_0, \ldots, v_n] \Rightarrow$$
$$\Rightarrow A_0 \rhd \Phi_\varphi(\boldsymbol{m}_0, \ldots, \boldsymbol{m}_{n-1}, \boldsymbol{m}_n),$$
$$\langle m_0, \ldots, m_{n-1}, m_n\rangle \notin \varphi[v_0, \ldots, v_n] \Rightarrow$$
$$\Rightarrow A_0 \rhd \neg \Phi_\varphi(\boldsymbol{m}_0, \ldots, \boldsymbol{m}_{n-1}, \boldsymbol{m}_n).$$

Рассмотрим формулу $\Phi(v_0, \ldots, v_{n-1}) = \exists v_n \Phi_\varphi(v_0, \ldots, v_{n-1}, v_n)$ и докажем следующее соотношение: для любых $m_0, \ldots, m_{n-1} \in \omega$

$$\langle m_0, \ldots, m_{n-1}\rangle \in R^0 \Leftrightarrow$$
$$\Leftrightarrow A_0 \rhd (\Phi)^{v_0, \ldots, v_{n-1}}_{\boldsymbol{m}_0, \ldots, \boldsymbol{m}_{n-1}} (= \Phi(\boldsymbol{m}_0, \ldots, \boldsymbol{m}_{n-1})).$$

Действительно, если $\langle m_0, \ldots, m_{n-1}\rangle \in R^0$, то для некоторого $m_n \in \omega$ $\langle m_0, \ldots, m_{n-1}, m_n\rangle \in \varphi[v_0, \ldots, v_n]$; тогда

$A_0 \triangleright \Phi_\varphi(m_0, \ldots, m_{n-1}, m_n)$ и

$$A_0 \triangleright \Phi(m_0, \ldots, m_{n-1}) (= \exists v_n \Phi_\varphi(m_0, \ldots, m_{n-1}, v_n)).$$

Наоборот, пусть $A_0 \triangleright \Phi(m_0, \ldots, m_{n-1})$; тогда $\Omega \models \exists v_n \Phi_\varphi(m_0, \ldots, m_{n-1}, v_n)$, так как Ω есть модель A_0; следовательно, для некоторого $m_n \in \omega$ $\Omega \models \Phi_\varphi(m_0, \ldots, m_{n-1}, m_n)$. Покажем теперь, что $\langle m_0, \ldots, m_{n-1}, m_n \rangle \in \varphi[v_0, \ldots, v_n]$; действительно, если бы это было не так, то $A_0 \triangleright \neg\Phi_\varphi(m_0, \ldots, m_{n-1}, m_n)$ и, следовательно, $\Omega \models \neg\Phi_\varphi(m_0, \ldots, m_{n-1}, m_n)$. Итак, $\langle m_0, \ldots, m_{n-1}, m_n \rangle \in \varphi[v_0, \ldots v_n]$ и, следовательно, $\langle m_0, \ldots, m_{n-1} \rangle \in R^0$. Пусть $k = \gamma(\Phi)$, тогда из доказанного выше имеем:

для любых $m_0, \ldots, m_{n-1} \in \omega$

$$\langle k, m_0, \ldots, m_{n-1} \rangle \in R \Leftrightarrow A_0 \triangleright (\Phi)^{v_0, \ldots, v_{n-1}}_{m_0, \ldots, m_{n-1}} \Leftrightarrow$$
$$\Leftrightarrow \langle m_0, \ldots, m_{n-1} \rangle \in R^0.$$

Таким образом, $R^0 = R_k$. □

Следствие 1. *Для любого $n \in \omega$, $n \neq 0$, существует $(n+1)$-местная частично рекурсивная функция, универсальная для семейства всех n-местных частично рекурсивных функций.*

Это следует из теоремы и предложения 37.6. □

В ходе доказательства теоремы по существу был установлен и следующий факт.

Следствие 2. *Множество X_0 гёделевых номеров теорем $ИП_1^{\Sigma_0}$ является m-универсальным рекурсивно перечислимым множеством.* □

Упражнения

1. Пусть T — теория сигнатуры Σ, $\Phi_0(x, w_1, \ldots, w_s)$, $\Phi_1(x, y, z, w_1, \ldots, w_n)$, $\Phi_2(x, y, z, w_1, \ldots, w_m) \in F(\Sigma)$. Показать, что если существуют модель $\mathfrak{A}$ теории T, элементы $c_1, \ldots, c_s$, $a_1, \ldots, a_n$, $b_1, \ldots, b_m \in A$ и отображение $f\colon \omega \to A$, для которых выполняются условия:

а) $f[\omega] = \{a \mid \mathfrak{A} \models \Phi_0(a, c_1, \ldots, c_s)\}$,

б) $k + l = r \Leftrightarrow \mathfrak{A} \models \Phi_1(fk, fl, fr, a_1, \ldots, a_n)$,

в) $k \cdot l = r \Leftrightarrow \mathfrak{A} \models \Phi_2(fk, fl, fr, b_1, \ldots, b_m)$,

то теория T неразрешима, т. е. множество $X_T = \{\Phi \in F(\Sigma) \mid T \triangleright \Phi\}$ нерекурсивно. (Указание. Применить теорему 6.)

2. Используя упражнение 1, доказать, что нерекурсивны множества теорем $ИП^{\Sigma_1}$ и $ИП^{\Sigma_2}$, где $\Sigma_1 = \langle f^2 \rangle$ и $\Sigma_2 = \langle r^2 \rangle$ содержат один двухместный функциональный и предикатный символ соответственно, а значит, неразрешимо исчисление $ИП^\Sigma$ для любой сигнатуры Σ, содержащей более чем одноместные символы.

§ 39. Разрешимые теории

Теорема о неразрешимости элементарной арифметики (теорема 6) положила конец попыткам построить универсальный алгоритм решения всех математических задач. Однако нахождение алгоритмов для решения различных классов математических задач было и остается одной из важнейших целей математики. Построенные в математической логике формальные языки значительно расширили возможности нахождения классов задач с разрешающим алгоритмом. В частности, про любую элементарную теорию T мы можем спросить, разрешима ли она, т. е. существует ли алгоритм, устанавливающий по любому предложению φ, принадлежит ли φ данной теории T. К сожалению, многие важные для математики теории оказались неразрешимыми. В § 40 будет продолжен список неразрешимых теорий, начатый в § 38, и будут приведены плодотворные методы доказательства неразрешимости элементарных теорий.

В данном параграфе на нескольких важных примерах будут продемонстрированы некоторые методы доказательства разрешимости элементарных теорий. Один из таких методов дают предложение 29.1 и лемма 38.4. Следующее предложение является следствием этих утверждений.

Предложение 1. а) *Элементарная теория ПЛП плотных линейных порядков без наименьшего и наибольшего элемента* (см. пример 15.3) *разрешима.*

б) *Элементарная теория* $АЗП_0$ *поля* $\langle C, +, \cdot, 0, 1\rangle$ *комплексных чисел разрешима.*

Доказательство. а) По предложению 15.4 теория ПЛП ω-категорична, следовательно, по предложению 29.1 она полна. Так как ПЛП имеет конечное множество аксиом, то она аксиоматизируема. Лемма 38.4 дает разрешимость ПЛП.

б) Рассмотрим теорию T_0, аксиомами которой будут аксиомы теории полей вместе со всеми предложениями вида

$$\forall x_0 \ldots \forall x_n \exists y\, x_0 + x_1 y + \ldots + x_n y^n \approx 0, \quad n \in \omega,$$

и всеми предложениями вида

$$\forall x\,(nx \approx 0 \to x \approx 0), \quad n \in \omega \setminus \{0\}.$$

Модели теории T_0 в алгебре называются *алгебраически замкнутыми полями нулевой характеристики.* Из алгебры известно, что любое алгебраически замкнутое поле нулевой характеристики определяется с точностью до изоморфизма максимальной мощностью своих алгебраически независимых подмножеств. Отсюда получаем, что T_0 категорична в несчетных мощностях, следовательно, по предложению 29.1 T_0 полна. Так как поле комплексных чисел является моделью теории T_0, а теория T_0 полна, то получаем АЗП$_0 = T_0$. Рекурсивность множества аксиом для АЗП$_0$ и лемма 38.4 дают разрешимость АЗП$_0$. □

Теория ПЛП, разрешимость которой установлена в предложении 1 а), совпадает с $\mathrm{Th}(\langle R, \leqslant\rangle)$, где R — множество действительных чисел. Имеется, однако, значительно более сильный результат: теория $\mathrm{Th}(\langle R, +, \cdot, <, 0, 1\rangle)$ разрешима. Для доказательства этой теоремы нам будут нужны некоторые общие факты.

Пусть T — некоторая теория сигнатуры Σ. Будем говорить, что в теории T имеется *элиминация кванторов*, если для любой формулы $\Phi(x_1, \ldots, x_n)$ сигнатуры Σ найдется бескванторная формула $\Phi^*(x_1, \ldots, x_n)$ сигнатуры Σ, эквивалентная в T формуле Φ (т. е. $T \rhd (\Phi \to \Phi^*) \wedge \wedge (\Phi^* \to \Phi)$).

Предложение 2. *Пусть элементарная теория T имеет по крайней мере одну константу в сигнатуре. Тогда следующие условия эквивалентны:*

1) *в T имеется элиминация кванторов;*

2) *для любой модели $\mathfrak{A}$ теории T, любой ω-насыщенной* (см. § 28) *модели $\mathfrak{B}$ теории T, любых $a_1, \ldots, a_n, b \in A$ и любого изоморфного вложения φ подсистемы $\mathfrak{A}(a_1, \ldots, a_n)$* (см. § 15) *в $\mathfrak{B}$ найдется продолжение φ до изоморфного вложения φ' подсистемы $\mathfrak{A}(a_1, \ldots, a_n, b)$ в $\mathfrak{B}$.*

Доказательство. 1)$\Rightarrow$2). Пусть выполнено 1) и выбраны $\mathfrak{A}$, $\mathfrak{B}$, $a_1, \ldots, a_n$, b и φ, как в 2). Рассмотрим множество

$$V = \{\Phi(x, \varphi a_1, \ldots, \varphi a_n) \mid \mathfrak{A} \models \Phi(b, a_1, \ldots, a_n),\ \Phi \text{ бескванторная}\}.$$

Для доказательства 2) достаточно показать, что V реализуется в $\mathfrak{B}$. В силу ω-насыщенности $\mathfrak{B}$ и замкнутости V относительно конъюнкции достаточно показать, что

$$\mathfrak{B} \models \exists x \Phi(x, \varphi a_1, \ldots, \varphi a_n) \tag{1}$$

для любой $\Phi(x, \varphi a_1, \ldots, \varphi a_n) \in V$. Пусть $\Phi^*(x_1, \ldots, x_n)$ —

бескванторная формула, эквивалентная в T формуле $\exists x\Phi(x, x_1, \ldots, x_n)$. Так как $\mathfrak{A} \models \exists x\Phi(x, a_1, \ldots, a_n)$, то $\mathfrak{A} \models \Phi^*(a_1, \ldots, a_n)$. Из того, что φ — изоморфное вложение и Φ^* бескванторная, вытекает $\mathfrak{B} \models \Phi^*(\varphi a_1, \ldots \ldots, \varphi a_n)$. Из эквивалентности в T формул Φ^* и $\exists x\Phi$ получаем (1).

2) $\Rightarrow$ 1). Пусть выполнено 2). Индукцией по числу кванторов в Φ будем находить бескванторную формулу Φ^*, эквивалентную в T формуле Φ. В силу эквивалентности $\forall x\Psi \equiv \neg\exists x\neg\Psi$ для любой формулы Ψ, достаточно рассмотреть случай, когда

$$\Phi(x_1, \ldots, x_n) = \exists x\Psi(x, x_1, \ldots, x_n),$$

где Ψ — бескванторная формула. Если $T \cup \{\Phi\}$ несовместно, то в качестве Φ^* можно взять $\neg c \approx c$, где c — некоторая константа. Пусть теперь $T \cup \{\Phi\}$ совместно. Рассмотрим множество

$$U = \{\Theta(x_1, \ldots, x_n) \mid T \rhd \Phi \to \Theta,\ \Theta \text{ бескванторная}\}.$$

Покажем, что $T \cup U \rhd \Phi$. Предположим, что это не так, т. е. существуют модель $\mathfrak{B}$ теории T и элементы $b_1, \ldots b_n \in B$ такие, что $\mathfrak{B} \models \Theta(b_1, \ldots, b_n)$ для всех $\Theta(x_1, \ldots \ldots, x_n) \in U$ и $\mathfrak{B} \models \neg\Phi(b_1, \ldots, b_n)$. Пусть

$$Y = \{\mathrm{X}(x_1, \ldots, x_n) \mid \mathfrak{B} \models \mathrm{X}(b_1, \ldots, b_n),\ \mathrm{X} \text{ бескванторная}\}.$$

Если бы множество $T \cup Y \cup \{\Phi\}$ было несовместным, то в силу замкнутости Y относительно конъюнкции выполнялось бы $T \rhd \Phi \to \neg\mathrm{X}_0$ для некоторого $\mathrm{X}_0 \in Y$. Тогда $\neg\mathrm{X}_0 \in U$ и в силу $U \subseteq Y$ это противоречило бы выполнимости Y. Итак, $T \cup Y \cup \{\Phi\}$ совместно, и пусть $\mathfrak{A}$ — модель теории T, $a_1, \ldots, a_n, b \in A$,

$$\mathfrak{A} \models \mathrm{X}(a_1, \ldots, a_n),\ \mathrm{X}(x_1, \ldots, x_n) \in Y, \qquad (2)$$

и $\mathfrak{A} \models \Psi(b, a_1, \ldots, a_n)$. Взяв, если нужно, ультрастепень $\mathfrak{B}$ по неглавному ультрафильтру на ω, можно считать, что $\mathfrak{B}$ ω-насыщена (предложение 28.6). Из (2) вытекает, что отображение φ_0: $\{a_1, \ldots, a_n\} \to B$, для которого $\varphi_0 a_i = b_i$, продолжается до изоморфного вложения φ подсистемы $\mathfrak{A}(a_1, \ldots, a_n)$ в $\mathfrak{B}$. (Если $n = 0$, то в качестве φ берем изоморфизм подсистем значений термов без переменных.) По 2) φ продолжается до изоморфного вложения φ' подсистемы $\mathfrak{A}(a_1, \ldots, a_n, b)$ в $\mathfrak{B}$. Так как Ψ бескванторная, то $\mathfrak{B} \models \Psi(\varphi' b, b_1, \ldots, b_n)$, следовательно,

$\mathfrak{B} \models \exists x \Psi(x, b_1, \ldots, b_n)$. Это противоречит условию $\mathfrak{B} \models$ $\models \neg \Phi(b_1, \ldots, b_n)$. Берем $\Phi^* \in U$, для которой $T \cup$ $\cup \{\Phi^*\} \rhd \Phi$. $\square$

Следующая система аксиом определяет теорию ВЗП (вещественно замкнутых полей):

1) аксиомы полей,

2) $\neg x < x$,

3) $(x < y \wedge y < z) \to x < z$,

4) $x < y \vee x \approx y \vee y < x$,

5) $(0 < x \wedge 0 < y) \to 0 < x \cdot y$,

6) $x < y \to x + z < y + z$,

7) $0 < x \to \exists y \ x \approx y^2$,

8) $\exists y \left(y^{2n+1} + \sum\limits_{i \leqslant 2n} x_i y^i \right) \approx 0, \quad n \in \omega.$

Заметим, что если $\langle F, +, \cdot, <, 0, 1 \rangle$ — вещественно замкнутое поле, то поле $\langle F, +, \cdot, 0, 1 \rangle$ имеет нулевую характеристику, а $\langle F, < \rangle$ — плотный строгий порядок (т. е. $\langle F, < \rangle \models x < y \to \exists z (x < z \wedge z < y)$). В самом деле, из аксиом 6) и 3) мы получаем $x < 0 \to nx < 0$ и $0 < x \to 0 < nx$, $n \in \omega \setminus \{0\}$, что вместе с 2) и 4) дает $\neg x \approx 0 \to \neg nx \approx 0$, $n \in \omega \setminus \{0\}$. Из аксиом 1) — 6) легко выводится также $x < y \to \left(x < \frac{x+y}{2} < y \right)$, что доказывает плотность $\langle F, < \rangle$.

Предложение 3. *В теории ВЗП имеется элиминация кванторов.*

Доказательство. Применим критерий предложения 2. Пусть $\mathfrak{A}$, $\mathfrak{B}$ — вещественно замкнутые поля, $\mathfrak{B}$ ω-насыщено, $a_1, \ldots, a_n, b \in A$ и φ_0 — изоморфное вложение $\mathfrak{A}(a_1, \ldots, a_n)$ в $\mathfrak{B}$. Система $\mathfrak{A}(a_1, \ldots, a_n)$ не является полем, однако аксиомы 1) — 6) позволяют единственным образом продолжить φ_0 до изоморфного вложения φ минимального подполя $\mathfrak{A}_0 \subseteq \mathfrak{A}$, содержащего $\mathfrak{A}(a_1, \ldots, a_n)$, в $\mathfrak{B}$.

Случай 1: b алгебраичен над $\mathfrak{A}_0$ в $\mathfrak{A}$, т. е. $\mathfrak{A} \models f(b) \approx 0$, где $f(x)$ — многочлен с коэффициентами из $\mathfrak{A}_0$. Существование требуемого в 2) предложения 2 вложения φ' вытекает из следующей леммы курса алгебры: если K — упорядоченное поле и K_1, K_2 — его вещественные замыкания, индуцирующие заданное упорядочение на K, то существует изоморфизм K_1 на K_2, тождественный на K.

