

СПРАВОЧНАЯ КНИГА ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ

В ЧЕТЫРЕХ ЧАСТЯХ

ПОД РЕДАКЦИЕЙ
ДЖ. БАРВАЙСА

Часть III

ТЕОРИЯ РЕКУРСИИ

ПЕРЕВОД С АНГЛИЙСКОГО

С. Г. Дворникова

И. А. Лаврова

ПОД РЕДАКЦИЕЙ

Ю. Л. Ершова

Принято 89

МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1982

51

22.12

С 74

УДК 012.8

HANDBOOK OF MATHEMATICAL LOGIC

J. BARWISE (ED.)

North-Holland
Publishing Company
Amsterdam. New York. Oxford

1977

Справочная книга по математической логике: В 4-х частях/Под ред. Дж. Барвайса.— Ч. III. Теория рекурсии: Пер. с англ.— М.: Наука. Главная редакция физико-математической литературы, 1982. — 360 с.

© North-Holland
Publishing Company—1977

© Перевод на русский язык.
Издательство «Наука»
Главная редакция
физико-математической
литературы, 1982

1702020000 152
051 (02) 82 Полное

ПРЕДИСЛОВИЕ РЕДАКТОРА РУССКОГО ПЕРЕВОДА

Понятие алгоритма становится в настоящее время одним из важнейших понятий как теоретической, так и прикладной математики. Это связано в первую очередь с современным развитием электронной вычислительной техники и необходимостью создания мощного математического обеспечения для этой техники. Немаловажными являются и связи теории алгоритмов с математической логикой и основаниями математики; точное математическое определение понятия алгоритма впервые было найдено в рамках формальных систем математической логики. Теория рекурсии—так называется этот третий том «Справочной книги по математической логике» — составляет теоретическую основу современного учения об алгоритмах.

Первая вводная глава этого тома, написанная Эндертоном, довольно подробно и мотивированно знакомит читателя с тем разделом теории алгоритмов, который теперь называется «классической» теорией рекурсии.

Две следующие главы, написанные соответственно Девисом и Рабином, знакомят читателя с постановками различных алгоритмических проблем, возникающих в арифметике, алгебре, математической логике и других разделах математики. Наряду с формулировками проблем здесь имеются указания на методы решения таких проблем и даны примеры. Следует отметить, что обе эти главы не могут служить обзорами по рассматриваемой проблематике, так как отбор материала в этих главах отражает довольно субъективные взгляды авторов, не заботившихся, по-видимому, ни о достаточно полном обзоре результатов, ни о точности указаний на авторство приводимых утверждений. Советскому читателю, заинтересовавшемуся алгоритмическими проблемами, можно рекомендовать ознакомиться с обзорами Ершова, Лаврова, Тайманова и Тайцлина [1], Корина и Пинуса [1] и с книгой Ершова [1].

Четвертая глава, написанная Симпсоном, знакомит читателя с одним из наиболее развитых разделов собственной (внутренней) теории алгоритмов — теорией (тьюринговых) степеней неразрешимости. Обзор результатов довольно полон и хорошо написан. Для читателей, желающих познакомиться с результатами в других степенях неразрешимости (tt - и m -степенях), можно рекомендовать недавний обзор Одифредди [1].

571199

Остальные три главы этой части посвящены различным обобщениям классической теории рекурсии. Пятая глава, написанная Шором, является содержательным обзором по так называемой теории α -рекурсии. По этой главе можно хорошо познакомиться как с результатами, так и с идеями и методами этой теории. В шестой главе, написанной Кекрисом и Московакисом, излагается новый подход к изложению теории рекурсии по Клини для функционалов конечных типов, позволяющий более просто получить основные результаты этой трудной теории. Седьмая глава, написанная Ацелом, является введением в общую теорию индуктивных определений. Из заслуживших внимание специалистов обобщений теории рекурсии, не нашедших отражения в этой книге, можно указать еще рекурсию на допустимых множествах (познакомиться с понятием допустимого множества можно по седьмой главе первой части этого издания, изложение теории рекурсии на допустимых множествах можно найти в книге Барвайса [1]) и рекурсию на непрерывных функционалах (книга Нурмана [1] является первым монографическим изложением этой теории).

Приложение, написанное автором предисловия, содержит краткое введение в теорию нумераций, обсуждение ряда проблем теории конструктивных полей и полное изложение недавних результатов об алгоритмической природе элементарных теорий регулярно замкнутых полей.

ЛИТЕРАТУРА

- Барвайс (Barwise J.)
1. Admissible Sets and Structures. — Berlin; Göttingen; Heidelberg: Springer, 1976.
- Ершов Ю. Л.
1. Проблемы разрешимости и конструктивные модели. — М.: Наука, 1980.
- Ершов Ю. Л., Лавров И. А., Тайманов А. Д. и Тайцлин М. А.
1. Элементарные теории. — УМН, 1965, 20, № 4, с. 37—108.
- Кокорин А. И., Пинус А. Г.
1. Вопросы разрешимости расширенных теорий. — УМН, 1978, 33, № 2, с. 49—84.
- Нурман (Normann D.)
1. Recursion on the Countable Functionals. — Berlin; Heidelberg; N. Y.: Springer, 1980.
- Одифредди (Odifreddi P.)
1. Strong reducibilities. — Bull. Amer. Math. Soc. (N. S.), 1981, 4, № 1, с. 37—86.

Ю. Л. Ершов

ВВЕДЕНИЕ

Если говорить строго, теория рекурсии — наука, которая изучает класс рекурсивных или эффективно вычислимых функций и их применения в математике. При более широкой интерпретации теория рекурсии рассматривается как изучение общих процессов определения с помощью рекурсии, но не только на натуральных числах, а и на всех типах математических структур. Первые четыре главы этой книги подходят под более узкое определение, а последние три — под более широкое.

Класс рекурсивных функций определяется и изучается во вступительной главе, написанной Эндертоном. В этой главе обсуждаются доводы в пользу отождествления этого класса с «эффективно вычислимыми» функциями (тезис Чёрча). Здесь читатель знакомится с многими способами применения основных понятий.

Следующие три главы углубляются в темы, введенные в главе 1. Целью главы 2, написанной Мартином Девисом, является использование теории рекурсивных функций для доказательства того, что некоторые проблемы не могут быть эффективно решены — проблема слов для группы является одной из наиболее известных таких проблем. Родственная проблема о разрешимых (в противовес неразрешимым) теориях логики первого порядка обсуждается в главе 3, написанной Рабином.

Среди неразрешимых проблем некоторые более неразрешимы, чем другие. Определение «степени» неразрешимости вводится в § 8 главы 1, а обзор важных результатов об этих степенях дан в главе 4, написанной Симпсоном.

Переходя к более широкому пониманию теории рекурсии, мы приходим к написанной Шором главе 5 об обобщении теории рекурсии на допустимые ординалы. Шор дает прекрасное введение в основные понятия и, в качестве примера, показывает, какие новые обстоятельства возникают, когда на допустимые ординалы обобщается теорема о разложении. Эта глава содержит также очень полезную библиографию с аннотациями для изучения теории α -рекурсии.

Изучение рекурсии в высших типах по Клини (рекурсивные функции на функциях от функций, скажем, а не рекурсивные

функции на натуральных числах) всегда было более или менее недоступно всем, за исключением лишь узких специалистов, вследствие трудности основополагающих статей этого направления. Это положение должно улучшиться благодаря главе 6, написанной Кекрисом и Московакисом, где предлагается более простой подход, связанный с индуктивной определемостью.

Изучению индуктивных определений в целом посвящена глава 7, написанная Ацелом. Она должна быть интересна логикам всех убеждений, так как в ней комбинируется теоретико-рекурсивный подход с полезными приемами из теории моделей и теории доказательств.

Мы планировали включить и главу о более «практических» аспектах теории рекурсии, в которых появляются время выполнения программ и сложность вычисления, но эта глава не написана. Среди других глав данного справочника, имеющих отношение к теории рекурсии, хотелось бы выделить *) написанную Стетменом главу об исчислении равенств (глава 3 «Теории доказательств и конструктивной математики») и написанную Маккаи главу о допустимых множествах (глава 7 «Теории моделей»). Специалисту по теории рекурсии может быть интересно посмотреть применение теории рекурсии в теории доказательств в написанной Феферманом главе 4 «Теории доказательств и конструктивной математики».

Я. Московакис

*) Следует напомнить, что в английском оригинале эта часть содержала главу «Дескриптивная теория множеств: проективные множества», написанную Д. А. Мартином; при переводе эта глава перенесена во вторую часть. — *Прим. ред.*

ЭЛЕМЕНТЫ ТЕОРИИ РЕКУРСИИ

Герберт Б. Эндертон

СОДЕРЖАНИЕ

Введение	9
§ 1. Неформальная вычислимость	9
§ 2. Машины Тьюринга	12
§ 3. Тезис Чёрча	15
§ 4. Универсальные машины и нормальная форма	17
§ 5. Оракулы и функционалы	21
§ 6. Рекурсивная перечислимость	23
§ 7. Логика и теория рекурсии	28
§ 8. Степени неразрешимости	31
§ 9. Креативные и меньшие множества	35
§ 10. Определимость и рекурсия	37
§ 11. Рекурсивные аналоги классических объектов	44
Литература	48

Введение

В этой главе представлены элементы теории рекурсивных функций. Изложение не претендует на то, что оно подведет к самым границам исследований в этой области. Здесь сделана попытка лишь указать тот минимум, который будет нужен всякому, следующему по этому пути.

Доказательства в этой главе часто только намечены с указанием встречающихся главных идей. Имеется несколько книг, где эти темы изложены более подробно. Основным источником в этой области является книга Роджерса [1]. Более сжатое изложение можно найти в главах 6 и 7 книги Шенфилда [3]. Машины Тьюринга обсуждаются, в частности, в книгах Ясухари [1] и Девиса [1]. По степеням неразрешимости имеется довольно новая книга Шенфилда [4] и более старая книга Сакса [1]. Наконец, классическая книга Клини [5] содержит много материала по теории рекурсии.

§ 1. Неформальная вычислимость

Проще всего считать рекурсивные функции «эффективно вычислимыми» функциями. Вначале мы рассматриваем функции на натуральных числах в натуральные числа, откладывая на

дальнейшее рассмотрение функций на других множествах. Пусть $\mathbb{N}$ обозначает множество натуральных чисел $\{0, 1, 2, \dots\}$, а $\mathbb{N}^k$ — прямое произведение $\mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N}$ с k сомножителями. Объекты, которые мы хотим рассматривать, будут функциями с $\text{dom } f \subseteq \mathbb{N}^k$ для некоторого положительного числа k и $\text{ran } f \subseteq \mathbb{N}$. Такие объекты будут называться k -местными *частичными функциями*. Слово «частичная» напоминает, что область определения является, вообще говоря, подмножеством — возможно, собственным — множества $\mathbb{N}^k$. (Частичная функция называется *всюду определенной*, если ее область определения есть все $\mathbb{N}^k$.)

Из мощностных соображений ясно, что для каждого положительного k существует $2^{\aleph_0}$ k -местных функций. Из этого громадного количества мы хотим выбрать $\aleph_0$ функций, которые являются рекурсивными. Мы начинаем в этом параграфе с интуитивного описания искомых понятий, а в следующем параграфе мы обратимся к методам, которые сделают наши идеи точными.

Назовем k -местную частичную функцию f *эффективно вычислимой*, если существует эффективная процедура (т. е. алгоритм), которая правильно вычисляет f . Эффективная процедура должна удовлетворять следующим критериям:

(i) Для этой процедуры должны иметься точные инструкции (т. е. программа) конечной длины. Эти инструкции не должны предполагать никакой изобретательности или даже понимания со стороны человека или машины, которые следуют этим инструкциям. Исполнение инструкций должно состоять только в аккуратном следовании указаниям.

(ii) Если процедуре дан кортеж x длины k из $\text{dom } f$, то вычисление должно закончиться после конечного числа дискретных шагов и выдать $f(x)$.

(iii) Если процедуре дан кортеж x длины k , не принадлежащий $\text{dom } f$, то процедура может продолжать исполняться, никогда не останавливаясь, или же процедура может застрять в некоторой точке, которую нельзя истолковать как выдачу значения f на x .

Можно представить себе усердного и прилежного клерка, имеющего много бумаги и неутомимо следующего своим инструкциям, или же можно представить себе некоторый автоматизированный вариант — цифровую вычислительную машину, исполняющую какую-то программу.

Несмотря на то, что мы даем лишь приблизительное описание, а не математическое определение, уже можно развить только на этом неформальном уровне почти всю теорию рекурсивных функций. (Рекурсивные функции являются в точности эф-

фективно вычислимыми функциями, но мы сохраняем термин «рекурсивная» для математически определенного понятия.) Как реализуется эта возможность, читатель может увидеть в книге Роджерса [1].

В качестве примеров эффективно вычисляемых функций мы можем указать сложение и умножение натуральных чисел. Эффективные процедуры для этих функций (использующие их десятичные представления) изучаются в начальной школе. Любая функция с конечной областью определения эффективно вычислима. Инструкции для вычисления такой функции могут содержать список всех ее значений.

Существуют некоторые типы ограничений, идущие от практики, но которые мы не налагаем на эффективные процедуры.

(i) Хотя каждый аргумент, подаваемый на вход нашей процедуры, должен быть (конечным) натуральным числом, нет никакой заранее заданной границы на размеры этих аргументов. Например, мы не исключаем аргументы, которые превышают число электронов во вселенной.

(ii) Хотя процедура должна выдать $f(x)$, когда $x \in \text{dom } f$, после конечного числа шагов, нет никакой заранее заданной границы на это число.

(iii) Аналогично нет никакой заранее заданной границы на количество бумаги (пространство памяти), которая потребуется для выполнения процедуры. Даже умножение очень больших чисел может потребовать большого количества бумаги.

Все эти рассуждения относятся к сравнению эффективной вычислимости с «практической вычислимостью». Вычислитель, работающий на цифровой вычислительной машине, может считать функцию f вычислимой, только если $f(x)$ вычисляется на его машине в разумное время. Конечно, само понятие разумности может изменяться ото дня ко дню. А на следующий год он надеется получить более быструю машину с большим пространством памяти и лентой. К тому времени его идея, что считать практически вычислимым, значительно расширится.

Класс эффективно вычисляемых функций получается в идеале, когда все практические ограничения на требуемое время и пространство памяти снимаются. Поэтому наш класс функций — теоретический предел того, что будет рассматриваться вычислимым независимо от того, в каком веке это происходит.

Должно быть ясно, что если f и g — функции, которые совпадают на всех аргументах (за исключением, быть может, конечного числа), то f эффективно вычислима тогда и только тогда, когда g эффективно вычислима. Поэтому вопрос о том, будет ли какая-то функция эффективно вычислимой, целиком зависит от поведения этой функции в окрестностях бесконечности.

§ 2. Машины Тьюринга

Существует много эквивалентных способов формулировки определения рекурсивности. Формулировка, выраженная в терминах воображаемой вычислительной машины, была дана английским математиком Аланом Тьюрингом в его фундаментальной статье [1]. (Аналогичная работа была сделана одновременно, но независимо, Эмилем Постом из Нью-Йорка; см. Пост [1].) Главная трудность при нахождении этого определения была в том, что Тьюринг искал его до создания реальных цифровых вычислительных машин. На самом деле познание шло от абстрактного к конкретному: фон Нейман был знаком с работой Тьюринга, и сам Тьюринг позднее сыграл вдохновляющую роль в развитии вычислительных машин.

На неформальном уровне мы можем начать описывать машину Тьюринга как некий черный ящик с лентой. Лента разбита на ячейки и каждая ячейка может содержать пустой символ 0, либо непустой символ 1. Лента потенциально бесконечна в обе стороны в том смысле, что мы никогда не приходим к ее концу, но в любое время лишь конечное число ячеек может быть непустым. В начале лента содержит числа входа, в конце — числовых выходов. В промежуточное время лента используется как пространство памяти для вычисления.

Если мы откроем черный ящик, то обнаружим, что он устроен очень просто. В любой момент времени он может обозревать лишь одну ячейку памяти. Устройство содержит конечный список инструкций (или состояний) $q_0, q_1, \dots, q_n$. Каждая инструкция может указать два возможных направления действий; одного нужно придерживаться, если на обозреваемой ячейке ленты находится 0, а другого, — если там находится 1. В любом случае следующее действие может состоять из таких трех типов элементарных шагов:

(i) символ (возможно, такой же, как старый) пишется на обозреваемой ячейке ленты, при этом предыдущий символ стирается;

(ii) лента сдвигается на одну ячейку влево или вправо;

(iii) указывается следующая инструкция.

Таким образом, список инструкций определяет некоторую функцию перехода, которая по данной инструкции и обозреваемому символу указывает три компоненты того, что нужно делать. Мы можем формализовать эти идеи, взяв в качестве машины Тьюринга эту функцию перехода.

2.1. Определение. Машина Тьюринга — это функция M такая, что для некоторого натурального числа n

$$\begin{aligned} \text{dom } M &\subseteq \{0, 1, \dots, n\} \times \{0, 1\}, \\ \text{ran } M &\subseteq \{0, 1\} \times \{L, R\} \times \{0, 1, \dots, n\}. \end{aligned}$$

Например, пусть $M(3,1) = (0, L, 2)$. Подразумеваемый смысл этого состоит в том, что как только машина дойдет до инструкции q_3 , а на обозреваемой ячейке написан символ 1, она должна стереть 1 (оставляя на ячейке 0), передвинуть ленту так, чтобы обозреваемой ячейкой стала левая соседняя ячейка от той, которая обозревалась, и перейти к следующей инструкции q_2 . Если $M(3,1)$ не определено, то как только машина дойдет до инструкции q_3 , а на обозреваемой ячейке написан символ 1, то машина останавливается. (Это единственный путь остановки вычисления.)

Такая подразумеваемая интерпретация не включена в формальное определение машины Тьюринга, но она мотивирует и подсказывает формулировки всех следующих определений. В частности, можно определить, что означает для машины M передвижение (за один шаг) от одной конфигурации к другой. Нам не нужно здесь давать формальных определений, так как они являются простыми переводами наших неформальных идей.

Входные и выходные данные — это строки из 1, разделенные 0. Пусть $\ulcorner x \urcorner$ будет строкой из 1 длины $x + 1$. Тогда

$$\ulcorner x_1 \urcorner 0 \ulcorner x_2 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$$

получено комбинацией k строчек из 1, каждая отделена от другой 0.

Наконец, мы можем определить рекурсивность, k -местная частичная функция называется *рекурсивной*, если существует машина Тьюринга M такая, что как только M начинает с инструкции q_0 , обозревая самый левый символ строки

$$\ulcorner x_1 \urcorner 0 \ulcorner x_2 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$$

(вся остальная часть ленты пуста), тогда:

(i) если $f(x_1, \dots, x_k)$ определено, то M в конце концов остановится, обозревая самый левый символ строки

$$\ulcorner f(x_1, \dots, x_k) \urcorner,$$

при этом часть, находящаяся справа от этой строчки, пустая;

(ii) если $f(x_1, \dots, x_k)$ не определено, то M никогда не останавливается.

Если R — k -местный предикат на натуральных числах, то можем, что R *рекурсивен*, если его характеристическая функция $\chi_R: \mathbb{N}^k \rightarrow \{0, 1\}$ рекурсивна. (Предостережение: если k -местная частичная функция рекурсивна, то отсюда не следует, что ее график есть рекурсивный $(k+1)$ -местный предикат.)

Например, тождественная функция $f(x) = x$ рекурсивна, так как она вычисляется на пустой машине. Менее тривиальный случай — сложение $x + y$, которое вычисляется на машине, график которой указаны в таблице 1. Комментарии, расположен-

ные в таблице справа, даны в помощь читателю, а не машине. (Тьюринг определял M как некоторое множество пятерок вместо функции из пар в тройки. Наша таблица, являющаяся графиком M , по существу есть множество пятерок.)

ТАБЛИЦА 1

0 1	1 П 0	прохождение через x
0 0	1 П 1	заполнение промежутка
1 1	1 П 1	прохождение через y
1 0	0 Л 2	конец y
2 1	0 Л 3	стирание 1
3 1	0 Л 4	стирание другой 1
4 1	1 Л 4	движение назад
4 0	0 П 5	остановка

Хорошим упражнением в программировании является построение машин Тьюринга для произведения и возведения в степень.

Мы должны заметить, что многие детали нашего определения машины Тьюринга до некоторой степени произвольны. Если бы было более одной ленты, то класс вычислимых функций остался бы неизменным (хотя некоторые функции могли бы быть вычислены более быстро). Аналогично мы могли бы допускать больше символов, чем 0 и 1, или же у нас могла бы быть лента, бесконечная только в одну сторону от начальной точки вместо имеющейся бесконечной в обоих направлениях. Ни одно из этих изменений не затрагивает класса вычислимых функций. Что действительно существенно в определении — это разрешение произвольно большого количества материала для запоминающего устройства и произвольно длинных вычислений.

Мы можем дать специфический пример нерекурсивной функции, использующий «соревнование по трудолюбию» Радо [1]. Участник соревнования с n состояниями — это машина Тьюринга M с $n+1$ инструкцией $q_0, \dots, q_n$, последняя из которых используется только для остановки (т. е. $M(n, 0)$ и $M(n, 1)$ не определены), и такая, что, начиная работать на пустой ленте, M в конце концов остановится. Когда M останавливается, число единиц на ленте указывает количество очков M в этом соревновании. Таким образом, машина пытается написать как можно больше единиц на ленте, но обязана остановиться. Пусть $\Sigma(n)$ — максимально возможное число очков для участников соревнования с n состояниями.

2.2. Теорема (Радо [1]). *Функция Σ не рекурсивна. В действительности, для любой всюду определенной рекурсивной функции f на $\mathbb{N}$ мы имеем $f(x) < \Sigma(x)$ для всех достаточно больших x .*

Доказательство. Функция, значение которой для x равно

$$\max[f(2x+2), f(2x+3)],$$

рекурсивна и, значит, вычислима на некоторой машине M , имеющей, скажем, k инструкций. Для каждого x рассмотрим машину N_x , которая пишет « x » на пустой ленте и затем работает, как M . Тогда N_x является участником соревнования по трудолюбию с $x+k+2$ состояниями. Ее количество очков (число указанных выше единиц плюс еще 1) ограничено $\Sigma(x+k+2)$, что в свою очередь для всех $x \geq k$ ограничено $\Sigma(2x+2)$. $\square$

Позднее мы построим и другие нерекурсивные функции, но функция Σ поразительно проста. Несколько начальных значений Σ известны: $\Sigma(1)=1$, $\Sigma(2)=4$ и $\Sigma(3)=6$ (Лин и Радо [1]). Далее, $\Sigma(4)=13$ (Бреди [1], [2]). Далее известны лишь нижние оценки. $\Sigma(5) \geq 17$, $\Sigma(6) \geq 35$, $\Sigma(7) \geq 22961$ и $\Sigma(8) > 8 \times 10^{44}$ (Грин [1]).

§ 3. Тезис Чёрча

В § 1 обсуждалось неформальное понятие вычислимости. В § 2 определено математическое понятие рекурсивности. Равносильны ли эти понятия? Другими словами, является ли понятие рекурсивности правильной формализацией нашего интуитивного понятия эффективной вычислимости? Утверждение о том, что это в действительности так, известно как **тезис Чёрча**. Впервые такое утверждение было выдвинуто и аргументировано Чёрчем [1], [2] и принимается почти всеми.

Имеется два довода в пользу того, что класс рекурсивных функций достаточно широк, чтобы содержать все эффективно вычисляемые функции. Первый довод связан с конкретными процедурами. На проверку оказалось, что все процедуры, про которые чувствовалось, что они эффективны, могут быть проведены на машинах Тьюринга. Второй довод связан со всем классом эффективных процедур: различные попытки формализации понятия вычислимости приводят к понятиям, эквивалентным рекурсивности. В частности, естественные пути снятия некоторых ограничений в понятии рекурсивности (такие, как разрешение нескольких лент) в итоге приводят к понятиям, эквивалентным рекурсивности. (Доказательства таких результатов большей частью нетрудны, если известна техника, указанная в следующем параграфе.)

Исторически первое появление определения рекурсивности имеется в основополагающей статье Курта Гёделя [2] о неполноте формальных систем. Он называл предикат разрешимым (*entscheidungsdefinit*), если он бинумеруем в некоторой

формальной системе теории чисел. (Понятие бинумеруемости можно найти в главе I «Теории доказательств и конструктивной математики».) Это эквивалентно нашему определению рекурсивного предиката. Но в то время Гёдель не стремился к формализации концепции эффективной разрешимости или вычислимости и его внимание не было сосредоточено на этом. В той же статье он определил класс функций, назвав их рекурсивными (*rekursiv*); сейчас этот класс называется классом примитивно рекурсивных функций. Прилагательное «рекурсивный» было уместным, так как главной особенностью определения было указание, как находить $f(n+1)$ по $f(n)$.

Гёдель посещал Принстон несколько раз в тридцатые годы перед тем, как переехать туда в 1940 г. насовсем. В 1934 г. во время одного из этих визитов он прочел лекцию, mimeографические записи которой были распространены. Записки были составлены Клини и Россером, которые заканчивали в это время свои диссертации у Чёрча в Принстоне. (Эти записки были в дальнейшем опубликованы, см. Гёдель [2].) В этой лекции Гёдель поставил вопрос об эффективной вычислимости. Он заметил, что к рекурсивным функциям, определенным им ранее, нужно было бы добавить более общие формы рекурсии, чтобы этот класс включал все вычислимые функции. Затем он определил класс, который назвал «общерекурсивными функциями», используя идеи, которые высказал в письме к нему Эрбран. (Это определение, которое содержит формальные правила вывода некоторых равенств из других, также эквивалентно нашему определению рекурсивности.)

Чёрч жил в Принстоне с 1929 г. и вместе со своим учеником Клини выработал концепцию λ -определимых функций. Вопрос о соотношении между λ -определимостью и эффективной вычислимостью изучался Чёрчем. Чёрч [2] не только высказал тезис, носящий теперь его имя, но и привел также первый пример неразрешимой проблемы разрешимости. Эта проблема — будет ли формула в λ -исчислении иметь нормальную форму — может рассматриваться как некоторая проблема разрешимости в элементарной теории чисел. Доказательство эквивалентности понятия λ -определимых функций и понятия общерекурсивных функций было впервые дано Клини [2].

Тьюринг [1] ссылается на статью Чёрча и дает еще одно определение рекурсивности (по существу определение из § 2). Тьюринг независимо пришел к идее формализации понятия эффективной вычислимости, но решил опубликовать ее только после того, как статья Чёрча вышла в свет. В приложении Тьюринг доказал эквивалентность своего определения λ -определимости.

Пост [1] рассматривает тезис Чёрча не как определение или аксиому, а как нуждающийся в «постоянном подтвержде-

нии» закон природы, «фундаментальное открытие», характеризующее «математическую способность Homo Sapiens».

До сих пор основными объектами нашего изучения были функции, и мы мало упоминали k -местные предикаты на $\mathbb{N}$. В действительности теория рекурсии может быть развита с равнозначными результатами как в терминах функций, так и в терминах предикатов. Мы можем неформально называть предикат R разрешимым, если существует эффективная процедура, которая для любого данного x отвечает «да», если $x \in R$, и отвечает «нет», если $x \notin R$. (Имея дело с предикатами, мы пишем как $x \in R$, так и $R(x)$.) Тогда R разрешим тогда и только тогда, когда его характеристическая функция эффективно вычислима. По этой причине следствием тезиса Чёрча (а в действительности утверждением, ему эквивалентным) является то, что понятие рекурсивного предиката является правильной формализацией неформального понятия разрешимого предиката.

§ 4. Универсальные машины и нормальная форма

Первым использованием рекурсивных функций было доказательство логических теорем неполноты. Но для этого не требуется никаких глубоких результатов о внутренней структуре класса рекурсивных функций. В действительности было бы достаточно довольно ограниченного класса, такого, например, как класс примитивно рекурсивных функций, упомянутого в предыдущем параграфе.

Как будет видно, существуют и другие применения рекурсивных функций. Но даже и без этого рекурсивные функции изучались бы, так как они интересны сами по себе как эффективно вычислимые функции. И основной факт, который добавляет основания для такого изучения, есть возможность кодирования машин числами, которые можно использовать как вход для других (или той же самой) машин.

Здесь имеется прямая аналогия с реальными цифровыми машинами. Самые первые такие машины программировались с помощью установки переключателей и соединительных проводов на коммутационных досках. Далее было понято (фон Нейманом), что для подходяще устроенной машины программа может быть закодирована машинными словами (т. е. целыми числами) и запоминаться в машине точно так же, как исходные данные, — это будет машина с запоминающим устройством. Первая практическая польза такого подхода к программам — скорость, с которой новая программа может быть введена в машину вместо старой программы. Но наиболее замечательная выгода (для наших целей) — возможность исполнительных программ, например операционных систем. Исполнительная программа допускает в

521199

БИБЛИОТЕКА
КРАСНОЯРСКОГО УНИВЕРСИТЕТА

качестве своих входных данных другую программу. Такая исполнительная программа могла бы затем взять введенную в нее программу и проследить за выполнением ее инструкций.

Идеи машин с запоминающим устройством могут быть перенесены на машины Тьюринга (исторически все было наоборот). Машине Тьюринга M можно давать два числа на вход, одно из которых является подходящим кодом машины Тьюринга N , а другое — число x . Машина M тогда могла бы служить исполнительной программой, а на выходе будет находиться результат применения N к x . Такую машину можно назвать *универсальной машиной Тьюринга*.

Реализация этих идей и построение универсальной машины Тьюринга является прямолинейной, хотя и длинной процедурой. В самых общих чертах опишем, как это происходит. Прежде всего, каждая машина Тьюринга есть конечный объект и, следовательно, может быть закодирована натуральным числом с помощью некоторой фиксированной системы кодировки. Мы можем, например, определить кодирующую функцию

$$\langle x_0, x_1, \dots, x_n \rangle = 2^{x_0+1} \cdot 3^{x_1+1} \cdot \dots \cdot p_n^{x_n+1}$$

с помощью степеней простых чисел; таким путем мы заменяем конечную строчку чисел одним числом. Далее, нам нужна декодирующая функция $(x)_y$ со свойством: для $i \leq n$

$$(\langle x_0, x_1, \dots, x_n \rangle)_i = x_i.$$

Машины Тьюринга могут использоваться как для описанного выше кодирования, так и для декодирования.

На любом этапе вычисления машины Тьюринга точная конфигурация машины (запись на ленте, номер инструкции и обозреваемая ячейка) может быть описана при помощи конечного количества информации и, следовательно, снова может быть закодирована числом, называемым *мгновенным описанием*. Тогда *протоколом вычисления* для машины M будет число, кодирующее конечную последовательность мгновенных описаний, удовлетворяющих следующим условиям:

- (i) первое мгновенное описание имеет дело с инструкцией q_0 («начальное состояние»);
- (ii) последнее мгновенное описание имеет дело с инструкцией q_i и обозреваемым символом s , для которых $M(i, s)$ не определено («конфигурация остановки»);
- (iii) каждое мгновенное описание связано с последующим так, что при работе машины M конфигурация, заданная этим мгновенным описанием, переходит за один шаг в конфигурацию, заданную следующим.

Таким образом, протокол вычисления — натуральное число, которое кодирует все этапы одного из вычислений на M от начального состояния q_0 (предполагается, что на ленте записаны входные данные) до остановки.

Все это кодирование было бы бессмысленно, если бы не было выполнено следующее условие: в результате кодирования получаются *рекурсивные функции* и предикаты. Это значит, что, углубляясь в детали этого кодирования, можно проверить на каждом шаге, что существуют машины Тьюринга для вычисления соответствующих функций. Получаем следующие два результата.

(i) Существует трехместный рекурсивный предикат T , который выполняется на $e, \langle x_1, \dots, x_k \rangle$ и y тогда и только тогда, когда e кодирует некоторую машину Тьюринга, а y — протокол вычисления этой машины, начинающей работать, когда на ленте записано $\ulcorner x_1 \urcorner 0 \ulcorner x_2 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$.

(ii) Существует рекурсивная функция U такая, что как только выполняется $T(e, \langle x_1, \dots, x_k \rangle, y)$, то $U(y)$ — заключение протокола y — есть выходное значение вычисления (при условии, что конфигурация остановки такова, что все это имеет смысл).

Даже не вдаваясь в детали, должно быть ясно, что предикат T интуитивно разрешим, а функция U вычислима, так что можно предполагать, что они и рекурсивны, и это предположение правильно. Далее, для каждого k мы определяем k -местную частичную функцию

$$\{e\}^k(x_1, \dots, x_k) = U \text{ [наименьшее } y \text{ такое, что}$$

$$T(e, \langle x_1, \dots, x_k \rangle, y)].$$

Здесь мы пишем «наименьшее y », хотя вполне возможно, что такого y не существует; если такого y не существует, то функция не определена в данной точке. Мы будем все это записывать сокращенно с помощью символа μ :

$$\{e\}^k(x_1, \dots, x_k) = U(\mu y T(e, \langle x_1, \dots, x_k \rangle, y)).$$

(Обозначение $\{e\}^k$ введено Клини, Роджерс использует для этого обозначение $\varphi_e^{(k)}$. Верхний индекс k по возможности будет опускаться.)

Теперь мы можем сформулировать следующую фундаментальную теорему. Данная форма этой теоремы принадлежит Клини [1], [4], хотя универсальные машины Тьюринга встречались уже в исходной работе Тьюринга [1].

4.1. Теорема о нормальной форме. (i) $(k+1)$ -местная *частичная функция*, значение которой в точке $(e, x_1, \dots, x_k)$ равно $\{e\}^k(x_1, \dots, x_k)$, *рекурсивна*.

(ii) Для каждого e k -местная *частичная функция* $\{e\}^k$ *рекурсивна*.

(iii) Каждая k -местная частично рекурсивная функция равна $\{e\}^k$ для некоторого e .

Число e будет называться индексом функции $\{e\}^k$. Таким образом, частичная функция рекурсивна тогда и только тогда, когда она имеет некоторый индекс.

Теперь же мы хотим все сделанное использовать для доказательства неразрешимости проблемы остановки. Допустим, что мы даем x на вход машине M и запускаем ее в работу. После первого миллиона шагов у нас могло бы зародиться подозрение, что машина никогда не остановится. С другой стороны, может быть, что если мы проявим чуточку терпения, то машина остановится после еще небольшого числа шагов. Существует ли способ узнать, какая из этих двух ситуаций произойдет? Нет, такого способа не существует. Не существует эффективной процедуры, которая по данным M и x решала бы, будет данное вычисление закончено или нет. Это составляет содержание теоремы, приведенной ниже. Для частичной функции f мы пишем $f(x) < \infty$ для обозначения того, что $f(x)$ определено.

4.2. Теорема (неразрешимость проблемы остановки). Ни $\{(x, y): \{x\}(y) < \infty\}$, ни $\{x: \{x\}(x) < \infty\}$ не рекурсивны.

Доказательство. Наше описание данного доказательства (а также и других) опирается на неформальные идеи эффективной вычислимости, но оно может быть легко переведено в строгое рассуждение, использующее машины Тьюринга.

Пусть $K = \{x: \{x\}(x) < \infty\}$. Достаточно показать, что K — диагонализация проблемы остановки — не рекурсивно. Будет использоваться классическое диагональное рассуждение. Рассмотрим функцию

$$g(x) = \begin{cases} \{x\}(x) + 1, & \text{если } x \in K, \\ 0 & , \text{если } x \notin K. \end{cases}$$

Функция g всюду определена, но не может быть рекурсивной (потому что $g(e) \neq \{e\}(e)$ для каждого e). Но если бы K было рекурсивным, то и g была бы рекурсивной. Следовательно, K не рекурсивно. $\square$

В предыдущих параграфах мы совсем не интересовались вопросом о том, как долго работает машина Тьюринга, когда она вычисляет какое-то значение функции. Теперь допустим, что мы исследуем функцию $\Phi_e(x)$ — число шагов машины с индексом e , используемых при вычислении $\{e\}(x)$. Для любой рекурсивной функции у нас есть бесконечно много различных машин, ее вычисляющих. Некоторые рекурсивные функции настолько каверзны, что любой вычисляющей их машине требуется очень много времени.

4.3. Теорема (Рабин [1]). Для любой всюду определенной рекурсивной функции H на $\mathbb{N}$ можно найти всюду опреде-

ленную рекурсивную функцию $F: \mathbb{N} \rightarrow \{0, 1\}$ такую, что для каждого индекса e функции F

$$\Phi_e(x) > H(x)$$

для всех достаточно больших x .

Доказательство состоит в постоянном обнаружении индексов быстрых машин и определении F так, чтобы ее значение где-нибудь не совпадало с результатом таких машин.

Более сильным результатом является теорема об ускорении, которая утверждает, что некоторая функция не обязана иметь самый быстрый индекс или даже почти самый быстрый индекс при любом разумном понимании понятия «почти».

4.4. Теорема об ускорении (Блум [1]). Для любой всюду определенной рекурсивной функции G на $\mathbb{N} \times \mathbb{N}$ можно найти всюду определенную рекурсивную функцию $F: \mathbb{N} \rightarrow \{0, 1\}$ такую, что для каждого индекса i функции F существует другой индекс j функции F такой, что

$$G(x, \Phi_j(x)) < \Phi_i(x)$$

для всех достаточно больших x .

Например, возьмем $G(x, y) = 2^y$. Тогда для любой машины, вычисляющей F , существует другая машина, экспоненциально более быстрая для почти всех входов. Теоремы Рабина и Блума в действительности являются более общими, чем мы указали. В этих теоремах $\Phi_e(x)$ может быть любой разумной мерой сложности вычисления $\{e\}(x)$, удовлетворяющей очень слабым предположениям.