Случай 2: b не алгебраичен над $\mathfrak{A}_0$ в $\mathfrak{A}$. Пусть

$$A_1 = \{a \in A_0 \mid \mathfrak{A}_0 \models a < b\}, \quad A_2 = \{a \in A_0 \mid \mathfrak{A}_0 \models b < a\}.$$

Обозначим через $p(x)$ множество всех формул вида $\varphi a < x$, $a \in A_1$, $x < \varphi a$, $a \in A_2$ и $\neg \sum\limits_{i<n} \varphi(c_i) x^i \approx 0$ для всех многочленов $\sum\limits_{i<n} c_i x^i$, $c_i \in A_0$, не равных тождественно нулю в $\mathfrak{A}_0$. Из плотности порядка в $\mathfrak{A}_0$ вытекает, что для любых $a_1 \in A_1$ и $a_2 \in A_2$ множество $\{a \mid \mathfrak{A}_0 \models a_1 < a \wedge a < a_2\}$ бесконечно. Так как корней любого многочлена в любом поле конечное число, то $p(x)$ локально выполнимо в $\mathfrak{B}$. Ввиду ω-насыщенности $\mathfrak{B}$ тип $p(x)$ реализуется в $\mathfrak{B}$ некоторым элементом b'. Ясно, что $\varphi \cup \{\langle b, b' \rangle\}$ однозначно продолжается до изоморфного вложения $\mathfrak{A}(A_0 \cup \{b\})$ в $\mathfrak{B}$. □

Следствие 1. *Теория ВЗП разрешима и совпадает с теорией* $\mathrm{Th}(\langle R, +, \cdot, <, 0, 1 \rangle)$ *упорядоченного поля действительных чисел.*

Доказательство. Атомарные предложения теории ВЗП эквивалентны $\mathbf{n} \approx \mathbf{m}$ и $\mathbf{n} < \mathbf{m}$, где через $\mathbf{n}$ мы обозначаем терм $1 + \ldots + 1$, являющийся суммой n единиц, если $n \in \omega \setminus \{0\}$, и $\mathbf{0}$ совпадает с константой 0. Из аксиом ВЗП легко вытекают свойства

$$n \neq m \Rightarrow \text{ВЗП} \rhd \neg\, \mathbf{n} \approx \mathbf{m},$$
$$n < m \Rightarrow \text{ВЗП} \rhd \mathbf{n} < \mathbf{m},$$
$$m \leqslant n \Rightarrow \text{ВЗП} \rhd \neg\, \mathbf{n} < \mathbf{m}.$$

Отсюда мы получаем, что для любой замкнутой бескванторной формулы Φ сигнатуры $\langle +, \cdot, <, 0, 1 \rangle$ мы имеем ВЗП $\rhd \Phi$ или ВЗП $\rhd \neg \Phi$. В силу предложения 3 теория ВЗП полна. Так как $\langle R, +, \cdot, <, 0, 1 \rangle$ является моделью теории ВЗП, то из полноты ВЗП получаем совпадение ВЗП и $\mathrm{Th}(\langle R, +, \cdot, <, 0, 1 \rangle)$. Так как ВЗП имеет рекурсивное множество аксиом, то по лемме 38.4 ВЗП разрешима. □

В отличие от полей действительных и комплексных чисел, теории поля рациональных чисел и кольца целых чисел являются неразрешимыми. Наша следующая цель — показать разрешимость теорий $\mathrm{Th}(\langle Z, +, 0 \rangle)$ и $\mathrm{Th}(\langle Q, +, 0 \rangle)$ сложения целых и рациональных чисел.

Для этого сначала докажем некоторые утверждения, касающиеся произвольных абелевых групп.

Пусть H — абелева группа, H_1 — подгруппа H. Если $a \in H$, то множество $H_1 + a = \{h + a \mid h \in H_1\}$ называется, как известно, *классом смежности* подгруппы H_1 в группе H. Мощность множества классов смежности H_1 в H называется *индексом* H_1 в H и обозначается $[H : H_1]$. Если индекс $[H : H_1]$ бесконечен, то пишем $[H : H_1] = \infty$. Если H_2 — еще одна подгруппа в H, то индекс $H_1 \cap H_2$ в H_1 также будем называть индексом H_2 в H_1 и обозначать $[H_1 : H_2]$.

Лемма 1. *Пусть H — абелева группа, H_1, H_2 — подгруппы H. Тогда*

а) $[(H_1 + H_2) : H_2] = [H_1 : H_2]$;

б) $[H_1 : H_2] \cdot [H : H_1] \geqslant [H : H_2]$;

в) *если $a \in H$, то число классов смежности по H_2, имеющих непустое пересечение с $H_1 + a$, равно $[H_1 : H_2]$.*

Доказательство. Легко получается из определения индексов. □

Лемма 2. *Пусть $H_0, \ldots, H_n$ — подгруппы некоторой абелевой группы A, $a_0, \ldots, a_n \in A$, $H_0 + a_0 \subseteq \bigcup\limits_{1 \leqslant i \leqslant n} (H_i + a_i)$ и $[H_0 : H_n] > n!$. Тогда $H_0 + a_0 \subseteq \bigcup\limits_{1 \leqslant i \leqslant n-1} (H_i + a_i)$.*

Доказательство. Покажем сначала, что если для подгрупп $K_0, \ldots, K_m$ группы A и $a_0, \ldots, a_m \in A$ мы имеем $[K_0 : K_i] = \infty$ для всех $i \in \{1, \ldots, m\}$, то включение

$$K_0 + a_0 \subseteq \bigcup_{1 \leqslant i \leqslant m} (K_i + a_i) \qquad (3)$$

не выполняется. Будем доказывать этот факт индукцией по числу l различных подгрупп среди $K_0 \cap K_1, \ldots, K_0 \cap K_m$. Если $K_0 \cap K_1 = \ldots = K_0 \cap K_m = K^*$, то (3) не выполняется, так как $K_0 + a_0$ содержит бесконечное число классов смежности по K^*. Пусть $l > 1$ и $K_i' = K_i \cap K_0$.

Случай 1: $1 < [K_0 \cap K_1 \colon K_{i_0}] < \infty$ для некоторого $i_0 \in \{2, \ldots, m\}$. Из леммы 1 а), б) вытекает $[K_0 : (K_1' + K_{i_0}')] = \infty$. Заменяя в последовательности $K_1, \ldots, K_m$ все подгруппы, совпадающие с K_1 или K_{i_0}, на $K_1' + K_{i_0}'$, мы уменьшим l и воспользуемся индукционным предположением.

Случай 2: отрицание случая 1. Пусть $s = \{i \in \{1, \ldots, m\} \mid K_0 \cap K_i = K_0 \cap K_1\}$. Так как $[K_0 : K_1] = \infty$, то найдется такое $a \in K_0 + a_0$, что $K_0 \cap K_1 + a \neq K_0 \cap K_i + a_i$ для всех $i \in s$. Если выполнено (3), то

$$K_0 \cap K_1 + a \subseteq \bigcup_{i \in \{1, \ldots, m\} \setminus s} (K_0 \cap K_i + a_i),$$

что противоречит индукционному предположению.

Теперь покажем, что в условиях леммы 2 найдется $i_0 \in \{1, \ldots, n\}$, для которого $[H_0 : H_{i_0}] \leqslant n$. Предположим, что это не так. Пусть $H_{i_1}, \ldots, H_{i_k}$ — все подгруппы из последовательности $H_1, \ldots, H_n$, имеющие конечный индекс в H_0. Пусть $H^* = H_{i_1} \cap \ldots \cap H_{i_k}$. По лемме 1 б) $[H_0 : H^*] = m < \infty$. По предположению и лемме 1 в) множество $(H_0 + a_0) \cap (H_{i_s} + a_{i_s})$, где $1 \leqslant s \leqslant k$, содержит менее m/n классов смежности по подгруппе H^*. Следовательно, найдется $a \in (H_0 + a_0) \setminus \bigcup_{i \in r} (H_i + a_i)$, где $r = \{i_1, \ldots, i_k\}$. Тогда

$$H_0 \cap H^* + a \subseteq \bigcup_{i \in \{1, \ldots, n\} \setminus r} (H_i + a_i). \tag{4}$$

Так как $[H_0 \cap H^* : H_i] = \infty$ для любого $i \in \{1, \ldots, n\} \setminus r$, то (4) противоречит факту, установленному в начале доказательства.

Докажем теперь утверждение леммы индукцией по n. Для $n = 1$ утверждение тривиально. Пусть оно верно для $n - 1$. Так как $[H_0 : H_n] > n!$ и $[H_0 : H_{i_0}] \leqslant n$, то по лемме 1 б) $[(H_0 \cap H_{i_0}) : H_n] > (n-1)!$. По индукционному предположению для любого $a \in (H_0 + a_0) \setminus (H_{i_0} + a_{i_0})$ имеем

$$(H_0 \cap H_{i_0}) + a \subseteq \bigcup_{i \in \{1, \ldots, n\} \setminus \{i_0, n\}} (H_i + a_i),$$

откуда получаем утверждение леммы. □

Для формулировки следующей леммы напомним, что для множества X через $|X|$ обозначается его мощность, и если $I = \varnothing$, то множество $A \cap \bigcap_{i \in I} A_i$ будем считать совпадающим с A.

Лемма 3. *Пусть $A_0, \ldots, A_n$ — конечные множества. Тогда*

$$A_0 \subseteq \bigcup_{1 \leqslant i \leqslant n} A_i \Leftrightarrow \sum_{r \subseteq \{1, \ldots, n\}} (-1)^{|r|} \cdot \left| A_0 \cap \bigcap_{i \in r} A_i \right| = 0. \tag{5}$$

Доказательство. Пусть $A_0 = \{a\}$ и $r_0 = \{i \mid a \in A_i\}$. Тогда

$$\left(A_0 \cap \bigcap_{i \in r} A_i\right) \neq \varnothing \Leftrightarrow \left|A_0 \cap \bigcap_{i \in r} A_i\right| = 1 \Leftrightarrow r \subseteq r_0. \quad (6)$$

Правая часть (5) в случае одноэлементного A_0 тогда и только тогда равна нулю, когда имеется одинаковое число четных и нечетных $|r|$ с условием $\left(A_0 \cap \bigcap\limits_{i \in r} A_i\right) \neq \varnothing$. В силу (6) это равносильно $r_0 \neq \varnothing$, т. е. $A_0 \subseteq \bigcup\limits_{1 \leqslant i \leqslant n} A_i$. Итак, (5) для одноэлементных A_0 доказано.

Заметим, что функция $F(X_0, X_1, \ldots, X_n) = \sum\limits_{r \subseteq \{1, \ldots, n\}} (-1)^{|r|} \cdot \left|X_0 \cap \bigcap\limits_{i \in r} X_i\right|$ аддитивна по X_0, т. е. если $A_0 = A_0^1 \cup A_0^2$ и $A_0^1 \cap A_0^2 = \varnothing$, то $F(A_0, A_1, \ldots, A_n) = F(A_0^1, A_1, \ldots, A_n) + F(A_0^2, A_1, \ldots, A_n)$. Из справедливости (5) для одноэлементного A_0 и аддитивности F получаем

$$F(A_0, A_1, \ldots, A_n) = F\left(A_0 \setminus \bigcup_{i=1}^n A_i, A_1, \ldots, A_n\right). \quad (7)$$

Так как $F\left(A_0 \setminus \bigcup\limits_{i=1}^n A_i, A_1, \ldots, A_n\right) = \left|A_0 \setminus \bigcup\limits_{i=1}^n A_i\right|$, то (5) выполнено для любого конечного A_0. □

Формула вида $\exists x_1 \ldots \exists x_n \Theta$, где Θ — коньюнкция атомарных формул, называется *позитивно примитивной формулой*. Сигнатурой абелевых групп мы называем сигнатуру $\Sigma^+ = \langle +, -, 0\rangle$, где $+$, $-$ являются двухместной и одноместной операциями, 0 — константой.

Предложение 4. *Пусть $\Phi(x_1, \ldots, x_n)$ — позитивно примитивная формула сигнатуры Σ^+ и A — абелева группа. Тогда*:

а) *$\Phi(x_1, \ldots, x_n)$ определяет подгруппу в декартовой степени A^n группы A, т. е. множество $\{\langle a_1, \ldots, a_n\rangle \mid A \models \Phi(a_1, \ldots, a_n)\}$ непусто и замкнуто относительно $+$ и $-$*;

б) *для любых $a_1, \ldots, a_n \in A$ и $l \geqslant 1$ формула $\Phi(x_1, \ldots, x_{l-1}, a_l, \ldots, a_n)$ либо не выполняется в A, либо определяет в A^{l-1} смежный класс по подгруппе, определяемой в A^{l-1} позитивно примитивной формулой $\Phi(x_1, \ldots, x_{l-1}, 0, \ldots, 0)$.*

Доказательство. Сразу следует из выполнимости в A свойств $t(0, \ldots, 0) = 0$ и

$$t(a_1 + b_1, \ldots, a_n + b_n) = t(a_1, \ldots, a_n) + t(b_1, \ldots, b_n)$$

для любого терма $t(x_1, \ldots, x_n)$ сигнатуры Σ^+ и любых $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$. □

Если $\Phi_1(x)$, $\Phi_2(x)$ — позитивно примитивные формулы сигнатуры Σ^+, A — абелева группа, то через $[\Phi_1 : \Phi_2, A]$ будем обозначать индекс $[H_1 : H_2]$, где H_i — подгруппа $\Phi_i(A)$, определяемая в A формулой $\Phi_i(x)$.

Будем говорить, что абелева группа A имеет *разрешимую проблему элементарных индексов*, если существует алгоритм, который по любым позитивно примитивным формулам $\Phi(x)$, $\Psi(x)$ сигнатуры Σ^+ и любому $n \in \omega$ определяет, выполняется ли условие $[\Phi : \Psi, A] \geqslant n$.

Будем называть формулу Φ *булевой комбинацией* формул множества X, если Φ получается из формул множества X с помощью связок $\wedge$, $\vee$, $\to$ и $\neg$.

Лемма 4. *Пусть A — абелева группа. Любая формула $\Phi(x_1, \ldots, x_n)$ сигнатуры Σ^+ эквивалентна в* $\mathrm{Th}(A)$ *булевой комбинации $\Phi^*(x_1, \ldots, x_n)$ позитивно примитивных формул. При этом, если в A разрешима проблема элементарных индексов, то существует алгоритм, дающий по Φ формулу Φ^*.*

Доказательство. Индукция по числу кванторов в Φ. В силу эквивалентностей § 19 достаточно рассмотреть случай $\Phi = \forall x(\Theta_1 \vee \ldots \vee \Theta_n)$, где Θ_i, $i \in \{1, \ldots, n\}$,— позитивно примитивные формулы или их отрицания. Так как дизъюнкция отрицаний позитивно примитивных формул эквивалентна отрицанию одной позитивно примитивной формулы, то, добавив, если нужно, формулу $\neg \exists x\, x \approx x$, можно считать, что $\Phi = \forall x(\neg\Phi_0 \vee \vee \Phi_1 \vee \ldots \vee \Phi_n)$, где Φ_i, $i \leqslant n$,— позитивно примитивные формулы. Так как $\forall x \neg\Phi_0$ эквивалентна отрицанию позитивно примитивной формулы, то можно считать $n > 0$. Итак, достаточно рассмотреть случай, когда Φ есть

$$\forall x (\Phi_0(x, x_1, \ldots, x_n) \to \\ \to (\Phi_1(x, x_1, \ldots, x_n) \vee \ldots \vee \Phi_n(x, x_1, \ldots, x_n))).$$

Пусть B_i, $i \leqslant n$,— подгруппы группы A, определенные соответственно формулами $\Phi_i(x, 0, \ldots, 0)$, $i \leqslant n$. В силу леммы 2 и предложения 4 можно считать, что $[B_0 : B_i] \leqslant \leqslant n!$, $i \in \{1, \ldots, n\}$. По лемме 1 в) и предложению 4 б) для $b_1, \ldots, b_n \in A$ и $\alpha \subseteq \{1, \ldots, n\}$ позитивно примитивная формула

$$\Phi_0(x, b_1, \ldots, b_n) \wedge \bigwedge_{i \in \alpha} \Phi_i(x, b_1, \ldots, b_n)$$

определяет в A либо пустое множество, либо множество, содержащее $n(\alpha)=\left[B_0 \cap \bigcap\limits_{i\in\alpha} B_i : B^*\right]$ классов смежности по подгруппе $B^* = B_0 \cap \ldots \cap B_n$. Рассмотрим множество

$$V=\left\{S \mid S \subseteq P(\{1, \ldots, n\}),\ \sum_{\alpha\in S}(-1)^{|\alpha|}\cdot n(\alpha)=0\right\}.$$

Для любого $S \subseteq P(\{1, \ldots, n\})$ определим формулу

$$\Phi^S(x_1, \ldots, x_n) = \Bigl(\bigwedge_{\alpha\in S} \exists x \bigwedge_{i\in\alpha\cup\{0\}} \Phi_i(x, x_1, \ldots, x_n)\Bigr) \wedge$$
$$\wedge \Bigl(\bigwedge_{\substack{\alpha\subseteq\{1,\ldots,n\}\\ \alpha\notin S}} \neg\exists x \bigwedge_{i\in\alpha\cup\{0\}} \Phi_i(x, x_1, \ldots, x_n)\Bigr).$$

По лемме 3 мы имеем, что $\Phi(x_1, \ldots, x_n)$ эквивалентна в $\mathrm{Th}(A)$ формуле $\bigvee\limits_{S\in V} \Phi^S(x_1, \ldots, x_n)$. Заменяя в формуле $\bigvee\limits_{S\in V} \Phi^S(x_1, \ldots, x_n)$ формулы $\exists x \bigwedge\limits_{i\in\alpha} \Phi_i$ на эквивалентные им позитивно примитивные формулы, получим требуемую Φ^*.