Для любой всюду определенной рекурсивной функции L на $\mathbb{N}$ можно определить класс сложности C_L функций, почти всюду вычисляемых за число шагов, ограниченное функцией L :

$$G_L = \{F: \text{для некоторого индекса } j \text{ функции } F$$

$$\Phi_j(x) \leq L(x) \text{ для всех достаточно больших } x\}.$$

Эти классы сложности расслаивают рекурсивные функции по трудности их вычисления. В частности, можно сказать, что F вычисляется не труднее, чем G , если F принадлежит каждому классу сложности, которому принадлежит G . Это случается тогда и только тогда, когда для каждого индекса функции G существует индекс функции F , который почти всюду вычисляет ее столь же быстро.

§ 5. Оракулы и функционалы

Через три года после своей основополагающей работы ([1]) Тьюринг [2] ввел обобщение своего понятия вычислимости. Вообразим некоторого вычислителя (прилежного клерка или

машину), обладающего, как обычно, точными инструкциями и достаточным количеством бумаги. Но дополнительно мы теперь рассматриваем и новую деталь: оракул для конкретной функции α из $\mathbb{N}$ в $\mathbb{N}$. (Здесь требуется, чтобы $\text{dom } \alpha$ равнялось всему $\mathbb{N}$; пусть $\mathbb{N}^{\mathbb{N}}$ обозначает множество всех таких функций.)

Оракулом для α является некое устройство, которое по данному числу x выдает значение $\alpha(x)$. Если α рекурсивна, то в качестве оракула для α можно взять машину Тьюринга. Более общо, можно представить себе оракул и для произвольной функции α . При помощи такого оракула наш вычислитель может теперь вычислять не только эффективно вычислимые частичные функции, но и (когда даны правильные инструкции) любую частичную функцию, которая «вычислима относительно α ».

На первый взгляд понятие вычислимости относительно α кажется довольно странным. Оно соединяет наиболее конструктивный подход к функциям (т. е. вычислимость) с наименее конструктивным (т. е. оракулом). Но, несмотря на такое парадоксальное положение, данная концепция оказывается ценной, и она привела в конечном счете (в 1950-х гг.) к понятию *рекурсивного функционала*, т. е. к рекурсивным функциям, допускающим в качестве аргументов элементы из $\mathbb{N}^{\mathbb{N}}$.

Вообще мы будем рассматривать (k, m) -местные частичные функции; областями определения таких функций являются подмножества пространства

$$\mathcal{N} = \mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N} \times \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}} \times \dots \times \mathbb{N}^{\mathbb{N}}$$

(с k сомножителями $\mathbb{N}$ и m сомножителями $\mathbb{N}^{\mathbb{N}}$), а областями значений — подмножества множества $\mathbb{N}$. До сих пор мы рассматривали только случай, когда пространство $\mathcal{N}$ счетно (т. е. $m = 0$). Далее мы для простоты обозначений часто будем ограничиваться случаем $k = m = 1$, подразумевая при этом, что все сказанное будет справедливо и в общем случае. Через $x, y, \dots$ будут обозначаться переменные, областью изменения которых является пространство $\mathcal{N}$.

Мы обобщаем наше понятие машин Тьюринга, допуская m оракулов. Теперь машина может писать число x на ленте, а оракул за один шаг будет заменять это число на $\alpha(x)$. Частичная функция f на $\mathcal{N}$ будет называться *рекурсивной*, если существует машина Тьюринга, вычисляющая f , как и раньше, но теперь функциональные аргументы f будут доставляться в виде оракулов.

Как и в § 4, возможно закодировать все этапы какого-либо вычисления в число y — протокол этого вычисления. Кроме этого, в y закодирована вся информация, доставляемая оракулом. Конечно, при любом завершающемся вычислении может быть

использована только конечная часть потенциально бесконечной мудрости оракулов. При любых разумных кодированиях вычислений, если y — протокол вычисления, то всякое значение $\alpha(i)$, доставленное вычислению оракулом, будет таково, что $i < y$. Определим для α из $\mathbb{N}^{\mathbb{N}}$ «производящую функцию» $\bar{\alpha}$ следующим образом:

$$\bar{\alpha}(y) = \langle \alpha(0), \alpha(1), \dots, \alpha(y-1) \rangle.$$

Таким образом, $\bar{\alpha}$ — снова функция из $\mathbb{N}^{\mathbb{N}}$ и $\bar{\alpha}(y)$ кодирует первые y значений α . (В частности, $\bar{\alpha}(0) = \langle \rangle = 1$ независимо от α .) Для протокола вычисления y число $\bar{\alpha}(y)$ кодирует все значения α , которые используются в вычислении, так как для $i < y$ значение $\alpha(i)$ может быть декодировано из $\bar{\alpha}(y)$; действительно, $\alpha(i) = (\bar{\alpha}(y))_i$. Это обстоятельство приводит к следующим двум результатам:

(i) Существует рекурсивный 4-местный предикат T , который выполняется на $e, \langle x_1, \dots, x_k \rangle, \langle \bar{\alpha}_1(y), \dots, \bar{\alpha}_m(y) \rangle$ и y тогда и только тогда, когда e кодирует машину Тьюринга, а y — протокол вычисления этой машины, когда на ленте записано $\ulcorner x_1 \urcorner 0 \ulcorner x_2 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$ и машина снабжена оракулами для $\alpha_1, \dots, \alpha_m$.

(ii) Существует рекурсивная функция U такая, что как только выполняется T на описанных выше четырех аргументах, то $U(y)$ — выходное значение вычисления.

Таким образом, мы можем обобщить результаты о нормальной форме из предыдущего параграфа, определяя (k, m) -местную частичную функцию $\{e\}^{k, m}$, где

$$\{e\}^{1, 1}(x, \alpha) = U(\mu y T(e, \langle x \rangle, \langle \bar{\alpha}(y) \rangle, y)).$$

Как обычно, мы опускаем, где это возможно, верхние индексы. Тогда, с необходимыми изменениями, справедлива теорема 4.1 о нормальной форме. Интересно отметить, что, так как U и T в качестве своих аргументов имеют лишь натуральные числа, рекурсивность на $\mathcal{N}$ может быть охарактеризована в терминах рекурсивности на $\mathbb{N}$.

§ 6. Рекурсивная перечислимость

Мы определили подмножество пространства $\mathcal{N}$ как рекурсивный (k, m) -местный предикат, если его характеристическая функция рекурсивна. По тезису Чёрча это является правильной формализацией неформального понятия разрешимого множества.

Теперь же мы хотим рассмотреть множества, являющиеся рекурсивными только наполовину. Назовем множество R *полуразрешимым*, если существует эффективная процедура, которая

для данного x отвечает «да» тогда и только тогда, когда $x \in R$. Мы больше не требуем, чтобы процедура была процедурой разрешимости, теперь мы рассматриваем ее как некоторую процедуру принятия. Если $x \in R$, то процедура в конце концов скажет «да», и тем самым она принимает x . Но если $x \notin R$, то, вообще говоря, процедура никогда не закончится. Но никто заранее не знает, будет ли процедура продолжаться все время или же в конце концов остановится и примет x .

Когда $\mathcal{N}$ — счетное пространство, мы можем дать другую характеристику полуразрешимых множеств. Назовем R *эффективно перечислимым*, если существует эффективная процедура, которая выписывает в некотором порядке элементы R . (Конечно, если R бесконечно, то такой список никогда не будет полным. Но любой конкретный элемент из R будет выписан через конечное время.) Чтобы доказать, что эффективная перечислимость эквивалентна полуразрешимости, вначале предположим, что R эффективно перечислимо. Тогда по любому данному x мы можем, рассматривая появляющийся список элементов R , сказать «да», если и когда мы увидим x . Это показывает, что R полуразрешимо. Обратно, предположим, что R полуразрешимо. Чтобы породить список элементов R , мы должны разумно распорядиться нашим временем. Упорядочим $\mathbb{N}^k$ сначала по максимальной компоненте, а потом — лексикографически; такой порядок на $\mathbb{N}^k$ имеет тип ω . Затем просматриваем все кортежи в этом порядке: $x_1, x_2, \dots$. На шаге n порождающей процедуры мы тратим n минут на каждое $x_1, \dots, x_n$, проверяя, не будет ли оно принято для R . Если в каком-либо случае мы получим «да», то помещаем этот кортеж в наш список. Таким путем любой элемент R будет в конце концов опознан и помещен в список. (Очевидно, что подобное доказательство опирается на счетность пространства $\mathbb{N}^k$: несчетные полуразрешимые множества не могут быть перечислены в этом смысле.)

Теперь мы хотим дать точный аналог неформального понятия полуразрешимого множества. Одна возможность состоит в возвращении к машинам Тьюринга — рассматривать их не как преобразователи (и со входом, и с выходом), а как принимающие устройства. Но имеется более простая альтернатива. Любое полуразрешимое множество является областью определения вычислимой частичной функции, принимающей значение 0 на этом множестве и не определенной вне его. Однако область определения любой вычислимой частичной функции является полуразрешимым множеством; надо говорить «да», если и когда вычисление заканчивается. По этой причине мы можем сформулировать понятие полуразрешимости следующим образом.

6.1. Определение. Подмножество пространства $\mathcal{N}$ *полурекурсивно*, если оно является областью определения некоторой

рекурсивной частичной функции на $\mathcal{N}$. Если $\mathcal{N}$ счетно, то полурекурсивные множества называются *рекурсивно перечислимыми* (сокращенно р. п.).

Если R полурекурсивно и является областью определения функции f , то мы можем рассматривать машину Тьюринга, вычисляющую f , как принимающее устройство для R , у которого принятие интерпретируется остановкой. Термин «рекурсивно перечислимо» иногда используется в качестве синонима термина «полурекурсивно» без учета мощности $\mathcal{N}$, но мы употребляем этот термин лишь в случае счетного $\mathcal{N}$.

Если имеется одно принимающее устройство для R и другое для его дополнения (относительно $\mathcal{N}$), то эти два условия вместе решают вопрос о принадлежности к R . Следовательно, мы имеем следующий результат.

6.2. Теорема а. *Предикат рекурсивен тогда и только тогда, когда он и его дополнение полурекурсивны.*

Можно использовать нашу нумерацию частично рекурсивных функций для получения нумерации полурекурсивных множеств. Просто определим $W_e^{k,m}$ как область определения $\{e\}^{k,m}$. (Везде, где возможно, опускаем верхние индексы.) Тогда предикат R полурекурсивен тогда и только тогда, когда он есть W_e для некоторого e . Далее, $(k+1, m)$ -местный предикат

$$Q = \{(e, x) : x \in W_e\}$$

полурекурсивен (является областью определения функции, вычисляемой на универсальной машине Тьюринга). Полурекурсивный предикат Q «универсален» для (k, m) -местных полурекурсивных предикатов в том смысле, что предикат R полурекурсивен тогда и только тогда, когда он получается из Q при фиксировании параметра e .

6.3. Теорема а. *Следующие условия для (k, m) -местных предикатов эквивалентны:*

(i) R полурекурсивен.

(ii) Для некоторого рекурсивного $(k+1, m)$ -местного предиката Q имеем

$$R = \{x : \exists w Q(w, x)\}.$$

(iii) Для некоторого рекурсивного $(k+1, m)$ -местного предиката P имеем

$$R = \{x : \exists w_1 \dots w_l P(w_1, \dots, w_l, x)\}.$$

Доказательство. Имеем (i) $\rightarrow$ (ii), так как $x \in W_e \leftrightarrow \exists y T(e, \langle x \rangle, y)$. Утверждение (ii) $\rightarrow$ (iii) тривиально. Чтобы доказать (iii) $\rightarrow$ (i), используется кодирование последовательностей: $R = \text{dom } f$, где $f(x) = \mu w P(\langle w \rangle, \dots, \langle w \rangle, x)$. Для рекурсивного P частичная функция f также рекурсивна. $\square$

В § 4 мы показали, что множество

$$K = \{x: \{x\}(x) < \infty\}$$

не рекурсивно. Но K — рекурсивно перечислимое подмножество $\mathbb{N}$, так как

$$x \in K \leftrightarrow \exists y T(x, \langle x \rangle, y)$$

для рекурсивного предиката T . По этой причине мы заключаем, что дополнение $\bar{K}$ не является рекурсивно перечислимым.

Хотя K неразрешимо, в некотором смысле вопросы о принадлежности любому рекурсивно перечислимому подмножеству для $\mathbb{N}$ сводятся к аналогичным вопросам про K . Рассмотрим любое рекурсивно перечислимое подмножество W_e множества $\mathbb{N}$ и определим для каждого x функцию

$$f(t) = \{e\}(x).$$

Тогда $f(t)$ не зависит от t и в действительности f — пустая функция, если $x \notin W_e$. Но f всюду определена, если $x \in W_e$. Значит, f — частично рекурсивная функция, но, что более важно, мы можем рекурсивно найти индекс $\pi(e, x)$ для f . На неформальном уровне это ясно: описанное выше уравнение говорит, как вычислять f , и мы можем эффективно выписать это уравнение, если e и x даны. При формальном доказательстве мы используем теорему о параметризации, указанную ниже.

Если g — какая-то двуместная частично рекурсивная функция, то $g(8, y)$, как функция от y , конечно, рекурсивна. Более важно, что можно рекурсивно найти индекс для этой функции по индексу для g . Этот факт, утверждаемый в более общей постановке, составляет следующую теорему.

6.4. Теорема о параметризации. Для всех k и m существует всюду определенная рекурсивная одно-однозначная функция ρ такая, что всегда выполняется

$$\{e\}(x_1, \dots, x_n, y_1, \dots, y_k, \alpha_1, \dots, \alpha_m) = \{\rho(e, \langle x_1, \dots, x_n \rangle)\}(y_1, \dots, y_k, \alpha_1, \dots, \alpha_m).$$

Здесь $x_1, \dots, x_k$ рассматриваются как фиксированные параметры. Идея состоит в том, чтобы $\rho(e, v)$ кодировала инструкции для написания v слева от входных данных на ленте и затем выполняла инструкцию, закодированную числом e . (Теорема о параметризации по историческим причинам также известна как « S - m - n -теорема».)

Можно применить теорему о параметризации к функции

$$g(e, x, t) = \{e\}(x),$$

чтобы получить всюду определенную рекурсивную одно-однозначную функцию π такую, что $g(e, x, t) = \{\pi(e, x)\}(t)$ и,

следовательно,

$$x \in W_e \rightarrow \{\pi(e, x)\} \text{ всюду определена,}$$

$$x \notin W_e \rightarrow \{\pi(e, x)\} \text{ пустая,}$$

$$x \in W_e \leftrightarrow \pi(e, x) \in K.$$

Это сводит вопросы про W_e к вопросам про K . Помимо K , существуют и другие р. п. множества, для которых такое сведение существует. Наиболее очевидный пример: $\{\langle x, y \rangle: x \in W_y\}$.

Если A и B — подмножества $\mathbb{N}$, то говорим, что A *много-одно-сводимо* к B ($A \leq_m B$), если для некоторой всюду определенной рекурсивной f

$$x \in A \leftrightarrow f(x) \in B.$$

Назовем A *одно-одно-сводимым* к B ($A \leq_1 B$), если можно дополнительно потребовать, чтобы f являлась одно-однозначной функцией. Тогда любое р. п. подмножество $\mathbb{N}$ одно-одно-сводимо к K . Ясно также (по крайней мере на неформальном уровне), что если $A \leq_m B$ или $A \leq_1 B$ и B рекурсивно, то и A рекурсивно. То же верно, если слово рекурсивно заменить на «рекурсивно перечислимо».

Теорема о параметризации — стандартный прием при формализации сводимости одной проблемы разрешимости к другой. При таком сведении можно следующим образом доказывать, что какая-то проблема разрешимости неразрешима.

6.5. Теорема (Райс [1]). Пусть $\mathcal{E}$ — некоторое множество *одноместных частично рекурсивных функций*. Тогда множество $\{e: \{e\} \in \mathcal{E}\}$ *индексов элементов $\mathcal{E}$ рекурсивно тогда и только тогда, когда $\mathcal{E}$ пусто или содержит все одноместные частично рекурсивные функции.*

Доказательство. Часть $\leftarrow$ тривиальна. Предположим, что множество индексов

$$I = \{e: \{e\} \in \mathcal{E}\}$$

рекурсивно. Так как и предположения, и заключение теоремы симметричны относительно $\mathcal{E}$ и его дополнения, можно предполагать, что пустая функция $\emptyset$ не лежит в $\mathcal{E}$. Будем доказывать, что $\mathcal{E}$ — пустое множество, показав, что в противном случае мы могли бы свести вопросы о принадлежности к K к рекурсивному множеству I .

Поэтому предположим, вопреки нашим надеждам, что некоторая функция ψ лежит в $\mathcal{E}$. Идея состоит в приведении к положению, когда $x \in K \leftrightarrow g(x) \in I$, полагая $\{g(x)\}$ равным ψ или $\emptyset$ в зависимости от того, принадлежит x множеству K или нет. Неформально $g(x)$ кодирует инструкции для выполнения следующих действий: для данного y вычислить $\{x\}(x)$ и затем

$\psi(y)$. Формально $g(x) = \rho(e, \langle x \rangle)$, где

$$\{e\}(x, y) = U(\mu z [T(x, \langle x \rangle, (z)_0) \wedge T(q, \langle y \rangle, (z)_1)]),$$

а q — индекс ψ . Это дает нам $K \leq_1 I$, что противоречит тому, что I рекурсивно, а K нет. $\square$

Непосредственными следствиями теоремы Райса являются следующие отрицательные утверждения: множество индексов всюду определенных рекурсивных функций не рекурсивно; для любой фиксированной частично рекурсивной функции f на $\mathbb{N}$ множество ее индексов не рекурсивно (и, следовательно, бесконечно), множество $\{e: W_e \text{ конечно}\}$ не рекурсивно и т. д.

Более тонким следствием теоремы о параметризации является теорема о рекурсии, принадлежащая Клини [3].

6.6. Теорема о рекурсии. (i) Для любой всюду определенной рекурсивной функции $f: \mathbb{N} \rightarrow \mathbb{N}$ можно найти число e , для которого $\{e\} = \{f(e)\}$. (ii) Для любой частично рекурсивной функции g можно найти число e такое, что $\{e\}(x) = g(e, x)$ для всех x .

Доказательство очень похоже на то, которое дают нам «ссылающиеся на себя» предложения в теории чисел (например, теорема 2.2.1 в главе 1 «Теории доказательств и конструктивной математики»).

Доказательство. Утверждения (i) и (ii) эквивалентны. Чтобы доказать (i), получим по теореме о параметризации всюду определенную рекурсивную функцию γ такую, что $\{\gamma(x, y)\} = \{\{x\}(y)\}$ для любых x и y . Пусть r — индекс функции, значение которой в точке x равно $f(\gamma(x, x))$, и пусть $e = \gamma(r, r)$. Число e требуемое, так как

$$\{e\} = \{\gamma(r, r)\} = \{\{r\}(r)\} = \{f(\gamma(r, r))\} = \{f(e)\}.$$

Чтобы доказать (ii), вначале получим по теореме о параметризации всюду определенную рекурсивную функцию f такую, что $\{f(t)\}(x) = g(t, x)$. Тогда в силу (i) существует число e такое, что $\{e\}(x) = \{f(e)\}(x) = g(e, x)$. $\square$

Используя теорему о рекурсии, дадим короткое доказательство теоремы Райса. Предположим что $\{a\} \in \mathcal{C}$ и $\{b\} \notin \mathcal{C}$, и определим $f(x)$ равным b или a в зависимости от того, принадлежит x множеству I или нет. Число e с $\{e\} = \{f(e)\}$ не может существовать, и, следовательно, f не рекурсивна. Значит, и I не рекурсивно.

§ 7. Логика и теория рекурсии

Почему теория рекурсии является частью математической логики? Если бы логики не изобрели рекурсивных функций, то вычислители позднее все равно бы пришли к этому понятию. Но

то, что именно логики изобрели рекурсивные функции, не является простой исторической случайностью. Существуют определенные аспекты логики, которые неизбежно приводят к понятиям конструктивности и эффективности.

Основным понятием логики является понятие *доказательства*. Доказательство с абстрактной точки зрения — это ряд утверждений, которые без сомнения доказывают истинность заключения при данных истинных предположениях. Но, чтобы быть убежденным в истинности заключения, доказательство должно быть проверено другими. Поэтому должна существовать некая процедура, с помощью которой посторонний человек может проверить правильность доказательства, не имея при этом выдающихся способностей. Другими словами, должна быть возможность проверять правильность доказательств с помощью какой-то эффективной процедуры. Множество доказательств должно быть рекурсивным. Например, нельзя рассматривать любой ряд истинных предложений арифметики как доказательство последнего предложения, так как мы не можем для данного предложения арифметики эффективно сказать, будет ли оно истинным или нет, потому что множество истинных предложений арифметики не рекурсивно и даже не р. п. (§ 10).

Рассмотрим теперь множество всех теорем, т. е. доказуемых предложений. Предложение σ доказуемо тогда и только тогда, когда

$$\exists d [d \text{ — доказательство } \sigma].$$

Часть, заключенная в скобки, должна быть рекурсивной. Значит, множество теорем должно быть рекурсивно перечислимым. Итак, если предполагать, что можно эффективно распознавать правильные доказательства, то множество теорем обязано быть рекурсивно перечислимым! Теорема Гёделя о неполноте, обсуждаемая в главе 1 «Теории доказательств и конструктивной математики», вытекает из того, что доказуемость является рекурсивно перечислимым свойством, тогда как истинность таковым не является.

Чтобы быть более точным, рассмотрим некоторый язык L первого порядка такой, например, как язык теории множеств, имеющий конечное число нелогических символов. (В действительности можно брать и $\aleph_0$ нелогических символов, если их при этом аккуратно упорядочить.) Мы вначале некоторым естественным образом припишем числа (называемые *гёделевыми номерами*) выражениям языка. Это позволит нам использовать для этих выражений понятия теории рекурсии. (С тем же успехом мы могли бы использовать работу машин Тьюринга на символах языка.) В действительности мы не будем делать различия между выражениями и их гёделевыми номерами. Можно

проверить, что множество формул, как и множество предложений, рекурсивно. Теперь добавим множество A аксиом таких, например, как аксиомы теории множеств Цермело — Френкеля (ZF). Естественно, мы считаем, что A рекурсивно, и тогда при проверке правильности доказательства мы сможем эффективно отличать аксиомы от неаксиом. (К примеру, множество аксиом ZF рекурсивно.) Для рекурсивного множества A двуместное отношение

$$\{(\sigma, d): d \text{ — доказательство } \sigma \text{ из } A\}$$

рекурсивно, где доказательство понимается, как в § 4 главы I «Теории моделей» (на самом деле это относится к любой формальной системе из этой главы). Это не очень глубокий результат: мы интуитивно ждали, что понятие доказательства будет разрешимым, так что, когда все нужные концепции сделаны точными, не стоит удивляться, что данное понятие стало в действительности разрешимым. Назовем теорию *рекурсивно аксиоматизируемой*, если она задается описанным выше способом, с помощью рекурсивного множества аксиом A в языке L .

7.1. Теорема. *Всякая рекурсивно аксиоматизируемая теория имеет рекурсивно перечислимое множество теорем.*

Доказательство. τ — теорема тогда и только тогда, когда

$$\exists d [d \text{ — доказательство } \tau \text{ из } A],$$

где A — рекурсивное множество аксиом. Часть в скобках рекурсивна. $\square$

Возьмем снова пример теории множеств ZF. По теореме 7.1 множество теорем теории ZF р.п. Отсюда следует, что доказуемые в ZF арифметические предложения (это может быть уточнено) образуют р.п. множество. Следовательно, оно не может совпадать с множеством всех истинных арифметических предложений. Либо слишком многое является доказуемым (и теория ZF нас обманывает), либо слишком мало доказуемо.

Теперь пойдем еще дальше и предположим, что у нас есть рекурсивно аксиоматизируемая теория, которая *полна* (т. е. для любого предложения σ либо σ , либо $(\neg \sigma)$ является теоремой). Тогда можно усилить теорему 7.1: теория становится разрешимой.

7.2. Теорема. *Полная рекурсивно аксиоматизируемая теория имеет рекурсивное множество теорем.*

Доказательство. Утверждение конечно выполняется, если теория противоречива, так что предположим, что наша теория непротиворечива. Допустим, что нам дано предложение σ , и мы хотим узнать, является ли оно теоремой. Мы порождаем список всех теорем; по теореме 7.1 это возможно. В конце кон-

цов либо σ , либо $(\neg \sigma)$ встретятся в этом списке. Когда это случится, мы останавливаемся и даем правильный ответ. $\square$

Теорема 7.2 является основной при доказательстве многих результатов по разрешимости; см. главу 3. Конечно, некоторое неудобство доставляет ограничение, связанное с тем, что этот результат применяется лишь к полным теориям.

Собственно говоря, доказательства и вычисления являются объектами одной природы. Вычисление (написанное со всеми подробностями) является доказательством того, что значение функции при данном аргументе есть данное число. А всякое доказательство — это вычисление какого-то значения функции, область определения которой есть множество теорем. Это — вычисление в том смысле, что оно является конечной и проверяемой записью, сопровождающей работу правильной процедуры.

Например, множество чисел R рекурсивно тогда и только тогда, когда оно бинумеруемо в арифметике Пеано первого порядка (см. § 3). Здесь роль вычислений на машинах Тьюринга играют формальная дедукция, *modus ponens* и все, что привлекается для того, чтобы узнать, что данное число находится в нашем множестве.

Сами машины Тьюринга являются отличным инструментом решения многочисленных проблем о неразрешимости в логике. Одним из примеров является результат Кар, Мура и Вана [1] о том, что для любой формулы ϕ можно эффективно найти $\forall \exists \forall$ -формулу, которая выполнима тогда и только тогда, когда ϕ выполнима. Здесь доказательство не связано с разными синтаксическими манипуляциями с формулой ϕ , а для каждой машины Тьюринга M находится $\forall \exists \forall$ -формула, которая выполнима тогда и только тогда, когда M никогда не останавливается. А это вместе с результатом предыдущего параграфа дает существование нужной редукции.

Или предположим, что мы хотим доказать, что множество предложений, имеющих модели любой ненулевой мощности, неразрешимо. Можно сделать это, показав, как для данной машины Тьюринга M эффективно найти предложение, имеющее модели любой ненулевой мощности тогда и только тогда, когда M никогда не останавливается.

§ 8. Степени неразрешимости

Все нерекурсивные множества имеют неразрешимые проблемы разрешимости. Но некоторые из них более неразрешимы, чем другие. В этом параграфе мы покажем, как на неразрешимых проблемах можно ввести некоторый порядок.

Рассмотрим частичную функцию f на $\mathcal{N}$, и пусть $\mathcal{B}$ — некоторое подмножество из $\mathcal{N}^{\mathcal{N}}$. Возможно, что мы сумеем

вычислить f , если нам будут даны оракулы для всех функций из $\mathcal{B}$. Называем f *рекурсивной относительно $\mathcal{B}$* , если существует некоторая частично рекурсивная функция g и некоторые функции $\beta_1, \dots, \beta_n$ из $\mathcal{B}$ такие, что для всех x

$$f(x) = g(x, \beta_1, \dots, \beta_n).$$

Другие определения также могут быть «релятивизированы относительно $\mathcal{B}$ ». Например, подмножество из $\mathcal{N}$ рекурсивно относительно $\mathcal{B}$, если его характеристическая функция рекурсивна относительно $\mathcal{B}$; это подмножество *полурекурсивно относительно $\mathcal{B}$* , если оно есть область определения некоторой частичной функции, рекурсивной относительно $\mathcal{B}$. Обычно $\mathcal{B}$ является множеством $\{\beta\}$, состоящим из одной функции β , и тогда мы говорим о рекурсивности относительно β и т. п.

Экстремальный случай $\mathcal{B} = \mathcal{N}^{\mathcal{N}}$ требует специального рассмотрения. Когда даются оракулы для всех функций из $\mathcal{N}^{\mathcal{N}}$, содержание понятия рекурсивности размывается. При счетном пространстве $\mathcal{N}$ каждая функция рекурсивна относительно $\mathcal{N}^{\mathcal{N}}$. Но для несчетного $\mathcal{N}$ это не так. Если f рекурсивна относительно $\mathcal{N}^{\mathcal{N}}$, то вычисление $f(\alpha)$ существует, но с одним ограничением: можно использовать лишь конечное количество информации об α , т. е. должно существовать некоторое y (зависящее от α) такое, что $f(\alpha) = f(y)$ для любой γ , совпадающей с α на первых y значениях. Это в точности совпадает с определением непрерывной функции f , когда мы рассматриваем дискретную топологию на $\mathcal{N}$ и топологию произведения на $\mathcal{N}^{\mathcal{N}}$. Пространство $\mathcal{N}$ тогда также имеет топологию произведения.

8.1. Теорема а. (а) *Функция на $\mathcal{N}$ рекурсивна относительно $\mathcal{N}^{\mathcal{N}}$ тогда и только тогда, когда она непрерывна.*

(б) *Подмножество из $\mathcal{N}$ полурекурсивно относительно $\mathcal{N}^{\mathcal{N}}$ тогда и только тогда, когда оно открыто.*

Все несчетные пространства $\mathcal{N}$ гомеоморфны $\mathcal{N}^{\mathcal{N}}$. Например, гомеоморфизм из $\mathcal{N}^{\mathcal{N}} \times \mathcal{N}^{\mathcal{N}}$ на $\mathcal{N}^{\mathcal{N}}$ отображает (α, β) в функцию, принимающую на $2x$ значение $\alpha(x)$, а на $2x + 1$ значение $\beta(x)$. А $\mathcal{N}^{\mathcal{N}}$ гомеоморфно множеству иррациональных чисел — требуемое отображение осуществляется с помощью непрерывных дробей. Таким образом, возможно дать единообразную трактовку топологической теории множеств иррациональных чисел, с одной стороны, и теории рекурсии на $\mathcal{N}$ — с другой. Обе стороны выигрывают от такой связи. Дальнейшие рассмотрения в этом направлении имеются в главе 8 «Теории множеств» по дескриптивной теории множеств.

Но мы отклонились от нашей главной темы. Мы будем иметь дело со специальным случаем относительной рекурсивности.

Пусть α и β — элементы $\mathcal{N}^{\mathcal{N}}$. Тогда, согласно нашим предыдущим определениям, α рекурсивна относительно β в том и только в том случае, когда существует частично рекурсивная функция g , для которой

$$\alpha(x) = g(x, \beta).$$

(Хотя обе функции α и β всюду определены, мы не можем этого же требовать от функции g .) Если α рекурсивна относительно β , то мы пишем $\alpha \leq_T \beta$ и говорим, что α *сводится по Тьюрингу к β* . Можно также работать (по существу эквивалентным образом) с подмножествами множества $\mathcal{N}$: скажем, что A *рекурсивно в B* (пишем $A \leq_T B$), если характеристическая функция множества A рекурсивна относительно характеристической функции множества B .

8.2. Теорема а. *Двуместный предикат $\leq_T$ (и на $\mathcal{N}^{\mathcal{N}}$, и на $\mathcal{P}(\mathcal{N})$) рефлексивен и транзитивен.*

На неформальном уровне транзитивность $\leq_T$ соответствует последовательной работе машин.

Как следствие предыдущей теоремы симметричный предикат эквивалентности по Тьюрингу

$$\alpha \equiv_T \beta \text{ тогда и только тогда, когда } \alpha \leq_T \beta \text{ и } \beta \leq_T \alpha$$

является отношением эквивалентности на $\mathcal{N}^{\mathcal{N}}$. Пусть $[\alpha]$ — класс эквивалентности, содержащий α . Такие классы эквивалентности называются *степенями неразрешимости*. Степени частично упорядочены предикатом

$$[\alpha] \leq [\beta] \text{ тогда и только тогда, когда } \alpha \leq_T \beta.$$

(Ясно, что этот предикат корректно определен на классах эквивалентности.) На $\mathcal{P}(\mathcal{N})$ и на $\mathcal{N}^{\mathcal{N}}$ одни и те же структуры степеней, так как для любой α можно найти множество B , характеристическая функция которого эквивалентна по Тьюрингу α .

Итак, степени неразрешимости частично упорядочены согласно тому, насколько они неразрешимы. Очевидно, что существует наименьшая степень 0, содержащая все рекурсивные функции. Так как для любой фиксированной функции β множество $\{\alpha: \alpha \leq_T \beta\}$ счетно, то каждая степень состоит из счетного множества функций. Следовательно, существует $2^{\aleph_0}$ степеней. Другим следствием является следующее: наибольшая мощность цепи (любого линейно упорядоченного подмножества) степеней не больше $\aleph_1$. Это заставляет предположить, что существуют несравнимые степени. Такое предположение может быть строго доказано (без отрицания континуум-гипотезы). Мы можем одновременно строить α и β , некоторым образом обходя каждую машину, которая могла бы сводить одну функцию к другой.

Но в действительности верно много большее. Существует антицепь — множество степеней, никакие две из которых не сравнимы, — мощности $2^{\aleph_0}$. Этот результат — лишь небольшая часть обширной информации, известной о степенях. Многое из данной темы указано в главе 4.

Назовем степень *рекурсивно перечислимой* (р.п.), если она является степенью некоторого р.п. множества. Напомним, что множество

$$K = \{x: \{x\}(x) < \infty\}$$

— р.п., но не рекурсивное подмножество множества $\mathbb{N}$. Следовательно, степень K , обозначаемая через $0'$, есть р.п. степень, большая чем 0 . В § 9 будет изучен вопрос о том, существуют ли другие р.п. степени (проблема Поста).

Релятивизация перехода от $\emptyset$ к K приводит нас к функции $A \rightarrow A'$ на $\mathcal{P}(\mathbb{N})$. Определим скачок множества A (обозначаемый через A') как множество

$$\{x: \{x\}^A(x) < \infty\},$$

где $\{x\}^A$ — частично рекурсивная относительно A функция с индексом x , т. е.

$$\{x\}^A(y) = \{x\}(y, \chi_A),$$

где χ_A — характеристическая функция множества A . Тогда A' р.п. относительно A , но не рекурсивно относительно A — доказательство такое же, как и для K . В действительности, релятивизируя доказательство соответствующего результата для K , устанавливаем, что имеет место следующая

8.3. Теорема. (i) A' р.п. относительно A , но не рекурсивно относительно A .

(ii) B р.п. относительно A тогда и только тогда, когда $B \leq_1 A'$.

Таким образом, среди множеств, которые р.п. относительно A , скачок A' занимает самый высокий уровень относительно одно-односводимости. Как следует из упомянутой выше теоремы, операция скачка корректно определена на степенях.

8.4. Теорема. $A \leq_T B$ тогда и только тогда, когда $A' \leq_1 B'$.

Это позволяет нам определить для каждой степени a ее скачок a' . По теореме 8.3 имеем $a < a'$, и мы можем продолжать: $a < a' < a'' < \dots$. В частности, не существует наибольшей степени. Итак, выше любой степени можно найти цепь порядкового типа ω . В действительности можно найти цепь, порядковый тип которой — первый несчетный ординал; на предельных ординальных шагах мы собираем вместе некоторым систематическим образом все предыдущие множества.

§ 9. Креативные и меньшие множества

Как отмечалось в § 7, любая рекурсивно аксиоматизируемая теория имеет р.п. множество теорем. Таким образом, р.п. множества имеют особое значение для логики. Например, можно надеяться, что с помощью классификации р.п. множеств можно получить интересную классификацию аксиоматизируемых теорий. Так, разбиение р.п. множеств на рекурсивные и нерекурсивные множества приводит к разбиению теорий на разрешимые и неразрешимые. Но можно надеяться и на уточнение такого разбиения.

Первая рассматриваемая классификация идет от степеней неразрешимости. Далее можно исследовать уточнения, которые появляются из других видов сводимости. Ясно, что

$$A \leq_1 B \Rightarrow A \leq_m B \Rightarrow A \leq_T B,$$

и когда мы определяем

$$A \equiv_1 B \text{ тогда и только тогда, когда } A \leq_1 B \text{ \& } B \leq_1 A,$$

$$A \equiv_m B \text{ тогда и только тогда, когда } A \leq_m B \text{ \& } B \leq_m A,$$

отношение эквивалентности $\equiv_T$ уточняется с помощью $\equiv_m$ и далее с помощью $\equiv_1$. В § 6 показано, что существует наибольшая р.п. степень (степень множества K) относительно каждой из этих сводимостей.

Но что можно сказать о других р.п. степенях? Каждая такая степень содержит аксиоматизируемые теории.

9.1. Теорема (Фефферман [1]). *Каждая р.п. степень неразрешимости содержит рекурсивно аксиоматизируемую теорию.*

Доказательство. Для каждого числового множества A можно образовать теорию в языке с равенством, взяв в качестве аксиом множество

$$\{\neg e_n: n \in A\},$$

где e_n — предложение «существует ровно n предметов в универсуме». Тогда множество теорем будет эквивалентно по Гюрингу множеству A . Если A р.п., то, конечно, и множество аксиом р.п. Но любая теория, аксиомы которой могут быть рекурсивно перечислимы $\{\sigma_0, \sigma_1, \sigma_2, \dots\}$, имеет и рекурсивное множество аксиом $\{\sigma_0, \sigma_0 \wedge \sigma_1, \sigma_0 \wedge \sigma_1 \wedge \sigma_2, \dots\}$. $\square$

Ханф [1] показал, что эта теорема может быть усилена так, чтобы теория была конечно аксиоматизируемой. Но эффект этой теоремы несколько уменьшается эмпирическим наблюдением, что все «естественные» р.п. теории имеют либо степень 0 , либо степень $0'$. Доказательство, что какая-то теория T неразрешима, обычно состоит в сведении проблемы остановки машины Тьюринга к T , и сводимость, которая здесь применяется (или

может быть такой сделана), есть $\leq_1$; следовательно, такое доказательство показывает, что $K \leq_1 T$. Если T рекурсивно аксиоматизируема, то $T \equiv_1 K$.