Ясно, что позитивно примитивные формулы $\Phi_0, \ldots, \Phi_n$ эффективно находятся по Φ, и если в A разрешима проблема элементарных индексов, то по $\Phi_0, \ldots, \Phi_n$ эффективно находится множество V, а значит, и формула Φ^*. □

Следствие 2. *Для того чтобы элементарная теория* $\mathrm{Th}(A)$ *абелевой группы* A *была разрешимой, необходимо и достаточно, чтобы в* A *была разрешима проблема элементарных индексов.*

Доказательство. Необходимость вытекает из того, что условие $[\Phi : \Psi, A] \geqslant n$ равносильно условию

$$A \models \exists x_1 \ldots \exists x_n \Bigl(\bigwedge_{1\leqslant i\leqslant n} \Phi(x_i) \wedge \bigwedge_{1\leqslant i<j\leqslant n} \neg\Psi(x_i - x_j)\Bigr).$$

Так как в любой абелевой группе истинно $t(0, 0, \ldots, 0) \approx \approx 0$ для любого терма $t(x_1, \ldots, x_n)$ сигнатуры Σ^+, то любое позитивно примитивное предложение истинно в любой абелевой группе. Поэтому существует алгоритм, определяющий для любой булевой комбинации позитивно примитивных предложений Φ^*, истинно или ложно Φ^* в A. Отсюда по лемме 4 вытекает достаточность. □

Элементарную теорию класса всех абелевых групп в дальнейшем будем обозначать через АГ.

Лемма 5. *Любая позитивно примитивная формула* $\Phi(v_1, \ldots, v_n)$ *сигнатуры абелевых групп эквивалентна* *относительно теории АГ конъюнкции формул вида* $\exists v_0 \sum_{i=1}^{n} m_i v_i \approx p^k v_0$ *и* $\sum_{i=1}^{n} m_i v_i \approx 0$, *где* $m_i \in Z$, $k \in \omega$ *и* p — *простое число.*

Доказательство. Пусть даны матрицы

$$N = \begin{pmatrix} n_{11} & \ldots & n_{1k} \\ \cdot & \cdot & \cdot \\ n_{t1} & \ldots & n_{tk} \end{pmatrix}, \quad M = \begin{pmatrix} m_{11} & \ldots & m_{1n} \\ \cdot & \cdot & \cdot \\ m_{t1} & \ldots & m_{tn} \end{pmatrix}$$

над Z. Тогда через $\langle N, M\rangle$ будем обозначать позитивно примитивную формулу $\exists v_{n+1} \ldots \exists v_{n+k}\Theta$, где Θ есть конъюнкция равенств системы

$$\begin{array}{ccc} n_{11}v_{n+1} + \ldots + n_{1k}v_{n+k} & = & \sum\limits_{1 \leqslant s \leqslant n} m_{1s}v_s, \\ \vdots \qquad\qquad \vdots & & \vdots \\ n_{t1}v_{n+1} + \ldots + n_{tk}v_{n+k} & = & \sum\limits_{1 \leqslant s \leqslant n} m_{ts}v_s. \end{array} \tag{8}$$

Пусть даны $i, j \in \{1, \ldots, t\}$. Ясно, что если N' и M' получаются соответственно из N и M перестановкой i-й и j-й строк, то формула $\langle N', M'\rangle$ эквивалентна формуле $\langle N, M\rangle$. Из коммутативности операции $+$ вытекает, что если N' получается из N перестановкой столбцов, то формула $\langle N', M\rangle$ эквивалентна относительно АГ формуле $\langle N, M\rangle$. Ясно также, что если даны $i, j \in \{1, \ldots, t\}$, $i \neq j$, и $k \in Z$, то формула $\langle N', M'\rangle$ эквивалентна в АГ формуле $\langle N, M\rangle$, где N' и M' получаются из N и M заменой элементов n_{il} и m_{is} ($l \in \{1, \ldots, k\}$, $s \in \{1, \ldots, n\}$) на $n_{il} + kn_{jl}$ и $m_{is} + km_{js}$ соответственно. Пусть теперь даны $i, j \in \{1, \ldots, k\}$, $i \neq j$, и $k \in Z$. Рассмотрим систему S, полученную из (8) заменой чисел $n_{1i}, \ldots, n_{ti}$ соответственно на числа $n_{1i} + kn_{1j}, \ldots, n_{ti} + kn_{tj}$. Ясно, что для любой абелевой группы A, если набор $\langle b_1, \ldots, b_k, a_1, \ldots, a_n\rangle$ является решением в A системы (8), то набор

$$\langle b_1, \ldots, b_{j-1}, b_j - kb_i, b_{j+1}, \ldots, b_k, a_1, \ldots, a_n\rangle$$

будет решением в A системы S, и если $\langle b_1, \ldots, b_k, a_1, \ldots, a_n\rangle$ — решение в A системы S, то

$$\langle b_1, \ldots, b_{j-1}, b_j + kb_i, b_{j+1}, \ldots, b_k, a_1, \ldots, a_n\rangle$$

— решение в A системы (8). Таким образом, если матрица N' получается из N заменой элементов $n_{1i}, \ldots, n_{ti}$ соответственно на числа $n_{1i} + kn_{1j}, \ldots, n_{ti} + kn_{tj}$, то формула $\langle N', M\rangle$ эквивалентна относительно теории АГ формуле $\langle N, M\rangle$.

С помощью описанных выше преобразований матриц N и M мы можем перейти к таким матрицам N^* и M^*, что формула $\langle N, M\rangle$ эквивалентна формуле $\langle N^*, M^*\rangle$, а матрица N^* имеет вид $\begin{pmatrix} D \\ O \end{pmatrix}$ или $(D\ O)$, где D — диагональная матрица, а O нулевая или пустая. Так как формула $\langle N^*, M^*\rangle$ эквивалентна конъюнкции формул вида $\exists v_0 \sum\limits_{i=1}^{n} m_i v_i \approx k v_0$ и $\sum\limits_{i=1}^{n} m_i v_i \approx 0$, то для завершения доказательства леммы достаточно заметить, что формула $\exists v_0 \sum\limits_{i=1}^{n} m_i v_i \approx k v_0$ эквивалентна относительно АГ конъюнкции формул $\exists v_0 \sum\limits_{i=1}^{n} m_i v_i \approx p_i^{k_i} v_0$, $i \in \{1, \ldots, r\}$, где $p_1, \ldots, p_r$ — попарно различные простые числа и $k = p_1^{k_1} \ldots p_r^{k_r}$. Для доказательства последнего утверждения предположим, что для некоторой абелевой группы A и элементов $a_1, \ldots, a_r, b \in A$ мы имеем

$$p_1^{k_1} a_1 = p_2^{k_2} a_2 = \ldots = p_r^{k_r} a_r = b.$$

Обозначим через n_i, $i \in \{1, \ldots, r\}$, числа $p_1^{k_1} \ldots p_{i-1}^{k_{i-1}} \times$ $\times\, p_{i+1}^{k_{i+1}} \ldots p_r^{k_r}$. Так как наибольший общий делитель чисел $n_1, \ldots, n_r$ равен 1, то найдутся такие числа $l_1, \ldots, l_r$, что $n_1 l_1 + \ldots + n_r l_r = 1$. Тогда для элемента $c = l_1 a_1 + \ldots + l_r a_r$ мы имеем $kc = b$. □

Следствие 3. *Теория* $\mathrm{Th}(\langle Q, +, -, 0\rangle)$ *сложения рациональных чисел разрешима.*

Доказательство. Ясно, что формулы вида $\exists y\, nx \approx p^k y$ определяют в $\mathbb{Q} = \langle Q, +, -, 0\rangle$ всю группу Q, а формулы вида $nx \approx 0$ — нулевую подгруппу. Применяя лемму 5 и следствие 2, получаем требуемое утверждение. □

Следствие 4. *Теория* $\mathrm{Th}(\langle Z, +, -, 0\rangle)$ *сложения целых чисел разрешима.*

Доказательство. Ясно, что формула $\exists y\, nx \approx ky$ эквивалентна относительно $T_0 = \mathrm{Th}(\langle Z, +, -, 0\rangle)$ формуле $\exists y x \approx \frac{k}{(n, k)} y$, а конъюнкция $\exists y x \approx ky \wedge \exists y x \approx ny$ эквивалентна относительно T_0 формуле $\exists y x \approx [n, k]\, y$, где

(n, k) — наибольший общий делитель, а $[n, k]$ — наименьшее общее кратное чисел n, k. Ясно, что индекс $\delta = [\exists yx \approx ky\colon \exists yx \approx my, \mathbb{Z}]$ равен $\frac{m}{(m, k)}$, если $m \neq 0$ и $k \neq 0$. Если $k = 0$, то $\delta = 1$. Если $k \neq 0$ и $m = 0$, то $\delta = \infty$. Следовательно, в силу леммы 5 $\mathbb{Z} = \langle Z, +, -, 0 \rangle$ имеет разрешимую проблему элементарных индексов. По следствию 2 получаем разрешимость теории T_0. □

Наша следующая цель — показать разрешимость теории АГ класса всех абелевых групп (сигнатуры $\Sigma^+ = \langle +, -, 0 \rangle$). Важную роль в этом доказательстве играют инварианты, введенные В. Шмелёвой. В дальнейшем под группой мы будем подразумевать абелеву группу.

Пусть A — группа. Напомним, что через kA обозначается подгруппа $\{ka \mid a \in A\}$, а через $A[k]$ мы обозначаем подгруппу $\{a \in A \mid ka = 0\}$. Если p — простое число и $pA = 0$, то $\dim A$ обозначает размерность группы A, рассматриваемой как векторное пространство над полем из p элементов. В дальнейшем через p и q будут обозначаться простые числа, а через n, k, m, s — натуральные числа. Следующие числа для произвольных p и n будем называть *инвариантами Шмелёвой группы* A:

$$\alpha_{p,n}(A) = \min\{\dim((p^nA)[p]/(p^{n+1}A)[p]), \omega\},$$

$$\beta_p(A) = \min\{\inf\{\dim(p^nA)[p] \mid n \in \omega\}, \omega\},$$

$$\gamma_p(A) = \min\{\inf\{\dim((A/A[p^n])/p(A/A[p^n])) \mid n \in \omega\}, \omega\},$$

$$\varepsilon(A) = \min\{\inf\{|\, n!\, A\,| \mid n \in \omega\}, \omega\}.$$

Мы будем говорить, что *у абелевых групп* A_1 *и* A_2 *совпадают инварианты Шмелёвой* (обозначаем $\mathrm{Sh}(A_1) = \mathrm{Sh}(A_2)$), если для любых p и n выполнено $\alpha_{p,n}(A_1) = \alpha_{p,n}(A_2)$, $\beta_p(A_1) = \beta_p(A_2)$, $\gamma_p(A_1) = \gamma_p(A_2)$ и $\varepsilon(A_1) = \varepsilon(A_2)$.

Следующая теорема дает классификацию полных расширений теории АГ.

Теорема 9. *Следующие условия для любых абелевых групп* A_1 *и* A_2 *равносильны:*

1) *у* A_1 *и* A_2 *совпадают элементарные индексы по модулю* ω, *т. е. для любых позитивно примитивных формул* $\Phi(x)$ *и* $\Psi(x)$ *выполнено* $[\Phi : \Psi, A_1] = [\Phi : \Psi, A_2]$ *или* $[\Phi : \Psi, A_i] = \infty$ *для каждого* $i \in \{1, 2\}$;

2) A_1 *и* A_2 *элементарно эквивалентны, т. е.* $\mathrm{Th}(A_1) = \mathrm{Th}(A_2)$;

3) $\mathrm{Sh}(A_1) = \mathrm{Sh}(A_2)$, *т. е. у* A_1 *и* A_2 *совпадают инварианты Шмелёвой.*

Доказательство. Заметим, что если у A_1 и A_2 совпадают элементарные индексы, то формула Φ^*, построенная в доказательстве леммы 4 для A_1, совпадает с Φ^*, построенной для группы A_2. Так как любое позитивно примитивное предложение истинно в любой абелевой группе, то из этого замечания получаем 1) $\Rightarrow$ 2).

2) $\Rightarrow$ 3). Легко написать предложения $\alpha_{p,n,k}$, $\beta_{p,n,k}$, $\gamma_{p,n,k}$ и ε_n, истинность которых в группе A равносильна условиям:

а) $\dim((p^nA)[p]/(p^{n+1}A)[p]) \geqslant k$;

б) $\dim(p^nA)[p] \geqslant k$;

в) $\dim((A/A[p^n])/p(A/A[p^n])) \geqslant k$;

г) $n!\,A \neq 0$

соответственно. Отсюда получаем, что из $A_1 \equiv A_2$ следует $\mathrm{Sh}(A_1) = \mathrm{Sh}(A_2)$.

3) $\Rightarrow$ 1). Пусть у групп A_1 и A_2 совпадают инварианты Шмелёвой. Нужно показать, что $[\Phi : \Psi, A_1] = [\Phi : \Psi, A_2]$ для произвольных позитивно примитивных формул $\Phi(x)$ и $\Psi(x)$. По лемме 5 можно считать, что Φ и Ψ являются конъюнкциями формул вида $nx \approx 0$ и $\exists y p^l x \approx \approx p^k y$, которые назовем базисными позитивно примитивными формулами соответственно первого и второго рода. Так как для произвольных подгрупп H_1, H_2, H_3 любой группы A мы имеем

$$[H_1 : H_2 \cap H_3] = [H_1 : H_2] \cdot [H_2 \cap H_1 : H_3],$$

то можно считать, что Ψ является базисной позитивно примитивной формулой. Так как индексы $[\Phi : \Psi, A]$ и инварианты Шмелёвой сохраняются при переходе от A к $A' \equiv A$, то можно считать, что $|A_i| \leqslant \omega$, $i \in \{1, 2\}$. Если $\varepsilon(A_1) = 0$, то A_1 является прямой суммой циклических групп порядков p^n. Ясно, что число прямых слагаемых порядка p^{n+1} совпадает с $\alpha_{p,n}(A)$. Следовательно, при $\varepsilon(A_1) = 0$ мы имеем $A_1 \simeq A_2$ и $[\Phi : \Psi, A_1] = [\Phi : \Psi, A_2]$. Поэтому в дальнейшем можно предполагать, что $\varepsilon(A_i) = \omega$, $i \in \{1, 2\}$.

Напомним, что подгруппа H группы A называется *p-базисной* для A, если выполнены следующие условия:

а) H является прямой суммой циклических p-групп и бесконечных циклических групп;

б) H — p-сервантная подгруппа A, т. е. для любого $a \in H$ и $k \in \omega$ имеет место

$$A \models \exists y a \approx p^k y \Leftrightarrow H \models \exists y a \approx p^k y;$$

в) A/H — p-делимая группа, т. е. $p(A/H) = A/H$.

Известно, что для любой абелевой группы A и любого p существуют p-базисные подгруппы для A. Пусть H_1^p, H_2^p — p-базисные подгруппы групп A_1 и A_2 соответственно. Из свойств б) и в) p-базисных подгрупп легко выводятся следующие факты:

1) $\alpha_{p,n}(A_i) = \alpha_{p,n}(H_i^p)$, $\gamma_p(A_i) = \gamma_p(H_i^p)$, $i \in \{1, 2\}$;

2) если $\Psi = \exists y p^l x \approx p^k y$, то $[\Phi : \Psi, A_i] = [\Phi : \Psi, H_i^p]$, $i \in \{1, 2\}$.

Отметим еще несколько простых фактов.

3) Если A является прямой суммой $\bigoplus\limits_{i \in \omega} \langle a_i \rangle$ циклических p-групп и бесконечных циклических групп, то

$$\alpha_{p,n}(A) = |\{i \in \omega \mid o(a_i) = p^{n+1}\}|$$

и условие $\gamma_p(A) = n \in \omega$ равносильно тому, что периодическая часть $T(A)$ группы A ограничена и $|\{i \in \omega \mid o(a_i) = \infty\}| = n$, где $o(a)$ — порядок элемента a.

4) $\alpha_{p,n}(A) = \alpha_{p,n}(A^p)$ и $\beta_p(A) = \beta_p(A^p)$, где A^p — p-компонента группы A, т. е. подгруппа элементов $a \in A$ порядков $o(a) = p^k$, $k \in \omega$.

Обозначим через T_i^p периодическую часть p-базисной подгруппы H_i^p, $i \in \{1, 2\}$. Из 1), 3) и 4) вытекает

5) $T_1^p \simeq T_2^p$, и если T_1^p ограничена, то $H_1^p \simeq H_2^p$.

Случай 1: Φ содержит базисную позитивно примитивную формулу $nx \approx 0$ первого рода. Тогда $\Phi(A_i) = \Phi(T(A_i))$, где $T(A_i)$ — периодическая часть A_i. Так как $T(A_i) = \bigoplus\limits_p A_i^p$, а позитивно примитивные формулы являются фильтрующимися, то $[\Phi : \Psi, A_i] = \prod\limits_p [\Phi : \Psi, A_i^p]$. Таким образом, доказательство сводится к установлению равенства $[\Phi : \Psi, A_1^p] = [\Phi : \Psi, A_2^p]$ для p-компонент A_1^p и A_2^p.

Если Ψ является базисной позитивно примитивной формулой второго рода, то требуемое равенство следует из свойств 2) и 5), где в качестве H_i^p берется базисная подгруппа группы A_i^p, которая в данном случае совпадает с T_i^p. Пусть теперь $\Psi = mx \approx 0$ и $n_1x \approx 0, \ldots, n_kx \approx \approx 0$ — все базисные формулы первого рода, входящие в Φ. Пусть p^k и p^l — максимальные степени p, делящие соответственно все числа $n_1, \ldots, n_r$ и число m. Если $k \leqslant l$, то $[\Phi : \Psi, A] = 1$ для любой p-группы A и доказывать нечего. Пусть $k - l > 0$ и p^s — максимальная степень p, для которой формула $\exists ytx \approx p^s y$ входит в Φ (если таких формул в Φ нет, то $s = 0$). Так как $A \models \models \forall x \exists yx \approx q^k y$ для любой p-группы A и простого $q \neq p$, то если порядок циклической p-группы $\langle a \rangle$ превышает число p^{s+k}, то $[\Phi : \Psi, \langle a \rangle] = p^{k-l}$. Следовательно, если базисная подгруппа T_1^p группы A_1^p неограничена, то $[\Phi : \Psi, T_1^p] = \infty$. Из 5) получаем $[\Phi : \Psi, T_2^p] = \infty$. Так как Ψ бескванторная и Φ, как $\exists$-формула, сохраняется при расширениях, то $[\Phi : \Psi, A_i^p] = \infty$, $i \in \{1, 2\}$. Пусть теперь T_1^p ограничена. Тогда $A_1^p = T_1^p \oplus \bigoplus\limits_{i \in J} B_i$, где B_i — квазициклические группы. Так как $p^n T_1^p = 0$ для некоторого $n \in \omega$, то $|J| = \beta_p(A_1^p)$. По 4) мы имеем $\beta_p(A_1^p) = \beta_p(A_2^p)$, следовательно, $A_1^p \simeq A_2^p$ и $[\Phi : \Psi, A_1^p] = [\Phi : \Psi, A_2^p]$.

Случай 2: отрицание случая 1 и $\Psi = k_0 x \approx 0$. Обозначим через n_0 произведение всех коэффициентов, входящих в формулу Φ. Так как $\varepsilon(A_1) = \omega$, то найдутся такие $a_n \in A_1$, $n \in \omega$, что $n! k_0 n_0 a_n \neq 0$. Так как Φ не содержит базисных формул первого рода, то по выбору n_0 получаем $A_1 \models \Phi(n_0 a_n)$. Так как $k_0 n! n_0 a_n \neq 0$, то $n_0 a_n$, $2n_0 a_n, \ldots, nn_0 a_n$ будут принадлежать различным смежным классам по $\Psi(A_1)$. Следовательно, $[\Phi : \Psi, A_1] = \infty$. Так как $\varepsilon(A_2) = \varepsilon(A_1) = \omega$, то из предыдущего получаем также $[\Phi : \Psi, A_2] = \infty$.

Случай 3: отрицание случая 1 и $\Psi = \exists y p^{l_0} x \approx p^{k_0} y$. Если периодическая часть T_1^p базисной подгруппы H_1^p группы A ограничена, то в силу 2) и 5) получаем $[\Phi : \Psi, A_1] = [\Phi : \Psi, A_2]$. Пусть теперь T_1^p неограничена. Из того, что p-группы являются q-делимыми для любого простого $q \neq p$, легко устанавливается следующий факт.

6) Пусть $\langle a \rangle$ — циклическая группа с образующим a порядка p^s и X — конъюнкция базисных формул второго рода. Пусть m — максимум из чисел 0 и $k - l$ для всех таких k, l, что $\exists y p^l x \approx p^k y$ входит в X, и p^t — макси-

мальная степень p, делящая хотя бы один коэффициент в X. Тогда, если $s > t$, то $X(\langle a\rangle) = \langle p^m a\rangle$.

Пусть m_0 — максимальное число вида $k-l$ для таких k, l, что $\exists y p^l x \approx p^k y$ входит в Φ. Если $k_0 - l_0 \leqslant m_0$, то из свойств 2), 6) и фильтруемости Φ, Ψ вытекает $[\Phi:\Psi,\ H_1^p] = [\Phi:\Psi,\ H_2^p]$. Если $k_0 - l_0 > m_0$, то из неограниченности T_1^p и свойства 6) мы получаем $[\Phi:\Psi,\ T_1^p] = \infty$. Так как $T_1^p \simeq T_2^p$, то $[\Phi:\Psi,\ T_2^p] = \infty$. Из p-сервантности T_i^p в A_i получаем $[\Phi:\Psi,\ A_i] = \infty$, $i \in \{1, 2\}$. □

Инварианты Шмелёвой более удобны, чем элементарные индексы $[\Phi:\Psi,\ A]$, так как они обладают большей независимостью друг от друга. Единственная зависимость их выражается в следующем предложении.

Предложение 5. *Пусть для каждого p и n даны кардиналы $\alpha_{p,n}$, β_p, $\gamma_p \leqslant \omega$ и $\varepsilon \in \{0, \omega\}$. Для того чтобы существовала абелева группа A, для которой инварианты Шмелёвой $\alpha_{p,n}(A)$, $\beta_p(A)$, $\gamma_p(A)$ и $\varepsilon(A)$ совпадали соответственно с $\alpha_{p,n}$, β_p, γ_p и ε, необходимо и достаточно выполнение следующих условий:*

1) если для простого p множество $\{n \mid \alpha_{p,n} \neq 0\}$ бесконечно, то $\beta_p = \gamma_p = \omega$;

2) если $\varepsilon = 0$, то $\beta_p = \gamma_p = 0$ и множество $\{\langle p, n\rangle \mid \alpha_{p,n} \neq 0\}$ конечно.

Доказательство. Необходимость вытекает из определения инвариантов Шмелёвой. Если же условия 1) и 2) выполняются, то легко проверить, что в качестве искомой группы A подходит группа

$$A = \bigoplus_{p,n} C_{p^{n+1}}^{(\alpha_{p,n})} + C_{p^\infty}^{(\beta_p)} + R_p^{(\gamma_p)} + Q^{(\varepsilon)},$$

где C_{p^n} — циклическая группа порядка p^n, C_{p^∞} — квазициклическая группа, Q — аддитивная группа рациональных чисел, R_p — подгруппа Q, состоящая из несократимых дробей с взаимно простыми с p знаменателями, а $B^{(k)}$ обозначает прямую сумму k подгрупп, изоморфных группе B. □

Теорема 10. *Теория АГ разрешима.*

Доказательство. Совокупность условий любого вида, соединенных по правилам русского языка словами «и», «или», и «не», будем называть *булевой комбинацией* этих условий. Обычным образом понимается истинность таких булевых комбинаций. Из доказательства леммы 4 получаем, что истинность предложения φ сигнатуры абелевых групп в абелевой группе A эквивалентна булевой комбинации условий вида $[\Phi:\Psi,\ A] \geqslant k$ для позитивно примитивных формул $\Phi(x)$, $\Psi(x)$ и $k \in \omega$. При этом данная булева комбинация эффективно находится по φ и не зависит от A. Из доказательства теоремы 9 видно, что условие $[\Phi:\Psi,\ A] \geqslant k$ эквивалентно булевой комбинации условий вида $A \vDash \alpha_{p,n,s}$, $A \vDash \beta_{p,n,s}$, $A \vDash \gamma_{p,n,s}$ и $A \vDash \varepsilon_n$. При этом такая булева комбинация также находится эффективно по Φ, Ψ, k и не зависит от A. Так же, как в предложении 5, существует простой алгоритм, позволяющий по любой булевой комбинации условий вида $A \vDash \alpha_{p,n,s}$, $A \vDash \beta_{p,n,s}$, $A \vDash \gamma_{p,n,s}$ и $A \vDash \varepsilon_n$ узнавать, реализуется ли данная булева комбинация для некоторой абелевой группы A. Таким образом, существует алгоритм, позволяющий по любому предложению φ сигнатуры абелевых групп узнавать, истинно ли φ во всех абелевых группах. □

Заметим, что из предложения 5 и теоремы 9 вытекает, что мощность множества различных пополнений теории АГ равна континууму, т. е. 2^{ω}. Отсюда, в частности, вытекает, что существуют абелевы группы A, элементарная теория $\mathrm{Th}(A)$ которых неразрешима.

В оставшейся части этого параграфа мы покажем, что операция взятия конечного декартова произведения и любой декартовой степени сохраняет свойство иметь разрешимую теорию.

В дальнейшем мы будем рассматривать булевы алгебры в сигнатуре $\langle \cup, \cap, -, 0, 1\rangle$. Через 2^I мы будем обозначать булеву алгебру всех подмножеств множества I. Если D — фильтр на I, то через $2^I/D$ будем обозначать гомоморфный образ алгебры 2^I по конгруэнции

$$\{\langle I_1, I_2\rangle \mid \overline{(I_1 \cap \bar{I}_2) \cup (\bar{I}_1 \cap I_2)} \in D\}.$$

Класс этой конгруэнции, содержащий множество I_1, будем обозначать через I_1/D. Нетрудно проверить, что $2^I/D$ будет изоморфна фильтрованной степени (см. упражнение 3 к § 17) $\mathbf{2}^D$, где $\mathbf{2}$ обозначает двухэлементную булеву алгебру. Когда D равен $\{I\}$, мы будем отождествлять $2^I/D$ с 2^I.

Предложение 6. *Существует алгоритм, который по любой формуле $\Phi(x_1, \ldots, x_n)$ сигнатуры Σ строит формулу $\Phi^*(y_1, \ldots, y_{k_\Phi})$ сигнатуры булевых алгебр и* *формулы* $\Phi^1(x_1, \ldots, x_n), \ldots, \Phi^{k_\Phi}(x_1, \ldots, x_n)$ *сигнатуры* Σ, *для которых выполнено следующее условие: если* D — *фильтр на множестве* I, $\mathfrak{A}_i$, $i \in I$,— *алгебраические системы сигнатуры* Σ *и* $f_1, \ldots, f_n \in I\text{-prod}\, A_i$, *то*

$$D\text{-prod}\,\mathfrak{A}_i \vDash \Phi(Df_1, \ldots, Df_n) \Leftrightarrow 2^I/D \vDash \vDash \Phi^*(I_1/D, \ldots, I_{k_\Phi}/D), \qquad (9)$$

где $I_j = \{i \mid \mathfrak{A}_i \vDash \Phi^j(f_1 i, \ldots, f_n i)\}$, $j \in \{1, \ldots, k_\Phi\}$.

Доказательство. Переходя к эквивалентной формуле, можно считать, что Φ не содержит квантора $\forall$. Построение будем вести индукцией по длине Φ. Если Φ — атомарная формула, то по лемме 17.3 в качестве Φ^* можно взять $y_1 \approx 1$, а в качестве Φ^1 — формулу Φ. Если $\Phi = \neg \Phi_1$, то в качестве Φ^* берем $\neg \Phi_1^*$, а в качестве $\Phi^1, \ldots, \Phi^{k_\Phi}$ — последовательность формул $\Phi_1^1, \ldots, \Phi_1^{k_{\Phi_1}}$. Если $\Phi = \Phi_1 \tau \Phi_2$, где $\tau \in \{\wedge, \vee, \rightarrow\}$, то в качестве Φ^* берем $\Phi_1^*(y_1, \ldots, y_{k_{\Phi_1}}) \tau \Phi_2^*(y_{k_{\Phi_1}+1}, \ldots, y_{k_{\Phi_1}+k_{\Phi_2}})$, а в качестве $\Phi^1, \ldots, \Phi^{k_\Phi}$ — последовательность $\Phi_1^1, \ldots, \Phi_1^{k_{\Phi_1}}, \Phi_2^1, \ldots, \Phi_2^{k_{\Phi_2}}$.

Пусть теперь $\Phi = \exists x \alpha(x, x_1, \ldots, x_n)$. Зафиксируем некоторое взаимно однозначное отображение

$$\delta\colon \{1, \ldots, 2^{k_\alpha}\} \rightarrow P(\{1, \ldots, k_\alpha\}).$$

Рассмотрим формулы

$$\Phi'(y_1, \ldots, y_{2^{k_\alpha}}) = \alpha^*\Bigl(\bigcup_{1 \in \delta(i)} y_i, \ldots, \bigcup_{k_\alpha \in \delta(i)} y_i\Bigr),$$

$$\Theta_i \rightleftharpoons \bigwedge_{j \in \delta(i)} \alpha^j \wedge \bigwedge_{\substack{j \in \{1, \ldots, k_\alpha\} \\ j \notin \delta(i)}} \neg \alpha^j, \quad i \in \{1, \ldots, 2^{k_\alpha}\}.$$

Нетрудно проверить следующие свойства:

1) для любых $f, f_1, \ldots, f_n \in I\text{-prod}\, A_i$ выполнено

$$D\text{-prod}\,\mathfrak{A}_i \vDash \alpha(Df, Df_1, \ldots, Df_n) \Leftrightarrow \Leftrightarrow 2^I/D \vDash \Phi'(I_1/D, \ldots, I_{2^{k_\alpha}}/D),$$

где $I_j = \{i \mid \mathfrak{A}_i \vDash \Theta_j(fi, f_1 i, \ldots, f_n i)\}$, $1 \leqslant j \leqslant 2^{k_\alpha}$;

2) $\rhd \Theta_i \rightarrow \neg \Theta_j$, $1 \leqslant i < j \leqslant 2^{k_\alpha}$;

3) $\rhd \Theta_1 \vee \ldots \vee \Theta_{2^{k_\alpha}}$.

Полагаем $k_\Phi = 2^{k_\alpha}$. Обозначим через Φ^* формулу

$$\exists z_1 \ldots \exists z_{k_\Phi}\Big(\bigwedge_{1\leqslant i<j\leqslant k_\Phi} z_i \cap z_j \approx 0 \wedge (z_1 \cup \ldots \cup z_{k_\Phi}) \approx$$
$$\approx 1 \wedge \bigwedge_{1\leqslant i\leqslant k_\Phi} z_i \cap y_i \approx z_i \wedge \Phi'(z_1, \ldots, z_{k_\Phi})\Big),$$

и пусть $\Phi^l = \exists x\Theta_l, l \in \{1, \ldots, k_\Phi\}$. Докажем свойство (9). Пусть $D\text{-prod}\,\mathfrak{A}_i \vDash \Phi(Df_1, \ldots, Df_n)$. Тогда найдется $f \in I\text{-prod}\,A_i$, для которого выполнено $D\text{-prod}\,\mathfrak{A}_i \vDash \alpha(Df, Df_1, \ldots, Df_n)$. По свойству 1) имеем $2^I/D \vDash \Phi'(I'_1/D, \ldots, I'_{k_\Phi}/D)$ для

$$I'_j = \{i \mid \mathfrak{A}_i \vDash \Theta_j(fi, f_1 i, \ldots, f_n i)\}, \quad 1 \leqslant j \leqslant k_\Phi.$$

Тогда

$$I'_j \subseteq I_j = \{i \mid \mathfrak{A}_i \vDash \Phi^j(f_1 i, \ldots, f_n i)\}, \quad 1 \leqslant j \leqslant k_\Phi.$$

В силу свойств 2) и 3) имеем $I'_i \cap I'_j = \varnothing, 1 \leqslant i < j \leqslant k_\Phi$, и $I'_1 \cup \ldots \cup I'_{k_\Phi} = I$. Так как отображение D: $2^I \to 2^I/D$ является гомоморфизмом, то в $2^I/D$ истинны $I'_i/D \cap I_i/D \approx \approx I'_i/D$, $I'_i/D \cap I'_j/D \approx 0$ для $i, j \in \{1, \ldots, k_\Phi\}$, $i \neq j$, и $I'_1/D \cup \ldots \cup I'_{k_\Phi}/D \approx 1$. Таким образом,

$$2^I/D \vDash \Phi^*(I_1/D, \ldots, I_{k_\Phi}/D). \tag{10}$$

Пусть теперь выполнено (10). Тогда найдутся такие $I'_i \subseteq I$, $1 \leqslant i \leqslant k_\Phi$, что $I \setminus (I'_i \cap I'_j) \in D$ для $i, j \in \{1, \ldots, k_\Phi\}$, $i \neq j$, $I'_1 \cup \ldots \cup I'_{k_\Phi} \in D$, $I \setminus (I'_i \setminus I_i) \in D$ и выполнено

$$2^I/D \vDash \Phi'(I'_1/D, \ldots, I'_{k_\Phi}/D). \tag{11}$$

Из условия 3) вытекает $I_1 \cup \ldots \cup I_{k_\Phi} = I$. Поэтому найдутся такие $I''_i \subseteq I$, $1 \leqslant i \leqslant k_\Phi$, что для всех $i, j \in \{1, \ldots, k_\Phi\}$, $i \neq j$, выполнены условия:

4) $I''_i/D = I'_i/D$,

5) $I''_1 \cup \ldots \cup I''_{k_\Phi} = I$,

6) $I''_i \subseteq I_i$,

7) $I''_i \cap I''_j = \varnothing$.

В силу условий 6), 7) и 2) найдется такой $f \in I\text{-prod}\, A_i$, что для всех $j \in \{1, \ldots, k_\Phi\}$ выполнено

$$I_j'' = \{i \mid \mathfrak{A}_i \vDash \Theta_j(fi, f_1 i, \ldots, f_n i)\}.$$

Поэтому из условий 4), (11) и 1) получаем

$$D\text{-prod}\, \mathfrak{A}_i \vDash \alpha(Df, Df_1, \ldots, Df_n).$$

Следовательно,

$$D\text{-prod}\, \mathfrak{A}_i \vDash \Phi(Df_1, \ldots, Df_n). \ \square$$

Следствие 5. *Если алгебраические системы $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ сигнатуры Σ имеют разрешимые теории, то декартово произведение $\mathfrak{A}_1 \times \ldots \times \mathfrak{A}_n$ также имеет разрешимую теорию.*

Доказательство. По предыдущему предложению проверка условия $\mathfrak{A}_1 \times \ldots \times \mathfrak{A}_n \vDash \Phi$ сводится к проверке условия $2^{\{1,\ldots,n\}} \vDash \Phi^*(I_1, \ldots, I_{k_\Phi})$ для некоторых $I_1, \ldots, I_{k_\Phi} \subseteq \{1, \ldots, n\}$. Из разрешимости теорий $\mathrm{Th}(\mathfrak{A}_1), \ldots, \mathrm{Th}(\mathfrak{A}_n)$ получаем, что $I_1, \ldots, I_{k_\Phi}$ эффективно находятся по Φ. Так как $2^{\{1,\ldots,n\}}$ — конечная система, то существует алгоритм проверки истинности формул $\Phi^*(I_1, \ldots, I_{k_\Phi})$ на этой системе. $\square$

Булева алгебра $\mathfrak{A}$ называется *атомной*, если для любого $a \in A$ либо $a = 0$, либо в $\mathfrak{A}$ найдется атом (см. § 12) b, для которого $b \leqslant a$.