В случаях $\equiv_1$ и $\equiv_m$ мы можем дать некоторую внутреннюю характеристику множеств, имеющих наивысшую р.п. степень. Теорема 6.2 утверждает, что р.п. множество A не рекурсивно тогда и только тогда, когда каждое р.п. подмножество его дополнения $\bar{A}$ не совпадает с $\bar{A}$. Эффективизируя это последнее условие, получаем следующее определение, введенное Постом [2].

9.2. Определение. Числовое множество A *креативно*, если A р.п. и существует частично рекурсивная функция f такая, что как только $W_x \subseteq \bar{A}$, то $f(x) \in \bar{A} - W_x$.

Функция f из этого определения называется *продуктивной функцией* для $\bar{A}$. Например, наше множество K креативно — можно взять $f(x) = x$.

9.3. Теорема (Майхилл [1]). Следующие условия для числовых множеств эквивалентны:

- (i) A креативно;
- (ii) A — р.п. множество, к которому $\leq_1$ сводятся все р.п. множества;
- (iii) A — р.п. множество, к которому $\leq_m$ сводятся все р.п. множества.

Тривиально, что (ii) $\rightarrow$ (iii), и нетрудно показать, что (iii) $\rightarrow$ (i). Основная часть состоит в доказательстве (i) $\rightarrow$ (ii). Оно разбивается на две части: в первой показывается, что креативное множество имеет всюду определенную одно-однозначную продуктивную функцию; во второй используется некоторый вариант теоремы о рекурсии.

Из этой теоремы следует, что обычные неразрешимые аксиоматизируемые теории такие, как арифметика Пеано первого порядка, имеют креативное множество теорем.

Имеется еще один вопрос: что (если есть) лежит между рекурсивными и креативными множествами? Для сводимостей $\leq_m$ и $\leq_1$ существование промежуточных множеств было доказано Постом [2]. Он заметил, что креативное множество должно иметь очень богатое дополнение, и предложил конструкцию множеств с бедными дополнениями. Назовем р.п. множество S *простым*, если $\bar{S}$ бесконечно, но не содержит ни одного бесконечного р.п. подмножества.

9.4. Теорема (Пост [2]). Простые множества существуют.

Доказательство. Вообразим некоторый фиксированный метод перечисления всех р.п. множеств. Для каждого n будем класть в S первое из встретившихся (если такое будет) чисел из W_n , которое больше, чем $2n$. Тогда S р.п., S пересекает ка-

ждое бесконечное р.п. множество, но S содержит самое большее n штук из первых $2n + 1$ чисел. □

Очевидно, что простое множество не рекурсивно. Также легко построить бесконечное р.п. множество в дополнении к любому креативному множеству; таким образом, простое множество не может быть креативным. Итак, последняя теорема устанавливает существование р.п. множеств промежуточных степеней относительно $\equiv_m$ и $\equiv_1$. «Проблема Поста» — это следующий вопрос: существуют ли р.п. множества, имеющие тьюрингову степень между 0 и $0'$? На этот вопрос нельзя ответить с помощью простых множеств: они могут иметь степень $0'$. Пост надеялся, что, накладывая еще более сильные требования на S , он сможет вынудить S иметь промежуточную степень неразрешимости. Этот подход оказался безуспешным*). Наконец в 1956 г. (через два года после смерти Поста) проблема была одновременно и независимо решена Фридбергом (в его дипломной работе в Гарварде и в статье: Фридберг [1]) и Мучником [1] в Советском Союзе. Они показали, что промежуточные р.п. степени действительно существуют и в большом количестве. Их метод доказательства был назван «методом приоритета». В широком смысле этот метод состоит в конструкции, при которой нужно удовлетворить бесконечно много требований. Но некоторые из этих требований конфликтуют с другими, по этой причине на различных шагах конструкции должны удовлетворяться требования высшего приоритета, причем мы допускаем, что требования более низкого приоритета будут нарушаться. Если все будет хорошо, то в конце каждое требование получит достаточно внимания, чтобы конструкция была успешной.

С 1956 г. р.п. степени широко изучаются. Мы приведем здесь только две теоремы, обе принадлежащие Сакусу [1], [2]. Р.п. степени плотны, т. е. если $a < c$, то $a < b < c$ для некоторой третьей р.п. степени b . Любой счетный частичный порядок может быть вложен в частичный порядок р.п. степеней. (Для этого достаточно вложить некоторую счетную безатомную булеву алгебру — как частичный порядок — в р.п. степени.)

§ 10. Определимость и рекурсия

Математика, как это всегда и было, в большей своей части является наукой об измерении. Но при этом «измерение» должно истолковываться не просто как измерение рулеткой. Род

*) Удачный пример успешного результата, связанного с данным подходом Поста, имеется в статье: Марченко С. С. Об одном классе неполных множеств. — Матем. заметки, 1976, 20, с. 473—478. — Прим. ред.

топологической фигуры измеряет один из ее аспектов, объекты нулевого рода в некотором смысле проще объектов более высокого рода. В математике существуют много единиц измерения и они имеют много имен: характеристика, степень трансцендентности, мощность, фундаментальная группа и т. д. Время от времени мы так преуспеваем в искусстве измерения, что можем полностью охарактеризовать какой-то объект (по крайней мере в рамках некоторого понятия изоморфизма), указывая, так сказать, его широту и долготу, т. е. его измерения в подходящих единицах.

Обычно измеряемые значения в конкретных единицах могут быть упорядочены или по крайней мере частично упорядочены. Это приводит тогда к упорядочению самих измеряемых объектов в зависимости от большего или меньшего значения измерения для данного объекта.

Теперь рассмотрим случай, когда измеряются множества натуральных чисел. Этот случай не так специален, как это могло показаться, так как он применяется ко всему, что может быть закодировано с помощью числовых множеств, как, например, формальные языки (множество строчек символов). Прежде всего, мы имеем двузначное измерение: числовое множество может быть рекурсивным или нерекурсивным. Например, множество простых чисел рекурсивно, а множества теорем теории множеств или теории групп, подходящим образом закодированные, не рекурсивны. Существует счетное число рекурсивных множеств; следовательно, почти все множества (при обычной мере на $\mathcal{P}(\mathbb{N})$) не рекурсивны.

Степени неразрешимости составляют одну из шкал измерений, указывающую, как далеко множество отстоит от того, чтобы быть рекурсивным. Но степени сами расположены не очень хорошо и лишь небольшое число хорошо видимых отметок помогает нам найти наше направление.

Шкалой измерений, которая изучается в этом параграфе, является определимость. Она применима в настоящем контексте к множествам, определяемым в системе $\mathcal{N} = \langle \mathbb{N}, 0, S, +, \cdot \rangle$ формулами логики первого или второго порядка. Для каждого натурального числа n пусть n будет соответствующей цифрой в формальном языке для $\mathcal{N}$. Скажем, что формула $\varphi(x)$ с одной свободной переменной x определяет A в $\mathcal{N}$, если для каждого n

$$n \in A \leftrightarrow \mathcal{N} \models \varphi(n)$$

(это понятие из главы 1 «Теории моделей»). Следовательно, A состоит в точности из тех чисел, которые делают φ истинной в $\mathcal{N}$. Для k -местного предиката используется формула $\varphi(x_1, \dots, x_k)$ с несколькими свободными переменными.

Очевидно, что лишь счетное число множеств определимо. С помощью диагонализации можно привести искусственный пример неопределимого множества. Однако среди $\aleph_0$ определимых множеств в $\mathcal{N}$ находятся наиболее интересные числовые множества. В конце концов, если мы интересуемся множеством A , то, возможно, мы знаем, что такое A , и, возможно, это знание можно формализовать и получить определение A в $\mathcal{N}$.

Если некоторое множество определимо в $\mathcal{N}$, то мы хотим иметь какую-то меру, указывающую, как оно определимо. Для начала, назовем множество *арифметическим*, если оно определимо в $\mathcal{N}$ с помощью формулы логики первого порядка, и *аналитическим*, если оно определимо с помощью формулы логики второго порядка. Арифметические множества составляют подкласс аналитических множеств, и в этом подклассе находятся множества, определяемые проще, чем множества, лежащие в дополнении этого подкласса.

Внутри класса арифметических (или аналитических) множеств можно интересоваться более тонкими мерами, которые указывают, как именно данное множество определено. Например, мы могли бы использовать в качестве меры длину самой короткой определяющей формулы или число кванторов. Но, чтобы получить какую-нибудь существенно важную меру, нужно проявить некоторую осторожность.

Например, возведение в степень (как трехместный предикат) определим в $\mathcal{N}$, но нелегко найти определяющую формулу, и всякая такая формула будет достаточно длинна. Даже наше решение о включении в $\mathcal{N}$ сложения и умножения и невключении возведения в степень было довольно произвольным. Мы хотим иметь меру, свободную от таких произвольных выборов. По этой причине мы решаем измерять «определимость по модулю рекурсивности». Имеется теорема, по существу принадлежащая Гёделю [1].

10.1. Теорема. *Каждый рекурсивный предикат на $\mathbb{N}$ является арифметическим.*

Доказательство использует технику § 4 по переводу утверждений о машинах Тьюринга в утверждения о числах. При этом необходимо иметь арифметический способ кодирования последовательности чисел в одно число. Китайская теорема об остатках дает такой метод.

Из этой теоремы далее следует, что р. п. предикаты на $\mathbb{N}$ также арифметические, так как определяющая формула для $\{x: \exists y R(x, y)\}$ требует только один дополнительный квантор по сравнению с определяющей формулой для R , и дополнения р. п. предикатов арифметические и т. д.

Перед тем как более систематически изучать «и т. д.», мы хотим заметить, что сейчас можно доказать неразрешимость

теории чисел. Пусть T — множество предложений, истинных в $\mathfrak{N}$, подходящим образом закодированных числами. Множество K арифметическое и для некоторой формулы φ имеем $x \in K \leftrightarrow \varphi(x) \in T$. Но отсюда следует, что $K \leq_1 T$ и, следовательно, T не может быть рекурсивным. Вскоре мы увидим, что модификация такого рассуждения покажет нам, что T даже не арифметическое.

Возвращаясь к определимости, заметим, что другим следствием теоремы 10.1 является то, что арифметические предикаты на $\mathbb{N}$ — это в точности те предикаты, которые определимы в системе с основным множеством $\mathbb{N}$ и со всеми рекурсивными предикатами. Это — естественная система, в которой измеряется определимость по модулю рекурсивности. Любой предикат, определимый в этой системе, является определимым и с помощью формулы, находящейся в пренексной форме. Мы будем использовать число перемен между квантором всеобщности и кванторами существования в этой пренексной форме как некоторую меру определимости.

Можно формулировать эти идеи следующим образом и для произвольного пространства $\mathcal{M}$. Пусть Π_0 — класс рекурсивных предикатов. Определим Σ_{n+1} как класс всех проекций Π_n -предикатов; здесь P называется проекцией R , если

$$P = \{x: \exists y_1 \dots \exists y_l R(y_1, \dots, y_l, x)\}.$$

Таким образом, если R — $(k+l, m)$ -местный предикат, то P — (k, m) -местный предикат. Здесь допускаются проекции лишь по числовым, а не по функциональным осям. Чтобы определение было полным, положим Π_n — класс дополнений предикатов из Σ_n .

Эквивалентное определение Σ_n и Π_n может быть сформулировано, по крайней мере для счетного $\mathcal{M}$, в терминах системы $\mathfrak{N}$ с основным множеством $\mathbb{N}$ и со всеми рекурсивными предикатами. Предикат принадлежит Σ_{n+1} тогда и только тогда, когда он определен в $\mathfrak{N}$ формулой, в пренексной форме которой имеется n перемен между кванторами всеобщности и кванторами существования, а самый внешний квантор — квантор существования. Для Π_{n+1} можно дать аналогичное определение, лишь сказав, что самый внешний квантор — квантор всеобщности. (Для несчетных $\mathcal{M}$ аналогичные определения также возможны, нужно лишь побеспокоиться о функциональных переменных. Мы должны допускать формулы, выражающие $\bar{x}(x) = y$.)

Хотя мы умышленно перешли от системы $\mathfrak{N}$ к $\mathfrak{N}$, но, как было доказано в 1970 г., все, что написано в предыдущем абзаце, остается правильным, если заменить $\mathfrak{N}$ на $\mathfrak{N}$. Теорема Матиясевича, которая решает (или, лучше сказать, не решает) 10-ю про-

блему Гильберта, показывает, что всякое числовое р. п. множество может быть представлено в виде

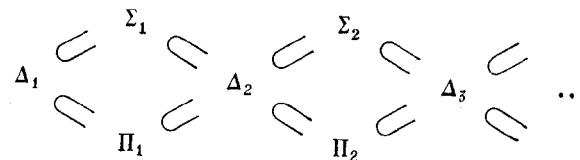
$$\{y: \exists x (p(x, y) = q(x, y))\},$$

где $x \in \mathbb{N}^k$, а p и q — многочлены над $\mathbb{N}$. Подробно об этой теореме написано в главе 2.

Возвращаясь к арифметической иерархии, удобно определить также класс

$$\Delta_n = \Sigma_n \cap \Pi_n,$$

когда $n \geq 1$. Например, из теоремы 6.2 следует, что Δ_1 — класс рекурсивных предикатов, поскольку Σ_1 — класс полурекурсивных предикатов, а Π_1 — класс дополнений полурекурсивных предикатов. Используя фиктивные кванторы, легко доказать следующие включения:



Класс арифметических предикатов является объединением всех этих классов. Все включения, указанные выше, собственные. Это получается из следующей теоремы об иерархии, принадлежащей Клини [4].

10.2. Теорема. Для всех k, m и n :

(i) Существует $(k+1, m)$ -местный предикат из Σ_{n+1} , являющийся универсальным для всех (k, m) -местных предикатов из Σ_{n+1} (т. е. каждый (k, m) -местный предикат получается фиксированием первой числовой переменной как параметра).

(ii) Существует (k, m) -местный предикат из Σ_{n+1} , не лежащий в Π_{n+1} .

Утверждение (ii) следует из утверждения (i), если применить диагонализацию; утверждение (i) следует из теоремы о нормальной форме.

Легко видеть, что классы Σ_n и Π_n замкнуты относительно много-однозначности. Они не замкнуты относительно сводимости по Тьюрингу, так как каждое числовое множество рекурсивно в своем дополнении.

Можно теперь обобщить наше доказательство, что множество T предложений, истинных в $\mathfrak{N}$, не рекурсивно, показав, что T не арифметическое. Вместо K берем подмножество A множества $\mathbb{N}$, лежащее в Σ_{n+1} , но не лежащее в Π_{n+1} . Тогда, как и раньше, $A \leq_1 T$, следовательно, T не может лежать в Π_{n+1} . Так как n произвольно, то T не может быть арифметическим.

Можно рассматривать вместе арифметическую иерархию и операцию скачка на степенях неразрешимости и тем самым связать понятие определимости с понятиями § 8. Операция скачка была там описана с помощью квантора существования, который соответствует проекции предикатов. Такой ход мысли приводит в итоге к следующей теореме, которая доказывается итерацией теоремы 8.3 (ii). Пусть $\mathcal{O}^{(n)}$ — результат n -кратного применения операции скачка к $\emptyset$.

10.3. Теорема (Пост [3]). *Подмножество множества $\mathbb{N}$ лежит в Σ_{n+1} тогда и только тогда, когда оно р.п. относительно $\mathcal{O}^{(n)}$ (а это выполняется тогда и только тогда, когда оно односводимо к $\mathcal{O}^{(n+1)}$). Подмножество множества $\mathbb{N}$ лежит в Δ_{n+1} тогда и только тогда, когда оно рекурсивно относительно $\mathcal{O}^{(n)}$.*

Напомним, что аналитические множества — это те множества, которые определены в $\mathfrak{A}$ формулами логики второго порядка. Как и в арифметической иерархии, можно использовать число перемен между кванторами всеобщности и кванторами существования (здесь квантификация по функциональным переменным) как некоторую меру определимости. Пусть

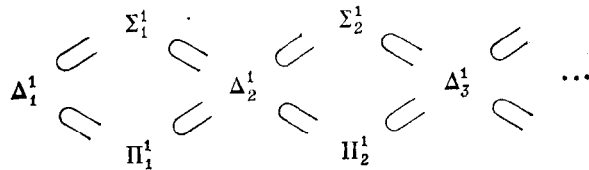
$\Sigma_0^1 = \Pi_0^1 =$ класс арифметических предикатов.

Определим Σ_{n+1}^1 как класс всех проекций предикатов из Π_n^1 вдоль функциональных осей. Таким образом, предикат из Σ_{n+1}^1 имеет вид

$$\{x: \exists \alpha_1 \dots \exists \alpha_l R(x, \alpha_1, \dots, \alpha_l)\},$$

где R лежит в Π_n^1 . Определим Π_n^1 как класс дополнений предикатов из Σ_n^1 , а $\Delta_n^1 = \Sigma_n^1 \cap \Pi_n^1$.

Простейшие факты об арифметической иерархии могут быть обобщены на аналитическую иерархию. Имеем включения:



И здесь все включения собственные, так как соответствующая теорема об иерархии доказывается аналогично теореме 10.2.

Данные классы в аналитической иерархии обладают более сильными замкнутыми свойствами, чем их аналоги в арифметической иерархии. Это иллюстрирует теорема 10.4, являющаяся количественным вариантом транзитивности определимости. Классы Σ_n^β и $\Sigma_n^{1,\beta}$ определяются аналогично с заменой рекурсивности на релятивизированное понятие рекурсивности относительно β .

10.4. Теорема о транзитивности. *Допустим, что $\mathcal{A} \in N$ и $\beta \in \mathbb{N}^N$.*

$$(i) \mathcal{A} \in \Sigma_{m+1}^\beta \text{ \& } \beta \in \Delta_{n+1} \Rightarrow \mathcal{A} \in \Sigma_{m+n+1};$$

$$(ii) \mathcal{A} \in \Sigma_m^{1,\beta} \text{ \& } \beta \in \Delta_n^1 \Rightarrow \mathcal{A} \in \Sigma_{\max(m,n)}^1.$$

Утверждение (i) доказывается непосредственно. Доказательство утверждения (ii), принадлежащее Шенфилду [2], начинается с записи

$$x \in \mathcal{A} \leftrightarrow \exists y [y = \beta \wedge Q(x, y)],$$

где Q лежит в Σ_m^1 . Далее выражение справа приводится к префиксной форме. Утверждение (ii) мешает выполняться в аналитической иерархии каким-либо аналогом теоремы Поста (теорема 10.3).

Какие множества лежат в Δ_1^1 ? Ключ к разгадке доставляет дескриптивная теория множеств. Когда мы релятивизируем относительно $\mathbb{N}^N$ понятие рекурсивности, Σ_1^1 становится классом проекций борелевских множеств конечного ранга. Это и есть аналитические или A -множества дескриптивной теории множеств. Теорема Суслина [1] показывает, что множество и его дополнение являются одновременно аналитическими тогда и только тогда, когда само множество является борелевским. Это подсказывает, по аналогии, что Δ_1^1 состоит из множеств, получаемых обобщением арифметической иерархии по трансфинитам. Это действительно так: такая иерархия называется гиперарифметической иерархией. Она может быть построена с помощью подходящей итерации операции скачка по всем ординалам, являющимся «рекурсивно счетными» в том смысле, что они являются порядковыми типами некоторых рекурсивных полных порядков на числах.

Вопрос о локализации данного множества в этих иерархиях сводится к двум задачам. Первая — прямое доказательство того, что данное множество принадлежит, скажем, Σ_2^1 (это обычно делается легко). Затем обратная задача — показать, что это наилучший возможный результат, доказав, что данное множество не принадлежит двойственному классу Π_2^1 . Возьмем, например, подмножество R из $\mathbb{N}^N$, состоящее из всюду определенных рекурсивных функций из $\mathbb{N}$ в $\mathbb{N}$. Тогда $R \in \Sigma_3$, потому что

$$\alpha \in R \leftrightarrow \exists e \forall x \exists y [T(e, \langle x \rangle, y) \wedge U(y) = \alpha(x)],$$

а выражение в скобках рекурсивно. Шенфилд [1] показал, что R не лежит в Π_3 .

Мы уже видели, что множество истинных в арифметике предикатов не арифметическое. В гиперарифметической иерархии

это множество находится на уровне ω . Это значительно уточняет теорему Гёделя о неполноте, которая утверждает, что это множество не р.п. Но рассмотрим характеристическую функцию τ множества истинных предложений. Тогда множество $\{\tau\}$, как подмножество N^N , лежит в Π_2 . Чтобы доказать это, нужно внимательно посмотреть на определение выполнимости в $\mathcal{R}$ (определение 3.8 из главы I «Теории моделей»). Это определение, рассматриваемое как условие на τ , является Π_2 -утверждением, которое истинно только на τ и ни на чем больше. Так как $\{\tau\}$ лежит в Π_2 , то легко заметить, что предикат истинности лежит в Δ_1^1 :

$$\begin{aligned} s - \text{истина} &\Leftrightarrow \forall \alpha [\alpha \in \{\tau\} \rightarrow \alpha(s) = 1] \\ &\Leftrightarrow \exists \alpha [\alpha \in \{\tau\} \wedge \alpha(s) = 1]. \end{aligned}$$

Класс полных порядков на N может быть отождествлен с подмножеством из N^N , а именно

$$\{\alpha \in N^N: \{(x, y): \alpha(\langle x, y \rangle) = 0\} \text{ вполне упорядочивает } N\}.$$

Легко видеть, что это множество лежит в Π_1^1 ; мы просто записываем это определение и считаем кванторы. Это множество не лежит в Σ_1^1 ; в действительности оно даже не является A -множеством, как утверждает один классический результат.

§ 11. Рекурсивные аналоги классических объектов

Рекурсивные функции — это в точности те функции, для которых мы фактически можем выписать вычисляющие их программы; другие же функции скользки и неуловимы. Если кто-то хочет подойти к математике с конструктивной точки зрения, то рекурсивные функции для него имеют более твердый онтологический статус, чем другие функции. В принципе можно смотреть на математический объект (в качестве примеров будет рассмотрено множество счетных ординалов и множество действительных чисел) с конструктивной точки зрения и извлечь ту его часть, которая достаточно конструктивна, чтобы быть рассматриваемой в теории рекурсии. Затем эта рекурсивная часть может быть рассмотрена как рекурсивный аналог оригинала.

В качестве предварительного примера рассмотрим, до какой степени семейство R всюду определенных рекурсивных функций на N аналогично семейству N^N всех функций на N . Имеется очевидное различие их мощностей — N^N несчетно, в то время как существует лишь счетное число рекурсивных функций. Но полная аналогия с несчетностью N^N должна говорить о том, что не существует рекурсивного одно-однозначного соответствия

между натуральными числами и индексами всюду определенных рекурсивных функций. Следующий простой результат есть одна из форм этого явления.

11.1. Теорема. *Не существует всюду определенной рекурсивной функции f на N такой, что $\{f(n): n \in N\}$ совпадает со всем семейством R всюду определенных рекурсивных функций.*

Доказательство. Как и при доказательстве несчетности N^N , мы используем диагонализацию. Равенство $g(x) = \{f(x)\}(x) + 1$ задает всюду определенную рекурсивную функцию g , которую f пропускает. Существует и другое доказательство, дающее больше количественной информации. Из того (см. § 10), что R не лежит в Π_3 , заключаем, что не может быть никакого Σ_2 -множества A такого, что $R = \{x: x \in A\}$. $\square$

Операции сложения, умножения и композиции функций применимы как в R , так и в N^N . Но с рекурсивной точки зрения нужна и некоторая дополнительная информация: нужно иметь возможность по данным индексам функций f и g эффективно находить индексы для $f + g$, $f \cdot g$ и $f \circ g$. Чтобы доказать, что это действительно можно сделать, заметим, например, что $\{x\}(z) + \{y\}(z)$ является частично рекурсивной функцией от x , y и z , и применим теорему о параметризации.

Резюмируя все сказанное, можно считать, что операции сложения, умножения и композиции функций «эффективны на индексах». Другими словами, каждая из наших функций имеет индексы, их обозначающие, а операции над функциями индуцируются операциями на индексах, оказывающимися в данном случае рекурсивными операциями. К этому явлению мы будем постоянно возвращаться в последующих примерах: конструктивные элементы классических объектов появляются вместе с номерами, их обозначающими; эффективные операции должны работать с этими именами.

Чтобы найти более сложный пример рекурсивного аналога некоторого классического объекта, возьмем (как классический объект) множество счетных ординалов. Зная, что ординальные числа полезны в трансфинитных конструкциях (таких, как борелевская иерархия), мы не будем сильно удивлены, обнаружив, что некоторый рекурсивный аналог будет полезен в трансфинитных конструкциях в теории рекурсии (таких, как гиперарифметическая иерархия, упомянутая в предыдущем параграфе).

Не слишком богатый аналог дается множеством

$$W = \{x: \{x\}^{2,0} \text{ кодирует полный порядок}\},$$

где то, что f кодирует полный порядок, означает, что f — всюду определенная функция из $N \times N$ в $\{0, 1\}$, а $\{(x, y): f(x, y) = 0\}$ —

полный порядок на $\mathbb{N}$. Короче, мы считаем множество W множеством рекурсивных полных порядков. Для x в W полагаем $\|x\|$ — ординал соответствующего полного порядка. Так как начальный отрезок любого рекурсивного полного порядка является другим полным порядком, то множество $\{\|x\| : x \in W\}$ есть начальный отрезок множества всех счетных ординалов. Наименьшая верхняя грань этого множества будет называться «рекурсивным ω_1 ». Хотя рекурсивный ω_1 счетен, это первый ординал, который не является рекурсивно счетным.

К сожалению, множество W имеет и некоторые недостатки, которые ослабляют его применения. Например, для данного x в W мы не можем эффективно сказать, будет ли $\|x\|$ последователем. Даже если он и является последователем, мы не можем эффективно найти элемент W , обозначающий предшественника $\|x\|$.

Более качественный аналог дается системой ординальных обозначений, введенной Клини [3]. Множество O построено снизу не так, как W . Мы дадим одно индуктивное определение для множества O , двуместного предиката $<_O$ и отображения $x \mapsto |x|$ из O в ординалы (наше определение лишь слегка отличается от данного Клини).

(i) $1 \in O$ и $|1| = 0$; 1 — единственное число, обозначающее ординал 0.

(ii) Если $x \in O$, то $2^x \in O$, $x <_O 2^x$ и $|2^x| = |x| + 1$. Этот шаг связан с получением последователя.

(iii) Если $x <_O y <_O z$, то $x <_O z$. Предикат $<_O$ окажется частичным полным порядком на O .

(iv) Если $\{e\}$ — всюду определенная возрастающая последовательность обозначений (т. е. $\{e\} : \mathbb{N} \rightarrow O$ и $\{e\}(n) <_O \{e\}(n+1)$ для каждого n), то $3 \cdot 5^e \in O$, $\{e\}(n) <_O 3 \cdot 5^e$ для каждого n и $|3 \cdot 5^e| = \sup \{|\{e\}(n)| : n \in \mathbb{N}\}$.

Это индуктивное определение приписывает обозначения начальному отрезку $\{|x| : x \in O\}$ счетных ординалов. И снова наименьший ординал, не получивший обозначения, — это рекурсивный ω_1 . В действительности существует несколько других путей характеристики рекурсивного ω_1 : это есть наименьший ординал, не являющийся порядковым типом ни для какого Σ_1^1 -полного порядка на числах или же это есть наименьший допустимый ординал после ω (в смысле главы 5).

Как последний пример рекурсивного аналога рассмотрим рекурсивные действительные числа. К этому понятию впервые обратился Тьюринг [1]; более поздние упоминания находятся у Райса [2]. Любое действительное число может быть аппроксимировано рациональными числами, но мы хотим выделить такие числа для которых можно указать эффективную рациональную

нальную аппроксимацию с хорошей оценкой ошибки. Эти числа — самые действительные из действительных.

Точно так же как существует несколько путей построения действительных чисел из рациональных, существует и несколько эквивалентных путей уточнения понятия рекурсивных действительных чисел. Например, мы могли бы потребовать, чтобы двоичная запись дробной части числа задавалась с помощью рекурсивной функции. Эквивалентно, мы могли бы приспособить конструкцию последовательностей Коши. Для каждого натурального числа n рассмотрим рациональное число $r(n) = ((n)_0 - (n)_1) / ((n)_2 + 1)$. Скажем, что e обозначает рекурсивное действительное число, если $\{e\}$ всюду определена, и как только $m > n$, то

$$|r(\{e\}(n)) - r(\{e\}(m))| < \frac{1}{2^n}.$$

Существенной особенностью обоих определений является то, что мы эффективно указываем верхние и нижние рациональные границы, сходящиеся к этому числу.

Рекурсивные действительные числа образуют поле, так как для $x \neq 0$ мы можем указать рациональные границы одного знака, которые затем могут быть преобразованы в рациональные границы для $1/x$. (Но, даже если e обозначает рекурсивное действительное число, не существует эффективного пути решения, будет это число нулем или нет.) Здесь доказано не только то, что у нас получается поле, — алгебраические операции являются «эффективными на индексах»; например, существует рекурсивная функция f такая, что если a и b обозначают рекурсивные действительные числа, то $f(a, b)$ обозначает их сумму.

Все алгебраические действительные числа рекурсивны. Нетрудно доказать, что рекурсивные действительные числа образуют вещественно замкнутое упорядоченное поле, т. е. упорядоченное поле, в котором любой многочлен, изменяющий знак, имеет промежуточный корень. Следовательно, результат присоединения $\sqrt{-1}$ к этому полю является алгебраически замкнутым полем (см. Ван дер Варден [1], § 70). Далее, по теореме Тарского поле рекурсивных действительных чисел элементарно эквивалентно полю всех действительных чисел (см. главу 2 «Теории моделей»).

Вместе с алгебраическими числами и некоторые трансцендентные числа, например e и π , рекурсивны, так как существуют хорошо известные методы получения сходящихся верхних и нижних рациональных граней.

Рекурсивные действительные числа не так хороши для аналитиков, как для алгебраистов. Следующий пример встречается у Райса [2]; см. также Шпекер [1]. Начнем с нерекурсивного

р.п. множества K . Существует одно-однозначная всюду определенная рекурсивная функция f , область значений которой есть K (можно считать, что $f(n)$ есть $(n+1)$ -е число, появляющееся в бесповторном эффективном перечислении K). Рассмотрим множество рациональных чисел:

$$\frac{1}{2^{f(0)}}, \frac{1}{2^{f(0)}} + \frac{1}{2^{f(1)}}, \frac{1}{2^{f(0)}} + \frac{1}{2^{f(1)}} + \frac{1}{2^{f(2)}}, \dots$$

Это ограниченное рекурсивное множество рациональных чисел. Но его наименьшая верхняя грань (которая является единственной предельной точкой этого множества) не является рекурсивным действительным числом, иначе K было бы рекурсивным.

Наконец, рассмотрим аналог функций действительной переменной. Функция F из множества рекурсивных действительных чисел в это же множество называется *рекурсивным оператором*, если существует частично рекурсивная функция f такая, что как только e обозначает рекурсивное действительное число, то $f(e)$ определено и обозначает $F(x)$. Таким образом, f моделирует F , работая на индексах. Мы приведем без доказательства следующий результат.

11.2. Теорема (Крайзел, Лакомб и Шенфилд [1], Цейтин [1]). *Каждый рекурсивный оператор непрерывен. Более того, для любого данного e , обозначающего рекурсивное действительное число, и положительного рационального числа δ эффективно находится требуемое δ .*

ЛИТЕРАТУРА

- Блюм (Blum M.)**
1. A machine independent theory of the complexity of recursive functions. — J. Assoc. Comput. Mach., 1967, 14, p. 322—336. [Русский перевод: Блюм М. Машинно-независимая теория сложности рекурсивных функций. — В кн.: Проблемы математической логики. М.: Мир, 1970, с. 401—422.]
- Брэдди (Brady A. H.)**
1. The conjectured highest scoring machines for Rado's $\Sigma(k)$ for the value $k=4$. — IEEE Trans. Computers, 1966, EC-15, p. 802—803.
2. The solution to Rado's «busy beaver game» is now decided for $k=4$ (Abstract). — Notices Amer. Math. Soc., 1975, 22, p. A-25.
- Ван дер Варден (van der Waerden B. L.)**
1. Modern Algebra. — Vol. I. — Revised English ed. — N. Y.: Frederick Ungar, 1953. [Русский перевод: ван дер Варден Б. Л. Алгебра. — М.: Наука, 1979.]
- Гёдель (Gödel K.)**
1. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I. — Monatsh. Math. Phys., 1931, 38, S. 173—198.
2. On undecidable propositions of formal mathematical systems. — In: The Undecidable; Basic Papers on Undecidable Propositions, Unsolvability Problems and Computable Functions. Hewlett, N. Y.: Raven Press, 1965, p. 41—71.

- Грин (Green M. W.)**
1. A lower bound on Rado's sigma function for binary Turing machines. — In: Switching Circuit Theory and Logical Design: Proc. of the fifth annual symposium, The Institute of Electrical and Electronics Engineers, 1964, p. 91—94.
- Девис (Davis M.)**
1. Computability and Unsolvability. — N. Y.: McGraw-Hill, 1958.
- Кар, Мур, Ван (Kahr A. S., Moore E. F., Wang H.)**
1. Entscheidungsproblem reduced to the $\forall\exists\forall$ case. — Proc. Nat. Acad. Sci. USA, 1962, 48, p. 365—377.
- Клини (Kleene S. C.)**
1. General recursive functions of natural numbers. — Math. Ann., 1936, 112, p. 727—742.
2. λ -definability and recursiveness. — Duke Math. J., 1936, 2, p. 340—353.
3. On notation for ordinal numbers. — J. Symbolic Logic, 1938, 3, p. 150—155.
4. Recursive predicates and quantifiers. — Trans. Amer. Math. Soc., 1943, 53, p. 41—73.
5. Introduction to Metamathematics. — Amsterdam: North-Holland, 1952. [Русский перевод: Клини С. К. Введение в метаматематику. — М.: ИЛ, 1957.]
- Крайзел, Лакомб и Шенфилд (Kreisel G., Lacombe D., Shoenfeld J. R.)**
1. Partial recursive functionals and effective operations. — In: Constructivity in Mathematics: Proc. of the colloquium held at Amsterdam, 1957. Amsterdam: North-Holland, 1957, p. 290—297.
- Лин и Раддо (Lin S., Rado T.)**
1. Computer studies of Turing machine problems. — J. Assoc. Comput. Mach., 1965, 12, p. 196—212.
- Майхилл (Myhill J.)**
1. Creative sets. — Z. math. Logik Grundl. Math., 1955, 1, p. 97—108.
- Матиясевич Ю. В.**
1. Диофантовость перечислимых множеств. — ДАН СССР, 1970, 191, с. 279—282.
- Мучник А. А.**
1. Неразрешимость проблемы сводимости теории алгоритмов. — ДАН СССР, 1956, 108, с. 194—197.
- Пост (Post E. L.)**
1. Finite combinatorial processes — formulation I. — J. Symbolic Logic, 1936, 1, p. 103—105. [Русский перевод: Пост Э. Конечные комбинаторные процессы, формулировка I. — В кн.: Успенский В. А. Машина Поста. М.: Наука, 1979, с. 89—95.]
2. Recursively enumerable sets of positive integers and their decision problems. — Bull. Amer. Math. Soc., 1944, 50, p. 284—316.
3. Degrees of recursive unsolvability (Abstract). — Bull. Amer. Math. Soc., 1948, 54, p. 641—642.
- Раббин (Rabin M. O.)**
1. Degree of difficulty of computing a function and a partial ordering of recursive sets. — Jerusalem: Hebrew University, 1960, technical report № 2.
- Раддо (Rado T.)**
1. On non-computable functions. — Bell System Tech. J., 1962, 41, p. 877—884.
- Райс (Rice H. G.)**
1. Classes of recursively enumerable sets and their decision problems. — Trans. Amer. Math. Soc., 1953, 74, p. 358—366.
2. Recursive real numbers. — Proc. Amer. Math. Soc., 1954, 5, p. 784—791.

ons and Effective Computability — N. Y.:
перевод: Роджерс Х. Теория рекурсив-
вычислимость. — М.: Мир, 1972.]

Princeton, N. J.: Princeton University Press,

degrees are dense. — Ann. Math., 1964, 80,

mbles mesurables B sans nombres transfi-
917, 164, p. 88—91.

ith an application to the Entscheidungs-
ath. Soc., Ser. 2, 1936, 42, p. 230—265.
rdinals. — Proc. London Math. Soc., Ser. 2,

ociated with formalized theories. — J. Sym-
—175.

sets of incomparable degrees of unsolvabi-
blem, 1944). — Proc. Nat. Acad. Sci. USA,

the study of elementary logic. — In: The
the 1963 International Symposium at Berke-
and, 1965, p. 132—145.

в конструктивно полных отделимых мет-
ДАН СССР, 1959, 128, с. 49—52.

elementary number theory (Abstract). — Bull.
p. 332—333.

elementary number theory. — Amer. J. Math.,

ctions. — Proc. Amer. Math. Soc., 1958, 9,

of a predicate. — In: Recursive Function
providence (Rhode Island): Amer. Math. Soc.,

ding (Mass.): Addison-Wesley, 1967. [Рус-
Дж. Математическая логика. — М.: Наука,

— Amsterdam: North-Holland, 1971. [Русский
х. Степени неразрешимости. — М.: Наука,

re Sätze der Analysis. — J. Symbolic Logic,

and logic. — N. Y.: Academic Press, 1971.