Лемма 6. *Если $\mathfrak{A}$ и $\mathfrak{B}$ — бесконечные атомные булевы алгебры, то $\mathfrak{A} \equiv \mathfrak{B}$.*

Доказательство. Воспользуемся следствием 24.1. Пусть $n \in \omega$. Для $i \in \{1, \ldots, n\}$ в качестве $F_i(n)$ возьмем все такие $f \in P(\mathfrak{A}, \mathfrak{B})$, которые удовлетворяют следующим условиям:

1) f — изоморфное вложение конечной подалгебры $\mathfrak{A}_f \subseteq \mathfrak{A}$ в $\mathfrak{B}$;

2) если $a \in A_f$ содержит $k < 2^{n-i}$ атомов в $\mathfrak{A}$, то $f(a)$ содержит k атомов в $\mathfrak{B}$;

3) если $a \in A_f$ содержит $\geqslant 2^{n-i}$ атомов в $\mathfrak{A}$, то $f(a)$ содержит $\geqslant 2^{n-i}$ атомов в $\mathfrak{B}$.

Покажем, что выполнено условие *) следствия 24.1. Пусть $a \in A$, $f \in F_i(n)$, $1 \leqslant i < n$. Так как A_f конечно, то найдутся такие попарно различные элементы $a_1, \ldots, a_k \in A_f$, что $a_1 \cup \ldots \cup a_k = 1$ и для любого $b \in A_f$ и любого $i \in \{1, \ldots, k\}$ выполняется $b \cap a_i = 0$ или $a_i \leqslant b$. Пусть

$a_i^1 = a_i \cap a$, $a_i^2 = a_i \cap \bar{a}$, $i \in \{1, \ldots, k\}$. В силу свойств 1)—3) для каждого $i \in \{1, \ldots, k\}$ найдутся такие b_i^1, $b_i^2 \in B$, что выполнены условия:

4) $b_i^1 \cap b_i^2 = 0$, $f(a_i) = b_i^1 \cup b_i^2$;

5) для каждого $j \in \{1, 2\}$, если a_i^j содержит $m < 2^{n-i-1}$ атомов в $\mathfrak{A}$, то b_i^j содержит m атомов в $\mathfrak{B}$;

6) для каждого $j \in \{1, 2\}$, если a_i^j содержит $\geqslant 2^{n-i-1}$ атомов в $\mathfrak{A}$, то b_i^j содержит $\geqslant 2^{n-i-1}$ атомов в $\mathfrak{B}$.

Нетрудно понять, что для любого элемента e алгебры $\mathfrak{A}(a_1, \ldots, a_k, a)$ найдутся такие $s(e)$, $r(e) \subseteq \{1, \ldots, k\}$, что

$$e = \bigcup_{i \in s(e)} a_i^1 \cup \bigcup_{i \in r(e)} a_i^2.$$

Следовательно, $a \in \operatorname{dom} g$ и в силу 4) $f \subseteq g$, где

$$g = \left\{ \left\langle \bigcup_{i \in s} a_i^1 \cup \bigcup_{i \in r} a_i^2, \ \bigcup_{i \in s} b_i^1 \cup \bigcup_{i \in r} b_i^2 \right\rangle \middle| \, s, r \subseteq \{1, \ldots, k\} \right\}.$$

Так как пересечение различных элементов вида a_i^j (вида b_i^j) в $\mathfrak{A}$ (в $\mathfrak{B}$) равно нулю, то из условий 1)—6) вытекает $g \in F_{i+1}(n)$.

Случай $b \in B$ в условии *) рассматривается аналогично, если вместо f рассмотреть f^{-1}. □

С л е д с т в и е 6. *Теория любой атомной булевой алгебры $\mathfrak{A}$ разрешима.*

Д о к а з а т е л ь с т в о. Нетрудно понять, что конечные булевы алгебры одинаковой мощности изоморфны. Поэтому множеством аксиом теории $\mathrm{Th}(\mathfrak{A})$ для булевой алгебры мощности $k \in \omega$ будет множество аксиом булевых алгебр вместе с предложением, утверждающим, что мощность булевой алгебры равна k. Таким образом, $\mathrm{Th}(\mathfrak{A})$ конечно аксиоматизируема. Так как условие атомности булевой алгебры записывается одним предложением, то в силу предыдущей леммы теория бесконечных атомных булевых алгебр полна и аксиоматизируема. Из этих фактов в силу 38.4 получаем требуемое утверждение. □

С л е д с т в и е 7. *Если $\mathfrak{A}$ — алгебраическая система и $\mathrm{Th}(\mathfrak{A})$ разрешима, то для любого непустого I теория декартовой степени $\mathfrak{A}^I$ разрешима.*

Д о к а з а т е л ь с т в о. Пусть Φ — предложение сигнатуры $\mathfrak{A}$. Применяя предложение 6, найдем $\Phi^*(y_1, \ldots$

$\ldots, y_{k_\Phi})$ и $\Phi^1, \ldots, \Phi^{k_\Phi}$, для которых

$$\mathfrak{A}^I \models \Phi \Leftrightarrow 2^I \models \Phi^* (I_1, \ldots, I_{k_\Phi}), \tag{12}$$

где $I_j = \{i \in I \mid \mathfrak{A} \models \Phi^j\}$. Так как $I_j \in \{\varnothing, I\}$, то

$$2^I \models \Phi^* (I_1, \ldots, I_{k_\Phi}) \Leftrightarrow 2^I \models \Phi^* \left(c_1^\Phi, \ldots, c_{k_\Phi}^\Phi\right), \tag{13}$$

где $c_i^\Phi \in \{0, 1\}$. Если $\mathrm{Th}(\mathfrak{A})$ разрешима, то существует алгоритм, находящий по Φ константы c_i^Φ, $i \in \{1, \ldots, k_\Phi\}$. Из (12), (13), атомности булевой алгебры 2^I и предыдущего следствия получаем тогда разрешимость $\mathrm{Th}(\mathfrak{A}^I)$. □

В заключение отметим, что разрешимы теории сложения натуральных чисел, поля p-адических чисел, теории всех конечных полей, всех булевых алгебр и теория любой булевой алгебры. Из последнего результата и предложения 6 вытекает обобщение следствия 7: если $\mathfrak{A}$ — алгебраическая система с разрешимой теорией, то любая ее фильтрованная степень $\mathfrak{A}^D$ имеет разрешимую теорию.

§ 40. Неразрешимые теории

В настоящем параграфе будет указан один общий метод доказательства неразрешимости элементарных теорий — метод относительной элементарной определимости — и будут даны примеры применений этого метода.

Элементарную теорию T назовем *наследственно неразрешимой*, если любая ее подтеория $T_0 \subseteq T$ является неразрешимой.

Заметим, что если T наследственно неразрешима и $T_0 \subseteq T$ — подтеория, то и T_0 наследственно неразрешима. В терминах классов моделей это свойство может быть сформулировано так: если $K_0 \subseteq K_1$, где K_0 и K_1 — классы моделей одной и той же сигнатуры, и $\mathrm{Th}(K_0)$ наследственно неразрешима, то и $\mathrm{Th}(K_1)$ наследственно неразрешима.

Пусть K_0 — класс алгебраических систем (чисто предикатной конечной) сигнатуры $\sigma_0 = \langle P_0^{n_0}, \ldots, P_k^{n_k} \rangle$, K_1 — класс алгебраических систем сигнатуры σ_1. Будем говорить, что класс K_0 *относительно элементарно определим* в классе K_1, если существуют такие формулы $\mathfrak{A}(\bar{x}; \bar{y})$,

$\mathfrak{B}(\bar{x};\ \bar{y}^1;\ \bar{y}^2)$, $\mathfrak{C}_0\left(\bar{x};\ \bar{y}^1;\ \ldots;\ \bar{y}^{n_0}\right), \ldots, \mathfrak{C}_k\left(\bar{x};\ \bar{y}^1;\ \ldots;\ \bar{y}^{n_k}\right)$ сигнатуры σ_1 (здесь и далее $\bar{x}=(x_1, \ldots, x_n)$, $\bar{y}^i = (y_1^i, \ldots, y_m^i)$), что для любой алгебраической системы $\mathfrak{M} \in K_0$ найдутся алгебраическая система $\mathfrak{N} \in K_1$ и элементы $a_1, \ldots, a_n \in N$, удовлетворяющие условиям:

(1) множество $L = \{\bar{b} \mid \bar{b} \in N^m,\ \mathfrak{N} \models \mathfrak{A}(\bar{a},\ \bar{b})\}$ непусто;

(2) формула $\mathfrak{B}(\bar{a};\ \bar{y}^1;\ \bar{y}^2)$ задает конгруэнтность η на алгебраической системе $\mathfrak{L}$ сигнатуры σ_0, основное множество которой есть L, а предикаты определены формулами $\mathfrak{C}_i\left(\bar{a};\ \bar{y}^1;\ \ldots;\ \bar{y}^{n_i}\right)$ $\left(\text{т. е. } \nu^{\mathfrak{L}}(P_i) = \left\{\left\langle \bar{b}^1, \ldots, \bar{b}^{n_i}\right\rangle \middle| \bar{b}^j \in L,\ j = 1, \ldots, n_i,\ \mathfrak{N} \models \mathfrak{C}_i\left(\bar{a};\ \bar{b}^1;\ \ldots;\ \bar{b}^{n_i}\right),\ i \leqslant k\right\}\right)$;

(3) факторсистема $\mathfrak{L}/\eta$ изоморфна $\mathfrak{M}$.

Если формулы $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}_0, \ldots, \mathfrak{C}_k$ удовлетворяют сформулированным выше условиям, то будем говорить, что они *относительно элементарно определяют* $\mathfrak{M}$ *в* $\mathfrak{N}$ (*класс* K_0 *в классе* K_1).

Если класс K_0 относительно элементарно определим в классе K_1, то обозначать это будем так: $K_0 \leqslant_{\mathrm{RED}} K_1$.

Отметим следующие простые свойства введенного понятия:

1. Если $K_0' \subseteq K_0$, $K_1 \subseteq K_1'$ и $K_0 \leqslant_{\mathrm{RED}} K_1$, то $K_0' \leqslant_{\mathrm{RED}} K_1'$.

2. Если $K_0 \leqslant_{\mathrm{RED}} K_1$ и $K_1 \leqslant_{\mathrm{RED}} K_2$, то $K_0 \leqslant_{\mathrm{RED}} K_2$.

Основой метода доказательства неразрешимости — метода относительно элементарной определимости — является следующая

Теорема 11. *Если элементарная теория* $\mathrm{Th}(K_0)$ *класса* K_0 *наследственно неразрешима и* $K_0 \leqslant_{\mathrm{RED}} K_1$, *то и теория* $\mathrm{Th}(K_1)$ *класса* K_1 *также наследственно неразрешима.*

Пусть формулы $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}_0, \ldots, \mathfrak{C}_k$ относительно элементарно определяют класс K_0 в K_1 и $\mathrm{Th}(K_0)$ наследственно неразрешима.

Для любой формулы $\varphi(y_1, \ldots, y_s)$ сигнатуры σ_0 эффективно построим формулу $\bar{\varphi}(\bar{x};\ \bar{y}^1;\ \ldots;\ \bar{y}^s)$ сигнатуры σ_1 по следующим правилам:

если $\varphi(y_1, \ldots, y_s)$ есть $y_i \approx y_j$, то $\bar{\varphi}(\bar{x};\ \bar{y}^1;\ \ldots;\ \bar{y}^s) = \mathfrak{B}(\bar{x};\ \bar{y}^i;\ \bar{y}^j)$;

если $\varphi(y_1, \ldots, y_s)$ есть $P_i\left(y_{l_1}, \ldots, y_{l_{n_i}}\right)$, то $\bar{\varphi}(\bar{x};\ \bar{y}^1;\ \ldots;\ \bar{y}^s) = \mathfrak{C}_i\left(\bar{x};\ \bar{y}^{l_1};\ \ldots;\ \bar{y}^{l_{n_i}}\right)$;

если $\varphi(y_1, \ldots, y_s)$ есть $\varphi_0(y_1, \ldots, y_s) \circ \varphi_1(y_1, \ldots, y_s)$ $(\circ \in \{\wedge, \vee, \to\})$, то $\overline{\varphi}(\overline{x}; \overline{y}^1; \ldots; \overline{y}^s) = (\overline{\varphi}_0(\overline{x}; \overline{y}^1; \ldots; \overline{y}^s) \circ \overline{\varphi}_1(\overline{x}; \overline{y}^1; \ldots; \overline{y}^s))$;

если $\varphi(y_1, \ldots, y_s)$ есть $\neg\psi(y_1, \ldots, y_s)$, то $\overline{\varphi}(\overline{x}; \overline{y}^1; \ldots; \overline{y}^s) = \neg\,\overline{\psi}(\overline{x}; \overline{y}^1; \ldots; \overline{y}^s)$;

если $\varphi(y_1, \ldots, y_s)$ есть $\exists y_{s+1} \psi(y_1, \ldots, y_s, y_{s+1})$ $(\forall y_{s+1} \psi(y_1, \ldots, y_s, y_{s+1}))$, то $\overline{\varphi}(\overline{x}; \overline{y}^1; \ldots; \overline{y}^s) = \exists y_1^{s+1} \ldots \exists y_m^{s+1} (\mathfrak{A}(\overline{x}; \overline{y}^{s+1}) \wedge \overline{\psi}(\overline{x}; \overline{y}^1; \ldots; \overline{y}^s; \overline{y}^{s+1}))$ $(\forall y_1^{s+1} \ldots \forall y_m^{s+1} (\mathfrak{A}(\overline{x}; \overline{y}^{s+1}) \to \overline{\psi}(\overline{x}; \overline{y}^1; \ldots; \overline{y}^s; \overline{y}^{s+1})))$.

Пусть $\mathfrak{D}(\overline{x}) = \mathfrak{D}(x_1, \ldots, x_n)$ — следующая формула:

$$\exists \overline{y} \mathfrak{A}(\overline{x}; \overline{y}) \wedge \forall \overline{y}^0 \forall \overline{y}^1 \forall \overline{y}^2 \Big[\Big(\bigwedge_{i \leqslant 2} \mathfrak{A}(\overline{x}; \overline{y}^i) \to \mathfrak{B}(\overline{x}; \overline{y}^0; \overline{y}^0)\Big) \wedge$$

$$\wedge (\mathfrak{B}(\overline{x}; \overline{y}^0; \overline{y}^1) \to \mathfrak{B}(\overline{x}; \overline{y}^1; \overline{y}^0)) \wedge (\mathfrak{B}(\overline{x}; \overline{y}^0; \overline{y}^1) \wedge$$

$$\wedge \mathfrak{B}(\overline{x}; \overline{y}^1; \overline{y}^2)) \to \mathfrak{B}(\overline{x}; \overline{y}^0; \overline{y}^2))\Big] \wedge \bigwedge_{i \leqslant k} \Big[\forall \overline{y}^1 \ldots \forall \overline{y}^{n_i} \forall \overline{z}^1 \ldots$$

$$\ldots \forall \overline{z}^{n_i} \Big(\Big(\bigwedge_{j=1}^{n_i} (\mathfrak{A}(\overline{x}; \overline{y}^j) \wedge \mathfrak{A}(\overline{x}; \overline{z}^j) \wedge \mathfrak{B}(\overline{x}; \overline{y}^j; \overline{z}^j)\Big) \wedge$$

$$\wedge\, \mathfrak{C}_i(\overline{x}; \overline{y}^1; \ldots; \overline{y}^{n_i})\Big) \to \mathfrak{C}_i(\overline{x}; \overline{z}^1; \ldots; \overline{z}^{n_i})\Big)\Big],$$

где $\forall \overline{y}\, (\exists \overline{y})$ означает $\forall y_1 \ldots \forall y_m (\exists y_1 \ldots \exists y_m)$. Формула $\mathfrak{D}$ выражает требования на «параметры» $\overline{x}$ удовлетворять условиям (1) и (2) из определения относительной элементарной определимости.

Для любого предложения φ сигнатуры σ_0 пусть $\varphi^* = \forall x_1 \ldots \forall x_n (\mathfrak{D}(x_1, \ldots, x_n) \to \overline{\varphi}(\overline{x}))$; установим следующий факт.

Множество $T^* = \{\varphi \mid \varphi$ — предложение сигнатуры σ_0, $\varphi^* \in \mathrm{Th}(K_1)\}$ является такой теорией сигнатуры σ_0, что $T^* \subseteq \mathrm{Th}(K_0)$.

Действительно, обозначим через K_0^* класс таких алгебраических систем $\mathfrak{M}$ сигнатуры σ_0, что для $\mathfrak{M}$ существуют алгебраическая система $\mathfrak{N} \in K_1$ и элементы $a_1, \ldots, a_n \in N$, удовлетворяющие условиям (1)—(3) в определении относительной элементарной определимости. Тогда по условию теоремы $K_0 \subseteq K_0^*$. А из определения отображения $*$ следует, что $\varphi \in \mathrm{Th}(K_0^*) \Leftrightarrow \varphi^* \in \mathrm{Th}(K_1)$ для любого предложения φ сигнатуры σ_0.

Отмеченная эквивалентность вытекает из следующего общего утверждения, проверяемого индукцией по сложности формулы φ:

Пусть $\mathfrak{N} \in K_1$ и $a_1, \ldots, a_n \in N$ таковы, что $\mathfrak{N} \models \mathfrak{D}(\bar{a})$. Пусть алгебраическая система $\mathfrak{L}$ и конгруэнтность η определены, как в (2). Тогда для любых $\bar{b}^1, \ldots, \bar{b}^s \in L$ и формулы $\varphi(y_1, \ldots, y_s)$ сигнатуры σ_0 имеет место эквивалентность

$$\mathfrak{L}/\eta \models \varphi(\bar{b}^1/\eta, \ldots, \bar{b}^s/\eta) \Leftrightarrow \mathfrak{N} \models \bar{\varphi}(\bar{a}; \bar{b}^1; \ldots; \bar{b}^s).$$

Поэтому $T^* = \mathrm{Th}(K_0^*)$, и так как $K_0 \subseteq K_0^*$, то $T^* \subseteq \subseteq \mathrm{Th}(K_0)$.

Если бы теория $\mathrm{Th}(K_1)$ была разрешима, то эквивалентность $\varphi \in T^* \Leftrightarrow \varphi^* \in \mathrm{Th}(K_1)$ и эффективность отображения $\varphi \mapsto \varphi^*$ дали бы нам эффективную процедуру разрешимости для теории T^*. Но наследственная неразрешимость теории $\mathrm{Th}(K_0)$ и включение $T^* \subseteq \mathrm{Th}(K_0)$ влекут неразрешимость T^* и, следовательно, неразрешимость $\mathrm{Th}(K_1)$.

Если теория T_1^* сигнатуры σ_1 содержится в $\mathrm{Th}(K_1)$ и K_1^* — класс всех систем $\mathfrak{M}$ таких, что $\mathfrak{M} \models T_1^*$, то $K_1 \subseteq \subseteq K_1^*$. Согласно замечанию выше из $K_0 \leqslant_{\mathrm{RED}} K_1$ следует $K_0 \leqslant_{\mathrm{RED}} K_1^*$, тогда в силу доказанного выше (заменяя K_1 на K_1^*) теория $T_1^* = \mathrm{Th}(K_1^*)$ неразрешима. Итак, $\mathrm{Th}(K_1)$ наследственно неразрешима. □

Доказанная теорема является весьма мощным редукционным методом доказательства неразрешимости. Однако для ее применимости нужно иметь удобные примеры наследственно неразрешимых теорий.

В конце параграфа будет доказана следующая

Теорема 13. *Пусть Π_n^3 — класс всех конечных моделей сигнатуры $\langle \Pi^3 \rangle$, имеющих $\geqslant n$ элементов, тогда элементарная теория $\mathrm{Th}(\Pi_n^3)$ этого класса (в языке с равенством) наследственно неразрешима для любого $n \in \omega$.*

Замечание. На самом деле будет доказано более общее утверждение:

Если $A \subseteq \omega$ бесконечно и Π_A^3 — класс всех моделей $\mathfrak{M}$ сигнатуры $\langle \Pi^3 \rangle$ таких, что мощность $\mathfrak{M}$ принадлежит A, то $\mathrm{Th}(\Pi_A^3)$ наследственно неразрешима.

Предложение 1. *Класс Γ всех конечных моделей теории сигнатуры T_0, определенной аксиомой*

$$\forall x(\neg P(x, x) \wedge \forall y(P(x, y) \to P(y, x))),$$

имеет наследственно неразрешимую теорию (даже в языке без равенства).

Докажем это, используя теорему 11, а именно, установим, что класс Π_4^3 относительно элементарно определим в классе Γ формулами сигнатуры $\langle P^2 \rangle$ без равенства.

Рассмотрим алгебраическую систему $\mathfrak{M} = \langle M, \Pi \rangle \in \Pi_4^3$ и определим по $\mathfrak{M}$ алгебраическую систему $\mathfrak{N} = \langle N, P \rangle$ теории T_0 следующим образом:

$$U = \{u_t \mid t \in \Pi\}, \quad V = \{v_t \mid t \in \Pi\},$$

$$W = \{w_t \mid t \in \Pi\}, \quad S = \{s_t \mid t \in \Pi\};$$

$$N = M \cup U \cup V \cup W \cup S,$$

$$P = \{\langle x, y \rangle \mid x, y \in M, x \neq y\} \cup$$
$$\cup \{\langle u_t, v_t \rangle, \langle v_t, u_t \rangle, \langle w_t, v_t \rangle, \langle v_t, w_t \rangle, \langle u_t, w_t \rangle, \langle w_t, u_t \rangle, \langle w_t, s_t \rangle, \langle s_t, w_t \rangle, \langle x, s_t \rangle, \langle s_t, x \rangle, \langle y, u_t \rangle, \langle u_t, y \rangle, \langle y, v_t \rangle, \langle v_t, y \rangle, \langle z, w_t \rangle, \langle w_t, z \rangle \mid t \in \Pi, t = \langle x, y, z \rangle\}.$$

Если $\mathfrak{A}(y_0) = \exists y_1 \exists y_2 \exists y_3 \left(\bigwedge\limits_{0 \leqslant i < j \leqslant 3} P(y_i, y_j) \right)$, то легко проверить, что для $a \in N$ имеем $\mathfrak{N} \models \mathfrak{A}(a) \Leftrightarrow a \in M$. Пусть $\mathfrak{B}(y_1, y_2) = \neg P(y_1, y_2)$ и $\mathfrak{C}(y_1, y_2, y_3) =$
$= \bigwedge\limits_{i=1}^{3} \mathfrak{A}(y_i) \wedge \exists s \exists u \exists v \exists w (\neg \mathfrak{A}(s) \wedge \neg \mathfrak{A}(u) \wedge \neg \mathfrak{A}(v) \wedge \neg \mathfrak{A}(w) \wedge$
$\wedge \neg P(v, s) \wedge P(u, s) \wedge P(s, w) \wedge P(u, w) \wedge P(v, w) \wedge P(w, u) \wedge$
$\wedge P(y_1, u) \wedge P(y_2, s) \wedge P(y_3, w))$. Формула $\mathfrak{B}$ на M определяет отношение равенства, а формула $\mathfrak{C}$ на M определяет в точности предикат Π. Это рассмотрение показывает, что формулы $\mathfrak{A}(y)$, $\mathfrak{B}(y_1, y_2)$ и $\mathfrak{C}(y_1, y_2, y_3)$ относительно элементарно определяют класс Π_4^3 в классе Γ. □

Предложение 2. *Класс Eq_2 всех конечных моделей теории T_1 двух эквивалентностей, т. е. теории сигнатуры $\langle \eta_0^2, \eta_1^2 \rangle$, определенной аксиомой, утверждающей, что η_0 и η_1 являются отношениями эквивалентности, имеет наследственно неразрешимую теорию (в языке без равенства).*

Докажем это, установив, что класс Γ (из предложения 1) относительно элементарно определим в Eq_2.

Пусть $\mathfrak{M} = \langle M, P\rangle \in \Gamma$; определим по $\mathfrak{M}$ алгебраическую систему $\mathfrak{N} = \langle N, \eta_0, \eta_1\rangle \in \mathrm{Eq}_2$ так:

$$N = M \cup P;$$

$$\eta_0 = \{\langle x, x\rangle | x \in N\} \cup \{\langle x, \langle x, y\rangle\rangle, \langle\langle x, y\rangle, x\rangle, \langle\langle x, y\rangle, \langle x, z\rangle\rangle | x \in M, \langle x, y\rangle, \langle x, z\rangle \in P\};$$

$$\eta_1 = \{\langle x, x\rangle | x \in N\} \cup \{\langle\langle x, y\rangle, \langle y, x\rangle\rangle | \langle x, y\rangle \in P\}.$$

Полагаем

$$\mathfrak{A}(y) = y \approx y; \quad \mathfrak{B}(y_1, y_2) = \eta_0(y_1, y_2);$$

$$\mathfrak{C}(y_1, y_2) = \neg\, \eta_0(y_1, y_2) \wedge \exists z_1 \exists z_2 (\eta_0(y_1, z_1) \wedge \eta_0(y_2, z_2) \wedge \wedge\, \eta_1(z_1, z_2)).$$

Тогда, как нетрудно проверить, формулы $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ относительно элементарно определяют $\mathfrak{M}$ в $\mathfrak{N}$ и, следовательно, Γ в Eq_2. □

Предложение 3. *Класс* LEq *всех конечных моделей теории* T_2 *отношения линейного порядка и эквивалентности (сигнатуры* $\langle \leqslant, \eta\rangle$*) имеет наследственно неразрешимую теорию.*

Докажем это, установив, что Eq_2 относительно элементарно определим в LEq.

Пусть $\mathfrak{M} = \langle M, \eta_0, \eta_1\rangle \in \mathrm{Eq}_2$; определим по $\mathfrak{M}$ алгебраическую систему $\mathfrak{N} = \langle N, \leqslant, \eta\rangle \in \mathrm{LEq}$ так:

Пусть $M_1, \ldots, M_k$ — попарно различные классы η_1-эквивалентных элементов из M. Пусть $N = M \cup \{a_0, \ldots, a_k\}$, $a_i \notin M$, $i \leqslant k$; зададим на N линейный порядок $\leqslant$ так, чтобы было выполнено условие $M_i = \{a | a \in M,\ a_{i-1} \leqslant a \leqslant a_i\}$, $i = 1, \ldots, k$; отношение эквивалентности η на N задаем так, что $\{a_0, \ldots, a_k\}$ образует один класс η-эквивалентных элементов, а ограничение η на M совпадает с η_0.

Полагаем

$$\mathfrak{A}(x, y) = \neg\, \eta(x, y);$$

$$\mathfrak{B}(x, y_1, y_2) = y_1 \leqslant y_2 \wedge y_2 \leqslant y_1;$$

$$\mathfrak{C}_0(x, y_1, y_2) = \eta(y_1, y_2);$$

$$\mathfrak{C}_1(x, y_1, y_2) = \forall u (\eta(x, u) \to (u \leqslant y_1 \leftrightarrow u \leqslant y_2)).$$

Тогда легко проверить, что $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}_0$, $\mathfrak{C}_1$ определяют $\mathfrak{M}$ в $\mathfrak{N}$, когда в качестве значения параметра x взято a_0. Отсюда $\mathrm{Eq}_2 \leqslant_{\mathrm{RED}} \mathrm{LEq}$. □

Предложение 4. *Класс L_2 всех конечных моделей теории T_2 двух линейных порядков (сигнатура $\langle\leqslant_0, \leqslant_1\rangle$) имеет наследственно неразрешимую теорию.*

Покажем, что $\mathrm{LEq}\leqslant_{\mathrm{RED}}L_2$. Пусть $\mathfrak{M}=\langle M, \leqslant, \eta\rangle\in\mathrm{LEq}$; определим по $\mathfrak{M}$ алгебраическую систему $\mathfrak{N}=\langle N, \leqslant_0, \leqslant_1\rangle\in L_2$ так:

Пусть $M_1, \ldots, M_k$ — попарно различные классы η-эквивалентных элементов из M. Пусть $N=M\cup\{a_0, \ldots, a_k\}$, $a_i\notin M$, и $\leqslant_1$ — линейный порядок на N такой, что $M_i=\{a\,|\,a\in M,\ a_{i-1}\leqslant_1 a\leqslant_1 a_i\}$, $i=1, \ldots, k$. Линейный порядок $\leqslant_0$ на N таков, что любой элемент из $\{a_0, \ldots, a_k\}$ меньше любого элемента из M, а на M порядок $\leqslant_0$ совпадает с $\leqslant$. Пусть b — наименьший элемент в M относительно порядка $\leqslant$.

Полагаем

$$\mathfrak{A}(x, y)=x\leqslant_0 y;$$

$$\mathfrak{B}(x, y_1, y_2)=y_1\leqslant_0 y_2\wedge y_2\leqslant_0 y_1;$$

$$\mathfrak{C}_0(x, y_1, y_2)=y_1\leqslant_0 y_2;$$

$$\mathfrak{C}_1(x, y_1, y_2)=\forall u\,((u\leqslant_0 x\wedge\neg(x\leqslant_0 u))\to(u\leqslant_1 y_1\leftrightarrow u\leqslant_1 y_2)).$$

Если в качестве значения параметра x взять элемент b, то $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}_0$, $\mathfrak{C}_1$ относительно элементарно определяют $\mathfrak{M}$ в $\mathfrak{N}$, следовательно, и $\mathrm{LEq}\leqslant_{\mathrm{RED}}L_2$. □

Предложение 5. *Класс* Sym *всех конечных симметрических групп имеет наследственно неразрешимую теорию.*

Докажем это, установив, что Eq_2 относительно элементарно определим в Sym.

Пусть $\mathfrak{M}=\langle M, \eta_0, \eta_1\rangle\in\mathrm{Eq}_2$, и предположим, что $|M|\geqslant 3$. Пусть $m_0, \ldots, m_k$ — различные элементы из M, а $\mathfrak{N}=\mathrm{Sym}(M)$ — группа всех перестановок множества M. Возьмем $a_0=(m_0, m_1)$, $a_1=(m_0, m_2)\in N$; a_2 и a_3 выбираем в $\mathfrak{N}$ так, что циклы подстановок a_2 и a_3 отвечают классам эквивалентных элементов η_0 и η_1 соответственно.

Рассмотрим множество $L=\{\langle a, b\rangle\,|$ существует $h\in N$ такой, что $a=a_0^h$ и $b=a_1^h\}$. Нетрудно проверить, что L состоит из всех пар транспозиций, имеющих общий элемент.

Сопоставим паре $\langle a, b\rangle\in L$ элемент $\varphi(a, b)\in M$, являющийся общим элементом транспозиции: например, $\varphi((m_0, m_1), (m_0, m_2))=m_0$. Заметим, что отношение эквивалентности $\sim$ на L, определенное отображением φ

(т. е. $\langle a, b\rangle \sim \langle c, d\rangle \Leftrightarrow \varphi(a, b)=\varphi(c, d)$), может быть определено и так:

$$\langle a, b\rangle \sim \langle c, d\rangle \Leftrightarrow \forall h\,(a^h = a \to (cb^h)^3 = (db^h)^3 = e).$$

Заметим, что если $\langle a, b\rangle \in L$, $m=\varphi(a, b)$, $h\in N$, то $\varphi(a^h, b^h)=h(m)$ (где $z^h = h^{-1}zh$).

Определим на $\mathrm{Sym}(M)$ отношение частичного порядка $\leqslant$ так:

$$h_0 \leqslant h_1 \Leftrightarrow \forall m \in M\,(h_0(m) = m \vee h_0(m) = h_1(m)).$$

Единица e группы $\mathfrak{N}$ является наименьшим элементом; минимальными элементами множества $N\backslash\{e\}$ являются в точности циклические подстановки.

С каждым элементом $h\in N$ можно связать следующее отношение эквивалентности η_h на M: $\eta_h = \{\langle m, m\rangle \mid m \in M\} \cup \{\langle m_0, m_1\rangle \mid m_0, m_1 \in M$, существует минимальный элемент h_0 в $N\backslash\{e\}$ такой, что $h_0 \leqslant h$ и $h_0(m_0)\ne m_0$, $h_0(m_1)\ne m_1\}$.

Из выбора элементов a_2, a_3 следует, что $\eta_{a_2}=\eta_0$, $\eta_{a_3}=\eta_1$.

Запишем теперь следующие формулы в языке теории групп:

$$\mathfrak{A}(x_1, x_2, x_3, x_4, y_1, y_2) = \exists z\,(y_1 \approx z^{-1}x_1z \wedge y_2 \approx z^{-1}x_2z);$$

$$\mathfrak{B}(\bar{x}, y_1, y_2, y_3, y_4) = \forall h\,(h^{-1}y_1h \approx y_1 \to \to (y_3h^{-1}y_2h)^3 \approx (y_4h^{-1}y_2h)^3 \approx e);$$

$$\mathfrak{C}_0(\bar{x}, y_1, y_2, y_3, y_4) = \\ = \exists z\,(z \leqslant x_3 \wedge z \ne e \wedge \forall u\,(u \leqslant z \to (u \approx e \vee u \approx z)) \wedge \\ \wedge (\mathfrak{B}(\bar{x}, y_1, y_2, y_3, y_4) \vee (\neg\,\mathfrak{B}(\bar{x}, y_1, y_2, y_1^z, y_2^z) \wedge \\ \wedge \neg\,\mathfrak{B}(\bar{x}, y_3, y_4, y_3^z, y_4^z)))),$$

где $z \leqslant x$ означает

$$\forall y_1 \forall y_2\,(\mathfrak{A}(\bar{x}, y_1, y_2) \to \mathfrak{B}(\bar{x}, y_1, y_2, y_1^z, y_2^z) \vee \\ \vee \mathfrak{B}(\bar{x}, y_1^z, y_2^z, y_1^x, y_2^x));$$

$$\mathfrak{C}_1(\bar{x}, y_1, y_2, y_3, y_4) = \\ = \exists z\,(z \leqslant x_4 \wedge z \ne e \wedge \forall u\,(u \leqslant z \to (u \approx e \vee u \approx z)) \wedge \\ \wedge (\mathfrak{B}(\bar{x}, y_1, y_2, y_3, y_4) \vee (\neg\,\mathfrak{B}(\bar{x}, y_1, y_2, y_1^z, y_2^z) \wedge \\ \wedge \neg\,\mathfrak{B}(\bar{x}, y_3, y_4, y_3^z, y_4^z)))).$$

Если «параметрам» x_1, x_2, x_3, x_4 приписать значения a_0, a_1, a_2, a_3 соответственно, то формула $\mathfrak{A}$ определит множество L; $\mathfrak{B}$ задает на L отношение $\sim$, а $\mathfrak{C}_0$ и $\mathfrak{C}_1$ определят на $L/\sim$ отношения эквивалентности $\varphi^{-1}(\eta_0)$ и $\varphi^{-1}(\eta_1)$ соответственно. Проведенное рассмотрение и показывает, что формулы $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}_0$, $\mathfrak{C}_1$ относительно элементарно определяют класс Eq_2 в Sym. □

Следствие 1. *Класс конечных групп имеет наследственно неразрешимую теорию.*

Следствие 2. *Класс всех групп имеет наследственно неразрешимую теорию.*

Займемся теперь подготовкой к доказательству теоремы 13.