НЕРАЗРЕШИМЫЕ ПРОБЛЕМЫ

Мартин Девис

СОДЕРЖАНИЕ

Введение	51
§ 1. Снова о проблеме остановки	52
§ 2. Полутуэвские процессы	55
§ 3. Полугруппы и группы	58
§ 4. Другие комбинаторные проблемы	63
§ 5. Диофантовы уравнения	67
Литература	75

Введение

Многие важные математические проблемы имеют вид: найти алгоритм (т. е. эффективную процедуру), с помощью которой можно определять (за конечное число шагов) для каждого элемента некоторого данного множества, будет этот элемент обладать некоторым данным свойством или нет. При этом «решение» такой проблемы «разрешимости» состоит в фактическом указании алгоритма и в доказательстве, что этот алгоритм делает то, что нужно.

Стандартным примером из элементарной теории чисел является нахождение алгоритма, с помощью которого можно определять для данной упорядоченной тройки $\langle a, b, c \rangle$ целых чисел, будет уравнение

$$ax + by = c$$

иметь решение в целых числах или нет. В данном случае решение имеется: найти наибольшее натуральное число d , которое одновременно делит a и b , и затем проверить, будет или нет d делителем c . (Это уравнение будет иметь целочисленное решение только в случае, когда d делит c .) Развитие теории рекурсии при уточнении интуитивного понятия эффективной вычислимости допускает следующую новую возможность: вместо положительного решения проблемы разрешимости с помощью доказательства существования алгоритма мы можем ее решить и отрицательно, доказав, что требуемого алгоритма не существует, или, как мы говорим, можно доказать, что эта проблема *неразрешима*. Так, десятая проблема Гильберта, заключающаяся в поиске алгоритма для определения того, имеет ли целочисленное

решение данное полиномиальное уравнение $P(x_1, \dots, x_k) = 0$ с целыми коэффициентами, оказывается неразрешимой, как было показано Матиясевичем [1].

Для понимания этой главы необходимо лишь знакомство с §§ 1—4 из главы 1 «Элементы теории рекурсии», на которую мы ссылаемся как на ЭТР и обозначениям которой мы следуем. Мы дадим обзор главных результатов о неразрешимости, которые получены для проблем, имеющих подлинный математический интерес. В некоторых случаях мы дадим полные доказательства, в других позволим себе обрисовать лишь главные идеи.

Математический смысл какого-либо результата о неразрешимости состоит в том, что некоторое конкретное множество не является рекурсивным. Действительно, если S — любое нерекурсивное множество натуральных чисел, то можно утверждать неразрешимость следующей проблемы разрешимости: *для данного $x \in \mathbb{N}$ определить, будет $x \in S$ или нет.* Конечно, это заявление основано на отождествлении интуитивного понятия « S разрешимо» с точным понятием « S рекурсивно», т. е. на том, что обычно называется тезисом Чёрча (ср. § 3 ЭТР). В этой главе мы свободно пользуемся тезисом Чёрча, часто без специального упоминания, и это необходимо, если мы из нерекурсивности какого-то множества хотим вывести, что на самом деле не существует соответствующего алгоритма. Но, кроме того, мы используем этот тезис и для упрощения доказательств: как только мы указываем алгоритм для вычисления значений частичной функции f , мы заключаем без всяких хлопот, что f — частично рекурсивная функция.

В дополнение к доказательству, что некоторая математическая проблема является неразрешимой, бывает интересно подсчитать степень неразрешимости такой проблемы в смысле, обсуждавшемся в § 8 ЭТР. Однако такие вопросы в данной главе мы не обсуждаем.

§ 1. Снова о проблеме остановки

Неразрешимость проблемы остановки указана в 4.2 ЭТР в следующем виде:

Множество $K = \{x: \{x\}(x) < \infty\}$ не рекурсивно.

По теореме о нормальной форме (ЭТР, 4.1) $\{x\}(x)$ является частично рекурсивной функцией от x . Поэтому, согласно замечанию из § 2 ЭТР, существует некоторая машина Тьюринга M (которую ценой довольно неблагодарной работы можно было бы конкретно указать) такая, что:

Если M начинает с состояния q_0 обозревать самый левый символ из $\ulcorner x \urcorner$ (остальные символы на ленте пустые), то M со

временем остановится тогда и только тогда, когда $\{x\}(x)$ определено, т. е. тогда и только тогда, когда $x \in K$. На протяжении всей главы M будет всегда означать эту машину Тьюринга.

Так как K не рекурсивно, заключаем, что имеет место

1.1. Теорема. *Не существует алгоритма, который по данному $x \in \mathbb{N}$ определяет, остановится ли со временем M , начав работу в состоянии q_0 и обозревая самый левый символ из $\ulcorner x \urcorner$.*

Несколько ослабляя этот результат, можно получить более изящный вариант (напомним из ЭТР, § 4, что *конфигурация* для машины Тьюринга состоит из текущего содержания машинной ленты, номера состояния и ячейки, которая обозревается):

1.2. Следствие. *Не существует алгоритма, который по данной конфигурации для M определяет, остановится ли со временем M , начав работу в данной конфигурации.*

Конечно, машина M формально является функцией (как описано в определении 2.1 ЭТР), которая может быть конкретно задана таблицей с пятью столбцами и подходящим числом строк или же, как мы будем говорить, *пятерками*. (Ср. в § 2 ЭТР пример машины Тьюринга, вычисляющей $x + y$.) Проблема остановки M становится тогда совершенно особой математической задачей: для каких конфигураций из данного множества некоторые вполне определенные комбинаторные процессы со временем обрываются?

Проблема остановки будет играть фундаментальную роль в этой статье. По существу, неразрешимость всех проблем, которые будут обсуждаться, следует из неразрешимости проблемы остановки.

1.3. Определение. k -местный предикат R на $\mathbb{N}$ называется *рекурсивно перечислимым* (сокращенно р.п.), если существует машина Тьюринга T такая, что, как только T начинает работать в состоянии q_0 , обозревая самый левый символ из

$$\ulcorner x_1 \urcorner 0 \ulcorner x_2 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$$

(остальные ячейки пустые), то T со временем останавливается тогда и только тогда, когда $\langle x_1, \dots, x_k \rangle \in R$.

Рекурсивная перечислимость k -местных предикатов на $\mathbb{N}$ определена в § 6 ЭТР (что формально не входит в требуемые нами предварительные знания) в несколько отличном, но эквивалентном виде. Доказательство эквивалентности требует преодоления не очень сложных технических трудностей. Естественно, в этой главе будет использоваться данное определение.

Интуитивно, если говорят, что R р.п., то имеют в виду наличие некоторого алгоритма, который будет давать правильный ответ «да» на вопрос вида «Верно ли, что $\langle x_1, \dots, x_k \rangle \in R$?» и не будет останавливаться, когда ответ — «нет».

Обозначая через $\bar{R}$ дополнение k -местного предиката R (т. е. $\langle x_1, \dots, x_k \rangle \in \bar{R}$ тогда и только тогда, когда $\langle x_1, \dots, x_k \rangle \notin R$), получаем, что имеет место

1.4. Теорема. R рекурсивен тогда и только тогда, когда R и $\bar{R}$ р. п.

Доказательство. Пусть R рекурсивен и его характеристическая функция (т. е. функция, равная 1, когда R истинен, и 0, когда R ложен) вычисляется на машине Тьюринга M_0 . Пусть $q_0, q_1, \dots, q_n$ — состояния M_0 . Изменим M_0 для получения новых машин M^+ и M^- , присоединив новые состояния и пятерки. Для каждой пары (i, α) , $0 \leq i \leq n$, $\alpha = 0$ или 1, такой, что в таблице M нет пятерки, начинающейся с $i\alpha$ (т. е. M_0 сразу останавливается, когда она приходит в состояние q_i и обозревает ячейку, на которой написан символ α), мы помещаем в таблицы для M^+ и M^- пятерки

$$i\alpha \text{ аП}(n+1).$$

Далее, когда M_0 останавливается, на обозреваемой ячейке находится 1, а на правой соседней ячейке находится 1, если R истинен для данного входа, и 0, если R ложен для данного входа. Таким образом, попадая в состояние $n+1$, машины M^+ и M^- обозревают 1 или 0 в зависимости от того, истинен или ложен предикат R для данного входа. Наконец, добавим в M^+ пятерку

$$(n+1)0 \text{ ОП}(n+1).$$

а в M^- пятерки

$$(n+1)1 \text{ ИП}(n+2),$$

$$(n+2)0 \text{ ОП}(n+2).$$

В этом случае M^+ останавливается для данного входа $\ulcorner x_1 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$ тогда и только тогда, когда $\langle x_1, \dots, x_k \rangle \in R$, а M^- останавливается тогда и только тогда, когда $\langle x_1, \dots, x_k \rangle \in \bar{R}$.

Обратно, если R и $\bar{R}$ р. п., то мы имеем машины Тьюринга M^+ и M^- , которые останавливаются для входа $\ulcorner x_1 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$ в случае $\langle x_1, \dots, x_k \rangle \in R$ или $\notin R$ соответственно. Таким образом, для определения того, будет $\langle x_1, \dots, x_k \rangle \in R$ для данных $x_1, \dots, x_k$ или нет, нам нужно включить одновременно M^+ и M^- и ждать, какая из них остановится. Следовательно, R интуитивно разрешим, а по тезису Чёрча он рекурсивен.

Так как машина M , используемая в нашем обсуждении проблемы остановки, со временем останавливается для данного x тогда и только тогда, когда $x \in K$, то имеет место

1.5 Теорема. Множество K р. п., но не рекурсивно. Следовательно, $\bar{K}$ не р. п.

§ 2. Полутуэвские процессы

Пусть $A = \{a_1, \dots, a_k\}$ — некоторое данное конечное множество объектов, которые мы называем символами. Тогда A называется алфавитом, а всякая конечная последовательность элементов из A называется цепочкой или словом над A . Основной операцией над цепочками является операция сцепления, т. е. если $u = a_{i_1} a_{i_2} \dots a_{i_k}$, $v = a_{j_1} a_{j_2} \dots a_{j_r}$ — цепочки над A , то мы пишем

$$uv = a_{i_1} a_{i_2} \dots a_{i_k} a_{j_1} a_{j_2} \dots a_{j_r}.$$

Заметим, что $u(vw) = (uv)w$. Удобно также рассматривать пустую цепочку Λ длины 0, где $u\Lambda = \Lambda u = u$ для всех цепочек u .

2.1. Определение. Полутуэвской продукцией (над A) (или просто продукцией) называется упорядоченная пара $(g, \bar{g})$ слов над A . Обычно продукцию записывают в виде $g \rightarrow \bar{g}$. Полутуэвским процессом (над A) называется всякое конечное непустое множество полутуэвских продукций над A .

2.2. Определение. Пусть P — полутуэвская продукция $g \rightarrow \bar{g}$. Тогда мы пишем $u \Rightarrow_P v$ (опуская P , когда это не вызывает двусмысленности), если $u = agb$ и $v = a\bar{g}b$ для (возможно пустых) цепочек a, b .

2.3. Определение. Пусть Π — полутуэвский процесс. Тогда мы пишем $u \Rightarrow_{\Pi} v$, если $u \Rightarrow_P v$ для некоторой продукции $P \in \Pi$. Пишем $u \Rightarrow_{\Pi}^* v$, если существует конечная последовательность $u = u_1 \Rightarrow_{\Pi} u_2 \Rightarrow_{\Pi} \dots \Rightarrow_{\Pi} u_n = v$ для $n \geq 1$. (В частности, $u \Rightarrow_{\Pi}^* u$.) Опять-таки мы опускаем Π , когда это не вызывает двусмысленности результата. (Обычно символы P и Π располагаются непосредственно под $\Rightarrow$, а символ $*$ — непосредственно над $\Rightarrow$.)

Проблемой слов для данного полутуэвского процесса Π является следующая проблема разрешимости: найти алгоритм, с помощью которого для данных слов u, v можно определять, будет $u \Rightarrow_{\Pi}^* v$ или нет.

Мы увидим, что существует полутуэвская система, проблема слов для которой неразрешима. В действительности мы покажем, как получить по всякой данной машине Тьюринга T соответствующую полутуэвскую систему $\Pi(T)$ такую, что алгоритм для решения проблемы слов для $\Pi(T)$ может быть также использован для решения проблемы остановки для T . Вместе с результатом § 1 это даст нам требуемый результат.

Итак, пусть T — машина Тьюринга с инструкциями $q_0, q_1, \dots, q_n$. Тогда $\Pi(T)$ будет полутуэвским процессом над алфавитом

$$A = \{0, 1, q_0, q_1, \dots, q_n, q', h\}.$$

Последовательные конфигурации T , возникающие в ходе какого-либо вычисления, будут представляться посредством так называемых слов Поста, т. е. слов над A вида

$$huq_i v h, \quad (1)$$

где u, v — слова над $\{0, 1\}$, $v \neq \Lambda$ и $0 \leq i \leq n$. Здесь слово Поста (1) представляет конфигурацию, при которой q_i является текущей инструкцией, записью на ленте является uv (дополненная бесконечными последовательностями из 0 слева и справа), и обозревается начальный символ из v . Символы h будут использоваться как знаки пунктуации; их важность скоро будет видна. Так как не запрещается, чтобы u начиналось с 0 или v кончалось 0, то существует бесконечно много различных слов Поста, соответствующих данной конфигурации машины T . Влияние машины T на последовательные конфигурации будет имитироваться (или, как иногда говорят, *моделироваться*) посредством продукций из $\Pi(T)$, которые будут соответствующим образом влиять на слова Поста.

В действительности продукции из $\Pi(T)$ будут следующие:
(i) Для каждой пятерки из таблицы машины T вида

$$i\alpha \beta Pj, \quad \alpha, \beta \in \{0, 1\},$$

$\Pi(T)$ содержит три продукции

$$\begin{aligned} q_i \alpha 0 &\rightarrow \beta q_j 0, \\ q_i \alpha 1 &\rightarrow \beta q_j 1, \\ q_i \alpha h &\rightarrow \beta q_j 0h. \end{aligned}$$

(ii) Для каждой пятерки из таблицы машины T вида

$$i\alpha \beta Pj, \quad \alpha, \beta \in \{0, 1\},$$

$\Pi(T)$ содержит три продукции:

$$\begin{aligned} 0q_i \alpha &\rightarrow q_j 0\beta, \\ 1q_i \alpha &\rightarrow q_j 1\beta, \\ hq_i \alpha &\rightarrow hq_j 0\beta. \end{aligned}$$

(iii) Для каждой пары $\langle i, \alpha \rangle$, $0 \leq i \leq n$, $\alpha \in \{0, 1\}$, для которой нет пятерки в таблице машины T , начинающейся с $i\alpha$, $\Pi(T)$ содержит продукцию

$$q_i \alpha \rightarrow q \alpha.$$

(iv) Наконец, $\Pi(T)$ содержит пять продукций:

$$\begin{aligned} q0 &\rightarrow q, \\ q1 &\rightarrow q, \\ qh &\rightarrow q'h, \\ 0q' &\rightarrow q' \\ 1q' &\rightarrow q'. \end{aligned}$$

Теперь предположим, что $huq_i \alpha v h$, где $\alpha, v \in \{0, 1\}$, является словом Поста, соответствующим данной конфигурации машины T , и таблица машины T содержит пятерку

$$i\alpha \beta Pj.$$

Тогда имеем

$$huq_i \alpha v h \xRightarrow{\Pi(T)} hu\beta q_j v h,$$

и в действительности $hu\beta q_j v h$ — слово Поста, соответствующее следующей конфигурации машины T (т. е. α заменяется на ленте на β , обозреваемая ячейка передвигается на одну вправо, а q_i — новая текущая инструкция). В случае, когда слово Поста имеет вид $huq_i \alpha h$, имеем

$$huq_i \alpha h \xRightarrow{\Pi(T)} hu\beta q_j 0h,$$

т. е. посредством единственной продукции, которую можно применить, добавляется необходимый 0 справа. Таким образом, полное действие продукций, перечисленных в (i), состоит в изменении слова Поста в точном соответствии с действием пятерки $i\alpha \beta Pj$ на конфигурацию машины. Легко заметить, что продукции, перечисленные в (ii), ведут себя аналогично для пятерок вида $i\alpha \beta Pj$.

Продукции, перечисленные в (iii), будут оперировать со словами Поста только в том случае, когда они соответствуют конфигурации машины T , при которой T вынуждена будет остановиться. Здесь символ инструкции q_i заменяется на q . Наконец, если u, v — слова над $\{0, 1\}$, то в соответствии с продуктами, перечисленными в (iv), имеем

$$huqvh \xRightarrow{*} huqh \xRightarrow{*} huq'h \xRightarrow{*} hq'h. \quad (2)$$

Пусть теперь T , имея инструкцию q_0 , начинает обозревать самый левый символ из $\ulcorner x \urcorner$ (вся остальная лента пустая). Соответствующим словом Поста будет $hq_0 \ulcorner x \urcorner h$. Вначале предположим, что T когда-нибудь остановится. Тогда, как это объяснялось выше (в частности, (2)), имеем

$$hq_0 \ulcorner x \urcorner h \xRightarrow{\Pi(T)} huqvh \xRightarrow{\Pi(T)} hq'h.$$

Обратно, если

$$hq_0 \vdash x^\top h \xRightarrow[\Pi(T)]{} hq'h,$$

то в последовательности

$$hq_0 \vdash x^\top h = u_1 \Rightarrow u_2 \Rightarrow \dots \Rightarrow u_n = hq'h$$

каждое u_i должно содержать ровно один q -символ (q -символами, конечно, являются $q_0, q_1, \dots, q_n, q, q'$), так как каждая продукция сохраняет это свойство. Продукции из (i), (ii) заменяют q_i на q_1 , а продукции из (iv) никогда не заменяют q_i . Следовательно, некоторая продукция из (iii) должна использоваться по крайней мере один раз (а значит, ровно один раз). Но отсюда следует, что T когда-либо остановится. Итак, доказана

2.4. Теорема. *Машина Тьюринга T , начавшая обозревать самый левый символ из $\vdash x^\top$ (вся остальная лента пустая) с инструкции q_0 , со временем остановится тогда и только тогда, когда*

$$hq_0 \vdash x^\top h \xRightarrow[\Pi(T)]{} hq'h.$$

Полагая $T = M$ и используя теорему 1.1, сразу получаем

2.5. Следствие. *Не существует алгоритма для определения того, будет ли выполняться для $x \in \mathbb{N}$*

$$hq_0 \vdash x^\top h \xRightarrow[\Pi(M)]{} hq'h.$$

В частности, имеем

2.6. Следствие. *Проблема слов для $\Pi(M)$ неразрешима.*

Закончим этот параграф некоторым техническим наблюдением про $\Pi(T)$, которое окажется полезным для нас в следующем параграфе.

2.7. Замечание. Если u — слово над алфавитом A , содержащее ровно один q -символ, то существует самое большее одна продукция $P \in \Pi(T)$ такая, что $u \Rightarrow_P v$ для некоторого слова v .

Это замечание отражает тот простой факт, что никакие две пятерки, начинающиеся с одинаковой пары ix , не могут входить в таблицу никакой машины Тьюринга.

§ 3. Полугруппы и группы

Мы уже замечали, что операция сцепления цепочек над алфавитом $A = \{a_1, \dots, a_k\}$ ассоциативна. На алгебраическом языке это выражается так: множество цепочек образует *полугруппу* относительно операции сцепления.

3.1. Определение. *Обратной к полутуэвской продукции $g \rightarrow \bar{g}$ является продукция $\bar{g} \rightarrow g$. Полутуэвский процесс Π на-*

зывается *туэвским процессом*, если для каждой $P \in \Pi$ обратная к P продукция также находится в Π .

Для любого полутуэвского процесса Π отношение $u \Rightarrow_\Pi^* v$, очевидно, рефлексивно и транзитивно. Если Π — туэвский процесс, то как только

$$u = u_1 \xRightarrow[\Pi]{} u_2 \xRightarrow[\Pi]{} \dots \xRightarrow[\Pi]{} u_n = v, \quad (3)$$

то ясно, что

$$v = u_n \xRightarrow[\Pi]{} u_{n-1} \xRightarrow[\Pi]{} \dots \xRightarrow[\Pi]{} u_1 = u,$$

так что отношение $u \Rightarrow_\Pi^* v$ также симметрично и, следовательно, является отношением эквивалентности, которое мы будем записывать как $u \sim_\Pi v$. Через $[u]$ мы будем обозначать класс эквивалентности, содержащий u . Ясно также, что как только (3) выполняется, то для всех слов w над A имеем

$$wu = wu_1 \xRightarrow[\Pi]{} wu_2 \xRightarrow[\Pi]{} \dots \xRightarrow[\Pi]{} wu_n = vw$$

и

$$uw = u_1w \xRightarrow[\Pi]{} u_2w \xRightarrow[\Pi]{} \dots \xRightarrow[\Pi]{} u_nw = vw.$$

Следовательно, если $u \sim_\Pi v$ и $u' \sim_\Pi v'$, то имеем

$$uu' \sim_\Pi vu' \sim_\Pi vv'.$$

Таким образом, записав

$$[u] \cdot [u'] = [uu'],$$

видим, что это произведение корректно определено, и так как эта операция ассоциативна, то получившаяся система является полугруппой.

Если S — полугруппа, определенная таким путем, то туэвский процесс Π называется *представлением S* . Каждая пара $\langle g, \bar{g} \rangle$ такая, что $g \rightarrow \bar{g}$ (а значит, и $\bar{g} \rightarrow g$) является продукцией из Π , называется *соотношением представления* и обычно записывается как $g \sim \bar{g}$ (или даже $g = \bar{g}$). Наконец, символы, принадлежащие A , называются *образующими представления*. Конечно, данная абстрактная полугруппа вполне может иметь много различных представлений (или ни одного).

Если Π — полутуэвский процесс, мы обозначаем через $\bar{\Pi}$ туэвский процесс, полученный из Π добавлением всех обратных продукций к продукциям из Π . Имеет место

3.2. Лемма (Пост [3]). *Для любой машины Тьюринга T $\Pi \in \mathbb{N}$ имеем*

$$hq_0 \vdash x^\top h \xRightarrow[\Pi(T)]{} hq'h$$

тогда и только тогда, когда

$$hq_0 \Gamma x \Gamma h \sim_{\bar{\Pi}(T)} hq'h.$$

Доказательство. Так как $\Pi(T) \subseteq \bar{\Pi}(T)$, то лемма очевидна в одном направлении.

Обратно, пусть

$$hq_0 \Gamma x \Gamma h = u_1 \Rightarrow_{\bar{\Pi}(T)} u_2 \Rightarrow_{\bar{\Pi}(T)} \dots \Rightarrow_{\bar{\Pi}(T)} u_n = hq'h.$$

Допустим, что

$$u_1 \Rightarrow_{P_1} u_2 \Rightarrow_{P_2} \dots \Rightarrow_{P_{i-1}} u_i \Rightarrow_{P_i} u_{i+1} \Rightarrow_{P_{i+1}} u_{i+2} \Rightarrow_{P_{i+2}} \dots \Rightarrow_{P_{n-1}} u_n,$$

где $P_{i+1}, \dots, P_{n-1} \in \Pi(T)$, но $P_i \notin \Pi(T)$. Так как никакая продукция из $\Pi(T)$ не может быть применима к $hq'h$, то никакая обратная продукция к такой продукции не может дать $hq'h$ как результат, т. е. $i < n-1$. Ясно, что каждое слово $u_1 \dots u_n$ содержит только один q -символ, так как продукции из $\bar{\Pi}(T)$ сохраняют это свойство. Пусть Q — обратная продукция к P_i , так что $Q \in \Pi(T)$ и $u_{i+1} \Rightarrow_Q u_i$. Так как также $u_{i+1} \Rightarrow_{P_{i+1}} u_{i+2}$ и $P_{i+1} \in \Pi(T)$, то из замечания 2.7 следует, что $u_i = u_{i+2}$. Следовательно, мы имеем

$$u_1 \Rightarrow_{P_1} u_2 \Rightarrow_{P_2} \dots \Rightarrow_{P_{i-1}} u_i \Rightarrow_{P_{i+2}} u_{i+3} \Rightarrow_{P_{i+3}} \dots \Rightarrow_{P_{n-1}} u_n,$$

и продукция P_i элиминируется. Повторяя этот процесс, можно элиминировать все продукции, которые не принадлежат $\Pi(T)$, и прийти к требуемому заключению. $\square$

Учитывая следствия 2.5 и 2.6, получаем

3.3. Следствие (Пост [3]). Не существует алгоритма для определения того, будет ли для данного $x \in \mathbb{N}$ иметь место

$$hq_0 \Gamma x \Gamma h \sim_{\bar{\Pi}(M)} hq'h.$$

3.4. Следствие (Пост [3], Марков [1]). Существует представление полугруппы с неразрешимой проблемой слов.

Проблема слов для полугрупп была впервые рассмотрена Туэ [1] задолго до того, как в теории рекурсии стала упоминаться возможность отрицательного решения. Это был исторически первый пример проблемы разрешимости, первоначальная формулировка которой не относилась к логике и для которой был доказан результат о неразрешимости.

Теперь обратимся к одному важному специальному виду представлений полугрупп. Пусть A содержит четное число символов:

$$A = \{a_1, \dots, a_k, b_1, \dots, b_k\},$$

а соотношения туэвского процесса Π содержат все соотношения

$$a_i b_i \sim \Lambda, \quad i = 1, 2, \dots, k.$$

(Конечно, в общем случае Π будет содержать и другие соотношения.) В этом случае Π называется групповым представлением и (как легко заметить) в действительности представляет группу. Об абстрактной группе G , которая имеет групповое представление, будем говорить как о конечно представимой группе. Особое внимание обращается на проблему слов для групповых представлений (или, как говорят, *проблему слов для групп*) вследствие ее важности в алгебраической топологии. Крупнейшим научным открытием является теорема Новикова — Буна, которая утверждает существование группового представления с неразрешимой проблемой слов. К сожалению, недостаток места не позволяет нам здесь дать доказательство этой теоремы. Мы отсылаем интересующегося читателя к Буну [1] (работа основана на конструкции $\bar{\Pi}(M)$), Новикову [1], Бриттону [1], Ротману [1], глава 12, и Маккензи и Томпсону [1]. Последняя из упомянутых статей имеется в книге Бун, Каннонито и Линдона [1], в которой имеется богатый интересный материал и библиография этого направления.

3.5. Определение. Мы скажем, что абстрактная группа G рекурсивно представима, если существуют такие элементы $c_1, \dots, c_k \in G$, что:

(i) любой элемент G представим в виде произведения элементов $c_1, \dots, c_k, c_1^{-1}, \dots, c_k^{-1}$, т. е. $c_1, \dots, c_k$ порождают группу G ;

(ii) множество W всех слов w алфавита $\{c_1, \dots, c_k, c_1^{-1}, \dots, c_k^{-1}\}$ таких, что соответствующий слову w элемент $[w]$ группы G равен единице группы G , рекурсивно перечислимо.

Конечно, нет никаких трудностей говорить о рекурсивной перечислимости множеств слов конечного алфавита $A = \{a_1, \dots, a_k\}$, $k > 1$. Для этого можно использовать либо прямо машины Тьюринга, либо естественную нумерацию v множества A^* всех слов алфавита A : если $n \in \mathbb{N}$ и $n+1$ представлено в виде $n+1 = i_0 + i_1 k + \dots + i_{s-1} k^{s-1} + i_s k^s$, $0 \leq i_j < k$, $j = 0, \dots, s$, $i_s \neq 0$, то $v n = a_{i_0+1} \dots a_{i_{s-1}+1}$ (если $s = 0$, то $v n = \Lambda$); назовем $W \subseteq A^*$ рекурсивно перечислимым, если множество $R = \{n: v n \in W\}$ рекурсивно перечислимо *).

*) Определение рекурсивно представимой группы у автора имеет некоторые неточности. По этой причине данный текст слегка модифицирован. — Прим. ред.

Теорема Новикова — Буна является простым следствием следующей теоремы:

3.6. Теорема (Хигмен [1]). *Группа является рекурсивно представимой тогда и только тогда, когда она изоморфна подгруппе некоторой конечно представимой группы.*

Эта удивительная теорема показывает, что некоторое теоретико-рекурсивное понятие (каким является понятие рекурсивно представимой группы) эквивалентно чисто алгебраическому понятию. Упрощенное доказательство теоремы Хигмена можно найти в книге Шенфилда [1], Приложение, у Ондеро [1] и у Ротмана [1], глава 12.

Будем говорить, что класс G групп:

(i) *инвариантен*, если из того, что $G \in G$ и H изоморфна G , следует, что $H \in G$;

(ii) *нетривиален*, если существуют конечно представимые группы G и H такие, что $G \in G$ и $H \notin G$;

(iii) *наследствен*, если из того, что $G \in G$ и H — подгруппа G , следует, что $H \in G$.

Показано, что справедлива

3.7. Теорема (Адяна [1], Рабин [1]). *Пусть G — класс групп, который инвариантен, нетривиален и наследствен. Тогда не существует алгоритма, с помощью которого для представления группы можно определять, будет эта группа принадлежать G или нет.*

Например, пусть G содержит лишь тривиальную группу $\{e\}$. Получаем

3.8. Следствие. *Не существует алгоритма, с помощью которого можно было бы определять по представлению группы, будет эта группа иметь по крайней мере один отличный от e элемент или нет.*

Другими групповыми свойствами, к которым может быть применена теорема Адяна — Рабина, являются следующие:

- (i) цикличность;
- (ii) конечность;
- (iii) свобода;
- (iv) коммутативность;
- (v) разрешимость.

Доказательство теоремы Адяна — Рабина использует существование группового представления с неразрешимой проблемой слов, т. е. теорему Новикова — Буна.

Используя прямую конструкцию (Хакен [1]), можно построить по данному групповому представлению группы G 2-мерный симплициальный комплекс, имеющий своей фундаментальной группой группу G . Так как симплициальный комплекс односвязен лишь в случае, когда его фундаментальная группа

тривиальна, т. е. содержит только единицу, из следствия 3.8 получаем

3.9. Следствие. *Не существует алгоритма для определения по данному 2-мерному симплициальному комплексу, будет он односвязным или нет.*

Используя намного более сложную и трудную конструкцию, Марков [2] показал, как для данного группового представления Π построить для каждого $n \geq 4$ пару симплициальных комплексов $M_1(\Pi)$, $M_2(\Pi)$, являющихся n -мерными многообразиями такими, что $M_1(\Pi)$ и $M_2(\Pi)$ гомеоморфны тогда и только тогда, когда группа, которую представляет Π , тривиальна. Снова используя следствие 3.8, заключаем, что справедлива

3.10. Теорема. *Проблема гомеоморфизма для многообразий размерности ≥ 4 неразрешима.*

Решение проблемы гомеоморфизма для двумерных многообразий — классический результат, восходящий к Риману. Для трехмерных многообразий проблема открыта. Дальнейшее обсуждение топологических проблем разрешимости можно найти в статьях Буна, Хакена и Поэнару [1] и Хакена [1].

§ 4. Другие комбинаторные проблемы

Один из самых ранних примеров неразрешимой проблемы чисто комбинаторной природы был дан Постом [2], это так называемая *проблема соответствия*. Как оказалось позднее, эта проблема нашла интересные приложения к формальной теории языков.

4.1. Определение. *Система соответствия Поста* состоит из алфавита A и конечного множества упорядоченных пар $\langle h_i, k_i \rangle$, $i = 1, \dots, m$, слово u над A называется *решением* этой системы, если для некоторой последовательности $1 \leq i_1, i_2, \dots, i_m \leq m$ (i_j не обязаны быть различными) имеем

$$u = h_{i_1} h_{i_2} \dots h_{i_n} = k_{i_1} k_{i_2} \dots k_{i_n}.$$

Пусть нам дан полутуэвский процесс Π , а u, v — пара слов над алфавитом для Π . Покажем, как построить по Π , u и v систему соответствия Поста, имеющую решение тогда и только тогда, когда $u \Rightarrow_{\Pi}^* v$. Тогда, используя следствие 2.6, мы сможем заключить, что имеет место

4.2. Теорема. *Не существует алгоритма для определения того, будет ли иметь решение данная система соответствия Поста.*

Доказательство. Доказательство 4.2, данное здесь, принадлежит Флойду (не опубликовано); оно значительно проще, чем первоначальное доказательство Поста. Оно также может быть найдено у Ясухарты [1].

Приступим к требуемой конструкции. Пусть Π — полутуэвский процесс над алфавитом $A = \{a_1, \dots, a_n\}$, а u и v — слова над A . Построим систему соответствия Поста над алфавитом

$$B = \{a_1, \dots, a_n, a'_1, \dots, a'_n, [,], *, *\}',$$

содержащим $2n + 4$ символа. Для всякого слова w над A мы обозначаем через w' слово, полученное из w приписыванием после каждого символа из w .

Пусть продукциями Π будут $g_i \rightarrow \bar{g}_i$, $i = 1, 2, \dots, k$, и предположим, что среди этих продукций встречаются все n «тождественных» продукций $a_i \rightarrow a_i$, $i = 1, 2, \dots, n$. Это последнее предположение не ограничивает общности (т. е. класс пар $\langle r, s \rangle$, для которых $r \Rightarrow_{\Pi}^* s$, никак не изменится, если включить тождественные продукции). Однако теперь можно утверждать, что $u \Rightarrow_{\Pi}^* v$ тогда и только тогда, когда мы можем написать

$$u = u_1 \xRightarrow{\Pi} u_2 \xRightarrow{\Pi} \dots \xRightarrow{\Pi} u_m = v,$$

где m — нечетное число. Система соответствия Поста над алфавитом B будет состоять из пар:

$$\begin{aligned} & \langle [u*, [\rangle, \quad \langle *, *\rangle, \quad \langle *, *\rangle, \\ & \left\{ \begin{array}{l} \langle \bar{g}_j, g'_j \rangle, \\ \langle g'_j, g_j \rangle, \end{array} \right\} \quad j = 1, 2, \dots, k; \quad \langle], *\rangle \end{aligned}$$

Теперь пусть

$$u = u_1 \xRightarrow{\Pi} u_2 \xRightarrow{\Pi} \dots \xRightarrow{\Pi} u_m = v,$$

где m — нечетное число. Тогда слово

$$w = [u_1 * u'_2 *' u'_3 *' \dots *' u'_{m-1} *' u_m]$$

является решением P , как легко следует из двух разложений

$$\begin{aligned} w &= [u_1 * [u'_2 *' [u'_3 *' \dots [\\ &= [[u_1 * [u'_2 *' \dots [*' u_m]. \end{aligned}$$

Чтобы увидеть, например, что $u'_2 *'$ соответствует $u_1 *$, заметим, что можно написать $u_1 = r g_1 s$, $u_2 = r \bar{g}_1 s$ для некоторого $j = 1, 2, \dots, k$. Тогда $u'_2 = r' \bar{g}'_1 s'$ и соответствие становится очевидным (напомним, что продукции $a_1 \rightarrow a_1, \dots, a_n \rightarrow a_n$ даны в Π).

Обратно, если $\bar{w}$ — решение, то, чтобы обеспечить согласование крайнего левого и правого символов между штрихованными и нештрихованными символами, $\bar{w}$ должно начинаться с $[$.

и кончаться на $]$. Следовательно, обозначив через w часть $\bar{w}$, идущую до первой $]$,

$$w = [u * \dots *' v],$$

получим прежде всего соответствия

$$w = [u * [\dots *' v]],$$

$$w = [[u * \dots [*' v].$$

Поэтому $u *$ должно соответствовать некоторому $r' *$, а $*' v$ — некоторому $* s'$, где $u \Rightarrow_{\Pi}^* r$ и $s \Rightarrow_{\Pi}^* v$. Продолжая этот процесс, мы придем к $u \Rightarrow_{\Pi}^* v$. Это заканчивает конструкцию, а вместе с ней и доказательство теоремы 4.2. $\square$

В формальной теории языков имеют дело с алфавитами $A = V \cup T$, где элементы из V (обычно записываемые большими буквами) называются *переменными*, а элементы из T называются *заключениями*. Если один из элементов V (обычно обозначаемый через S) выделен как *начальный символ*, то полутуэвский процесс Π над A называется *фразовой структурной грамматикой*, а множество всех слов v над подалфавитом T таких, что $S \Rightarrow_{\Pi}^* v$, называется *языком*, *порожденным Π* , и обозначается через $L(\Pi)$.

Интуитивно мы можем смотреть на переменные как на представления грамматических категорий. Например, пусть $V = \{S, U, P, N, J, R, D\}$, где мы можем истолковать эти буквы как представления следующих категорий: предложение, подлежащее, сказуемое, существительное, прилагательное, глагол, наречие соответственно. Пусть T состоит из (строчных) букв английского алфавита, дополненных знаками « $\#$ » (для «пробелов») и « $\cdot$ ». Здесь указана некоторая примитивная английская грамматика G :

$S \rightarrow UP,$	$N \rightarrow \text{man}$
$U \rightarrow \text{the} \# N \#$	$N \rightarrow \text{woman}$
$U \rightarrow \text{the} \# J \# N \#$	$J \rightarrow \text{good}$
$P \rightarrow R$	$J \rightarrow \text{bad}$
$P \rightarrow R \# D$	$R \rightarrow \text{runs}$
	$R \rightarrow \text{walks}$
	$D \rightarrow \text{quickly}$
	$D \rightarrow \text{slowly}$

Читатель легко проверит, что

$$S \xRightarrow{G} \text{the} \# \text{bad} \# \text{man} \# \text{runs} \# \text{quickly},$$

так что эта последняя фраза есть в языке, порожденном G .

4.3. Определение. Грамматика называется *контекстно свободной*, если все ее productions имеют вид $A \rightarrow g$, где A — какая-либо переменная.

Итак, наша грамматика G контекстно свободна. Покажем, как связывать с системой соответствия Поста некоторую контекстно свободную грамматику. Пусть $\langle h_i, k_i \rangle, i = 1, 2, \dots, m$, — система соответствия Поста над алфавитом A . Построим пару G_1, G_2 контекстно свободных языков, заключения которых состоят из A и m новых символов $c_1, \dots, c_m$.