Частичную n-местную функцию $f\colon A \to \omega$, $A \subseteq \omega^n$, назовем *спектрально представимой*, если существует предложение Φ_f сигнатуры $\sigma_f = \langle \delta_1^1, \ldots, \delta_n^1, \rho^1, \ldots \rangle$ такое, что выполнены следующие условия:

1. Для любой n-ки $\langle m_1, \ldots, m_n \rangle \in A$ существует конечная модель $\mathfrak{M}$ сигнатуры σ_f такая, что $\mathfrak{M} \models \Phi_f$, $|\nu^{\mathfrak{M}}(\delta_i)| = m_i$, $i = 1, \ldots, n$, $|\nu^{\mathfrak{M}}(\rho)| = f(m_1, \ldots, m_n)$.

2. Для любой конечной модели $\mathfrak{M}$ сигнатуры σ_f такой, что $\mathfrak{M} \models \Phi_f$, если $m_i = |\nu^{\mathfrak{M}}(\delta_i)|$, $i = 1, \ldots, n$, то $\langle m_1, \ldots, m_n \rangle \in A$ и $f(m_1, \ldots, m_n) = |\nu^{\mathfrak{M}}(\rho)|$.

Если предложение Φ_f удовлетворяет условиям 1, 2, то будем говорить, что оно *спектрально представляет* функцию f.

Теорема 12. *Всякая частично рекурсивная функция спектрально представима.*

Доказательство будет вестись индукцией по длине определяющей последовательности.

Доказывать будем чуть более сильное утверждение: для любой частично рекурсивной n-местной функции f существует предложение Φ_f, спектрально представляющее f и такое, что а) сигнатура σ_f содержит только одноместные и двухместные предикаты, и б) если $\mathfrak{M} \models \Phi_f$, то $\nu^{\mathfrak{M}}(\delta_i) \cap \nu^{\mathfrak{M}}(\delta_j) = \varnothing$, $1 \leqslant i < j \leqslant n$, $\nu^{\mathfrak{M}}(\delta_i) \cap \nu^{\mathfrak{M}}(\rho) = \varnothing$, $i = 1, \ldots, n$.

Условие б) выполнится, если выполнится формула

$$\Psi_n = \forall x \left(\bigwedge_{1 < i < j < n} (\neg \delta_i(x) \vee \neg \delta_j(x)) \wedge \bigwedge_{i=1}^{n} (\neg \delta_i(x) \vee \neg \rho(x)) \right).$$

В дальнейшем, говоря о спектральной представимости, будем предполагать выполнимость условий а) и б), Будем говорить, что двухместный предикат $\Pi \subseteq M^2$ над M *расслаивает* M над $N \subseteq M$, если выполнено

$$\langle a, b\rangle \in \Pi \Rightarrow a \in N \wedge b \notin N;$$

$$\langle a, b\rangle, \langle c, b\rangle \in \Pi \Rightarrow a = c;$$

для любого $b \notin N$ существует $a \in N$ такое, что $\langle a, b\rangle \in \Pi$. Для $a \in N$ через Π_a обозначим множество $\{b \mid \langle a, b\rangle \in \Pi\}$.

Будем говорить, что двухместный предикат $C \subseteq M^2$ над M есть *взаимно однозначное соответствие* между D и $L (D, L \subseteq M)$, если выполнены условия: для любого $d \in D$ существует единственный $l \in L$ такой, что $\langle d, l\rangle \in C$, и для любого $l \in L$ существует единственный $d \in D$ такой, что $\langle d, l\rangle \in C$.

Лемма 1. *Базисные функции* o, s, I_m^n *спектрально представимы.*

Доказательство. Определим

$$\sigma_o = \langle \delta, \rho\rangle, \quad \Phi_o = \forall x \neg \rho(x); \; \sigma_s = \langle \delta, \rho, C^2\rangle;$$

$\Phi_s = \Psi_1 \wedge \exists x [\neg \delta(x) \wedge (C$ есть взаимно однозначное соответствие между $\{x\} \cup \delta$ и $\rho)]$;

$$\sigma_{I_m^n} = \langle \delta_1, \ldots, \delta_n, \rho, C^2\rangle, \; \Phi_{I_m^n} = \Psi_n \wedge (C \text{ есть взаимно однозначное соответствие между } \delta_m \text{ и } \rho).$$

Легко проверяется, что предложения Φ_o, Φ_s и $\Phi_{I_m^n}$ представляют соответственно функции o, s, I_m^n. □

Лемма 2. *Если k-местная функция h получена регулярной суперпозицией из n-местной функции f и k-местных функций $g_1, \ldots, g_n$ и функции $f, g_1, \ldots, g_n$ спектрально представимы, то и h спектрально представима.*

Не уменьшая общности, можно считать, что формулы Φ_{g_l}, спектрально представляющие g_l, $l = 1, \ldots, n$, имеют одну и ту же сигнатуру $\sigma_1 = \langle \delta_1, \ldots, \delta_k, \rho, \ldots\rangle$. Пусть предложение Φ_f сигнатуры $\sigma_0 = \langle \delta_1, \ldots, \delta_n, \rho, \ldots\rangle$ спектрально представляет функцию f.

Определим сигнатуру $\sigma_h = \langle \delta_1, \ldots, \delta_k, \rho\rangle \cup \sigma_0' \cup \sigma_1'' \cup \cup \langle \leqslant^2, \Pi^2, C^2\rangle$, где σ_0' — «штрихованная» копия σ_0; аналогично понимается σ_1''.

Вместо выписывания предложения Φ_h, спектрально представляющего функцию h, будем описывать свойства такой произвольной модели $\mathfrak{M}$ сигнатуры σ_h, что $\mathfrak{M} \models \Phi_h$.

Модель $\mathfrak{M}$ удовлетворяет следующим условиям:

1. Предикат П расслаивает M над $D \subseteq M$.

2. Множество D имеет в точности $n+1$ элемент, и предикат $\leqslant$ линейно упорядочивает $D = \{d_0, \ldots, d_n\}$, $d_0 < \ldots < d_n$.

Через $\mathfrak{M}_0'$ обозначим обеднение до σ_0' подмодели модели $\mathfrak{M}$, определенной множеством $\Pi_{d_0}\left(= \{m \mid \langle d_0, m\rangle \in \in \nu^{\mathfrak{M}}(\Pi)\}\right)$; через $\mathfrak{M}_l''$ обозначим обеднение до σ_1'' подмодели модели $\mathfrak{M}$, определенной множеством Π_{d_l}, $l = 1, \ldots, n$.

3. $\mathfrak{M}_0' \models \Phi_f'$, $\mathfrak{M}_l'' \models \Phi_{g_l}''$, $l = 1, \ldots, n$, где предложение $\Phi_f'\left(\Phi_{g_l}''\right)$ получено из $\Phi_f\left(\Phi_{g_l}\right)$ заменой всех предикатных символов $P \in \sigma_0$ $(P \in \sigma_1)$ на $P' \in \sigma_0'$ $(P'' \in \sigma_1'')$.

4. $\nu^{\mathfrak{M}}(\delta_i) = \nu^{\mathfrak{M}_1''}(\delta_i'')$, $i = 1, \ldots, k$, $\nu^{\mathfrak{M}}(\rho) = \nu^{\mathfrak{M}_0'}(\rho')$.

5. Для любых $i = 1, \ldots, k$, $l = 1, \ldots, n$ C есть взаимно однозначное соответствие между $\nu^{\mathfrak{M}_1''}(\delta_i'')$ и $\nu^{\mathfrak{M}_l''}(\delta_i'')$; C есть взаимно однозначное соответствие между $\nu^{\mathfrak{M}_0'}(\delta_l')$ и $\nu^{\mathfrak{M}_l''}(\rho'')$.

Из указанного описания модели $\mathfrak{M}$ ясно, как можно построить искомое предложение Φ_h, которое и будет спектрально представлять h. □

Лемма 3. *Если n-местная функция h и $(n+2)$-местная функция g спектрально представимы, то и функция $f = R^{n+1}(h, g)$, полученная из h и g примитивной рекурсией, также спектрально представима.*

Пусть предложение Φ_h сигнатуры σ_0 спектрально представляет h, а предложение Φ_g сигнатуры σ_1 спектрально представляет g. Как и в предыдущей лемме, будем скорее описывать модели $\mathfrak{M}$ предложения Φ_f, чем само предложение Φ_f. Полагаем $\sigma_f = \langle \delta_1, \ldots, \delta_n, \delta_{n+1}, \rho\rangle \cup \cup \sigma_0' \cup \sigma_1'' \cup \langle \leqslant^2, \Pi^2, C^2\rangle$.

Модель $\mathfrak{M}$ удовлетворит следующим свойствам:

1. Предикат П расслаивает M над $D \subseteq M$.

2. Предикат $\leqslant$ линейно упорядочивает D так, что любой не наибольший элемент $x \in D$ имеет непосредственного последователя x'; D имеет наименьший элемент 0 и наибольший элемент m.

3. $\nu^{\mathfrak{M}}(\delta_{n+1}) = D\setminus\{0\}$; $\nu^{\mathfrak{M}}(\delta_i) = \nu^{\mathfrak{M}'_0}(\delta'_i)$, $i = 1, \ldots, n$.

4. $\mathfrak{M}'_0 \models \Phi'_h$; $\mathfrak{M}''_x \models \Phi''_g$, $x \in D\setminus\{0\}$.

5. Для любых $x, y \in D\setminus\{0\}$ C есть взаимно однозначное соответствие между $\nu^{\mathfrak{M}''_x}(\delta''_i)$ и $\nu^{\mathfrak{M}''_y}(\delta''_i)$, $i = 1, \ldots, n$; C есть взаимно однозначное соответствие между $\nu^{\mathfrak{M}'_0}(\delta'_i)$ и $\nu^{\mathfrak{M}''_x}(\delta''_i)$, $i = 1, \ldots, n$.

6. Для любого $x \in \nu^{\mathfrak{M}}(\delta_{n+1})$ C есть взаимно однозначное соответствие между $\hat{x} = \{y \mid y \in \nu^{\mathfrak{M}}(\delta_{n+1}),\ y < x\}$ и $\nu^{\mathfrak{M}''_x}(\delta''_{n+1})$.

7. Если $x \in \nu^{\mathfrak{M}}(\delta_{n+1})$ не наибольший в D и x' — его непосредственный последователь, то C есть взаимно однозначное соответствие между $\nu^{\mathfrak{M}''_x}(\rho'')$ и $\nu^{\mathfrak{M}''_{x'}}(\delta''_{n+2})$.

8. Если $D \neq \{0\}$ и $0'$ — непосредственный последователь 0, то C есть взаимно однозначное соответствие между $\nu^{\mathfrak{M}'_0}(\rho')$ и $\nu^{\mathfrak{M}''_{0'}}(\delta''_{n+2})$.

9. $\nu^{\mathfrak{M}}(\rho) = \nu^{\mathfrak{M}''_m}(\rho'')$, если $0 \neq m$, и $\nu^{\mathfrak{M}}(\rho) = \nu^{\mathfrak{M}'_0}(\rho')$, если $m = 0$.

Из указанного описания модели $\mathfrak{M}$ ясно, как построить искомое предложение Φ_f, которое, как нетрудно проверить, и будет спектрально представлять f. □

Лемма 4. *Если $(n+1)$-местная функция f спектрально представима, то и функция $g = M^n(f)$, полученная минимизацией из f, также спектрально представима.*

Пусть предложение Φ_f сигнатуры σ_f спектрально представляет f; полагаем $\sigma_g = \langle\delta_1, \ldots, \delta_n, \rho\rangle \cup \sigma'_f \cup \langle\leqslant, \Pi, C\rangle$.

Как и выше, опишем свойства произвольной модели $\mathfrak{M}$, на которой истинно предложение Φ_g.

1. Предикат Π расслаивает M над $D \subseteq M$.

2. Предикат $\leqslant$ линейно упорядочивает D так, что D имеет наименьший элемент 0 и наибольший элемент m.

3. $\nu^{\mathfrak{M}}(\delta_i) = \nu^{\mathfrak{M}'_0}(\delta'_i)$, $i = 1, \ldots, n$; $\nu^{\mathfrak{M}}(\rho) = D\setminus\{0\}$.

4. $\mathfrak{M}'_x \models \Phi'_f$, $x \in D$.

5. Для любого $x \in D\setminus\{0\}$ C есть взаимно однозначное соответствие между $\nu^{\mathfrak{M}'_0}(\delta'_i)$ и $\nu^{\mathfrak{M}'_x}(\delta'_i)$, $i = 1, \ldots, n$.

6. Для любого $x \in D$ C есть взаимно однозначное соответствие между $\nu^{\mathfrak{M}_x}(\delta'_{n+1})$ и $\hat{x} = \{y \mid y \in D,\ y < x\}$.

7. Для любого $x \in D \setminus \{m\}$ имеем $\nu^{\mathfrak{M}_x}(\rho') \neq \varnothing$, $\nu^{\mathfrak{M}_m}(\rho') = \varnothing$.

По указанным свойствам модели $\mathfrak{M}$ нетрудно указать предложение Φ_g, описывающее эти свойства.

Без труда проверяется, что Φ_g спектрально представляет функцию g. □

Из лемм 1—4 непосредственно следует и теорема 12.

Непересекающиеся рекурсивно перечисленные множества R_0 и R_1 называются *рекурсивно неотделимыми*, если не существует рекурсивного множества P такого, что $R_0 \subseteq P$, $P \cap R_1 = \varnothing$.

Предложение 6. *Существует пара R_0, R_1 рекурсивно неотделимых множеств.*

В силу следствия 1 теоремы 38.8 существует двухместная частично рекурсивная функция f, универсальная для одноместных частично рекурсивных функций.

Рассмотрим одноместную функцию $f_0(x) = \mathrm{sg}(f(x, x))$; полагаем $R_0 = \{n \mid f_0(n) = 0\}$, $R_1 = \{n \mid f_0(n) = 1\}$. Множества R_0, R_1 не пересекаются и рекурсивно перечислимы. Предположим, что существует рекурсивное множество P такое, что $R_0 \subseteq P$, $P \cap R_1 = \varnothing$. Рассмотрим характеристическую функцию χ_P этого множества; она рекурсивна.

Пусть $n \in \omega$ таково, что $f(n, x) = \chi_P(x)$ для любого $x \in \omega$; рассмотрим вопрос о принадлежности числа n множеству P.

Предположим, что $n \in P$, тогда $\chi_P(n) = 1$, $f_0(n) = \mathrm{sg}\, f(n, n) = \mathrm{sg}\, \chi_P(n) = \mathrm{sg}\, 1 = 1$, и $n \in R_1$, следовательно, $n \in P \cap R_1$ и $P \cap R_1 \neq \varnothing$; это невозможно.

Предположим, что $n \notin P$, тогда $\chi_P(n) = 0$, $f_0(n) = \mathrm{sg}\, f(n, n) = \mathrm{sg}\, \chi_P(n) = 0$, $n \in R_0$, $n \in R_0 \setminus P$, и, следовательно, $R_0 \not\subseteq P$; это также невозможно.

Получили противоречие, исходя из предположения о существовании рекурсивного множества P такого, что $R_0 \subseteq P$, $P \cap R_1 = \varnothing$. Предложение доказано.

Теорема 13. *Элементарная теория класса Π_n^3 в языке с равенством наследственно неразрешима для любого $n \in \omega$.*

Пусть R_0, R_1 — рекурсивно перечислимые, рекурсивно неотделимые множества. Легко понять тогда, что $R_i \neq \varnothing$, $i = 0, 1$. По предложению 37.2 существуют одноместные рекурсивные функции f_0 и f_1 такие, что $R_i = \{m \mid$ существует $n \in \omega$, для которого $m = f_i(n)\}$, $i = 0, 1$. По теореме 12 существуют предложения Φ_{f_0}, Φ_{f_1}, спектрально представляющие f_0 и f_1 соответственно. Не уменьшая общности, можно считать, что Φ_{f_0} и Φ_{f_1} — предложения одной и той же сигнатуры $\sigma = \langle Q_0 = \delta_1, Q_1 = \rho, Q_2^1, \ldots, Q_n^1; P_0^2, \ldots, P_m^2\rangle$.

Полагаем

$$\Phi_0 = \Phi_{f_0} \bigwedge \forall x \neg \rho(x);$$

$$\Phi_1 = \Phi_{f_0} \bigwedge \exists x(\rho(x) \bigwedge \forall y\ (\rho(y) \to x \approx y));$$

$$\Phi_n = \Phi_{f_0} \bigwedge \exists x_1 \ldots \exists x_n \Bigg(\bigwedge_{1 \leqslant i < j \leqslant n} \neg (x_i \approx x_j) \bigwedge$$

$$\bigwedge \bigwedge_{i=1}^{n} \rho(x_i) \bigwedge \forall y \Bigg(\rho(y) \to \bigvee_{i=1}^{n} y \approx x_i \Bigg)\Bigg), \quad n > 1, \quad n \in \omega;$$

$$\Psi_0 = \Phi_{f_1} \bigwedge \forall x \neg \rho(x);$$

$$\Psi_1 = \Phi_{f_1} \bigwedge \exists x\ (\rho(x) \bigwedge \forall y\ (\rho(y) \to x \approx y));$$

$$\Psi_n = \Phi_{f_1} \bigwedge \exists x_1 \ldots \exists x_n \Bigg(\bigwedge_{1 \leqslant i < j \leqslant n} \neg (x_i \approx x_j) \bigwedge \bigwedge_{i=1}^{n} \rho(x_i) \bigwedge$$

$$\bigwedge \forall y\ (\rho(y) \to \bigvee_{i=1}^{n} y \approx x_i \Bigg)\Bigg), \quad n > 1, \quad n \in \omega.$$

Отметим, что для формулы Φ_n (Ψ_n) существует конечная модель тогда и только тогда, когда $n \in R_0$ ($n \in R_1$).