Далее, алфавит для G_1 имеет единственную переменную S_1 в качестве начального символа, а G_2 — единственную переменную S_2 в качестве начального символа. Productions G_1 будут

$$\left. \begin{array}{l} S_1 \rightarrow h_i S_1 c_i, \\ S_1 \rightarrow h_i c_i, \end{array} \right\} \quad i = 1, 2, \dots, m,$$

а productions G_2 будут

$$\left. \begin{array}{l} S_2 \rightarrow k_i S_2 c_i, \\ S_2 \rightarrow k_i c_i, \end{array} \right\} \quad i = 1, 2, \dots, m.$$

Таким образом,

$$L(G_1) = \{h_{i_1} h_{i_2} \dots h_{i_m} c_{i_m} \dots c_{i_2} c_{i_1}\}$$

и

$$L(G_2) = \{k_{i_1} k_{i_2} \dots k_{i_m} c_{i_m} \dots c_{i_2} c_{i_1}\}.$$

Сразу получается

4.4. Лемма. Для данной системы соответствия Поста имеется решение тогда и только тогда, когда $L(G_1) \cap L(G_2) \neq \emptyset$.

Из теоремы 4.2 заключаем, что справедлива

4.5. Теорема. Не существует алгоритма для определения того, будет ли $L(\Pi_1) \cap L(\Pi_2) = \emptyset$ для данной пары контекстно свободных грамматик Π_1 и Π_2 .

4.6. Определение. Фразовая структурная грамматика Π с начальным символом S называется *двусмысленной*, если для некоторого слова $u \in L(\Pi)$ имеем

$$S \underset{\Pi}{\Rightarrow} u_1 \underset{\Pi}{\Rightarrow} u_2 \underset{\Pi}{\Rightarrow} \dots \underset{\Pi}{\Rightarrow} u_k = u$$

и

$$S \underset{\Pi}{\Rightarrow} v_1 \underset{\Pi}{\Rightarrow} v_2 \underset{\Pi}{\Rightarrow} \dots \underset{\Pi}{\Rightarrow} v_l = u,$$

где последовательности $\langle u_1, \dots, u_k \rangle$ и $\langle v_1, \dots, v_l \rangle$ не одинаковы.

Теперь пусть G_1 и G_2 такие, как выше. Пусть G имеет те же самые заключения, что G_1 и G_2 , переменные S, S_1, S_2 (S — начальный символ) и productions $S \rightarrow S_1, S \rightarrow S_2$ вместе с продук

циями из G_1 и G_2 . Тогда ясно, что $L(G) = L(G_1) \cup L(G_2)$. Так как G_1 и G_2 сами не являются двусмысленными, то легко видеть, что G будет двусмысленной только в случае, когда есть слово u , принадлежащее одновременно $L(G_1)$ и $L(G_2)$.

С помощью доказательства теоремы 4.5 получается

4.7. Теорема. Не существует алгоритма, посредством которого мы могли бы определить, будет ли двусмысленной данная контекстно свободная грамматика.

Другие примеры неразрешимых проблем в формальной теории языков и дальнейшие ссылки можно найти у Хопкрофта и Аллена [1]. Патерсон [1] показал, используя неразрешимость проблемы соответствия Поста, что не существует алгоритма, который можно было бы использовать для определения для данного конечного множества 3×3 -матриц с целыми коэффициентами, будет ли некоторое конечное произведение элементов этого множества равно нулевой матрице.

Другой комбинаторной проблемой, которая оказалась неразрешимой, является *таг-проблема*, впервые рассмотренная Э. Л. Постом в 1920 г. См. Пост [1], [4]. *Таг-система* задается с помощью алфавита $A = \{a_1, \dots, a_n\}$, слов $g_1, \dots, g_n$ и положительного числа k . Для такой таг-системы T мы записываем $u \Rightarrow_T v$, если u начинается с a_i , а v получается из u дописыванием g_i с правого конца и зачеркиванием первых k символов из u . (Конечно, возможно, что $v = \Lambda$.) Как и раньше, мы пишем $u \Rightarrow_T^* v$, если $u = u_1 \Rightarrow_T u_2 \Rightarrow_T \dots \Rightarrow_T u_n = v$ для слов $u_1, \dots, u_n$ и некоторого $n \geq 1$, и считаем проблемой слов для T проблему определения для данных u и v , будет ли $u \Rightarrow_T^* v$. Минский [1], [2] показал, как построить таг-систему с неразрешимой проблемой слов.

§ 5. Диофантовы уравнения

Мы уже упоминали десятую проблему Гильберта (см. введение), в которой спрашивается про алгоритм определения для полиномиальных уравнений $P(x_1, \dots, x_n) = 0$ (с целыми коэффициентами), обладают ли они решением в целых числах. В этом параграфе будет более удобно работать с неотрицательными целыми решениями, т. е. решениями в $\mathbb{N}$. Поэтому сразу начнем с замечания, что если не существует алгоритма определения для полиномиальных уравнений, обладают ли они решениями в $\mathbb{N}$, то отсюда сразу следует, что не существует алгоритма, который мог бы быть использован для ответа и о целых решениях. Действительно, если у нас есть алгоритм, который мог бы быть использован для целых решений (т. е. решал бы десятую проблему Гильберта), то мы могли бы использовать

его для решения вопроса о том, будет ли $P(x_1, \dots, x_n) = 0$ иметь решение в $\mathbb{N}$, с помощью простой проверки: будет ли

$$P(u_1^2 + v_1^2 + y_1^2 + z_1^2, \dots, u_n^2 + v_n^2 + y_n^2 + z_n^2) = 0$$

иметь целые решения. (Это так, потому что каждое неотрицательное целое число есть сумма четырех квадратов.)

Наши рассуждения будут связаны с понятием диофантова множества.

5.1. Определение. k -местный предикат R на $\mathbb{N}$ называется *диофантовым*, если для некоторого полинома $P(x_1, \dots, x_k, y_1, \dots, y_n)$ с целыми коэффициентами имеем

$$R = \{ \langle x_1, \dots, x_k \rangle : \exists y_1 \dots y_n \in \mathbb{N} [P(x_1, \dots, x_k, y_1, \dots, y_n) = 0] \}.$$

Пусть R — диофантов предикат, а $g_R: \mathbb{N}^k \rightarrow \mathbb{N}$ определяется так: $g_R(x_1, \dots, x_k) = 0$, если $\langle x_1, \dots, x_k \rangle \in R$, и $g_R(x_1, \dots, x_k)$ не определено в противном случае. Если предикат R связан с полиномом P так, как указано в 5.1, то алгоритм для вычисления частичной функции g_R состоит в эффективном упорядочивании всех n -ок $\langle y_1, \dots, y_n \rangle$ в подходящую последовательность и в последовательном вычислении $P(x_1, \dots, x_k, y_1, \dots, y_n)$, пока (если это вообще случится) не получится значение 0. Используя тезис Чёрча, мы делаем вывод, что g_R — частично рекурсивная функция, и, следовательно, имеется машина Тьюринга, вычисляющая g_R . Таким образом, по определению 1.3 заключаем, что R рекурсивно перечислим.

5.2. Теорема. *Каждый диофантов предикат р.п.*

Основная теорема этого направления состоит в доказательстве обратного утверждения:

5.3. Теорема (Матиясевич [1]). *Каждый р.п. предикат диофантов.*

Детальное доказательство теоремы 5.3 и историческая справка могут быть найдены в обзорной статье Девиса [4] (в которой, однако, рекурсивные функции не определяются в терминах машин Тьюринга); различные модификации этой теоремы рассматриваются в статье Девиса, Матиясевича и Робинсон [1]. Мы также отсылаем читателя к этим статьям за дальнейшими ссылками.

Перед обсуждением доказательства теоремы 5.3 рассмотрим некоторые ее следствия. Используя теоремы 5.3 и 1.5, получаем

5.4. Следствие. *Существует диофантово множество K , которое не рекурсивно.*

Записав

$$K = \{x: \exists y_1 \dots y_n [P(x, y_1, \dots, y_n) = 0]\},$$

видим, что не может существовать алгоритма определения для каждого из уравнений

$$P(0, y_1, \dots, y_n) = 0,$$

$$P(1, y_1, \dots, y_n) = 0,$$

$$\dots$$

имеет ли оно решение в $\mathbb{N}$. Следовательно, десятая проблема Гильберта неразрешима.

Для любого полинома $P(x_1, \dots, x_k)$ обозначаем через $\#(P)$ кардинальное число множества k -ок элементов из $\mathbb{N}$, которые удовлетворяют уравнению $P = 0$. Таким образом, $0 \leq \#(P) \leq \aleph_0$. Назовем множество кардинальных чисел $\leq \aleph_0$ *нетривиальным*, если это множество не пусто и не содержит всех кардинальных чисел $\leq \aleph_0$. Тогда доказывается

5.5. Теорема (Девис [3]). *Для данного нетривиального множества A кардинальных чисел $\leq \aleph_0$ не существует алгоритма, который можно было бы использовать для определения по данному полиному P , будет ли $\#(P) \in A$.*

Таким образом, не существует алгоритма для определения того, будет ли диофантово уравнение иметь четное число решений, бесконечное число решений и т. д. При доказательстве будет использоваться упрощенный вариант, принадлежащий Смюринскому (см. также Девис, Матиясевич и Робинсон [1]).

Итак, для каждого полинома $P(x_1, \dots, x_k)$ будем писать

$$T^+(P) = P(x_1, \dots, x_k) \cdot [(x_1 - a_1)^2 + \dots + (x_k - a_k)^2],$$

где $\langle a_1, \dots, a_k \rangle$ — первый (в любом подходящем упорядочении) кортеж длины k , который не удовлетворяет $P = 0$. Таким образом,

$$\#(T^+(P)) = \#(P) + 1.$$

Полагая $T^0(P) = P$, $T^{m+1}(P) = T^+(T^m(P))$, получаем

$$\#(T^m(P)) = \#(P) + m.$$

Наконец, пишем

$$T^\infty(P) = (u + 1) \cdot P,$$

где u — переменная, не встречающаяся в P . Имеем

$$\#(T^\infty(P)) = \begin{cases} 0, & \text{если } \#(P) = 0, \\ \aleph_0, & \text{если } \#(P) \neq 0. \end{cases}$$

Для доказательства 5.5 рассмотрим следующие случаи:

Случай 1. $A = \{0\}$. Это в точности задача определения того, будет ли диофантово уравнение иметь решение; эта задача, как мы видели, неразрешима.

Случай 2. $0, \aleph_0 \in A$. Пусть $m \notin A$. Тогда
 $\#(P) = 0 \leftrightarrow \#(T^m(T^\infty(P))) \notin A$.

Следовательно, алгоритм для этого случая порождает алгоритм для случая 1.

Случай 3. $0 \in A, \aleph_0 \notin A$. Тогда
 $\#(P) = 0 \leftrightarrow \#(T^\infty(P)) \in A$,

и мы сразу сводим все снова к случаю 1.

Случай 4. $0 \notin A$. Тогда множество B кардинальных чисел $\leq \aleph_0$, не лежащих в A , удовлетворяет либо случаю 2, либо случаю 3. Но алгоритм для решения $\#(P) \in A$ эквивалентен алгоритму для решения $\#(P) \in B$.

Используя теорему о нормальной форме (ЭТР, 4.1), т. е. существование универсальной машины Тьюринга, мы приходим к выводу, что существует диофантово уравнение $P(i, x, y_1, \dots, y_k) = 0$, которое универсально в том смысле, что, полагая

$$D_i = \{x: \exists y_1 \dots y_k [P(i, x, y_1, \dots, y_k) = 0]\},$$

получим последовательность $D_0, D_1, D_2, \dots$ всех диофантовых подмножеств множества $\mathbb{N}$. Проводились интересные исследования по нахождению наилучшего значения k в этом результате. В статье Матиясевича и Робинсон [1] показано, что можно взять $k = 13$; позднее Матиясевич объявил, что этот результат может быть улучшен до $k = 9$.

Сейчас уместно рассмотреть проблему разрешимости, неразрешимость которой была доказана на раннем этапе развития этой области (Чёрч [1], Тьюринг [1]), а именно, неразрешимость проблемы определения для конечного множества предложений T и предложения ϕ логики первого порядка, будет ли $T \vdash \phi$ в логике первого порядка, см. вводную главу 1 «Теории моделей». Так Гильберт провозгласил, что эта самая проблема, называемая *Entscheidungsproblem*, является самой фундаментальной проблемой математической логики, так как процедура для ее решения могла бы, видимо, быть использована для алгоритмического решения всех математических вопросов. (См. обсуждение программы Гильберта в § 5 главы 1 «Теории моделей».) По этой причине всякий, кто знает, что существуют неразрешимые математические проблемы, мог бы надеяться доказать неразрешимость и *Entscheidungsproblem*. Мы увидим, как это можно легко сделать, используя неразрешимость десятой проблемы Гильберта.

Рассмотрим язык

$$L = \{+, \cdot, 0, 1\},$$

где $0, 1$ — символы констант, $+$ и $\cdot$ — символы двухместных функций. Тогда система $\mathbb{N} = \langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ является системой

в языке L . Далее, по всякому диофантову уравнению $P = 0$ легко построить предложение ϕ языка L вида $\exists y_1 \dots \exists y_k (t_1 = t_2)$, где t_1, t_2 — термы такие, что $\mathbb{N} \models \phi$ тогда и только тогда, когда уравнение $P = 0$ разрешимо. Пусть T — множество предложений:

$$\begin{aligned} ((0 + 1) &= 1), \\ \forall x ((x + 0) &= x), \\ \forall x \forall y ((x + (y + 1)) &= ((x + y) + 1)), \\ \forall x ((x \cdot 0) &= 0), \\ \forall x \forall y ((x \cdot (y + 1)) &= ((x \cdot y) + x)). \end{aligned}$$

Тогда ясно, что для любого уравнения θ между термами языка L , не содержащими переменных, $\mathbb{N} \models \theta$ тогда и только тогда, когда $T \vdash \theta$, так как T , очевидно, достаточно, чтобы проводить конкретные вычисления в $\mathbb{N}$. Наконец, используя соответствующее правило вывода логики первого порядка для введения кванторов существования, получаем

$T \vdash \phi$ тогда и только тогда, когда $P = 0$ имеет решение.

Из неразрешимости десятой проблемы Гильберта немедленно следует, что *Entscheidungsproblem* для L неразрешима. Более сильные результаты можно найти у Кар, Мура и Вана [1] и Ондеро и Льюиса [1].

Теперь обсудим доказательство теоремы 5.3. Ясно, что так как

$$P_1 = 0 \wedge P_2 = 0 \leftrightarrow P_1^2 + P_2^2 = 0,$$

$$P_1 = 0 \vee P_2 = 0 \leftrightarrow P_1 \cdot P_2 = 0,$$

то класс диофантовых предикатов замкнут относительно объединения и пересечения. По этой причине диофантовы «определения» могут комбинироваться с помощью $\vee$, $\wedge$ и кванторов существования, чтобы получать новые определения диофантовых предикатов. Ясно также, что предикаты $x < y$, $x \leq y$, $x \equiv y \pmod{z}$ диофантовы, так как

$$x < y \leftrightarrow \exists z (x + z + 1 = y),$$

$$x \leq y \leftrightarrow \exists z (x + z = y),$$

$$x \equiv y \pmod{z} \leftrightarrow \exists t (x + tz = y \vee y + tz = x).$$

Дальнейшими шагами в доказательстве теоремы 5.3 являются следующие:

(i) Предикат $z = x^y$ диофантов. Этот ключевой шаг был исторически самым поздним. Мы не будем доказывать его здесь, а отсылаем читателя к любому из следующих детальных доказательств: Матиясевич [2], Девис [2], [4], Матиясевич и Робинсон [1].

(ii) Предикаты $m = C_n^k$, $m = n!$ диофантовы. Пусть $\Phi(k, u, w)$ означает коэффициент при u^k в разложении w по степеням u . Тогда предикат

$$q = \Phi(k, u, w)$$

является диофантовым. Действительно, этот предикат может быть выражен как одновременная выполнимость в $\mathbb{N}$ условий:

$$\begin{aligned} w &= p + qu^k + r, \\ q &< u, \quad p < u^k, \\ r &\equiv 0 \pmod{u^{k+1}}. \end{aligned}$$

Теперь, если $u > 2^n$, то разложение

$$(u+1)^n = \sum_{i=0}^n C_n^i u^i$$

показывает, что C_n^k есть в точности коэффициент при u^k в разложении $(u+1)^n$ по степеням u . Следовательно,

$$m = C_n^k \leftrightarrow m = \Phi(k, 2^n + 1, ((2n+1) + 1)^n),$$

так что $m = C_n^k$ диофантов.

Элементарные неравенства показывают, что когда $r \gg (2n)^{n+1}$, имеем

$$n! < \frac{r^n}{C_n^n} < n! + 1.$$

(По поводу деталей можно, например, посмотреть Девис [4].) Следовательно,

$$m = n! \leftrightarrow \exists r \exists s \exists t \exists u \{s = 2n + 1 \wedge r = s^{n+1}$$

$$\wedge t = r^n \wedge u = C_r^n \wedge ut < t < u(m+1)\}.$$

(iii) Теорема об ограниченном кванторе. Пусть $P(u, x, y, h, z_1, \dots, z_n)$ — полином. Тогда существует полином $Q(u, x, y)$ такой, что

$$\forall k \leq x \exists z_1 \dots z_n \leq y [P(u, x, y, k, z_1, \dots, z_n) = 0]$$

$$\leftrightarrow \exists b_1 \dots b_n [C_{b_1}^{y+1} \equiv \dots \equiv C_{b_n}^{y+1}$$

$$\equiv P(u, x, y, Q! - 1, b_1, \dots, b_n) \equiv 0 \pmod{C_{Q!-1}^{x+1}}].$$

Это является некоторым усовершенствованием одного результата из статьи Девиса, Патнема и Робинсон [1]. Доказательство может быть найдено в статье Девиса, Матиясевича и Робинсон [1], с. 244.

(iv) Теперь имеет место

5.6. Теорема. Пусть R — диофантов предикат и

$$\langle x_1, \dots, x_k, x \rangle \in S \leftrightarrow \forall t \leq x [\langle x_1, \dots, x_k, t \rangle \in R].$$

Тогда S диофантов.

Доказательство. Для подходящего полинома P имеем

$$\langle x_1, \dots, x_k, x \rangle \in S$$

$$\leftrightarrow \forall t \leq x \exists z_1 \dots z_n [P(t, x_1, \dots, x_k, z_1, \dots, z_n) = 0]$$

$$\leftrightarrow \exists y \forall t \leq x \exists z_1 \dots z_n \leq y [P(t, x_1, \dots, x_k, z_1, \dots, z_n) = 0],$$

так как граница y может быть выбрана как наибольшее из $n(x+1)$ целых чисел. Результат следует из (ii) и (iii). $\square$

(v) Теперь пусть P будет произвольным k -местным р.п. предикатом. Пусть T — машина Тьюринга с инструкциями $q_0, \dots, q_v$ такая, что когда T начинает работу с q_0 , обозревая самый левый символ из $\ulcorner x_1 \urcorner 0 \ulcorner x_2 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$, она со временем останавливается тогда и только тогда, когда $\langle x_1, x_2, \dots, x_k \rangle \in P$. Пусть T' получается из T добавлением к ее таблице всех пятерок:

$$i\alpha \alpha P(v+1),$$

где $0 \leq i \leq v$ и таблица для T не содержит пятерок, начинающихся с $i\alpha$. Таким образом, $\langle x_1, \dots, x_k \rangle \in P$ тогда и только тогда, когда T' со временем встретит инструкцию q_{v+1} (и затем остановится), начав работу с q_0 и обозревая при этом самый левый символ из $\ulcorner x_1 \urcorner 0 \ulcorner x_2 \urcorner 0 \dots 0 \ulcorner x_k \urcorner$.

Будем кодировать конфигурации для T' тройками $\langle l, n, r \rangle$ натуральных чисел. Здесь n есть просто номер инструкции, которая выполняется, и l — код для последовательности из 0 и 1 на ленте слева от обозреваемой ячейки; конкретно, l есть натуральное число, двоичное представление которого есть эта последовательность (где, конечно, бесконечная последовательность из 0 слева не влияет на l). Аналогично r — натуральное число, двоичное представление которого есть последовательность 0 и 1, начинающаяся с обозреваемой ячейки и идущая от нее вправо, причем она читается справа налево. Так, например, тройка $\langle 13, 4, 19 \rangle$ представляет машинную конфигурацию, при которой на ленте записано

$$\dots 000110111001000 \dots,$$

обозреваемая ячейка, а также непосредственно примыкающие к ней слева и справа ячейки содержат 1, а исполняемая инструкция есть q_4 .

Начальная конфигурация для T' со входами $x_1, \dots, x_k$ представляется тройкой $\langle 0, 0, g_k(x_1, \dots, x_k) \rangle$, где

$$g_1(x) = 2^{x+1} - 1,$$

$$g_{k+1}(x_1, \dots, x_{k+1}) = 2g_k(x_2, \dots, x_{k+1}) + g_1(x_1).$$

Здесь, как легко доказать с помощью индукции, предикат $z = g_k(x_1, \dots, x_k)$ диофантов для каждого фиксированного k .

Пусть для пятерки Q из таблицы T' S_Q обозначает множество всех $\langle l, n, r, l', n', r' \rangle$ таких, что Q перерабатывает конфигурацию $\langle l, n, r \rangle$ в конфигурацию $\langle l', n', r' \rangle$. Мы хотим сейчас показать, что для каждой фиксированной пятерки Q множество S_Q является диофантовым.

Действительно, если Q имеет вид

$$\text{ia } \beta \Pi j,$$

то

$$\langle l, n, r, l', n', r' \rangle \in S_Q \leftrightarrow n = i \wedge n' = j \wedge l' = 2l + \beta \wedge r = 2r' + \alpha.$$

С другой стороны, если Q имеет вид

$$\text{ia } \beta \Pi j,$$

то

$$\begin{aligned} \langle l, n, r, l', n', r' \rangle \in S_Q \\ \leftrightarrow n = i \wedge n' = j \wedge [(l = 2l' \wedge r' = 2(r + \beta - \alpha) \\ \vee (l = 2l' + 1 \wedge r' = 2(r + \beta - \alpha) + 1)]. \end{aligned}$$

Пусть $Q_1, Q_2, \dots, Q_\mu$ — список всех пятерок из таблицы для машины T' и $S = \bigcup_{i=1}^{\mu} S_{Q_i}$. Следовательно, S — диофантово множество, а $\langle l, n, r, l', n', r' \rangle \in S$ только в том случае, когда некоторая пятерка для T' перерабатывает конфигурацию $\langle l, n, r \rangle$ в конфигурацию $\langle l', n', r' \rangle$.

Далее, всякое вычисление на T' есть последовательность конфигураций $\langle l_i, n_i, r_i \rangle$, $i = 0, 1, \dots, k+1$, таких, что $\langle l_i, n_i, r_i, l_{i+1}, n_{i+1}, r_{i+1} \rangle \in S$ для $i = 0, 1, \dots, k$ и $n_{k+1} = v + 1$. Мы будем считать l_i, n_i, r_i разрядами при достаточно большом основании B , т. е. полагаем

$$L = \sum_{i=0}^k l_i B^i, \quad N = \sum_{i=0}^k n_i B^i, \quad R = \sum_{i=0}^k r_i B^i.$$

Используя функцию Φ из (ii), наконец получаем

$$\begin{aligned} \langle x_1, \dots, x_k \rangle \in P \\ \leftrightarrow \exists BLNRK \{ \Phi(0, B, L) = 0 \wedge \Phi(0, B, N) = 0 \\ \wedge \Phi(0, B, R) = g_k(x_1, \dots, x_k) \wedge \Phi(k+1, B, N) = v+1 \\ \wedge \forall i \leq k [\langle \Phi(i, B, L), \Phi(i, B, N), \Phi(i, B, R), \\ \Phi(i+1, B, L), \Phi(i+1, B, N), \Phi(i+1, B, R) \rangle \in S] \}. \end{aligned}$$

Применив теорему 5.6, получаем, что P диофантов.

ЛИТЕРАТУРА

Лян С. И.

1. Алгоритмическая неразрешимость проблемы распознавания некоторых свойств групп. — ДАН СССР, 1955, 103, с. 533—535.

Бриттон (Britton J. L.)

1. The word problem. — Ann. Math., 1963, 77, p. 16—32.

Бун (Boone W. W.)

1. The word problem. — Ann. Math., 1959, 70, p. 207—265.

Бун, Каннито и Линдон (Boone W. W., Cannonito F. B., Lyndon R. C.)

1. Word Problems. — Amsterdam: North-Holland, 1973.

Бун, Хакен и Поэнару (Boone W. W., Haken W., Poenaru V.)

1. On recursively unsolvable problems in topology and their classification. — In: Contributions to Mathematical Logic/Ed. by H. N. Schmidt et al. Amsterdam: North-Holland, 1968, p. 37—74.

Девис (Davis M.)

1. The Undecidable. — Hewlett (N. Y.): Raven Press, 1965.
2. An explicit Diophantine definition of the exponential function. — Comm. Pure Appl. Math., 1971, 24, p. 137—145.
3. On the number of solutions of Diophantine equations. — Proc. Amer. Math. Soc., 1972, 35, p. 552—554.
4. Hilbert's Tenth Problem is unsolvable. — Amer. Math. Monthly, 1973, 80, p. 233—269.

Девис (Davis M.), Матиясевич Ю. В. и Робинсон (Robinson J.)

1. Hilbert's Tenth Problem. Diophantine equations: positive aspects of a negative solution. — Proc. Symposia Pure Math., 1976, 28, p. 223—378.

Девис, Патнем и Робинсон (Davis M., Putnam H., Robinson J.)

1. The decision problem for exponential Diophantine equations. — Ann. Math., 1961, 74, p. 425—436.

Кар, Мур и Ван (Kahr A. S., Moore E. F., Wang H.)

1. Entscheidungsproblem reduced to the $\forall \exists \forall$ case. — Proc. Nat. Acad. Sci. USA, 1962, 48, p. 365—377.

Маккензи и Томпсон (McKenzie R., Thompson R. J.)

1. An elementary construction of unsolvable word problem in group theory — In: Boone W. W., Cannonito F. B., Lyndon R. C. Word Problems. Amsterdam: North-Holland, 1973, p. 457—478.

Марков А. А.

1. Невозможность некоторых алгоритмов в теории ассоциативных систем. — ДАН СССР, 1947, 55, с. 587—590.
2. Неразрешимость проблемы гомеоморфизма. — В кн.: Proceedings of the International Congress of Mathematicians. London: Cambridge University Press, 1958, с. 300—306.

Матиясевич Ю. В.

1. Диофантовость перечислимых множеств. — ДАН СССР, 1970, 191, с. 279—282.
2. Диофантовы множества. — УМН, 1972, 27, с. 185—222.

Матиясевич Ю. В. и Робинсон (Robinson J.)

1. Reduction of an arbitrary Diophantine equation to one in 13 unknowns. — Acta Arithmetica, 1975, 27, p. 521—553.

Минский (Minsky M.)

1. Recursive unsolvability of Post's problem of tag and other topics in the theory of Turing machines. — Ann. Math., 1961, 74, p. 437—454.
2. Computation: Finite and Infinite Machines. — Englewood Cliffs (N. J.): Prentice-Hall, 1967. [Русский перевод: Минский М. Вычисления и автоматы — М.: Мир, 1971.]

Новиков П. С.

1. Об алгоритмической неразрешимости проблемы тождества слов в теории групп. — Тр. матем. ин-та АН СССР им. В. А. Стеклова, 44. М.: Изд. АН СССР, 1955

Онדרо (Aanderaa S.)

1. A proof of Higman's embedding theorem using Britton extensions of groups. — In: Boone W. W., Cannonito F. B., Lyndon R. C. Word Problems. Amsterdam: North-Holland, 1973, p. 1—18.

Ондеро и Льюис (Aanderaa S., Lewis H. R.)

1. Linear sampling and the $\forall\exists\forall$ case of the decision problem. — J. Symbolic Logic, 1974, 39, p. 519—548.

Патерсон (Paterson M. S.)

1. Unsolvability in 3×3 matrices. — Studies in Appl. Math., 1970, 49, p. 105—107.

Пост (Post E. L.)

1. Formal reductions of the general combinatorial decision problem. — Amer. J. Math., 1943, 65, p. 197—215.
2. A variant of a recursively unsolvable problem. — Bull. Amer. Math. Soc., 1946, 52, p. 264—268.
3. Recursive unsolvability of a problem of Thue. — J. Symbolic Logic, 1947, 12, 1—11.
4. Absolutely unsolvable problem and relatively undecidable propositions. Account of an anticipation. — In: Davis M. The Undecidable. Hewlett (N. Y.): Raven Press, 1965, p. 340—433.

Рабин (Rabin M. O.)

1. Recursive unsolvability of group theoretic problem. — Ann. Math., 1958, 67, p. 172—194.

Ротман (Rotman J. J.)

1. The Theory of Groups. — Boston (Mass.): Allyn and Bacon, 1973.

Туэ (Thue A.)

1. Probleme über Veränderungen von Zeichenreihen nach gegebenen Regeln. — Skr. utgitt av. Vid. Kristiania, I. Mat.-Naturv. Klasse, 1914, 10.

Тьюринг (Turing A. M.)

1. On computable numbers, with an application to the Entscheidungsproblem. — Proc. London Math. Soc., Ser. 2, 1936, 42, p. 230—265; 1936, 43, p. 544—546

Хакен (Haken W.)

1. Connections between topological and group theoretical decision problems. — In: Boone W. W., Cannonito F. B., Lyndon R. C. Word Problems. Amsterdam: North-Holland, 1973, p. 427—441.

Хигмен (Higman G.)

1. Subgroups of finitely presented groups. — Proc. Roy. Soc. London, Ser. A, 1961, 262, p. 455—475.

Хопкрофт и Алмен (Hopcroft J., Ullman J.)

1. Formal Languages and Their Relation to Automata. — Reading (Mass.): Addison-Wesley, 1969.

Чёрч (Church A.)

1. A note on the Entscheidungsproblem. — J. Symbolic Logic, 1936, 1, p. 40—41, 101—102; исправленный текст в кн: Davis M. The Undecidable. Hewlett (N. Y.): Raven Press, 1965, p. 108—115.

Шенфилд (Schoenfield J. R.)

1. Mathematical Logic. — Reading (Mass.): Addison-Wesley, 1967, [Русский перевод: Шенфилд Дж. Математическая логика. — М.: Наука, 1975.]

Ясухара (Yasuhara A.)

1. Recursive Function Theory and Logic — N. Y.: Academic Press, 1971.

РАЗРЕШИМЫЕ ТЕОРИИ

Михаэль О. Рабин

СОДЕРЖАНИЕ

Обзор и основные понятия	77
§ 1. Метод элиминации кванторов	82
1.1. Теории и модели (82). 1.2. Элиминация кванторов для дискретных порядков (85). 1.3. Арифметика Пресбургера (88). 1.4. Теория действительных чисел (88). 1.5. Другие теории (89).	
§ 2. Теоретико-модельные методы	89
2.1. Категоричность, полнота и разрешимость (89). 2.2. Алгебраически замкнутые поля (90). 2.3. Вещественно замкнутые поля (91). 2.4. Снова о теории ДО (92). 2.5. Дальнейшие результаты (93).	
§ 3. Метод интерпретаций	94
3.1. Семантические интерпретации (94). 3.2. Разрешимые теории второго порядка (97). 3.3. Теорема о дереве (98). 3.4. Снова об арифметике Пресбургера (98). 3.5. Теория второго порядка для линейного порядка (99). 3.6. Разрешимость в топологии (100). 3.7. Булевы алгебры (101). 3.8. Неклассические логики (102).	
§ 4. Сложность разрешающих процедур	103
4.1. Вычисления на машинах Тьюринга (103). 4.2. Теория WSIS (104). 4.3. Теории сложения и вещественно замкнутых полей (106). 4.4. Пропозициональные исчисления и $P = NP$ (107).	
Литература	109

Обзор и основные понятия *)

Исследования по разрешимости касаются попыток установить для данной математической теории T или данной проблемы P существование разрешающего алгоритма AL , который будет выполнять следующее. Для данного предложения A , выраженного в языке теории T , алгоритм AL будет определять, будет ли A истинным в T , т. е. будет ли $A \models T$. В случае проблемы P для каждого частного случая I проблемы P алгоритм AL будет выдавать правильный ответ для этого частного случая. В зависимости от проблемы P ответ может быть дан в виде «да» или «нет», целым числом и т. д.

Если такой алгоритм действительно существует, то мы будем говорить, что *проблема разрешимости для T или P разрешима*

*) Читателю можно порекомендовать для ознакомления также книгу Ершова [3] и обзорную статью Ершова, Лаврова, Тайманова и Тайцлина [1]. — Прим. ред.

или что теория T разрешима, или просто, что проблема P разрешима. Об AL будем говорить как о разрешающей процедуре для T или P . Проиллюстрируем наши понятия двумя знаменитыми результатами, связанными с разрешимостью.

Пусть L — язык первого порядка, подходящий для выражения утверждений евклидовой геометрии на плоскости. Итак, L имеет список переменных, областью значения которых будут точки; два трехместных предиката $L(x, y, z)$ и $B(x, y, z)$, обозначающие предикаты «лежать на одной прямой» и «лежать между»; два предиката $C(x, y, z, u, v, w)$ и $A(x, y, z, u, v, w)$, обозначающие равенство треугольников и равенство углов (т. е. $\triangle xyz \cong \triangle uvw$ и $\angle xyz = \angle uvw$); четырехместный предикат $E(x, y, u, v)$, обозначающий равенство длин (т. е. $xy = uv$). Например, формула

$$\forall x y z u v [A(x, y, v, z, y, v) \wedge A(x, z, u, y, z, u) \wedge B(x, y, u) \wedge B(x, z, v) \wedge E(u, z, v, y) \rightarrow E(x, y, x, z)]$$

выражает в L известный из средней школы факт, что если в треугольнике биссектрисы двух углов равны, то данный треугольник равнобедренный.

Тарский [2] доказал, что теория EG , содержащая все предложения из L , истинные в евклидовой геометрии на плоскости, — так называемая элементарная геометрия — разрешима.

В действительности Тарский доказал более сильный результат. Пусть $\mathbb{R} = \langle R, +, \cdot \rangle$ — поле действительных чисел, тогда теория первого порядка $Th(\mathbb{R})$ разрешима. Из этого последнего результата следует разрешимость элементарной геометрии путем введения декартовых координат и сведения геометрических утверждений к эквивалентным алгебраическим утверждениям.

Наш второй пример также связан с Евклидом. Проблема НОД состоит в нахождении для пар a, b натуральных чисел их наибольшего общего делителя (a, b) . Способ, незначительно отличающийся от известного алгоритма Евклида, основан на двух фактах: $(a, 0) = a$ и $(a, b) = (a, b - a)$ для $a \leq b$. Последовательными шагами второго типа можно преобразовать любой Н.О.Д. (a, b) в $(c, 0)$ так, чтобы $(a, b) = c$. Так, $(27, 15) = (12, 15) = (12, 3) = (9, 3) = (6, 3) = (3, 3) = (3, 0) = 3$.

Для того чтобы придать точный математический смысл разрешимости, нам нужно понятие вычислимой или рекурсивной функции. С помощью подходящей гёделевой нумерации G множество всех предложений языка L одно-однозначно отображается в некоторое рекурсивное подмножество $S \subseteq \mathbb{N}$ множества натуральных чисел $\mathbb{N}$. При этом T отображается в множество $G(T) \subseteq S$. Теория T по определению разрешима тогда и только

тогда, когда $G(T)$ — рекурсивное множество, т. е. его характеристическая функция f_T вычислима. Решение проблемы разрешимости для T предполагает указание программы или алгоритма для вычисления f_T или по крайней мере доказательства того, что f_T вычислима. Понятие разрешимости проблемы P уточняется подобным же образом.

Везде в этой книге считается, что теория T неразрешима, если f_T не рекурсивна.

Имеется значительное методологическое различие между изучением разрешимости и изучением неразрешимости, и это несмотря на тот очевидный факт, что эти два понятия являются противоположными сторонами одной медали. Попытки установить неразрешимость теории T предполагают наличие какого-то математически точного понятия вычислимых функций. Ибо только после того, когда мы знаем, что такое вычислимая функция, можно доказать, что f_T невычислима.

С другой стороны, проблема разрешения для T может быть решена посредством указания разрешающего алгоритма AL , который признается и допускается математиками в качестве эффективной вычислительной процедуры. Так, например, алгоритм Евклида, указанный выше, дополненный точными правилами для сравнения и вычитания натуральных чисел, признается как вычислимый метод всеми.

Данное утверждение объясняет исторические факты о том, что некоторые результаты о разрешимости были получены до определения рекурсивных функций в середине тридцатых годов, в то время как первые результаты о неразрешимости были получены лишь после формулировки этого определения.

Имеется три главных метода для доказательства разрешимости теорий. Первым и старейшим является элиминация кванторов. Этот метод состоит в преобразовании данного предложения A в другое предложение B такое, что $T \vdash A \leftrightarrow B$ и B принадлежит классу предложений $\mathcal{H}$, для элементов которого мы можем прямо решить, будут ли они лежать в T .

Второй метод теоретико-модельный. В своем типичном виде он имеет дело с (рекурсивным) множеством аксиом AX для теории T . Теоретико-модельные методы применяются либо для того, чтобы показать, что AX полное, в этом случае легко видеть, что T разрешима, либо для того, чтобы систематически обозреть все пополнения для AX . В последнем случае мы будем считать для каждого предложения A , будет ли $T \cup \{A\}$ непротиворечивым и, следовательно, будет ли $T \vdash A$.