Обратимся к последовательности формул с равенством сигнатуры $\sigma^3 = \langle \Pi^3 \rangle$.

Полагаем $P_0(x) = \exists y \exists z \Pi(y, z, x)$. Рассмотрим формулы:

(1) $\forall x \forall y \forall z (\Pi(x, y, z) \to (\neg P_0(x) \bigwedge P_0(y)))$;

(2) $\exists x \forall y \forall z \neg \Pi(x, y, z)$;

(3) $\forall y \forall z (P_0(y) \bigwedge P_0(z) \to \exists x\ (\Pi(x, y, z) \bigwedge \forall u \forall v (\Pi(x, u, v) \to$
$\to (u \approx y \bigwedge v \approx z))))$;

(4) $\forall x_0 \forall x_1 \exists x \forall y \forall z ((\Pi(x, y, z) \to (\Pi(x_0, y, z) \bigvee \Pi(x_1, y, z))) \bigwedge$
$\bigwedge ((\Pi(x_0, y, z) \bigvee \Pi(x_1, y, z)) \to \Pi(x, y, z)))$.

Обозначим через Γ конъюнкцию формул (1)—(4). Пусть $\mathfrak{M}$ — модель для Γ, $M_0 = \{m \mid m \in M = |\mathfrak{M}|, \mathfrak{M} \models P_0(m)\}$. Каждый элемент $m \in M$ определяет двухместный предикат P_m над M_0 так: $P_m = \{\langle m_0, m_1\rangle \mid \langle m, m_0, m_1\rangle \in \nu^{\mathfrak{M}}(\Pi)\}$. Истинность формулы (2) в $\mathfrak{M}$ влечет, что среди предикатов $\{P_m | m \in M\}$ есть пустой; истинность (3) означает, что для любой пары $\langle m_0, m_1\rangle \in M_0^2$ существует предикат вида P_m такой, что $P_m = \{\langle m_0, m_1\rangle\}$; истинность (4) означает, что семейство предикатов P_m, $m \in M$, замкнуто относительно объединения. Отсюда следует, что семейство $\{P_m | m \in M\}$ содержит все конечные двухместные предикаты над M_0. Если рассмотреть семейство одноместных предикатов $\{P_{m_0, m_1} | m_0, m_1 \in M\}$, где $P_{m_0, m_1} = \{m \mid \langle m_0, m_1, m\rangle \in \nu^{\mathfrak{M}}(\Pi)\}$, то оно также содержит все конечные одноместные предикаты над M_0.

Зафиксируем последовательность различных переменных $u, v, u_0, v_0, \ldots, u_n, v_n, z_0, \ldots, z_m$ и для любой формулы Φ сигнатуры σ, не содержащей указанных переменных, определим формулу Φ^* сигнатуры σ^3 следующим индуктивным правилом:

$$(t_0 \approx t_1)^* = (t_0 \approx t_1);$$
$$(Q_i(t))^* = \Pi(u_i, v_i, t), \quad i = 0, \ldots, n;$$
$$(P_j(t_0, t_1))^* = \Pi(z_j, t_0, t_1), \quad j = 0, \ldots, m;$$
$$(\Phi \circ \Psi)^* = (\Phi^* \circ \Psi^*), \quad \circ \in \{\vee, \wedge, \to\};$$
$$(\neg \Phi)^* = \neg \Phi^*;$$
$$(\forall x \Phi)^* = \forall x (\Pi(u, v, x) \to \Phi^*);$$
$$(\exists x \Phi)^* = \exists x (\Pi(u, v, x) \wedge \Phi^*).$$

Определим теперь последовательность предложений Γ_n, $n \in \omega$, сигнатуры σ^3 так:

$$\Gamma_n = \Gamma \to (\exists u \exists v \exists u_0 \ldots \exists v_n \exists z_0 \ldots \exists z_m \exists x (\Pi(u, v, x) \wedge$$
$$\wedge \Psi_n^*) \to \exists u \exists v \exists u_0 \ldots \exists v_n \exists z_0 \ldots \exists z_m \exists x (\Pi(u, v, x) \wedge \Phi^*)).$$

Установим два следующих факта:

1. Если $n \in R_0$, то Γ_n — тождественно истинное предложение.

2. Если $n \in R_1$, то существует конечная модель $\mathfrak{M}$ такая, что $\mathfrak{M} \models \neg \Gamma_n$.

Пусть $n \in R_0$ и $\mathfrak{M}$ — произвольная модель сигнатуры σ^3.

Если $\mathfrak{M} \models \neg \Gamma$, то $\mathfrak{M} \models \Gamma_n$. Будем теперь предполагать, что $\mathfrak{M} \models \Gamma$. Рассмотрим два случая:

а) Множество $M_0 = \{m \mid m \in M = |\mathfrak{M}|,\ \mathfrak{M} \models P_0(m)\}$ бесконечно. Так как $n \in R_0$, то существует конечная модель $\mathfrak{M}_1$ сигнатуры σ такая, что $\mathfrak{M}_1 \models \Phi_{f_0}$ и $\left|\nu^{\mathfrak{M}_1}(\rho)\right| = n$. Модель $\mathfrak{M}_1$ можно выбрать такой, что $M_1 = |\mathfrak{M}_1| \subseteq M_0$. Пусть $\bar{u}, \bar{v}, \bar{u}_0, \ldots, \bar{v}_n, \bar{z}_0, \ldots, \bar{z}_m \in M$ таковы, что $P_{\bar{u},\bar{v}} = M_1$; $P_{\bar{u}_i,\bar{v}_i} = \nu^{\mathfrak{M}_1}(Q_i)$, $i = 0, \ldots, n$; $P_{\bar{z}_j} = \nu^{\mathfrak{M}_1}(P_j)$, $j = 0, \ldots, m$. Тогда, как нетрудно проверить, в $\mathfrak{M}$ будет истинна формула Φ_n^*, когда переменным $u, v, \ldots, z_m$ в качестве значений присвоить $\bar{u}, \bar{v}, \ldots, \bar{z}_m$ соответственно. Но тогда $\mathfrak{M} \models \exists u \ldots \exists z_m \Phi_n^*$ и $\mathfrak{M} \models \Gamma_n$.

б) Множество M_0 конечно. Покажем, что тогда $\mathfrak{M} \models \neg \exists u \ldots \exists z_m \exists x \left(\Pi(u, v, x) \wedge \Psi_n^*\right)$. Предположим противное, пусть $\bar{u}, \bar{v}, \ldots, \bar{z}_m \in M$ таковы, что $\mathfrak{M} \models \exists x \Pi(\bar{u}, \bar{v}, x) \wedge \Psi_n^*(\bar{u}, \bar{v}, \ldots, \bar{z}_m)$. Полагаем $M_1 = P_{\bar{u},\bar{v}}$; $\nu^{\mathfrak{M}_1}(Q_i) = P_{\bar{u}_i,\bar{v}_i} \cap$ $\cap M_1$, $i = 0, \ldots, n$; $\nu^{\mathfrak{M}_1}(P_j) = P_{\bar{z}_j} \cap M_1^2$, $j = 0, \ldots, m$; $\mathfrak{M}_1 =$ $= \left\langle M_1, \ldots, \nu^{\mathfrak{M}_1}(Q_i), \ldots, \nu^{\mathfrak{M}_1}(P_j), \ldots \right\rangle$ — конечная модель сигнатуры σ, причем такая, что $\mathfrak{M}_1 \models \Psi_n$, но это влечет $n \in R_1$, $n \in R_0 \cap R_1$, что невозможно. Итак, $\mathfrak{M} \models$ $\models \neg \exists u \ldots \exists z_m \exists x \left(\Pi(u, v, x) \wedge \Psi_n^*\right)$ и, следовательно, $\mathfrak{M} \models \Gamma_n$.

Пусть теперь $n \in R_1$. Тогда существует конечная модель $\mathfrak{M}_0$ сигнатуры σ такая, что $\mathfrak{M}_0 \models \Psi_n$. Полагаем $M = M_0 \cup P\left(M_0^2\right)$; $\Pi \subseteq M^3$ определится как множество $\{\langle P, m_0, m_1\rangle \mid P \subseteq M^2,\ \langle m_0, m_1\rangle \in P\}$. Легко проверить, что $\mathfrak{M} = \langle M, \Pi\rangle \models \Gamma$. Нетрудно выбрать $\bar{u}, \bar{v}, \bar{u}_0, \ldots, \bar{v}_n, \bar{z}_0, \ldots$ $\ldots, \bar{z}_m \in M$ такие, что $P_{\bar{u},\bar{v}} = M_0$; $P_{\bar{u}_i,\bar{v}_i} = \nu^{\mathfrak{M}_0}(Q_i)$, $i = 0, \ldots$ $\ldots, n$; $P_{\bar{z}_j} = \nu^{\mathfrak{M}_0}(P_j)$, $j = 0, \ldots, m$. Тогда $\mathfrak{M} \models \Psi_n^*(\bar{u}, \bar{v}, \ldots$ $\ldots, \bar{z}_m)$ и $\mathfrak{M} \models \exists u \ldots \exists z_m \exists x \left(\Pi(u, v, x) \wedge \Psi_n^*\right)$. Однако в $\mathfrak{M}$ будет истинно $\neg \exists u \ldots \exists z_m \exists x (\Pi(u, v, x) \wedge \Phi_n^*)$; это доказывается, как в случае б), рассмотренном выше. Следовательно, $\mathfrak{M} \models \neg \Gamma_n$.

З а м е ч а н и е. В построении модели $\mathfrak{M}$ выше можно как угодно расширить основное множество M, не меняя предиката Π. Поэтому установлено свойство, более сильное, чем свойство 2.

Если $n \in R_1$, то существует сколь угодно большая конечная модель $\mathfrak{M}$ такая, что $\mathfrak{M} \models \neg \Gamma_n$.

Завершим теперь доказательство теоремы. Предположим, что существует разрешимая теория $T \subseteq \mathrm{Th}(\Pi_n^3)$. Рассмотрим множество $R = \{k \mid \Gamma_k \in T\}$. Так как предложения Γ_k строятся эффективно по k, а T разрешима, то множество R является рекурсивным. Покажем, что $R_0 \subseteq R$ и $R \cap R_1 = \varnothing$. Пусть $k \in R_0$, тогда Γ_k тождественно истинно и принадлежит любой теории, следовательно, $\Gamma_k \in T$ и $k \in R$. Итак, $R_0 \subseteq R$. Пусть $k \in R_1$, тогда по замечанию найдется модель $\mathfrak{M} \in \Pi_n^3$ такая, что $\mathfrak{M} \models \neg \Gamma_k$, следовательно, $\Gamma_k \notin \mathrm{Th}(\Pi_n^3) \supseteq T$ и $k \notin R$. Отсюда $R_1 \cap R = \varnothing$. Однако существование рекурсивного множества R такого, что $R_0 \subseteq R$ и $R \cap R_1 = \varnothing$, противоречит рекурсивной неотделимости множеств R_0 и R_1. Это противоречие и доказывает наследственную неразрешимость теории $\mathrm{Th}(\Pi_n^3)$. □

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Аксиома выбора 75
— исчисления 19
— регулярности 90
— экстенсиональности 65
Алгебраическая система 97
— — насыщенная 189
— — однородная 187
— — универсальная 189
Алгебраические системы изоморфные 98
— — элементарно эквивалентные 152
Алгоритм 12, 241

Булева алгебра 73
— — атомная 316

Вполне упорядоченное множество 74
Вывод в $ИВ_1$ 53
— — $ИП^{\Sigma}_1$ 143

Гомоморфизм 98
График 18
— частично рекурсивной функции 270

Декартово произведение 66
— — алгебраических систем 113
Диаграмма алгебраической системы 159
— — — полная 159
Дизъюнктивная нормальная форма (д. н. ф.) 40, 132
Дизъюнкция 22
— элементарная 39
Доказательство 12
— в ИВ в виде дерева 28
— — — линейное 27
— — $ИП^{\Sigma}$ в виде дерева 121
— — — линейное 121

Изоморфизм алгебраических систем 98
— — — частичный 152
— — — — конечный 152
Импликация 22
Истинность формулы на алгебраической системе при интерпретации 107
Исчисление 19
— высказываний (ИВ) 22
— — гильбертовского типа ($ИВ_1$) 52
— независимое 50
— непротиворечивое 43
— — по отношению к семантике 50
— предикатов сигнатуры Σ ($ИП^{\Sigma}$) 119
— — — — гильбертовского типа ($ИП^{\Sigma}_1$) 142
— разрешимое 50, 281
— резольвент 236

Кардинал 86
Квазивывод секвенции в ИВ 31
— — — $ИП^{\Sigma}$ 121
Квазимногообразие 166
Квазитождество 166
Квантор всеобщности 105
Квантор существования 105
Класс 114
— алгебраических систем аксиоматизируемый 161
— — — категоричный в мощности 194
Консервативное расширение исчисления 56
Конъюнктивная нормальная форма (к. н. ф.) 40
Конъюнкция 33
— элементарная 40
Кортеж 18, 66

Линейно упорядоченное множество 70
Линейный порядок 70

Машина Тьюринга 242, 248
Машинное слово 248
Многообразие 166
Множества подобные 76
— равномощные 83
Множество 15
— бесконечное 87
— конечное 16, 87
— натуральных чисел 65
— рекурсивно перечислимое 274
— рекурсивное 274
— счетное 87
— транзитивное 84
— формул выполнимое 117
— — локально выполнимое 117
— — непротиворечивое 135
— центрированное 79
Множество-степень 20
Мощность алгебраической системы 97
— множества 87
— сигнатуры 97

Натуральное число 65
Нормальный алгорифм 242, 244
— —, вычисляющий функцию 247
Носитель алгебраической системы 97
Нумерация гёделевская 281

Обеднение алгебраической системы 100
Область действия вхождения квантора 106
— значений функции 68
— определения операции 18
— — функции 68
Обогащение алгебраической системы 99
Оператор минимизации 253
— примитивной рекурсии 253
— регулярной суперпозиции 252
Ординал 84
Отношение 66
— антисимметричное 67
— обратное 67
— рефлексивное 67
— симметричное 67
— транзитивное 67
Отображение 18, 68
— в 68
— на 68
— разнозначное 68

Пара 18

Парадокс лжеца 14
— Рассела 9
Переменная 103
— пропозициональная 22
Подсистема алгебраической системы 98
— — —, порожденная множеством 99
— — — элементарная 156
Порядок плотный 101
Посылка правила 19
Правило вывода 12, 19
— —, допустимое в ИВ 30
— — независимое в исчислении 50
Предикат 66
— рекурсивно перечислимый 269
— рекурсивный 259
— универсальный 278
Предложение 108
— n-общезначимое 109
Пренексная нормальная форма 132
Приведенная нормальная форма 134
Принцип максимума 75
— нормализации 246
— полного упорядочения 75
— трансфинитной индукции 74
Проблема разрешимости исчисления 50
Произведение отношений 67

Расширение исчисления консервативное 56
Рекурсия кусочно возвратная 285
Решетка 71

Свободная переменная формулы 106
Связка логическая 22
Секвенция 19
— ИПЧ 147
— ИП $^{\Sigma}$ 119
— исчисления G 204
— — G_0 60
Сигнатура 96
Система аксиом для теории 169
— — Цермело — Френкеля 92
Скулемизация алгебраической системы 171
— теории 171
Слово абстрактное 17
— машинное 248
Совершенная д. н. ф. 41
— к. н. ф. 41

Тезис Тьюринга 251
— Чёрча 254
Теорема 12
— Гёделя о неполноте 293
— — — полноте 139
— интерполяционная Крейга — Линдона 179
— Кантора 83
— Кантора — Бернштейна 83
— компактности 117, 142
— Лося 116
— о графике 270
— — дедукции 54, 144
— — замене 35, 130
— — подстановке 33
— — полноте ИВ 49
— — редукции 277
— — существовании модели 136
Теорема о функциональной полноте ИВ 47
— об опускании типов 178
— — устранении сечения 214
— Рыль-Нардзевского 194
— Эрбрана 232
Теория 169
— аксиоматизируемая 292
— алгебраической системы 152
— категоричная в мощности 194
— класса алгебраических систем 152
— модельно полная 169
— наследственно неразрешимая 318
— полная 169
— с элиминацией кванторов 170, 297
— универсально аксиоматизируемая 169
— элементарная 169
Терм 103
— базисный 173
— рекурсивный 267
Тождество 166

Ультрафильтр булевой алгебры 80
Упорядоченный набор 66
Условие несмешанности переменных 204

Фильтр булевой алгебры 79
— главный 81
— на множестве 79
— Фреше 79
Формула 19, 22, 105, 119
— атомарная 22, 105
— атомная 105
—, выполнимая в алгебраической системе 109
— замкнутая 108
— ИВ 22
— —, тождественно истинная 45
— — элементарная 22
— ИПЧ 147
— ИП $^{\Sigma}$ 119
— исчисления резольвент 237
— — G 204
— общезначимая 108
— позитивно примитивная 303
— положительная 183
— рекурсивная 267
— рекурсивно перечислимая 269
— тождественно истинная 108
— условно фильтрующаяся 115
— фильтрующаяся 115
Формулы конгруэнтные 131
— пропозиционально эквивалентные 129
— эквивалентные 34, 129, 144
Функция 68
— базисная 253
— рекурсивная 253
— спектрально представимая 326
— универсальная 279
— характеристическая 259
— частичная 246
— — вычислимая 246
— — — по Тьюрингу 249
— — нормально вычислимая 247
— частично рекурсивная 253
Частично упорядоченное множество 70
— — — фундированное 73
Частичный порядок 70