В некоторых случаях используется комбинация этих двух методов. А именно, разумным образом выбирается множество $\mathcal{H}$ предложений языка L так, чтобы для каждого предложения A из L существовало предложение $B \in \mathcal{H}$, эквивалентное A по

отношению к T , что устанавливается теоретико-модельными средствами. При этом предложения $B \in \mathcal{H}$, истинные в T , выбираются посредством обозрения моделей теории T .

Третий метод использует интерпретации. Пусть известно, что теория T_0 разрешима, а T — любая теория. Допустим, что у нас есть (вычислимое) отображение t , которое переделывает или переводит каждое предложение A языка L в предложение $t(A)$ языка L_0 так, чтобы $t(A) \in T_0$ тогда и только тогда, когда $A \in T$. При этих условиях T разрешима. Действительно, для определения того, будет ли $A \in T$, мы должны лишь найти $t(A)$ и проверить, будет ли $t(A) \in T_0$. Обычно интерпретация t также имеет дело с теоретико-модельными рассуждениями. Показывается, что модели для T могут быть изоморфно воспроизведены из моделей для T_0 с помощью определимых в L_0 предикатов. Этот метод был применен Рабином [2] для получения большинства известных результатов о разрешимости, а также некоторых новых результатов.

Метод интерпретаций с необходимыми изменениями является сильным инструментом и для доказательств неразрешимости. Действительно, если про теорию T известно, что она неразрешима, и интерпретируема в T_0 в том смысле, как это объяснялось в предыдущем абзаце, то T_0 должна быть неразрешима, см. Рабин [1].

На изучение разрешимости можно смотреть и как на часть, или естественное ответвление, *программы Гильберта* обоснования математики. Идея Гильберта состоит в кодификации различных разделов математики системами аксиом, а аксиоматизированная логика остается общей основой для выведения следствий (теорем) из аксиом. Гильберт надеялся, что такая формализация превратит вывод математических результатов в механическую игру с цепочками символов. Согласно плану Гильберта это помогло бы нам дать исчерпывающий список всех формальных теорем внутри любой математической дисциплины, а это поможет доказать, что нет никакого формального утверждения и его отрицания, которые доказываются вместе, что в свою очередь демонстрировало бы непротиворечивость математики. В программу Гильберта включена и вера в то, что процесс вывода теорем может быть механизирован, или, говоря по-современному, что математические теории разрешимы. Потерпев неудачу в попытке реализовать программу Гильберта для математики вообще как целого, доказав непротиворечивость и разрешимость, скажем, теории множеств, исследователи обратились к изучению более ограниченных разделов математики. Многие из результатов о разрешимости, которые мы обсудим позднее, такие, как разрешающий метод Пресбургера для теории сложения натуральных чисел, были получены в двадца-

тых и начале тридцатых годов и были вызваны программой Гильберта.

Знаменитые теоремы Гёделя о неполноте и результат Чёрча о неразрешимости, полученные в начале и середине тридцатых годов, разбили все надежды реализации программы Гильберта в ее первоначальной форме. А именно, Гёдель продемонстрировал невозможность доказательства непротиворечивости любой значительной части математики посредством финитных методов, которые отстаивал Гильберт, а Чёрч доказал, что исчисление предикатов, как и арифметика сложения и умножения натуральных чисел, неразрешимы. Эти результаты открывают перспективу изучения разрешимости и вызвали массу исследований о разрешимости и неразрешимости различных математических теорий.

Только в последние годы стали обращать внимание на вопрос о вычислительной сложности разрешимых проблем разрешимости. Как в программе Гильберта, так и при тьюринговском анализе вычислимости молчаливо предполагается, что для теории T , про которую доказано, что она разрешима, вопрос, будет ли данное предложение теоремой теории T , тривиален. Действительно, нужно лишь применять механическую процедуру для того, чтобы ответить на любой такой вопрос. Никакого творчества и разумного осмысления не требуется для этого процесса. С этой точки зрения любая разрешимая теория тривиальна и неинтересна. Работы Фишера, Мейера и Рабина и других вызвали переоценку такого отношения. Они показали, что многие теории, хотя они и разрешимы, с практической точки зрения неразрешимы, потому что любой разрешающий алгоритм требовал бы практически невозможного числа вычислительных шагов. Для арифметики сложения натуральных чисел, разрешимость которой доказана Пресбургером, Фишер и Рабин [1] показали, что для каждого разрешающего алгоритма AL существует предложение A размера (т. е. с числом символов) n такое, что для AL требуется 2^{2^n} вычислительных шагов для ответа на вопрос по поводу A . Мейер [1] доказал даже еще более обескураживающие результаты о сложности для теорий таких, как теория линейного порядка. Фишер и Рабин также показали, что элементарная геометрия имеет проблему разрешимости, которая по своей природе является экспоненциально сложной. Результаты, подобные этим, подвергают сомнению утверждение, что любая теория, о которой доказано, что она разрешима, тривиальна, так как ее теоремы можно было бы выявить с помощью вычислительной программы. Вычисления, требующие, скажем, $2^{2^{30}}$ шагов, нельзя рассматривать как возможный метод подтверждения истинности математического утверждения.

Существуют ли какие-нибудь теории с практически разрешимыми проблемами разрешимости? Как это ни странно, ответ на

этот фундаментальный вопрос еще неизвестен. Легко видеть, что проблема разрешимости любой формализованной теории по крайней мере так же сложна, как и проблема разрешимости для пропозиционального исчисления РС. Далее, Кук [1] заметил, что многие комбинаторные проблемы разрешимости, которые не поддались попыткам создания эффективной, а не экспоненциально сложной разрешающей процедуры, сводятся к РС. Это заставляет верить в гипотезу, что РС экспоненциально сложно. Кук рассматривал сходный вопрос, по отношению к использованию машин Тьюринга о том, будут ли недетерминированные вычисления, требующие числа шагов, полиномиально зависящего от размера проблемы, всегда эквивалентны обычным детерминированным вычислениям, требующим полиномиального числа шагов. Эта так называемая проблема $P = NP$ является в момент написания данной главы одной из центральных открытых проблем в теории вычислительных машин. Она также имеет отношение к старой «проблеме спектра», относящейся к моделям предложений предикатного исчисления. Детали будут даны в тексте.

Так как исследования по разрешимости включают в себя методы из пропозициональных и предикатных логик, теории вычислимых функций и теории моделей, мы будем опираться на них в своем изложении. В большинстве случаев для дальнейшего требуются лишь элементарные знания об этих предметах. Неподготовленному читателю необходимо познакомиться с соответствующими главами этой книги для получения всей нужной вспомогательной информации.

§ 1. Метод элиминации кванторов

1.1. Теории и модели. Теории, с которыми имеют дело при изучении разрешимости, будут представляться одним из двух путей: *аксиоматически* или *семантически*, как множество предложений, истинных в какой-либо системе или классе систем. Обычно мы будем рассматривать теории первого порядка, т. е. теории, выраженные в некотором предикатном языке первого порядка. Это правило будет, однако, иметь некоторые важные исключения.

Определение 1. Пусть L — некоторый фиксированный язык первого порядка и H — некоторое непротиворечивое рекурсивное множество предложений языка L . *Теорией, аксиоматизированной посредством H* , по определению является множество $\text{Th}(H)$ всех логических следствий из H .

$$\text{Th}(H) = \{A: H \vdash A\}.$$

Теория $\text{Th}(H)$ и множество аксиом H называются *полными*, если для каждого предложения A из L имеем $A \in \text{Th}(H)$ или $\neg A \in \text{Th}(H)$.

Теорема 1. Если теория T аксиоматизирована и полна, то T разрешима.

Доказательство. Пусть H — аксиоматизация теории T . Последовательности $S_i = (A_{i1}, A_{i2}, \dots, A_{in_i})$, являющиеся формальными доказательствами из аксиом H , могут быть эффективно перечислены. Это можно сделать, например, перечисляя все конечные последовательности (слова) над алфавитом для L и выбрасывая те последовательности, которые не являются доказательствами. Последние элементы A_{in_i} перечисляемых доказательств пробегают все утверждения A , которые доказываются из H , т. е. все элементы из $\text{Th}(H) = T$.

Таким образом, все теоремы из T могут быть эффективно (вычислимо) перечислены в последовательность $S = (A_1, A_2, \dots)$. Пусть теперь A — любое предложение языка L . Начнем перечислять S и для каждого A_n проверяем, будет ли $A_n = A$ или $A_n = \neg A$. Так как T полна, то один из этих случаев должен в конце концов встретиться, и в это время мы узнаем, будет ли $A \in T$ или $A \notin T$. $\square$

Люди, встречающиеся с подобными рассуждениями впервые, часто испытывают некоторую трудность, чтобы убедить себя, что предложенная процедура является правильным вычислительным процессом для разрешения T . Это связано с тем, что существенная особенность вычисления состоит в том, что мы уверены, что оно закончится, в то время как здесь, когда дается A , мы не имеем заранее никакой границы на число шагов, требующихся для окончания вычисления. Однако полнота T гарантирует, что вычисление будет закончено, и либо A , либо $\neg A$ встретится в вычислении. Это и составляет доказательство того, что алгоритм закончится. В действительности тем самым показывается, что и функция «число шагов» будет вычислимой, хотя и не такой общеизвестной, как, например, n^2 .

Основная идея теоремы 1 может быть обобщена и на случай, когда T не полна.

Теорема 2. Пусть T — аксиоматизируемая теория, и предположим, что существует рекурсивная (вычислимая) последовательность $A_1, A_2, \dots$ предложений, удовлетворяющих следующим условиям:

- (1) $T \cup \{A_n\}$ непротиворечива для каждого n .
- (2) Каждое пополнение $T \subseteq T_1$ теории T имеет (не обязательно рекурсивное) множество аксиом $B = \{B_1, \dots, B_k, \dots\}$ такое, что $T_1 = \text{Th}(B)$ и для каждого k существует n , для которого $T \vdash A_n \leftrightarrow B_1 \wedge \dots \wedge B_k$.

Из условий (1), (2) следует, что T разрешима.

Доказательство. Пусть H — рекурсивная аксиоматизация для T . С помощью процесса, похожего на вышеуказанный, мы можем эффективно перечислить в одну последовательность $D_1, D_2, \dots$ логические следствия всех множеств $H_n = H \cup \{A_n\}$, $n = 1, 2, \dots$. А именно, начнем с эффективного перечисления следствий из H_1 , как в доказательстве теоремы 1. Когда первое следствие $H_1 \vdash D_1$ встретится, начинаем перечислять следствия из H_2 до тех пор, пока не получится D_2 . Затем возвращаемся к порождению второго следствия, назовем его D_3 , из H_1 . Затем возвращаемся к H_2 для получения $H_2 \vdash D_4$, а следующим получаем первое следствие, назовем его D_5 , из H_3 и т. д.

Снова, как указано выше, эффективно перечисляем указанную последовательность $D_1, \dots, D_n, \dots$, а также последовательность $E_1, \dots, E_n, \dots$ всех следствий из H . Вторая последовательность есть в действительности перечисление $T = \text{Th}(H)$. Следовательно, если $A \in T$, то A встретится среди E_i . Мы утверждаем, что если $A \notin T$, то $\neg A$ встретится среди D_i . Таким образом, двойное перечисление эффективно позволит нам ответить на вопрос, будет ли $A \in T$.

Чтобы доказать данное утверждение, заметим, что если $A \notin T$, то $T \cup \{\neg A\}$ непротиворечиво. Следовательно, оно есть подмножество некоторой полной теории $T \cup \{\neg A\} \subseteq T_1$. Пусть $B = \{B_1, B_2, \dots\}$ — множество аксиом для T_1 , упоминаемое в предположении о последовательности $A_1, A_2, \dots$. Тогда $B \vdash \neg A$, и, следовательно, для некоторого целого числа k имеем $B_1 \wedge \dots \wedge B_k \vdash \neg A$. По нашим предположениям существует n такое, что $T \vdash A_n \leftrightarrow B_1 \wedge \dots \wedge B_k$. Таким образом, $T \cup \{A_n\} \vdash \neg A$ и $\neg A$ встретится в последовательности $D_1, D_2, \dots$ $\square$

Теорема 2 используется для доказательства разрешимости в случаях, когда T не полна, но однако мы можем как-то обобщить все возможные пополнения.

Определение 2. Пусть $\mathfrak{A} = \langle A, R_1, R_2, \dots \rangle$ — система и L — язык первого порядка, соответствующий $\mathfrak{A}$, т. е. L имеет символы P_i , соответствующие всем предикатам и функциям R_i из $\mathfrak{A}$. Теорией $\text{Th}(\mathfrak{A})$ системы $\mathfrak{A}$ называется множество предложений из L , истинных в $\mathfrak{A}$,

$$\text{Th}(\mathfrak{A}) = \{B: \mathfrak{A} \models B\}.$$

Если $\mathcal{K}$ — класс однотипных систем, а L — язык, соответствующий одной, а значит, и всем системам из $\mathcal{K}$, то по определению

$$\text{Th}(\mathcal{K}) = \bigcap_{\mathfrak{A} \in \mathcal{K}} \text{Th}(\mathfrak{A}).$$

Теперь дадим несколько примеров теорий как заданных аксиомами, так и заданных моделями, т. е. определенных семантически.

Пример 1. Пусть L — язык только с одним двухместным предикатным символом $\leq$ (больше или равно, чем). Рассмотрим аксиомы OR:

1. $\forall x \forall y [x \leq y \wedge y \leq x \rightarrow x = y]$,
2. $\forall x \forall y [x \leq y \vee y \leq x]$,
3. $\forall x \forall y \forall z [x \leq y \wedge y \leq z \rightarrow x \leq z]$.

Любая модель $\langle A, \leq \rangle \models \text{OR}$ является линейно упорядоченным множеством.

Пусть $x < y$ является сокращением для $x \leq y \wedge \neg x = y$.

Пример 2. Рассмотрим аксиомы DO, полученные добавлением к OR аксиом

4. $\exists x \forall y [y \leq x \rightarrow x = y]$,
5. $\forall x \exists y [x < y \wedge \forall z [x < z \rightarrow y \leq z]]$,
6. $\forall x \forall y [y < x \rightarrow \exists z \forall w [z < x \wedge [z < w \rightarrow x \leq w]]]$.

Любая модель $\langle A, \leq \rangle \models \text{DO}$ является линейно упорядоченным множеством, которое имеет первый элемент, каждый элемент имеет единственный непосредственно следующий элемент и каждый элемент, за исключением первого элемента, имеет единственный предшественник. Такие порядки будут называться дискретными порядками.

Обозначая, как обычно, $\omega = \{0, 1, 2, \dots\}$, видим, что $\mathfrak{A} = \langle \omega, \leq \rangle \models \text{DO}$. Если мы обозначим через ω^* обратный порядковый тип для ω (т. е. $0 > 1 > 2 > \dots$), то каждое упорядоченное множество, являющееся моделью для DO, имеет порядковый тип $\omega + (\omega^* + \omega) \cdot \lambda$, где λ — любой порядковый тип.

Пример 3. Рассмотрим класс $\mathcal{K}_{\text{uf}}$ всех систем $\langle A, f \rangle$, где f — одноместная функция $f: A \rightarrow A$. $\text{Th}(\mathcal{K}_{\text{uf}})$ — теория одноместных функций.

Пример 4. Пусть $\langle \omega, + \rangle$ — система целых чисел со сложением, $\text{Th}(\langle \omega, + \rangle) = \text{PAR}$ будет называться арифметикой Пресбургера или теорией сложения натуральных чисел.

1.2. Элиминация кванторов для дискретных порядков. До сих пор мы рассматривали аксиоматически и семантически определенные теории. Мы также указали два метода доказательства разрешимости для аксиоматизированных теорий. Теперь проиллюстрируем метод элиминации кванторов, доказав разрешимость $\text{Th}(\langle \omega, \leq \rangle)$, этот результат доказан К. Х. Ленгфордом в 1927 г.

Теорема 3. $\text{Th}(\mathfrak{A})$ разрешима.

Доказательство. Обогатим систему $\mathfrak{A}$, сделав 0 выделенным элементом и добавив функцию следования $S(x) = x + 1$ (элемент, следующий по порядку за x). Полученную систему обозначим через $\mathfrak{A}_1 = \langle \omega, 0, \leq, S \rangle$, а соответствующий язык —

L_1 . Докажем разрешимость $\text{Th}(\mathfrak{N}_1)$, из этого результата следует разрешимость и $\text{Th}(\mathfrak{N})$.

Будем использовать сокращение $S^n(t)$, чтобы обозначить n применений S к терму t , таким образом, $S^3(x) = S(S(S(x)))$. В частности, $S^0(y) = y$. Термами языка являются $0, x, y, \dots, S^n(0), S^n(x), \dots, 1 \leq n$.

Класс формул $\mathcal{R}$, к которым мы будем сводить каждую формулу из L_1 , будет состоять из следующих формул:

- (1) $t_1 = t_2, t_1 < t_2$, где t_1, t_2 — термы;
- (2) формулы, являющиеся дизъюнкциями конъюнкций формул из (1).

Например, формула $[S^3(0) = x \wedge S(y) < z] \vee S^5(z) < S^3(y)$ находится в $\mathcal{R}$.

Покажем, что каждая формула A из L_1 эквивалентна в $\mathfrak{N}$ некоторой формуле $B \in \mathcal{R}$. Наше доказательство будет также давать метод эффективного преобразования A в B .

Утверждение, что две формулы C и D эквивалентны в $\mathfrak{N}_1$, означает, что $\mathfrak{N}_1 \models C \leftrightarrow D$. Мы сделаем некоторые утверждения об эквивалентности формул, оставляя их проверку читателю.

Пусть A — открытая формула, т. е. не содержащая кванторов. Выразим все другие пропозициональные связи через $\wedge, \vee, \neg$. Пронесим все $\neg$ на атомные формулы, используя правила такие, как $\neg[C \vee D] \equiv \neg C \wedge \neg D$. Уберем все вхождения двойного отрицания $\neg\neg$. Заменяем все части вида $t_1 \leq t_2$ на $t_1 = t_2 \vee t_1 < t_2$, $t_1 = t_2$ на $t_1 < t_2 \vee t_2 < t_1$ и $t_1 < t_2$ на $t_1 = t_2 \vee t_2 < t_1$. Наконец, используя дистрибутивный закон для $\wedge$ и $\vee$, преобразуем формулу в некоторую формулу из $\mathcal{R}$. Таким образом, видим, что, повторяя применение вышеуказанных правил, мы преобразуем любую открытую формулу в эквивалентную формулу из $\mathcal{R}$.

Допустим теперь, что A_1 имеет вид $\exists y [C_1 \vee \dots \vee C_n]$, где каждое C_i является конъюнкцией формул $t_1 = t_2$ или $t_1 < t_2$. Имеем $A_1 \equiv \exists y C_1 \vee \dots \vee \exists y C_n$. Таким образом, достаточно дать правила преобразования формул вида

$$A_1 = \exists y [t_1 = t_2 \wedge \dots \wedge t_{2i-1} = t_{2i} \\ \wedge t_{2i+1} < t_{2i+2} \wedge \dots \wedge t_{2k-1} < t_{2k}].$$

Читатель может сам понять, как обращаться в случае, когда некоторое равенство или неравенство из A_1 имеет форму $S^m(y) = S^i(y)$ или $S^m(y) < S^i(y)$. Таким образом, мы можем предполагать, что в каждом равенстве или неравенстве из A_1 не более чем одна из частей имеет вид $S^i(y)$.

Для любых термов t_1, t_2 и $1 \leq n$ имеем

$$\mathfrak{N}_1 \models t_1 < t_2 \leftrightarrow S^n(t_1) < S^n(t_2)$$

и подобную эквивалентность для $t_1 = t_2$. Заменяя обе части всех равенств и неравенств в A_1 подходящими степенями S^i , преобразуем A_1 в эквивалентную формулу, в которой все вхождения y имеют вид $S^m(y)$ с одним и тем же $1 < m$. Предположим, что A_1 уже имеет это свойство. «Элиминируем» $\exists y$ из A_1 следующим образом: (1) убираем $\exists y$ из A_1 ; (2) для каждой части $S^m(y) = t_j$ добавляем конъюнктивный член $S^{m-1}(0) < t_j$; (3) для каждой части $S^m(y) < t_j$ добавляем конъюнктивный член $S^m(0) < t_j$; (4) если какое-то равенство $S^m(y) = t_j$ входит в A_1 , то заменяем все вхождения $S^m(y)$ в A_1 на t_j ; (5) предположим, что никакого такого равенства нет, а все неравенства имеют вид $S^m(y) < t_j$ или же имеют вид $t_j < S^m(y)$, тогда убираем все части, содержащие $S^m(y)$; (6) наконец, если нет равенства, содержащего $S^m(y)$, но встречаются неравенства обоих видов, то для каждой пары $t_j < S^m(y)$ и $S^m(y) < t_p$ добавляем конъюнктивный член $S(t_j) < t_p$ и затем убираем все части, содержащие $S^m(y)$. Ясно, что шаги (1) — (6) преобразуют A_1 в эквивалентную формулу $B \in \mathcal{R}$, не содержащую y .

Теперь пусть A — любая формула из L_1 . Так как $\forall x F \equiv \neg \exists x \neg F$, то можно предполагать, что A содержит лишь кванторы существования, скажем n штук. Пусть $\exists y D$ — самое внутреннее вхождение $\exists$, т. е. D открыта. Преобразуем D в дизъюнкцию конъюнкций, как это только что было описано. Тогда $\exists y D \equiv A_1$, где A_1 имеет вид, указанный выше. Распределяем $\exists y$ по дизъюнкции и обрабатываем каждую часть с помощью шагов (1) — (6). Этими преобразованиями $\exists y D$ заменится в A эквивалентной открытой формулой, а A преобразуется в эквивалентную формулу с $n - 1$ квантором. Повторяя этот процесс n раз, эффективно преобразуем A в $B \in \mathcal{R}$.

Наконец, если A было предложением, то преобразованная формула также является предложением и, следовательно, пропозициональной комбинацией формул $S^m(0) = S^i(0)$ или $S^m(0) < S^i(0)$. Истинность или ложность этого предложения может быть вычислена непосредственно. Итак, мы имеем процедуру разрешения для $\text{Th}(\mathfrak{N}_1)$, а значит, и для $\text{Th}(\mathfrak{N})$. $\square$

Заметим, что можно было бы избежать перехода от $\mathfrak{N}$ к $\mathfrak{N}_1$ по той причине, что предикат $y = S^n(x)$ определим подходящей формулой $D_n(x, y)$ в $\mathfrak{N}$. Это позволяет нам переводить любую базисную формулу $t_1 < t_2$ или $t_1 = t_2$ в формулы из L_1 и, следовательно, получить класс сведения формул из L_1 .

Заметим, что если мы выполним процедуру элиминации кванторов в $\mathfrak{N}$, то мы в действительности не освободимся от всех кванторов. Скорее, мы «прячем» их в формулах $D_n(x, y)$. Но все же это дает нам требуемый результат. Вообще говоря, на

метод элиминации кванторов надо смотреть с этой более широкой точки зрения.

Та же самая разрешающая процедура может быть применена к $\text{Th}(\text{DO})$, лишь требуются изменения, связанные с тем, что различные утверждения об эквивалентности формул, которые были математически подтверждены для $\mathfrak{N}_1$, теперь должны быть выведены как формальные следствия аксиом DO . Следуя этому пути, мы не только докажем разрешимость $\text{Th}(\text{DO})$, но и покажем, что $\text{Th}(\text{DO}) = \text{Th}(\mathfrak{N})$, т. е. докажем, что $\text{Th}(\text{DO})$ полна.

1.3. Арифметика Пресбургера. Разрешимость PAR была доказана Пресбургером [1], использовавшим метод элиминации кванторов. С помощью подходящей формулы $x <_n y$ мы можем выразить для каждого фиксированного n предикат $x < y \wedge \Delta x \equiv y \pmod{n}$. Так, например, $x <_3 y$ есть $\exists z [\Delta z = 0 \wedge x + z + z + z = y]$. Обогатим систему $\langle \omega, + \rangle$, сделав 0 и 1 выделенными элементами. Термами языка являются теперь 0, 1, $x, y, \dots$ и все выражения, которые являются их суммами, например $x + z + z + 1 + 1 + 1$, которое сокращается до $x + 2z + 3$.

Множество сведений $\mathcal{H}$ будет состоять из всех формул, получающихся из базисных формул $t_1 = t_2$, $t_1 <_n t_2$ (t_1, t_2 — термы, n — целое число) с помощью конъюнкций и дизъюнкций. Доказательство хотя и нетривиально, но нетрудно и следует доказательству 1.2.

1.4. Теория действительных чисел. Это, возможно, одно из наилучших применений метода элиминации кванторов. Рассматриваем поле действительных чисел $\mathfrak{R} = \langle \mathbb{R}, 0, 1, +, \cdot, \leq \rangle$ как упорядоченное поле. Вместо разрешающей процедуры, указанной впервые Тарским, в общих чертах опишем алгоритм Коэна [1], используя формулировку, указанную в диссертации Монка.

Введем, в качестве временного, понятие, подобное алгебраической функции. Пусть $P(x_1, \dots, x_n) \in Z[x_1, \dots, x_n]$ — полином с целыми коэффициентами, $d_n(P)$ — степень x_n в P и $\eta \in R^{n-1}$. Определим $P_\eta(x_n) = P(\eta_1, \dots, \eta_{n-1}, x_n)$. Для $1 \leq i \leq d_n(P)$ пусть $f_{P,i}(\eta)$ равна 0, если $P_\eta \equiv 0$ или P не имеет действительных корней, в противном случае i -му действительному корню уравнения $P_\eta = 0$, если существует по крайней мере i таких корней, а если не существует, то наибольшему действительному корню. Это позволяет рассматривать $f_{P,i}(x_1, \dots, x_{n-1})$ как терм, обозначающий функцию $f_{P,i}: R^{n-1} \rightarrow R$. Назовем такие термы алгебраическими функциями.

Полиномиальный предикат — это булева комбинация атомных формул вида $0 \leq P$, где $P \in Z[x_1, \dots, x_n]$. Алгебраический предикат — это булева комбинация полиномиальных предикатов и формул вида $0 \leq P(x_1, \dots, x_{n-1}, f_1(x_1, \dots, x_{n-1}))$ или $f_1 \leq f_2$, где $P \in Z[x_1, \dots, x_n]$, а f_1, f_2 — алгебраические функции. С ка-

ждым алгебраическим предикатом связываем *ранг* таким путем, что рангом полиномиального предиката является 0.

Процедура элиминации кванторов будет сводить всякую формулу первоначального языка к открытой формуле (т. е. полиномиальному предикату), при этом временно будут использоваться и более общие алгебраические предикаты.

Доказательство содержит две леммы. Первая лемма утверждает, что формула $\exists x_n A$, где A — полиномиальный предикат, эквивалентна некоторому алгебраическому предикату B . Вторая лемма говорит, что всякий алгебраический предикат B ранга $1 \leq k$ эквивалентен некоторому алгебраическому предикату ранга не более чем $k - 1$. Из этой леммы следует по индукции, что каждый алгебраический предикат эквивалентен полиномиальному предикату. Вместе эти факты гарантируют, что каждая формула эквивалентна открытой формуле.

При доказательстве этих лемм используется теорема Ролля, говорящая о том, что между всякими двумя последовательными корнями уравнения $p(x) = 0$ лежит корень уравнения $p'(x) = 0$. Если $p(x)$ — полином, то может быть достигнута локализация корней уравнения $p(x) = 0$ с достаточной для нас точностью посредством локализации корней уравнения $p'(x) = 0$ и значений $p(-\infty)$, $p(+\infty)$. Для $P \in Z[x_1, \dots, x_n]$ обозначим $P' = \partial P / \partial x_n$. Оказывается, грубо говоря, что утверждение, включающее $f_{P,i}$, т. е. утверждение об i -м корне уравнения $P = 0$, может быть переделано в утверждение, включающее термы $f_{P',j}$. В рамках нашего понятия ранга это влечет понижение ранга, что и является ключевым местом доказательства второй леммы.

1.5. Другие теории. Коротко укажем некоторые другие теории, разрешимость которых установлена методом элиминации кванторов.

Пусть $\mathbb{Q}$ — рациональные числа, $\eta = \langle \mathbb{Q}, \leq \rangle$ — их порядковый тип. $\text{Th}(\eta)$ разрешима.

Пусть ALC — класс алгебраически замкнутых полей, тогда $\text{Th}(\text{ALC})$ разрешима. Здесь каждая формула эквивалентна открытой формуле; это можно доказать, например, используя классическую алгебраическую теорию исключения.

Если BA — класс булевых алгебр, то $\text{Th}(\text{BA})$ разрешима. Этот результат принадлежит Тарскому [1] и сравнительно труден *).

§ 2. Теоретико-модельные методы

2.1. Категоричность, полнота и разрешимость. Теория T называется *категоричной в мощности α* , если все модели $\mathfrak{A} \models T$ мощ-

*) Доказательство можно найти в работе Ершова [1] или в книге Ершова [3]. — Прим. ред.

ности $c(\mathcal{A}) = \alpha$ попарно изоморфны. Под мощностью модели $\mathcal{A}$ мы понимаем мощность основного множества модели $\mathcal{A}$. Следующее простое замечание принадлежит Р. Вооту. Здесь предполагается, что T не более чем счетна.

Теорема 4. Если теория T не имеет конечных моделей и она категорична в некоторой (необходимо бесконечной) мощности α , то T полна.

Доказательство. Допустим с целью прийти к противоречию, что T не полна. Тогда существует предложение S языка теории T такое, что теории $T_1 = T \cup \{S\}$ и $T_2 = T \cup \{\neg S\}$ непротиворечивы. Поэтому существуют не более чем счетные (т. е. конечные или счетные) модели $T_1 \models \mathcal{A}_1$, $T_2 \models \mathcal{A}_2$. Так как T не имеет конечных моделей, то $c(\mathcal{A}_1) = c(\mathcal{A}_2) = \omega$. Если $\alpha = \omega$, то $\mathcal{A}_1 \approx \mathcal{A}_2$, но $\mathcal{A}_1 \models S$ и $\mathcal{A}_2 \models \neg S$, что невозможно. В противном случае по теореме Скулема — Тарского — Воота существуют элементарные расширения $\mathcal{A}_1 < \mathfrak{B}_1$, $\mathcal{A}_2 < \mathfrak{B}_2$ такие, что $c(\mathfrak{B}_1) = c(\mathfrak{B}_2) = \alpha$. Снова $\mathfrak{B}_1 \approx \mathfrak{B}_2$, $\mathfrak{B}_1 \models S$ и $\mathfrak{B}_2 \models \neg S$. $\square$

Условие о том, что T не имеет конечных моделей, существенно. Рассмотрим теорию E только одного равенства $=$. E категорична в каждой мощности. Однако как $E \cup \{\forall x \forall y [x = y]\}$, так и $E \cup \{\exists x \exists y [\neg x = y]\}$ непротиворечивы.

Возможно простейшим использованием этого результата является доказательство того, что $\text{Th}(\eta)$ разрешима. Рассмотрим аксиомы DNO, содержащие аксиомы линейного порядка и

$$\begin{aligned} \forall x \forall y \exists z [x < y \rightarrow x < z < y], \\ \forall x \exists y \exists z [z < x < y]. \end{aligned}$$

Каждая модель $\langle A, \leq \rangle \models \text{DNO}$ является линейно и плотно упорядоченным множеством без первого и последнего элементов. Из канторовской характеристики порядкового типа $\eta = \langle Q, \leq \rangle$ получаем, что если $c(A) = \omega$, то $\eta \approx \langle A, \leq \rangle$. Следовательно, $\text{Th}(\text{DNO})$ полна, а значит, по теореме 1 разрешима. Далее, $\eta \models \text{DNO}$, так что $\text{Th}(\text{DNO}) \subseteq \text{Th}(\eta)$, но $\text{Th}(\text{DNO})$ полна, и, следовательно, $\text{Th}(\text{DNO}) = \text{Th}(\eta)$. $\square$

2.2. Алгебраически замкнутые поля. Следующей мы рассмотрим теорию AL алгебраически замкнутых полей. Эту теорию можно аксиоматизировать в языке L , имеющем символы $0, 1, +, \cdot$, записав обычные аксиомы поля и добавив последовательность аксиом A_n , $n = 1, 2, \dots$,

$$A_n = \forall y_0 \dots y_{n-1} \exists x [y_0 + y_1 x + \dots + y_{n-1} x^{n-1} + x^n = 0].$$

Аксиома A_n записана с использованием некоторых обычных сокращений.

Аксиомы ALC не полны, потому что не определена характеристика поля. Это можно сделать, добавив для простого p

аксиому $C_p = p \cdot 1 = 0$, где левая часть есть сокращение суммы термов 1. Чтобы получить аксиомы для характеристики 0, положим $C_0 = \{\neg C_2, \neg C_3, \dots\}$.

Покажем теперь, что $T_p = \text{ALC} \cup \{C_p\}$ полна для любого простого p , а также, что $T_0 = \text{ALC} \cup C_0$ тоже полна. Пусть $F \models T_p$, где p — простое число или $p = 0$, будет алгебраически замкнутым полем характеристики p и мощности $\omega < c(F) = \alpha$. Пусть $P \subset F$ — простое поле в F , тогда $P = \mathbb{Z}/p\mathbb{Z}$ для $p \neq 0$ и $P = \mathbb{Q}$, если $p = 0$. По структурной теореме Штейница для алгебраически замкнутых полей существует множество $X \subseteq F$ элементов, алгебраически независимых над P так, что $F \supset P(X) \supset P$ есть алгебраическое замыкание $P(X)$. Тип изоморфизма F зависит только от P (т. е. p) и $c(X)$ — так называемой степени трансцендентности F . Далее, если $\omega < c(F)$, то $c(X) = c(F) = \alpha$. Следовательно, для всех p теория T_p категорична в каждой несчетной мощности $\omega < \alpha$.

Используя теорему 1, получаем, что для каждого $p \geq 0$ теория T_p алгебраически замкнутых полей характеристики p разрешима.

Так как $\text{ALC} \cup C_0$, $\text{ALC} \cup \{C_p\}$, p — простое число, дает перечисление всех пополнений ALC, то из теоремы 2 следует, что теория алгебраически замкнутых полей $\text{Th}(\text{ALC})$ разрешима.

2.3. Вещественно замкнутые поля. Результат Тарского о разрешимости теории полей действительных чисел может быть также получен и теоретико-модельными методами. Во-первых, нам нужны аксиомы поля действительных чисел. Они были получены Артином и Шрейером в их знаменитом исследовании вещественно замкнутых полей.

Рассмотрим язык L_1 , который подобно L из 2.2 имеет $0, 1, +, \cdot$, но еще и символ «меньше или равно» $\leq$. Аксиомы RLC содержат следующее: аксиомы поля, аксиомы, утверждающие, что $\leq$ является линейным порядком, и

$$\begin{aligned} \forall x \forall y \forall z [x \leq y \wedge 0 \leq z \rightarrow xz \leq yz], \\ \forall x \forall y \forall z [x \leq y \rightarrow x + z \leq y + z], \\ \forall x \exists y [0 \leq x \rightarrow y^2 = x], \\ A_n \text{ для } n = 1, 3, 5, \dots \end{aligned}$$

Здесь, как и в 2.2, A_n есть утверждение, что полином n -й степени имеет корень.

Поле действительных чисел является моделью теории RLC, но ни в коем случае не единственной. Любое упорядоченное поле $\langle F, 0, 1, +, \cdot, \leq \rangle \models \text{RLC}$ будет называться (упорядоченным) вещественно замкнутым. $\text{Th}(\text{RLC})$ не категорична ни в какой мощности, так что свойство Воота не может быть приме-

нено. Полнота, а значит, разрешимость доказываются при помощи понятия модельной полноты Робинсона.

Теория T модельно полна, если для любых двух моделей $T \models \mathfrak{A}$, $T \models \mathfrak{B}$ таких, что $\mathfrak{A} \subseteq \mathfrak{B}$, мы имеем $\mathfrak{A} < \mathfrak{B}$ ($\mathfrak{B}$ — элементарное расширение $\mathfrak{A}$).

Робинсон [1] дал критерий проверки модельной полноты. Из его критерия может быть выведена модельная полнота RLC. Доказательство, хотя и не очень трудное, требует некоторых усилий. Вместо этого можно использовать следующий критерий.

T модельно полна, если для любых двух моделей $\mathfrak{A} \subseteq \mathfrak{B}$ теории T существует элементарное расширение $\mathfrak{A} < \mathfrak{C}$ такое, что $\mathfrak{B} \subseteq \mathfrak{C}$. Комбинируя это с алгебраическими свойствами вещественно замкнутых полей и с методом ультрапроизведений, мы можем получить отчасти другое доказательство модельной полноты $\text{Th}(\text{RLC})$.

Далее, модельно полная теория T не обязана быть полной. Однако если T модельно полна и имеет простую модель P , которая изоморфно вкладывается как подмодель во всякую модель теории T , то T полна. При этих условиях, как это легко увидеть, каждые две модели теории T элементарно эквивалентны.

Теория $\text{Th}(\text{RLC})$ имеет простую модель. А именно, каждое вещественно замкнутое поле F имеет характеристику 0 и, следовательно, содержит поле рациональных чисел $\mathbb{Q}$. Оно по этой причине также содержит изоморфную копию поля действительных алгебраических чисел, а оно и есть общее простое поле. Следовательно, $\text{Th}(\text{RLC})$ полна и разрешима. Поле действительных чисел $\mathfrak{R}$ также является моделью теории RLC, следовательно, $\text{Th}(\mathfrak{R}) = \text{Th}(\text{RLC})$, и теория разрешима.

Нужно заметить, что такой подход к разрешимости поля действительных чисел, несмотря на различие в методах, не так сильно отличается от классического метода элиминации кванторов. В основе доказательства модельной полноты лежит то, что если два упорядоченных поля F_1, F_2 изоморфны (отображение сохраняет также порядок), то их вещественные замыкания изоморфны. Это доказывается с помощью информации о локализации корней уравнений. Используемый здесь анализ также не отличается от способа локализации корней в методе элиминации кванторов. С другой стороны, можно утверждать, что единственность вещественного замыкания является по праву основным алгебраическим результатом. При теоретико-модельном доказательстве разрешимости $\text{Th}(\text{RLC})$ мы оперируем стандартными результатами и с этой точки зрения оно более элементарно.

2.4. Снова о теории DO. С целью проиллюстрировать, как теоретико-модельные методы используются для доказательства

разрешимости даже при отсутствии категоричности, снова рассмотрим $\text{Th}(\text{DO})$.

В 1.1, пример 2 замечено, что каждая модель теории DO имеет порядковый тип $\omega + (\omega^* + \omega) \cdot \lambda$. Покажем, что каждая счетная модель $\mathfrak{A} = \langle A, \leq \rangle \models \text{DO}$ имеет элементарное расширение $\mathfrak{A} < \mathfrak{B}$, для которого λ есть η . Отсюда будет следовать, что $\text{Th}(\mathfrak{A}) = \text{Th}(\mathfrak{B})$, следовательно, каждые две счетные модели теории DO элементарно эквивалентны, а значит, теория $\text{Th}(\text{DO})$ полна и разрешима.

Определим отношение эквивалентности E на любой модели $\mathfrak{A} \models \text{DO}$. $x E y \equiv c(\{z: x < z < y \vee y < z < x\}) < \omega$, т. е. число элементов между x и y конечно. Видно, что в модели $\mathfrak{A}$ порядкового типа $\omega + (\omega^* + \omega) \cdot \lambda$ классами эквивалентности относительно E являются «блоки» ω и каждый $\omega^* + \omega$. Рассмотрим любые два блока (классы эквивалентности) B_1, B_2 модели $\mathfrak{A}$; без ограничения общности предположим, что $x < y$ для всех $x \in B_1, y \in B_2$. Без противоречия со всеми элементарными утверждениями о $\mathfrak{A}$, т. е. с полной диаграммой $\text{CD}(\mathfrak{A})$ модели $\mathfrak{A}$, предположим, что существует элемент c такой, что $x < c < y$ для всех $x \in B_1, y \in B_2$. Таким образом, $\text{CD}(\mathfrak{A})$ и все эти неравенства имеют счетную модель $\mathfrak{A}_1$, которая является элементарным расширением $\mathfrak{A} < \mathfrak{A}_1$ модели $\mathfrak{A}$. В этой $\mathfrak{A}_1$ блок B с c лежит между B_1 и B_2 . Аналогично можем построить расширение с блоком выше B_2 . Так как расширение $\mathfrak{A} < \mathfrak{A}_1$ счетно, то можно построить башню элементарных расширений $\mathfrak{A} < \mathfrak{A}_1 < \dots$ так, чтобы каждая $\mathfrak{A}_n$ была счетной и для каждой пары B_1, B_2 блоков из каждой $\mathfrak{A}_n$ существовало $n < k$ и блок B модели $\mathfrak{A}_k$, расположенный между B_1 и B_2 ; аналогично для блока выше B_2 . Пусть $\mathfrak{B} = \bigcup_{n < \omega} \mathfrak{A}_n$, тогда $\mathfrak{A} < \mathfrak{B}$, $\mathfrak{B}$ счетна и блоки из $\mathfrak{B}$ плотно

упорядочены. Таким образом, порядковым типом $\mathfrak{B}$ является $\omega + (\omega^* + \omega) \cdot \eta$, что и заканчивает доказательство.

2.5. Дальнейшие результаты. Еще много важных результатов получается с помощью теоретико-модельных методов, иногда в комбинации с методом элиминации кванторов. Приведем без доказательств несколько выдающихся теорем. Их доказательства обычно включают в себя глубокие математические результаты о рассматриваемых системах, доставляя интересные комбинации стандартной математики и логики.

Теорема 5 (Акс и Кочен [1]—[3]) *. Теория поля p -адических чисел разрешима.

Этот результат хоронит давно стоящую проблему о том, что лишь вещественно замкнутые и алгебраически замкнутые поля являются разрешимыми.

*) Этот результат независимо получен Ершовым [2]. — Прим. ред.

Теорема 6 (Акс [1]). Теория класса всех конечных полей разрешима.

Теорема 7 (Шмелева [1]). Теория коммутативных групп разрешима.

Теорема 8 (Эренфойхт [1]). Теория линейно упорядоченных множеств разрешима.

Этот результат был объявлен в короткой заметке. Первое полное доказательство опубликовано Лейхли и Леонардом [1]. Как будет видно в следующей главе, этот результат является простым следствием метода статьи Рабина [2].

Наконец, приведем один специальный случай более общего результата о моделях, относящегося к разрешимости.

Пусть $\mathfrak{A} = \langle A, f_0, \dots, f_i, \dots \rangle_{i < \alpha}$ и $\mathfrak{B} = \langle B, g_0, \dots, g_i, \dots \rangle_{i < \alpha}$, $\alpha \leq \omega$, — подобные алгебры одного типа, т. е. f_i и g_i являются n_i -арными операциями на $\mathfrak{A}$ и $\mathfrak{B}$ соответственно. Прямое произведение $\mathfrak{A} \times \mathfrak{B}$ определяется очевидным образом.

Теорема 9. Если $\text{Th}(\mathfrak{A})$ и $\text{Th}(\mathfrak{B})$ разрешимы, то разрешима и $\text{Th}(\mathfrak{A} \times \mathfrak{B})$.

Это есть лишь особый случай общего изучения выражимых в логике первого порядка свойств произведений систем и классов систем, начатого Мостовским [1] и развитого Феферманом и Воотом [1]. Мы ограничиваем себя лишь этим специальным случаем для того, чтобы избежать сложных определений, появляющихся в общей теории.

Метод произведений является мощным средством получения новых результатов о разрешимости из уже известных. Следующий пример принадлежит Мостовскому. Мы знаем, что $\text{Th}(\langle \omega, + \rangle)$ разрешима, см. 1.3. Из теории общих произведений следует, что прямая сумма $\mathfrak{B}$ из ω копий $\langle \omega, + \rangle$ имеет разрешимую теорию. Основное множество P состоит из всех векторов длины ω :

$$v = \langle n_0, \dots, n_k, 0, 0, \dots \rangle, \quad n_i \in \omega, \quad k = 0, 1, \dots,$$

а операцией является покомпонентное сложение. Определим отображение $\psi(v) = p_0^{n_0} \dots p_k^{n_k}$, где $p_i = (i+1)$ -е простое число. Отображение ψ является изоморфизмом $\psi: \mathfrak{B} \rightarrow \langle \omega, \{0\}, \cdot \rangle = \mathfrak{M}$ на мультипликативную полугруппу целых чисел. Следовательно, $\text{Th}(\mathfrak{M})$ разрешима; этот результат принадлежит Скулему.

§ 3. Метод интерпретаций

3.1. Семантические интерпретации. Для начала опишем в общих чертах, что означает построение системы $\mathfrak{A} = \langle A, R \rangle$ из системы $\mathfrak{B} = \langle B, S_1, S_2, \dots \rangle$ посредством определенных предикатов. Нам нужны некоторые предварительные понятия. Пусть

L — язык для $\mathfrak{A}$, а L_1 — язык для $\mathfrak{B}$. Пусть $D(x, y, \dots)$ — некоторая формула языка L_1 , где x — свободная переменная, но, возможно, имеются и другие свободные переменные $y, \dots$, играющие роль параметров. Будем сокращать $D(x, y, \dots)$ до $D(x)$ или даже до D .

Если F — некоторая формула языка L_1 , то формула F^D получается из F посредством релятивизации всех кванторов формулы F к D ; эта релятивизация определяется индуктивно по сложности F с помощью следующих правил. Если F не содержит связок, то $F^D = F$. Если $F = E \vee G$ или $F = \neg E$, то $F^D = E^D \vee G^D$ или $F^D = \neg E^D$ соответственно. Основными являются случаи, когда $F = \exists u G$ и $F = \forall u G$:

$$(\exists u G)^D = \exists u [D(u) \wedge G^D], \quad (\forall u G)^D = \forall u [D(u) \rightarrow G^D].$$

Здесь $D(u)$ означает $D(u, y, \dots)$, т. е. u подставляется вместо x в D . Заметим, что для правильного проведения релятивизации мы должны иногда алфавитно изменить имена некоторых переменных в F , чтобы избежать связывания переменных, отличных от x , но свободных в D .

Пусть $b \in B, \dots$ — последовательность значений в B для параметров $y, \dots$ из D . Определим $C = \{a: \mathfrak{B} \models D(a, b, \dots)\}$. Это множество определяется посредством D и специализации параметров $y = b, \dots$. Подмножество $C \subseteq B$ порождает подсистему $\mathfrak{C} = \langle C, S_1|_C, S_2|_C, \dots \rangle$ системы $\mathfrak{B}$.

Лемма. Пусть $F(z_1, \dots, z_n)$ — формула языка L_1 , а $D, B, b \in B, \dots$ и C таковы, как описано выше, тогда для $c_1, \dots, c_n \in C$

$\mathfrak{B} \models F^D(c_1, \dots, c_n)$ тогда и только тогда, когда $\mathfrak{C} \models F(c_1, \dots, c_n)$.

Итак, результатом релятивизации является преобразование выполнимости формулы F в системе $\mathfrak{B}$ в выполнимость в подсистеме $\mathfrak{C}$.

Следующая конструкция является несколько более сложной. Для упрощения обозначений ограничимся лишь формулой $D(x)$ языка L_1 , содержащей единственную свободную переменную x (параметров нет), и формулой $E(u, v)$ с двумя свободными переменными.

Определение 3. Система $\mathfrak{B}(D, E) = \langle C, R \rangle$, индуцированная в $\mathfrak{B}$ посредством $D(x)$ и $E(u, v)$, по определению имеет основное множество $C = \{c: \mathfrak{B} \models D(c)\}$ и бинарный предикат $R \subseteq C \times C$, $R = \{(b, c): b, c \in C, \mathfrak{B} \models E(b, c)\}$.

Пусть теперь $F(z_1, \dots, z_n)$ — формула языка с бинарным предикатным символом P , определим $F^{D, E}$ как формулу, полученную из F сначала с помощью преобразования F^D , а затем замены в F^D всех атомных формул $P(z_1, z_2)$ на $E(z_1, z_2)$. Заметим, что кванторы в $E(u, v)$ не релятивизируются к D . Следую-

шая лемма является по существу следствием предыдущей леммы. Она связывает выполнимость в индуцированной системе с выполнимостью в $\mathfrak{B}$.

Лемма. Для $c_1, \dots, c_n \in C$ имеем

$\mathfrak{B}(D, E) \models F(c_1, \dots, c_n)$ тогда и только тогда, когда

$$\mathfrak{B} \models F^{D, E}(c_1, \dots, c_n).$$

Применение к разрешимости основывается на следующей теореме, взятой из статьи Рабина [1].

Пусть T и T_1 — теории в языках L и L_1 соответственно, и пусть $\mathcal{K}$ и $\mathcal{K}_1$ — классы систем такие, что $T = \text{Th}(\mathcal{K})$, $T_1 = \text{Th}(\mathcal{K}_1)$. Предположим, что L имеет предикатные символы $P_0, \dots, P_k$ и не имеет функциональных символов.

Теорема 10. Пусть $D(x, y, \dots)$ — формула языка L_1 , а $E = (E_0, \dots, E_k)$ — последовательность формул таких, что если P_i является n_i -арным предикатным символом, то E_i имеет n_i свободных переменных, $0 \leq i \leq k$.

Предположим, что:

(1) для всех $\mathfrak{B} \in \mathcal{K}_1$ и всех значений $y = b, \dots$ параметров D имеем $\mathfrak{B}(D, E) \models T$;

(2) для каждой $\mathfrak{A} = \langle A, R_0, \dots, R_k \rangle \in \mathcal{K}$ существует модель $\mathfrak{B} \in \mathcal{K}_1$ и специализация $y = b \in B, \dots$ такая, что для этой специализации $\mathfrak{A} \approx \mathfrak{B}(D, E)$.

При этих условиях, если T_1 разрешима, то разрешима и T . Обратно, если T неразрешима, то неразрешима и T_1 .

Доказательство. Пусть F — предложение языка L , положим $G = \forall y \dots F^{D, E}$, где кванторы всеобщности навешиваются на все переменные-параметры в $D(x, y, \dots)$ (эти переменные свободны в F , если F содержит кванторы). По второй лемме для любой $\mathfrak{B} \in \mathcal{K}_1$ и специализации $y = b \in B, \dots$

$\mathfrak{B} \models F^{D, E}(b, \dots)$ тогда и только тогда, когда $\mathfrak{B}(D, E) \models F$. (*)

Теперь пусть $F \in T$. Из условия (1) следует, что $\mathfrak{B}(D, E) \models F$ для любых $\mathfrak{B} \in \mathcal{K}_1$, $y = b, \dots$. Следовательно, левая часть (*) выполняется, а значит, $\mathfrak{B} \models G$. Но $\mathfrak{B} \in \mathcal{K}_1$ была произвольной, поэтому $G \in \text{Th}(\mathcal{K}_1) = T_1$.

Далее допустим, что $G \in T_1$. Пусть $\mathfrak{A} \in \mathcal{K}$, тогда в силу (2) для некоторых $\mathfrak{B} \in \mathcal{K}_1$ и $y = b, \dots$ получаем $\mathfrak{A} \approx \mathfrak{B}(D, E)$. Имеем $\mathfrak{B} \models G$, следовательно, $\mathfrak{B} \models F^{D, E}(b, \dots)$. Тогда в силу (*) $\mathfrak{B}(D, E) \models F$, а значит, $\mathfrak{A} \models F$; итак, $\mathcal{K} \models F$ и $F \in T$.

Пусть T_1 разрешима и F — любое предложение языка L . Построим G ; так как $G \in T_1$ тогда и только тогда, когда $F \in T$, то мы можем определить, будет ли $F \in T$. $\square$

Замечание. Легко видеть, что если T конечно аксиоматизируема, то условие (1) может быть отброшено при подходящей модификации построения G .

Мы формулировали теорему 10 для языков первого порядка. С подходящими изменениями она выполняется также, если язык L_1 или даже оба языка L и L_1 являются языками второго порядка. Единственным случаем языка второго порядка, который интересен с точки зрения разрешимости, является монадический язык второго порядка, переменные в котором изменяются по подмножествам основного множества, но не изменяются по предикатам на основном множестве. Это так, потому что, как только переменные будут изменяться, скажем, по бинарным предикатам, то теория всех истинных предложений языка второго порядка станет неразрешимой.

Допустим, что L_1 имеет переменные $A, B, \dots$, значениями которых являются множества. Тогда релятивизованная формула $D(x)$ может иметь вид $x \in A$ и A будет параметром в $F^{D, E}$. Если L имеет переменные, то они также должны быть релятивизованы к D по правилам таким, как

$$(\forall A F)^D = \forall A [\forall x [x \in A \rightarrow D(x)] \rightarrow F^D].$$

С этими естественными изменениями теорема 10 выполняется для монадических языков второго порядка.

3.2. Разрешимые теории второго порядка. Рассмотрим монадический язык второго порядка L_1 с переменными $A, B, \dots$, значениями которых являются множества, и с предикатом $\in$. Чтобы быть подходящим для системы $\mathfrak{A} = \langle A, R \rangle$, где R , например, — бинарный предикат, L_1 должен иметь также бинарный предикатный символ R . Для такого языка L_1 (монадической) теорией второго порядка $\text{Th}_2(\mathfrak{A})$ для $\mathfrak{A}$ называется множество всех предложений языка L_1 , истинных в $\mathfrak{A}$. Аналогично определяется $\text{Th}_2(\mathcal{K})$ для класса $\mathcal{K}$ однотипных систем как $\text{Th}_2(\mathcal{K}) = \bigcap_{\mathfrak{A} \in \mathcal{K}} \text{Th}_2(\mathfrak{A})$.

Первые важные результаты о разрешимости теорий второго порядка, кроме разрешимости чистой монадической логики второго порядка, имеют дело с разрешимостью $\text{Th}_2(\langle \omega, S \rangle)$, где $S(x) = x + 1$ является функцией следования.

Теорема 11 (Бюхи [2]). $\text{Th}_2(\langle \omega, S \rangle)$ разрешима.

Этот результат вначале был доказан в более слабой форме. Рассмотрим слабый монадический язык второго порядка LW с переменными $\alpha, \beta, \dots$, значениями которых являются конечные подмножества основного множества. Теория системы $\mathfrak{A}$ в языке LW будет называться слабой (монадической) теорией второго порядка для $\mathfrak{A}$ и обозначаться через $\text{Th}_w(\mathfrak{A})$.

Бюхи [1] и Элгот [1] доказали, что $\text{Th}_w(\langle \omega, S \rangle)$ разрешима.

Для дальнейших ссылок обозначим $\text{Th}_2(\omega, S) = \text{SIS}$ (теория второго порядка одной функции следования) и $\text{Th}_w(\langle \omega, S \rangle) = \text{WSIS}$.

Мы не можем входить в детали этих доказательств о разрешимости. Скажем только, что они используют методы и результаты теории автоматов. В случае WSIS используются понятия и результаты из теории автоматов, оперирующих конечными последовательностями; этот случай очень прост и ясен. Доказательство разрешимости SIS требует нового понятия автомата, действующего на бесконечных ω -последовательностях.

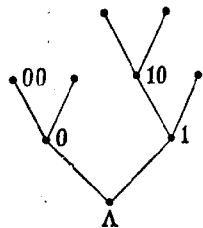


Рис. 1.

3.3. Теорема о дереве. Большинство доказательств о разрешимости посредством интерпретаций использует теорему о дереве, принадлежащую Рабину [2].

Пусть $T = \{0, 1\}^*$ — множество всех конечных слов (последовательностей) $x = x_1 x_2 \dots x_n$, $x_i \in \{0, 1\}$, над алфавитом $\{0, 1\}$. Пустая последовательность Λ также лежит в $\{0, 1\}^*$.

Множество T можно также интерпретировать как бесконечное бинарное дерево (рис. 1). Условившись помещать 0 налево, а 1 направо, устанавливаем соответствие между вершинами дерева и множеством T следующим образом. Корень соответствует Λ ; правый последователь соответствует 1, а левый последователь — 0; левый последователь для 1 есть 10 и т. д.

Итак, у нас есть на T две функции следования $r_0(x) = x0$, $r_1(x) = x1$, $x \in T$. Пусть L_1 — подходящий монадический язык второго порядка, имеющий функциональные символы r_0, r_1 . Множество всех предложений из L_1 , истинных в $\langle T, r_0, r_1 \rangle$, будет обозначаться, как обычно, через $\text{Th}_2(\langle T, r_0, r_1 \rangle)$.

Теорема 12 (теорема о разрешимости для дерева). Теория второго порядка для двух функций следования $\text{S2S} = \text{Th}_2(\langle T, r_0, r_1 \rangle)$ разрешима.

Для доказательства этой теоремы требуется далеко идущее расширение теории автоматов, включающее в себя конечные автоматы, оперирующие бесконечными деревьями. Одна из интересных особенностей доказательства состоит в том, что даже если мы хотим получить некоторые факты о конечных объектах, а именно о конечных автоматах, существенно используется трансфинитная индукция по ординалам до первого несчетного кардинала ω_1 .

3.4. Снова об арифметике Пресбургера. Бюхи и Элгот использовали разрешимость WSIS для доказательства разрешимости PAR.

Ключевая идея — использовать конечные множества $\alpha \subset \omega$, чтобы закодировать целые числа. Пусть χ_α — характеристическая функция множества α . Определим

$$n(\alpha) = 1 \cdot \chi_\alpha(0) + 2 \cdot \chi_\alpha(1) + \dots + 2^x \cdot \chi_\alpha(x) + \dots$$

Построим формулу $A(\alpha, \beta, \gamma)$ в языке для WSIS, которая будет истинной в $\langle \omega, S \rangle$ для $\alpha, \beta, \gamma \subset \omega$ тогда и только тогда, когда $n(\alpha) + n(\beta) = n(\gamma)$. Это делается путем рассмотрения последовательности χ_δ , осуществляющей добавление $n(\beta)$ к $n(\alpha)$, где $n(\alpha)$ и $n(2)$ рассматриваются как двоичные числа:

$$A(\alpha, \beta, \gamma) = \exists \delta \forall x [\neg 0 \in \delta$$

$$\wedge [S(x) \in \delta \leftrightarrow (x \in \alpha \wedge x \in \beta)$$

$$\vee (x \in \alpha \wedge x \in \delta) \vee (x \in \beta \wedge x \in \delta)] \wedge [x \in \gamma$$

$$\leftrightarrow (x \in \alpha \wedge x \in \beta \wedge x \in \delta)$$

$$\vee (x \in \alpha \wedge \neg x \in \beta \wedge \neg x \in \delta \dots)].$$

Систематически используя $A(\alpha, \beta, \gamma)$ для замены $a + b = c$ в предложении F из PAR, получим предложение G в языке для WSIS. Имеем $F \in \text{Th}(\langle \omega, + \rangle)$ тогда и только тогда, когда $G \in \text{WSIS}$; таким образом, мы можем решать, будет ли F истинным.

3.5. Теория второго порядка для линейного порядка. Пусть $K_{\leq}^{\omega}$ — класс всех линейных упорядоченных множеств $\langle A, \leq \rangle \models \text{OR}$ с не более чем счетным основным множеством, $c(A) \leq \omega$.

Теорема 13 (Рабин [2]). $\text{Th}_2(K_{\leq}^{\omega})$ разрешима.

Доказательство. Определим на T частичный порядок, где x — начальный отрезок y , посредством формулы $x \leq y$. А именно:

$$x \leq y = \forall A [x \in A \wedge \forall z [z \in A \rightarrow r_0(z) \in A \wedge r_1(z) \in A] \rightarrow y \in A].$$

Также определим лексикографический порядок

$$x \leq y = x \leq y \vee \exists z [r_0(z) \leq x \wedge r_1(z) \leq y].$$

Упорядоченное множество $\langle \{x1: x \in T\}, \leq \rangle$ имеет порядковый тип η . Следовательно, для каждого не более чем счетного упорядоченного множества $\langle A, \leq \rangle$ существует множество $\bar{A} \subseteq T$ такое, что $\langle A, \leq \rangle \approx \langle \bar{A}, \leq \rangle$. Используя релятивизованную формулу $D(x, A) = x \in A$ и заменяя $\leq$ на $\leq$, видим, что $\text{Th}_2(K_{\leq}^{\omega})$ может быть интерпретирована в S2S в смысле теоремы 9. Следовательно, $\text{Th}_2(K_{\leq}^{\omega})$ разрешима. $\square$

В качестве простых следствий получаются некоторые трудные классические результаты.

Следствие. $\text{Th}(\text{OR})$ — теория линейно упорядоченных множеств — разрешима.

Из теоремы Скулема — Лёвенгейма следует, что каждая система $\langle A, \leq \rangle \models \text{OR}$ элементарно эквивалентна некоторому $B \in K_{\leq}^{\omega}$. Следовательно, $\text{Th}(\text{OR}) = \text{Th}(K_{\leq}^{\omega})$. Последняя теория, конечно, разрешима.

Монадический язык второго порядка достаточно силен, чтобы в нем было выражено то, что какое-то множество вполне упорядочено. А именно, предложение

$$W = \forall A \forall x \exists y \forall z [x \in A \rightarrow y \in A \wedge [z \in A \rightarrow y \leq z]]$$

имеет следующее свойство: линейно упорядоченное множество $\mathfrak{A}$ удовлетворяет $\mathfrak{A} \models W$ тогда и только тогда, когда $\mathfrak{A}$ вполне упорядочено. Сразу получаем

Следствие. Монадическая теория второго порядка не более чем счетных вполне упорядоченных множеств разрешима.

Доказательство. Для любого предложения F имеем $K_{\leq}^{\omega} \models W \rightarrow F$ тогда и только тогда, когда F истинно во всех не более чем счетных вполне упорядоченных множествах. $\square$

Каждое вполне упорядоченное множество $\langle B, \leq \rangle$ имеет не более чем счетную элементарную подмодель $\mathfrak{A} = \langle A, \leq \rangle < \langle B, \leq \rangle$. Следовательно, теория первого порядка для вполне упорядоченных множеств такова же, как и теория первого порядка для не более чем счетных вполне упорядоченных множеств, которая по предыдущему следствию разрешима. Итак, теория первого порядка для вполне упорядоченных множеств разрешима; этот результат принадлежит Тарскому и Мостовскому [1].

3.6. Разрешимость в топологии. В S2S можно определить понятие пути $A \subseteq T$, ведущего от корня в бесконечность:

$$\text{Path}(A) = A \in A \wedge \forall x \forall y [x \in A \rightarrow [r_0(x) \in A \vee r_1(x) \in A] \wedge [y \leq x \rightarrow y \in A] \wedge \neg [r_0(x) \in A \wedge r_1(x) \in A]].$$

Рассмотрим $\{0, 1\}^{\omega}$ с обычной тихоновской топологией произведения. Это хорошо известный канторовский дисконтинуум CD. Для каждой точки $p: \omega \rightarrow \{0, 1\}$ множества $A \subseteq T$ всех начальных сегментов p составляет путь в T , и это соответствие взаимно однозначно. Мы также можем ввести в S2S топологию CD. Пусть $B \subseteq T$ — произвольное множество, являющееся объединением некоторых путей, тогда множество всех путей $A \subseteq B$ является замкнутым подмножеством CD и снова такое соответствие будет взаимно однозначным. Определим

$$\text{CL}(B) = \forall x [x \in B \rightarrow \exists A [\text{Path}(A) \wedge A \subseteq B \wedge x \in A]].$$

Теорема 14 (Рабин [2]). Монадическая теория второго порядка CD, значениями переменных которой являются замкнутые множества, разрешима.

Доказательство. Пусть F — любое предложение в языке для CD. Релятивизуем все предметные переменные к $\text{Path}(X)$ и все (замкнутые) переменные по множествам к $\text{CL}(B)$, заменим все формулы $x \in B$ из F на $X \subseteq B$. Получившееся предложение E истинно в S2S тогда и только тогда, когда $\text{CD} \models F$. $\square$

С некоторыми изменениями, учитывающими то, что две различные последовательности $p, q \in \{0, 1\}^{\omega}$ могут представлять один и тот же элемент сегмента $[0, 1]$ действительной прямой, вышеприведенное доказательство может быть изменено, чтобы охватить и случай $[0, 1]$.

3.7. Булевы алгебры. Следующая теорема утверждает разрешимость $\text{Th}(\text{BA})$ — элементарной теории булевых алгебр — и даже нечто большее.

Теорема 15 (Рабин [2]). Пусть $\mathfrak{B}_{\omega}$ — свободная булева алгебра с ω образующими и LI — язык второго порядка, соответствующий булевым алгебрам, значениями переменных по множествам для которого являются идеалы этих алгебр. Теория $\text{Th}_1(\mathfrak{B}_{\omega})$ алгебры $\mathfrak{B}_{\omega}$ в языке LI разрешима.

Доказательство. Множество всех открыто-замкнутых подмножеств множества CD является булевой алгеброй, изоморфной $\mathfrak{B}_{\omega}$, поэтому мы можем отождествить его с $\mathfrak{B}_{\omega}$. Если $I \subseteq \mathfrak{B}_{\omega}$ — любой идеал, то $U(I) = \bigcup_{S \in I} S$ является открытым мно-

жеством из CD. Множества $U(I)$ пробегают по всем открытым множествам из CD и это соответствие взаимно однозначно. Далее, для $S \in \mathfrak{B}_{\omega}$ имеем, что $S \subseteq U(I)$ тогда и только тогда, когда $S \in I$.

Каждое предложение языка LI может быть, следовательно, переведено в предложение о CD посредством релятивизации предметных переменных к переменным, изменяющимся по открыто-замкнутым подмножествам из CD, релятивизации переменных, изменяющихся по идеалам, к переменным, изменяющимся по открытым множествам (т. е. дополнениям к замкнутым множествам) из CD, и замены $x \in I$ на $X \subseteq I$. Получившееся предложение истинно в CD тогда и только тогда, когда исходное предложение истинно в $\text{Th}_1(\mathfrak{B}_{\omega})$, а первая из этих проблем разрешима. $\square$

Теперь пусть $\mathfrak{B}$ — любая счетная булева алгебра. Тогда существует идеал $I \subseteq \mathfrak{B}_{\omega}$ такой, что $\mathfrak{B} \approx \mathfrak{B}_{\omega}/I$, и идеалы $J \subseteq \mathfrak{B}$ находятся в естественном одно-однозначном соответствии с идеалами $J \subseteq I \subseteq \mathfrak{B}_{\omega}$. По теореме об интерпретации это приводит к следующей теореме. Обозначим через BA^{ω} класс всех счетных булевых алгебр.

Теорема 16. Теория $\text{Th}_1(\text{BA}^{\omega})$ в языке LI всех счетных булевых алгебр разрешима.

Если ограничиться предложением $G = \forall I_1 \dots \forall I_n F(I_1, \dots, I_n)$, где F — формула без кванторов по идеалам, то $G \in \text{Th}_1(\text{BA}^\omega)$ тогда и только тогда, когда $F(I_1, \dots, I_n)$ истинна в каждой счетной булевой алгебре $\mathfrak{B} = \langle B, \cup, \cap, ', I_1, I_2, \dots \rangle$, где $I_1, I_2, \dots$ — идеалы B . Используя теорему Скулема — Лёвенгейма, немедленно получаем, что справедлива

Теорема 17 (Рабин [2]). *Элементарная теория всех булевых алгебр с последовательностью выделенных идеалов разрешима.*

Эту теорему можно рассматривать как усиление результата Ершова [1], который утверждает разрешимость булевых алгебр с выделенным простым идеалом (ультрафильтр).

3.8. Неклассические логики. До сих пор все представленные в этой главе результаты имели дело с теориями, формализованными внутри классической логики. В литературе встречаются многие обобщения и модификации классической логики. Одни получаются отбрасыванием некоторых аксиом классической логики, например интуиционистская логика, другие — добавлением логических операций или связей, как в модальной или временной логиках. Важные философские рассуждения и положения, связанные с основаниями математики и логики, оправдывают введение и изучение этих систем.

Хотя разрешимость классического пропозиционального исчисления тривиальна, разрешимость этих фрагментов и обогащений (добавлением логических операций) даже для пропозициональной логики во многих случаях далеко не очевидна. Метод интерпретаций оказывается мощным инструментом для решения почти всех вопросов о разрешимости в этом направлении. Проиллюстрируем это двумя примерами. Интересующийся читатель может обратиться к статье Габбая [1], которая является источником для этих примеров и в которой можно найти много других результатов и ссылок.

Рассматриваемый здесь класс *модальных пропозициональных логик* имеет, помимо обычных пропозициональных связей, оператор $\Box$, предназначенный для выражения необходимости, так что $\Box A$ должно обозначать «необходимо A ».

Основная аксиоматическая система S_2 содержит все теоремы и правила классической логики и вдобавок следующие аксиомы и правила вывода:

$\Box [A \rightarrow B] \rightarrow [\Box A \rightarrow \Box B]$, из $\vdash A \rightarrow B$ выводится $\vdash \Box A \rightarrow \Box B$.

Система K получается из S_2 добавлением правила

из $\vdash A$ выводится $\vdash \Box A$.

Система T есть система K плюс аксиома $\Box A \rightarrow A$, а система S_4 есть система T плюс аксиома $\Box A \rightarrow \Box \Box A$.

Имеется много и других расширений системы S_2 . Конкретные аксиомы варьируются разными авторами в зависимости от их веры в то, какие правильные свойства должны быть у $\Box$.

Опишем теперь *интуиционистскую временную логику* J_1 . Эта система имеет, помимо связей $\rightarrow, \vee, \wedge, f$ (обозначающее ложность), операторы G и H . Для формулы A формула GA читается « A будет всегда истинной», а формула HA читается « A была всегда истинной». Формула $\neg A$ является сокращением $A \rightarrow f$.

Аксиомы и правила вывода для J_1 будут такие же, как и для интуиционистской логики (включая *modus ponens*), и еще следующие:

$$G[A \rightarrow B] \rightarrow [GA \rightarrow GB],$$

$$H[A \rightarrow B] \rightarrow [HA \rightarrow HB],$$

$$A \vee G \neg HA, \quad A \vee H \neg GA,$$

из $\vdash A$ выводятся $\vdash GA$ и $\vdash HA$.

Крипке, Габбай и другие построили для многих неклассических логик семантические системы, основанные на деревьях и оценке на деревьях. Тогда формула оказывается выводимой, если она имеет некоторое свойство при всех возможных оценках или интерпретациях. Детальное определение интерпретации должно, конечно, зависеть от изучаемой системы аксиом.

Оказывается, что эти семантики, связанные с деревьями, выразимы в S_2S и в ее вариантах. Это делает возможным вывести многие позитивные результаты о разрешимости из теоремы о дереве.

§ 4. Сложность разрешающих процедур

4.1. Вычисления на машинах Тьюринга. Как было отмечено во введении, многие результаты о нижних границах на сложность решения проблем разрешимости получены лишь в последние годы. В частности, почти для всех теорий, упоминаемых в этой главе, были указаны проблемы разрешимости, которые не допускают никаких более простых разрешающих процедур.

Так как нашей задачей будет доказательство того, что каждая разрешающая процедура для теории T сложна, мы должны остановиться на каком-нибудь определенном уточнении понятия алгоритма и определенном соглашении для подсчета вычислительных шагов. В качестве разрешающих процедур выберем алгоритмы, представленные в виде машин Тьюринга, а исполнение элементарной инструкции будет считаться основным шагом.

Все результаты будут иметь следующий вид: для любой разрешающей процедуры P для изучаемой теории T существуют

предложения A размера n (т. е. записанные с помощью n символов), для которых P требует по крайней мере $f(cn)$ шагов, чтобы получить ответ, будет $A \in T$ или нет. Здесь $f(n)$ будет по меньшей мере экспоненциальной функцией вида 2^n , а c — фиксированным числом $0 < c$. В связи с экспоненциальной природой результатов выбор уточнения понятия алгоритма и вычисления не играет большой роли. Время вычисления при различных точных формулировках для одного и того же алгоритма изменяется самое большее по полиномиальному закону.

Метод для получения этих результатов о внутренней сложности основывается на следующем рассмотрении.

Зашифруем программы для машин Тьюринга единообразным стандартным образом посредством последовательностей $P \in \{0, 1\}^*$. Для любого слова x определим $l(x)$ как длину x , т. е. число символов в x . В частности, для целого числа в двоичной записи $l(n)$ означает число разрядов в n .

Пусть T — теория в языке L , а $f(k)$ — функция, удовлетворяющая следующим условиям. Существует константа $0 < d$ такая, что для каждой программы P и целого числа n существует такое предложение $S(n, P)$ языка L , что:

- (i) $l(S(n, P)) \leq d(l(n) + l(P))$,
- (ii) $S(n, P) \in T$ тогда и только тогда, когда вычисление посредством программы P с входом n (рассматриваемым как последовательность из нулей и единиц) останавливается менее чем за $f(l(n))$ шагов,
- (iii) формула $S(n, P)$ может быть эффективно получена по n , P менее чем за $g(l(n) + l(P))$ шагов, где $g(k)$ — некоторый фиксированный полином.

Если $f(k)$ — функция, растущая по крайней мере с экспоненциальной скоростью, то при условиях, указанных выше, существует константа $0 < c$ такая, что для бесконечно многих n существует предложение F языка L , $l(F) = n$, для которого P требует по крайней мере $f(cn)$ шагов для ответа на вопрос о том, будет ли $F \in T$.

Доказательство вышеннаписанного утверждения проводится с помощью обычных диагональных рассуждений. Предположим, чтобы прийти к противоречию, что существует разрешающая процедура P для T , которая требует для каждого предложения F менее чем $f(cl(F))$ шагов для ответа на вопрос о том, будет ли $F \in T$. Если $c = 1/2d$, то, используя предложение $S(n, P)$, можно построить машину Тьюринга, которая останавливается на входе n_0 тогда и только тогда, когда она не останавливается на этом входе.

4.2. Теория WSIS. Мейер [1] доказал, что проблема разрешимости для WSIS имеет очень высокую внутреннюю сложность.

Определим функцию $F(n, m)$ так:

$$F(n, 1) = 2^n, \quad F(n, m+1) = 2^{F(n, m)}, \quad m = 1, 2, \dots$$

Если $0 < d$, то $f(n) = F(n, [dn])$ является функцией возведения в степень при помощи длинной серии двоек.

Теорема 18. *Существует константа $0 < d$ такая, что для функции $f(n) = F(n, [dn])$ и для каждого алгоритма P , решающего проблему разрешимости для WSIS, существует бесконечно много формул A таких, что P требует более чем $f(l(A))$ шагов для ответа на вопрос о том, будет ли $A \in \text{WSIS}$.*

Доказательство (набросок). В языке WSIS у нас имеются переменные $\alpha, \beta, \dots$, значениями которых являются конечные подмножества множества ω . Пара подмножеств α, β может быть использована для кодирования последовательности $p \in \{0, 1\}^*$, $l(p) = c(\alpha)$. Если $\alpha = \{i_0 < i_1 < \dots < i_{k-1}\}$, то $i_j \in \beta$ тогда и только тогда, когда $p(j) = 1$. Для фиксированного α и варьируемого β пара (α, β) будет пробегать коды всех последовательностей p таких, что $l(p) = c(\alpha)$.

Для описанного выше α и $x \in \alpha$, $y \in \alpha$ будем говорить, что x и y находятся на расстоянии d в α , если $x = i_j$, $y = i_{j+d}$ для $j \leq k-1-d$.

Теперь можно показать, что для каждого n существуют две формулы $A_n(\alpha)$ и $D_n(\alpha, x, y)$ из WSIS, имеющие длину $O(n)$ и обладающие следующим свойством. Из $A_n(\alpha)$ следует, что α имеет некоторую структуру и мощность по меньшей мере $(F(n, n))^2$. Для множеств α , для которых $A_n(\alpha)$ выполняется, $D_n(\alpha, x, y)$ означает, что x и y находятся на расстоянии $F(n, n)$ в α .

Допустим, что мы имеем вычисление на машине Тьюринга с числом шагов, меньшим чем $F(n, n)$. Тогда машинная головка никогда не отдалится от начальной ячейки более чем на $F(n, n)$ ячеек. Без ограничения общности можно предположить, что машина никогда не будет заходить левее начальной ячейки.

Напишем по порядку слева направо полное описание содержимого первых (слева) $F(n, n)$ ячеек после выполнения каждой из машинных инструкций. Это будет последовательность длины не больше чем $(F(n, n))^2$. Эта последовательность может быть закодирована с помощью некоторого $\alpha \subset \omega$, удовлетворяющего $A_n(\alpha)$, и дополнительных множеств $\beta_0, \beta_1, \dots, \beta_k$. Пара (α, β_0) будет кодировать содержимое ленты, а $((\alpha, \beta_1), \dots, (\alpha, \beta_k))$ будет кодировать последовательность положений головки и машинных состояний.

Формула $D_n(\alpha, x, y)$ играет роль «линейки», отмеривающей протяженность длины $F(n, n)$.

Вместе с (определимым) порядком на ω это поможет нам выразить то, что два последовательных массива из последова-

тельности, закодированной при помощи $(\alpha, \beta_0, \dots, \beta_k)$, связаны посредством выполнения одной инструкции машины Тьюринга.

Уточняя детали и комбинируя вышеописанные идеи, можно показать, что для WSIS существует конструкция формулы $S(n, P)$ со свойствами, перечисленными в 4.1. Отсюда следует теорема 18. $\square$

Э. Робертсон и Л. Стокмейер (в своей диссертации) независимо заметили при подробном рассмотрении полного доказательства теоремы 18, что оно проходит для относящихся к $\langle \omega, \leq \rangle$ предложений, являющихся универсальными в монадической логике второго порядка. Это означает, что предложение может содержать кванторы по множествам, которые все являются кванторами $\forall$ и находятся в начале предложения. На самом деле достаточно одной переменной, значениями которой являются множества. Из этого более подробного результата методом прямой интерпретации получается следующая теорема, принадлежащая Мейеру [1].

Теорема 19. *Теория первого порядка $\text{Th}(\text{OR})$ линейно упорядоченных множеств обладает внутренней сложностью $F(n, [dn])$ для некоторого $0 < d$.*

Подробная формулировка теоремы 19, так же как и результаты следующего пункта, делается аналогично теореме 18.

Анализ разрешающих процедур для WSIS и даже S2S, основанный на теории автоматов, показывает, что они занимают время $F(n, [cn])$ для формул A длины n при подходящем $0 < c$. Ввиду теорем 18, 19 эти результаты с количественной точки зрения являются наилучшими возможными. Возникает, конечно, вопрос о высоте $[cn]$ множества двоек, но он зависит от обозначений для формул и, по-видимому, на него нелегко ответить.

4.3. Теории сложения и вещественно замкнутых полей. Для классических теорий $\text{Th}(\langle \omega, + \rangle) = \text{PAR}$ и теории поля вещественных чисел $\text{Th}(\text{RLC})$ результаты о внутренней сложности не столь опустошительны, как для WSIS. Тем не менее оказалось, что эти теории по крайней мере экспоненциально сложны и в некоторых случаях сверхэкспоненциально сложны. Таким образом, заявление, что существование разрешающей процедуры делает эти теории тривиальными, не подтверждается.

Теорема 20 (Фишер и Рабин [1]). *Существует константа $0 < c$ такая, что разрешающая процедура для арифметики Пресбургера PAR обладает сложностью по меньшей мере $2^{2^{cn}}$.*

Доказательство (набросок). Мы видели, что возможность установления результатов о внутренней сложности для

функции сложности $f(n)$ основывается на возможности закодировать внутри теории последовательность длины $(f(n))^2$ при помощи формул размера $O(n)$.

В языке модели $\langle \omega, + \rangle$ существуют формулы $P_n(x, y, z)$ размера $O(n)$, которые выполняются для $x, y, z \in \omega$ тогда и только тогда, когда $x, y, z < F(n, 3)$ и $x \cdot y = z$. Таким образом, эта формула, включающая только $+$ и имеющая размер $O(n)$, ко-

дирует таблицу умножения до 2^{2^n} . Используя натуральные числа для кодирования последовательностей из 0 и 1, можно закодировать последовательности длины до $(2^{2^n})^2$, используя $P_{n+1}(x, y, z)$. $\square$

Нижняя граница на сложность теории $\text{Th}(\text{RLC}) = \text{Th}(\langle \mathbb{R}, +, \cdot \rangle)$, где $\mathbb{R}$ — поле вещественных чисел, получается при рассмотрении только $\langle \mathbb{R}, + \rangle$.

Теорема 21 (Фишер и Рабин [1]). *$\text{Th}(\langle \mathbb{R}, + \rangle)$, а поэтому и $\text{Th}(\text{RLC})$ обладает внутренней сложностью по меньшей мере 2^{cn} для некоторого $0 < c$.*

Доказательство аналогично доказательству теоремы 20. В этом случае возможно представить (с точностью до изоморфизма) при помощи короткой формулы таблицу умножения натуральных чисел до 2^{2^n} .

Для теории модели $\mathfrak{M} = \langle \omega, \cdot \rangle$ умножения натуральных чисел ситуация даже хуже в соответствии с упомянутой в работе Фишера и Рабина [1] теоремой, доказательство которой будет дано в намеченной к публикации статье Фишера и Рабина.

Теорема 22. *Теория $\text{Th}(\langle \omega, \cdot \rangle)$ умножения натуральных чисел обладает внутренней сложностью по меньшей мере $F(cn, 3)$, т. е. $2^{2^{cn}}$ для некоторого $0 < c$.*

Алгоритмы, тщательно построенные различными исследователями, все же наводят на мысль, что вышеупомянутые результаты о нижних границах являются наилучшими возможными.

4.4. Пропозициональные исчисления и $P = NP$. При изучении различных абстрактных вычислительных моделей обычно различают детерминированные и недетерминированные алгоритмы. Если машине Тьюринга задать некоторую комбинацию из состояния и символа, то она проделает вполне определенный основной шаг вычисления (атомарное движение). Общий процесс вычисления, следовательно, полностью определяется машиной Тьюринга (программой), начальным состоянием и начальными данными на ленте. Детерминированное поведение является, конечно, характерной чертой всех современных вычислительных машин.

Понятие *недетерминированных вычислений* или программ имеет фундаментальную важность при теоретическом изучении свойств алгоритмов. Недетерминированная программа P для

заданной комбинации состояния и символа разрешает выполнение одного из нескольких возможных основных движений. Например, состояние q_3 при заданной 1 может вызвать либо $(0, L, 7)$ (стереть 1, сдвинуться влево, перейти состояние q_7), либо $(1, P, 15)$. Таким образом, в недетерминированной программе каждой паре (q, b) , где q — состояние, а b — символ, соответствует множество троек (c, M, q_i) , где c — символ, $M \in \{L, P\}$, q_i — состояние.

Начав в состоянии q_0 на входной ленте, программа P имеет возможность пойти по любой из многих последовательностей основных шагов, т. е. выполнить различные вычисления над входом. Нужно иметь в виду, что при каждой конкретной последовательности шагов выполняется определенное, единственное вычисление. Но возможны несколько различных последовательностей шагов.

Проиллюстрируем эту идею, показав, что существует недетерминированная программа P , которая разлагает любое составное (не простое) число n за $f(l(n))$ шагов, где $f(k)$ — полином.

Программа P имеет недетерминированные инструкции, позволяющие ей при заданном входе n (в двоичной системе счисления) записать на ленте любые два числа $1 < b, c < n$. Как замечено выше, при любой данной последовательности шагов будет записана одна пара (b, c) . Но для каждой пары существует последовательность шагов, приводящая к этой паре. После того как написаны b, c , программа переключается на детерминированное поведение, вычисляет $b \cdot c$ и проверяет, будет ли $b \cdot c = n$. Машина остановится только в случае, если последняя проверка даст равенство.

Можно заметить следующие особенности. Не каждое выполнение P для данного n закончится. Но если n действительно составное, то имеются вычисления, которые закончатся после некоторого числа шагов вычисления, это число полиномиально относительно размера $l(n)$ входа.

Все это можно подытожить, сказав, что то, что число является составным, может быть недетерминистически распознано в полиномиальное время.

Рассмотрим теперь задачу определения того, обладает ли пропозициональная формула $F(p_1, \dots, p_n)$ подстановкой значений истинности вместо пропозициональных переменных, для которой F становится истинной. Это есть *проблема выполнимости* для пропозиционального исчисления.

Поскольку $F(p_1, \dots, p_n)$ не является выполнимой тогда и только тогда, когда $\neg F(p_1, \dots, p_n)$ является формальной теоремой пропозиционального исчисления, проблема выполнимости тесно связана с проблемой разрешимости РС.

Снова легко построить недетерминированную программу, определяющую выполнимость F за число шагов, являющееся полиномиальным от $l(F)$.

Существует ли обычная детерминированная разрешающая процедура для выполнимости, которая требует времени (т. е. числа шагов), которое было бы полиномиальным от размеров формулы? Искомый полином, конечно, может расти быстрее, чем полином для недетерминированной программы.

Ответ на этот вопрос неизвестен. Тем не менее Кук [1] показал, что имеет место

Теорема 23. Если проблема выполнимости для пропозиционального исчисления может быть (детерминированно) решена за полиномиальное время, то любая проблема, которая может быть решена недетерминированно за полиномиальное время, может быть также решена за полиномиальное время при помощи детерминированного алгоритма.

Таким образом, вопрос о том, существует ли эффективный (полиномиальный) алгоритм для выполнимости, эквивалентен вопросу о том, будет ли класс алгоритмов, требующих полиномиального времени, равносильным классу NP недетерминированных алгоритмов, требующих полиномиального времени. Это — знаменитая проблема $P = NP$.

Алгоритмы из NP очень сильные. Например, изоморфизм между двумя данными графами размера n может быть недетерминированно найден за полиномиальное время. Аналогично для гамильтонова цикла. Эти задачи являются трудными комбинаторно-вычислительными задачами, не поддавшимися попыткам найти простое решение.

Кук, Карп [1] и другие нашли много примеров комбинаторных проблем разрешимости, которые сводятся к (и в некотором смысле эквивалентны) проблеме выполнимости. Вескость этих доказательств может подсказать, что проблема выполнимости, являясь столь могущественной, не имеет полиномиальной сложности, и, следовательно, $P \neq NP$. Но эта фундаментальная проблема остается еще не решенной.

ЛИТЕРАТУРА *)

Акс (Ax J.)

1. The elementary theory of finite fields. — Ann. Math., 1968, 88, p. 239—271.

Акс и Кочен (Ax J., Kochen S.)

1. Diophantine problems over local fields, I. — Amer. J. Math., 1965, 87, p. 605—630.

*) Звездочкой отмечена литература, добавленная при переводе. — Прим. ред.

2. Diophantine problems over local fields, II: A complete set of axioms for p -adic number theory. — Amer. J. Math., 1965, 87, p. 631—648.
 3. Diophantine problems over local fields, III: Decidable fields. — Ann. Math., 1966, 83, p. 437—456.
- Бюхи (Büchi J. R.)
1. Weak second order arithmetic and finite automata. — Z. math. Logik Grundle. Math., 1960, 6, p. 66—92.
 2. On a decision method in restricted second order arithmetic. — In: Logic, Methodology and Philosophy of Science: Proceedings of the 1960 International Congress Stanford (Calif.): Stanford University Press, 1962, p. 1—11. [Русский перевод: Бюхи Д. Р. О разрешающем методе для ограниченной арифметики второго порядка. — Кибернетический сборник, 8, М.: Мир, 1964, с. 78—90.]
- Габбай (Gabbay D. M.)
1. Decidability results in non-classical logics, Part I. — Ann. Math. Logic, 1975, 8, p. 237—295.
- Ершов Ю. Л.
1. Разрешимость элементарной теории дистрибутивных структур с относительно большими дополнениями и теории фильтров. — Алгебра и логика, 1964, 3, № 3, с. 17—38.
 - 2*. Об элементарных теориях локальных полей. — Алгебра и логика, 1965, 4, № 2, с. 5—30.
 - 3*. Проблемы разрешимости и конструктивные модели — М.: Наука, 1980.
- Ершов Ю. Л., Лавров И. А., Тайманов А. Д., Тайцлин М. А.
- 1*. Элементарные теории. — УМН, 1965, 20, № 4, с. 37—108.
- Карп (Karp R. M.)
1. Reducibility among combinatorial problems. — In: Complexity of Computer Computations/Ed. R. E. Miller, J. W. Thatcher. N. Y.: Plenum Press, 1972, p. 85—104.
- Коэн (Cohen P. J.)
1. Decision procedures for real and p -adic fields. — Comm. Pure Appl. Math., 1969, 22, p. 131—151.
- Кук (Cook S. A.)
1. The complexity of theorem proving procedures. — In: Proceedings of the 3rd Annual ACM Symposium on theory of computing. 1971, p. 151—158.
- Лёйхли и Леонард (Läuchli H., Leonard J.)
1. On the elementary theory of linear order. — Fundam. math., 1966, 59, p. 109—116.
- Мейер (Meyer A. R.)
1. The inherent complexity of theories of ordered sets. — In: Proceedings of the International Congress of Mathematics, Vancouver, 1974, Canadian Math. Congress, 1975, p. 477—482.
- Мостовский (Mostowski A.)
1. On direct products of theories. — J. Symbolic Logic, 1952, 17, p. 1—31.
- Пресбургер (Presburger M.)
1. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. — In: Comptes Rendus du I Congrès des Mathématiciens des Pays Slaves. Warszawa, 1929, S. 92—101.
- Рабин (Rabin M. O.)
1. A simple method for undecidability proofs and some applications. — In: Logic, Methodology and Philosophy of Science, II/Ed. Y. Bar-Hillel. Amsterdam: North-Holland, 1965, p. 58—68.
 2. Decidability of second order theories and automata on infinite trees. — Trans. Amer. Math. Soc., 1969, 141, p. 1—35.

- Робинсон (Robinson A.)
1. Complete Theories. — Amsterdam: North-Holland, 1956.
- Тарский (Tarski A.)
1. Arithmetical classes and types of Boolean algebras: Preliminary report. — Bull. Amer. Math. Soc., 1949, 55, p. 64.
 2. A Decision Method for Elementary Algebra and Geometry. — Berkeley; Los Angeles, 1951.
- Тарский и Мостовский (Tarski A., Mostowski A.)
1. Arithmetical classes and types of well ordered systems. — Bull. Amer. Math. Soc., 1949, 55, p. 65.
- Феферман и Воот (Feferman S., Vaught R. L.)
1. The first order properties of products of algebraic systems. — Fundam. math., 1959, 47, p. 57—103.
- Фишер и Рабин (Fischer M. J., Rabin M. O.)
1. Super exponential complexity of Presburger's arithmetic. — SIAM AMS Proc., 1974, 7, p. 27—41.
- Шмелева (Szmielew W.)
1. Elementary properties of abelian groups. — Fundam. math., 1954, 41, p. 203—271.
- Элгот (Elgot C. C.)
1. Decision problems of finite automata design and related arithmetics. — Trans. Amer. Math. Soc., 1961, 98, p. 21—51.
- Эренфойхт (Ehrenfeucht A.)
1. Decidability of the theory of linear ordering relation. — Notices Amer. Math. Soc., 1959, 6, p. 268—269.

СТЕПЕНИ НЕРАЗРЕШИМОСТИ. ОБЗОР РЕЗУЛЬТАТОВ

Стивен Г. Симпсон

СОДЕРЖАНИЕ

§ 1. Введение	112
§ 2. Структура степеней без операции скачка	115
§ 3. Операция скачка	120
§ 4. $V = L$ против PD	122
§ 5. Между 0 и 0'	125
§ 6. Степени полных теорий	128
Литература	131

§ 1. Введение

Эта глава рассчитана на читателей, имеющих по крайней мере шапочное знакомство с некоторыми основными идеями теории рекурсивных функций. Эти идеи могут быть найдены в главе 1

Структура степеней по существу есть некоторая классификация всех множеств натуральных чисел по сложности. Рекурсивные множества натуральных чисел составляют минимальный уровень сложности. *Степень* (иногда называется *тьюринговой степенью* или *степенью неразрешимости*) — это просто класс эквивалентных множеств натуральных чисел при следующем отношении эквивалентности: S_1 рекурсивно относительно S_2 , а S_2 рекурсивно относительно S_1 . Ясно сразу, что каждое множество натуральных чисел попадает в один из этих классов эквивалентности. Степени частично упорядочены следующим образом: $d_1 > d_2$ тогда и только тогда, когда множества в классе эквивалентности d_1 более нерекурсивны, чем множества в классе эквивалентности d_2 .

Только что описанная простая идея приводит к богатой и интересной теории. В действительности в течение многих лет теория степеней является одной из наиболее технических и высоко развитых частей математической логики. В литературе имеются буквально сотни статей, которые посвящены исключительно степеням. Требования к оригинальности в этих статьях очень высоки. И хотя некоторые идеи повторяются, многообразие используемых методов громадно. Некоторые из специали-

стов даже предпочитают не опубликовывать свою теорему, если ее доказательство не демонстрирует новой техники.

Описанная ситуация доставляет тяжелое испытание всякому, кто попытается внести порядок и ясность в теорию степеней. Несмотря на это, имеются несколько поистине замечательных образцов, как например, Лахлан [5], Сакс [1], Шенфилд [3], Соар [3], Ейтс [5]. (Возможно, книга Шенфилда [3] наиболее удобна для начинающих.) Придерживаясь основного пути развития теории степеней, все эти работы делают особый упор на *методы доказательств*.

В данном обзоре мы позволили себе небольшое число методологических замечаний. Однако мы приняли сознательное решение пренебречь методологией, а вместо этого сконцентрировать внимание на результатах. Поэтому мы пытаемся указать исключительно такие теоремы, утверждения которых проливают наибольший свет на структуру и использование степеней. Такие теоремы не всегда имеют самые интересные доказательства. Причины нашего выбора в основном опираются на следующее:

(1) Как сказано выше, уже есть несколько замечательных методологических обзоров, превзойти которые мы не надеемся.

(2) Наш типичный читатель, возможно, не планирует заниматься исследованиями в теории степеней. Следовательно, ему более интересны результаты, а не методы доказательств.

(3) Мы чувствуем, что сейчас настало самое время, когда специалисты по теории степеней должны критически оглянуться на конкретные достижения в своей области. Мы надеемся, что обзор результатов будет способствовать такому самоанализу и в связи с этим укажем направление будущих исследований.

Другой аспект теории степеней, которым мы здесь пренебрегаем, — это история. Это отчасти связано с тем, что мы предпочитаем обсудить более поздние, но цельные результаты, а не ранние и отрывочные. Кроме того, исторический подход мог бы ввести в заблуждение, так как общая концепция о том, что такое теория степеней, кажется, с годами меняется. Однако чтобы избежать обвинений в полном пренебрежении историей, мы укажем на тот очевидный факт, что публикация статей по теории степеней началась со статьи Эмиля Л. Поста. (В §§ 5 и 6 настоящего обзора обсуждаются проблемы, идущие от Поста [1]; §§ 2, 3 и 4 ближе по духу к статьям Поста [2] и Клини и Поста [1]. Серьезные исторические трудности связаны и с тем, что многое из сделанного Постом не издано, не опубликовано и недоступно.)

Со времени Поста теория степеней обнаружила много связей с другими частями математической логики. К сожалению, ограниченность места помешала нам привести здесь эти аспекты. Другая важная тема, которую мы опустили — это обобщенная

теория степеней. Современный обзор об α -степенях содержится в главе 5. Понятие степени, которое особенно важно для дескриптивной теории множеств, обсуждается в публикуемых докторских диссертациях Дж. Стилла и У. Уэйджа; оба из Калифорнийского университета в Беркли.

В оставшейся части этого введения мы коротко определим некоторые основные понятия теории степеней. Дополнительные детали читатель может найти в § 8 главы 1.

Мы используем ω для обозначения как наименьшего бесконечного ординала, так и для множества $\{0, 1, 2, \dots\}$ неотрицательных целых чисел. Мы используем 2^ω для обозначения множества $\{0, 1\}$ -значных функций на ω . Такие буквы, как f, g, h , будут применяться для обозначения элементов из 2^ω .

Для $f, g \in 2^\omega$ обозначим через $f \oplus g$ единственную функцию $h \in 2^\omega$ такую, что $h(2n) = f(n)$, $h(2n+1) = g(n)$ для всех $n \in \omega$. Пишем $f \leq_T g$ (читается: f рекурсивна относительно g , f сводится по Тьюрингу к g , f вычисляется по g), если существует алгоритм, который вычисляет $f(n)$, используя оракул для g , для всех $n \in \omega$. Фиксируется гёделева нумерация всех алгоритмов. Для всех $f \in 2^\omega$ определим $f^* \in 2^\omega$ следующим образом: $f^*(n) = 1$, если n -й алгоритм в конце концов остановится, когда начнет работать на входе n с оракулом f ; в противном случае $f^*(n) = 0$.

1.1. Предложение. (i) $f \leq_T f$.

(ii) Из $f \leq_T g$, $g \leq_T h$ следует $f \leq_T h$.

(iii) $f \oplus g \leq_T h$ тогда и только тогда, когда $f \leq_T h$, $g \leq_T h$.

(iv) $f \leq_T f^*$ и неверно, что $f^* \leq_T f$.

(v) Из $f \leq_T g$ следует $f^* \leq_T g^*$.

Говорят, что две функции $f, g \in 2^\omega$ имеют одинаковую степень, если $f \leq_T g$ и $g \leq_T f$. Обозначим через D множество всех степеней. Буквы полужирного шрифта такие, как $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}$, используются для обозначения степеней. Степень функции f обозначается через $\deg(f)$. Степенью множества $A \subseteq \omega$ называется степень его характеристической функции $\mathbf{c}_A \in 2^\omega$.

Пусть $\mathbf{a} = \deg(f)$, $\mathbf{b} = \deg(g)$. Определим двуместный предикат $\leq$ на D следующим образом: $\mathbf{a} \leq \mathbf{b}$ тогда и только тогда, когда $f \leq_T g$. Двуместная операция $\cup$ на D определяется так: $\mathbf{a} \cup \mathbf{b} = \deg(f \oplus g)$. В силу 1.2 (ii) и 1.2 (v) D является верхней полурешеткой относительно $\cup$. Одноместная операция $j: D \rightarrow D$, называемая операцией скачка, определяется так: $j(\mathbf{a}) = \mathbf{a}' = \deg(f^*)$. Выделенный элемент из D определяется как $\mathbf{0} = \deg(\lambda n 0)$. Таким образом, $\mathbf{0}$ — степень рекурсивных функций.

1.2. Предложение (i) D имеет мощность $2^{\aleph_0}$.

(ii) D частично упорядочено предикатом $\leq$.

(iii) Подмножество из D имеет верхнюю грань (относительно $\leq$) тогда и только тогда, когда оно счетно.

(iv) $\mathbf{0}$ — наименьший элемент D .

(v) $\mathbf{a} \cup \mathbf{b}$ — наименьшая верхняя грань $\mathbf{a}$ и $\mathbf{b}$.

(vi) $\mathbf{a} < \mathbf{a}'$ для всех $\mathbf{a}$.

(vii) Из $\mathbf{a} \leq \mathbf{b}$ следует $\mathbf{a}' \leq \mathbf{b}'$.

В этой главе операция скачка будет играть фундаментальную роль. По этой причине приведем две важные характеристики этой операции:

(1) Подмножество из ω называется рекурсивно перечислим (р.п.) относительно степени $\mathbf{a}$, если оно либо пусто, либо есть область значений некоторой функции $p: \omega \rightarrow \omega$, рекурсивной относительно $\mathbf{a}$. Степень $\mathbf{b}$ называется р.п. относительно $\mathbf{a}$, если $\mathbf{b}$ — степень некоторого множества, рекурсивно перечислимого относительно $\mathbf{a}$. Имеем: $\mathbf{a}'$ — наибольшая степень, р.п. относительно $\mathbf{a}$.

(2) Скажем, что f предельно рекурсивна относительно g , если существует функция $p: \omega \times \omega \rightarrow \omega$ такая, что p рекурсивна относительно g и $f(m) = \lim_n p(m, n)$ для всех $n \in \omega$. Тогда для $\mathbf{a} = \deg(f)$, $\mathbf{b} = \deg(g)$ имеем: $\mathbf{a} \leq \mathbf{b}'$ тогда и только тогда, когда f предельно рекурсивна относительно g .

Если $\mathbf{a} = \deg(f)$ и $n \in \omega$, то мы пишем $\mathbf{a}^{(n)} = \deg(f^{(n)})$, где $f^{(0)} = f$, $f^{(n+1)} = (f^{(n)})^*$. Следовательно, $\mathbf{a}^{(0)} = \mathbf{a}$ и $\mathbf{a}^{(n+1)} = (\mathbf{a}^{(n)})'$, и, таким образом, мы определяем конечные итерации операции скачка. Началом обобщения итерации на трансфиниты является $\mathbf{a}^{(\omega)} = \deg(f^{(\omega)})$, где $f^{(\omega)} \in 2^\omega$ определяется следующим образом: для всех $m, n \in \omega$

$$f^{(\omega)}(2^m(2n+1)-1) = f^{(m)}(n).$$

Заметим, что степень $\mathbf{a}^{(\omega)}$ является верхней гранью возрастающей последовательности $\mathbf{a}, \mathbf{a}', \mathbf{a}'', \dots, \mathbf{a}^{(n)}, \mathbf{a}^{(n+1)}, \dots$ ($n \in \omega$). Дальнейшие трансфинитные итерации операции скачка будут определены в § 4.

§ 2. Структура степеней без операции скачка

В этом параграфе мы изучаем алгебраическую систему D , множество всех степеней, рассматриваемое как частично упорядоченное множество $\langle D, \leq \rangle$ или как верхнюю полурешетку $\langle D, \cup \rangle$. Результаты, в утверждениях которых встречается операция скачка, отложены до последующих параграфов. Основной вывод из результатов данного параграфа состоит в том, что система D очень богата и иногда трудно изучаема, но при этом имеет ряд замечательных свойств, таких, как 2.2 и 2.3.

Начнем обсуждение типов подпорядков для D . Пусть S — частично упорядоченное множество, вложимое в D . Из 1.2 тривиально получаем:

(i) мощность $S \leq 2^{\aleph_0}$;

(ii) каждый элемент из S имеет не более счетного числа предшественников.

Проблема Сакса [1], оставшаяся открытой, спрашивает: будет ли обратный результат истинным, т. е. будет ли каждое частично упорядоченное множество, удовлетворяющее (i) и (ii), вложимым в D ? Основной позитивный результат по этой проблеме, который полностью решает эту проблему, если выполняется континуум-гипотеза, состоит в следующем.

2.1. Теорема (Сакс [1]). Пусть S — частично упорядоченное множество, удовлетворяющее условиям (i), (ii) и (iii) каждый элемент из S имеет не более $\aleph_1$ последователей. Тогда S порядково вложимо в D .

Ясно, что следствием 2.1 является то, что каждое счетное упорядоченное множество вложимо в D .

При доказательстве 2.1 вложение S в D получается как предел трансфинитной последовательности расширений вложений все больших подмножеств для S . Это подсказывает и трудную общую проблему: когда вложение частично упорядоченного множества в D может быть продолжено до вложения большего частично упорядоченного множества в D ? Интересный специальный случай этой проблемы связан с независимыми множествами, т. е. множествами ненулевых степеней такими, что никакой элемент этого множества не является меньшим или равным наименьшей верхней грани конечного числа других элементов этого множества. По лемме Цорна любое независимое множество может быть расширено до максимального независимого множества. Нетрудно показать, что существует независимое множество мощности $2^{\aleph_0}$ и что каждое максимальное независимое множество имеет мощность $\geq \aleph_1$ (более общо, $\geq \aleph_{\alpha+1}$ при допущении аксиомы Мартина для $\aleph_\alpha$). Сакс [1] спрашивает: каждое ли максимальное независимое множество имеет мощность $2^{\aleph_0}$? Ответ на этот вопрос вполне может оказаться независимым от ZFC.

Введем важное понятие идеала в D . Множество $I \subseteq D$ называется идеалом, если:

(i) $0 \in I$;

(ii) из $a \leq b \in I$ следует $a \in I$;

(iii) из $a, b \in I$ следует $a \cup b \in I$.

Например, если a — любая степень, то мы имеем главный идеал

$$I(a) = \{d: d \leq a\}.$$

Заметим, что любой главный идеал счетен. Неглавный счетный идеал порождается любой счетной возрастающей последовательностью степеней, например $\{0^{(n)}: n \in \omega\}$. Другим примером неглавного идеала является само D .

Наше использование слова «идеал» не является стандартной терминологией, но, конечно, естественно, так как условия (i) — (iii) эквивалентны тому, что I — ядро некоторого гомоморфизма из $\langle D, \cup, 0 \rangle$ на другую верхнюю полурешетку с выделенным наименьшим элементом. Позднее мы скажем несколько больше об образах этих гомоморфизмов.

Временно будем смотреть на идеал как просто на подпорядок для D и спросим: что можно сказать про его порядковый тип? Ясно, что идеал — верхняя полурешетка с наименьшим элементом, но что еще можно сказать? Ответ в счетном случае очень приятен:

2.2. Теорема (Лаклан и Лебеф [1]). Каждая счетная верхняя полурешетка с наименьшим элементом изоморфна некоторому счетному идеалу в D .

Важный частный случай 2.2, принадлежащий Спектору [1], говорит о том, что существует минимальная степень, т. е. такая степень m , что 0 является единственной степенью, меньшей чем m .

Доказательство 2.2 комбинаторно сложно. Однако основная теоретико-рекурсивная идея доказательства восходит к Спектору [1] и не трудна. История 2.2 и главный вклад в комбинаторную часть этого доказательства содержатся в статье Лермана [1].

Несчетные обобщения 2.2 более таинственны; например, открытая проблема — будет ли D иметь идеал порядкового типа $\aleph_1$. Ейтс [2] заметил, что это последнее утверждение совместимо¹⁾ с ZFC, и сделал некоторые предположения. Один изолированный факт: D имеет идеал, порядково изоморфный решетке конечных множеств действительных чисел (см. Томасон [1]). Простым следствием этого факта является то, что каждое максимальное множество попарно несравнимых степеней имеет мощность $2^{\aleph_0}$ (Сакс [1]).

Следующая теорема утверждает нечто важное о том, как расположены в D счетные идеалы.

2.3. Теорема (Спектор [1]). Пусть I — любой счетный идеал в D . Тогда существует (неединственная) пара степеней a_1, a_2 такая, что

$$I = \{d: d < a_1 \text{ и } d < a_2\}.$$

¹⁾ Метаязыком в этой главе является ZFC — теория множеств Цермело — Френкеля с аксиомой выбора. Когда обсуждаются вопросы непротиворечивости и независимости, мы молчаливо предполагаем непротиворечивость ZFC.

В частном случае главных идеалов теорема 2.3 говорит нам, что каждая степень есть наибольшая нижняя грань двух больших степеней. Следствием теоремы 2.3 о неглавных идеалах является то, что бесконечная возрастающая последовательность степеней может не иметь наименьшей верхней грани.

Вообще, пара a_1, a_2 , удовлетворяющая заключению теоремы 2.3, называется *точной парой для I* . Из существования точных пар следует, что в теории первого порядка для $\langle D, U \rangle$ мы можем говорить о произвольных счетных идеалах и употреблять кванторы по ним. Эта выразительная сила будет использована далее при доказательстве теоремы 2.7. Точные пары еще будут использоваться и в теореме 4.3.

Теперь посмотрим, что случится, если мы будем рассматривать D «по модулю» некоторого счетного идеала I . Интуитивная идея — предположить, что все функции из

$$M_I = \{f: \deg(f) \in I\}$$

рекурсивны, и изучить, какой будет эффект такого отождествления на системе D . Существуют два разных пути уточнения этой идеи:

(1) Определим отношение эквивалентности $\equiv_I$ на D так: $a \equiv_I b$ тогда и только тогда, когда $a \cup d = b \cup d$ для некоторого $d \in I$. Пусть D/I означает множество всех классов эквивалентности.

(2) Пусть $D_I = \{a: a > d \text{ для всех } d \in I\}$.

И D/I , и D_I являются верхними полурешетками. Алгебраически более естественно D/I , так как оно имеет наименьший элемент, а именно, само I . D/I является фактором D по I в категории верхних полурешеток с выделенным наименьшим элементом. Ввиду 2.3 D_I никогда не имеет наименьшего элемента. (Однако существует естественный изоморфизм из D_I на некоторое замкнутое вверх подмножество множества D/I . Если I — главный, то это подмножество состоит из ненулевых элементов D/I .)

Интересно, что многие структурные результаты относительно D как алгебраической системы справедливы также для D/I и D_I , когда I — счетный идеал, лишь с небольшими изменениями в доказательствах. Например, 2.1 остается истинным, если его дословно переписать с заменой D на D/I или D_I , предполагая I счетным. Рутинная процедура проверки того, какие из теорем и их доказательства про D обобщаются на D/I и D_I , называется *релятивизацией к I* (см. 9.3 из книги Роджерса [1]). Правильность этой процедуры основана на том, что M_I имеет много таких же свойств замкнутости, как и множество рекурсивных функций; их становится еще больше, если I — главный идеал. Обычно говорят о *релятивизации к степени a* , а не к главному

идеалу $I(a)$. Релятивизованные варианты многих теорем таких, как 2.2, проверены для главных идеалов (иногда не для произвольных счетных идеалов, за исключением некоторых специальных случаев).

Танталова гипотеза Роджерса ([1], с. 261 (с. 335 русского перевода)) утверждает, что $D/I(a)$ изоморфно D для всех главных идеалов $I(a)$. Конечно, многие структурные свойства $D/I(a)$ и D совпадают*). Естественнее также рассмотреть следующее обобщение гипотезы Роджерса: для всех счетных идеалов I

$$D_I \cong D/I - \{I\} \cong D - \{0\}.$$

Еще две проблемы, также принадлежащие Роджерсу [2], остаются открытыми: будет ли какая-нибудь или каждая ненулевая степень инвариантной относительно всех автоморфизмов $\langle D, U \rangle$? Все эти проблемы все еще открыты. (Если мы изменим эти проблемы, потребовав от изоморфизмов и автоморфизмов сохранения операции скачка, то здесь сделан существенный прогресс. См. ниже следствия 3.6 и 3.8.)

До сих пор мы с опаской обходили операцию скачка. Сейчас мы хотим указать, что существует много теорем о верхней полурешетке для D , которые не имеют дела со скачком, но используют это понятие при доказательстве. Возможно простейшим примером такой теоремы является следующая. Скажем, что степень b *расщепляется*, если она есть наименьшая верхняя грань двух меньших степеней b_1 и b_2 . Не каждая ненулевая степень расщепляется, например минимальная степень. Однако имеет место

2.4. Теорема. $\exists a \forall b (b > a \rightarrow b \text{ расщепляется})$.

Это доказывается следующим образом. Возьмем $a = 0'$. Для данной $b > 0'$, используя теорему 3.1 Фридберга об обращении скачка, находим степень c такую, что $c' = c \cup 0' = b$. Затем положим $b_1 = c$, $b_2 = 0'$.

Следующие две теоремы усиливают 2.4 и, подобно 2.4, выводятся из теорем об операции скачка. Скажем, что b *чащеобразна*, если для всякой ненулевой $b_1 < b$ существует $b_2 < b$ такая, что $b_1 \cup b_2 = b$.

2.5. Теорема. $\exists a \forall b (b > a \rightarrow b \text{ чащеобразна})$.

2.6. Теорема. $\exists a \forall b (b > a \rightarrow b \text{ — наименьшая верхняя грань двух минимальных степеней})$.

Для 2.5 берем $a = 0'$ и используем 3.2, а также релятивизованный вариант теоремы Робинсона 5.3. Для 2.6 берем $a = 0''$ (см. теорему 2.4 из статьи Мартина и Миллера [1]).

*) Опровержение этой гипотезы можно найти в книге: Эпштейн (R. L. Epstein). Degrees of unsolvability: structure and theory. — Berlin: Springer, 1979. — Прим. ред.

Заканчиваем этот параграф указанием полного ответа на вопрос, который, кажется, впервые поставлен Шенфилдом (см. Шенфилд [1]). Вопрос таков: какова сложность теории первого порядка для верхней полурешетки $\langle D, \cup \rangle$?

2.7. Теорема (Симпсон [2]). Теория первого порядка для $\langle D, \cup \rangle$ рекурсивно изоморфна множеству истинных формул арифметики второго порядка.

Укажем здесь набросок доказательства. В силу 3.4 мы имеем тот же результат для обогащенной системы $\langle D, \cup, j \rangle$, где j — операция скачка. В доказательстве 3.4 операция скачка используется лишь для того, чтобы доказать существование некоторых конфигураций степеней, кодирующих арифметику второго порядка. Используя 2.3, мы можем говорить об этих конфигурациях в теории первого порядка для $\langle D, \cup \rangle$.

§ 3. Операция скачка

В предыдущем параграфе операция скачка $j: D \rightarrow D$ встречалась как вспомогательное понятие, используемое лишь для доказательства теорем, в которых про эту операцию ничего не говорится. Теперь изучим операцию скачка саму по себе. Основным результатом здесь является теорема Фридберга об обращении.

3.1. Теорема (Фридберг [2]). Для каждой степени $b \geq 0'$ существует степень a такая, что $a' = a \cup 0' = b$.

Из 3.1 и 1.2 легко выводится, что область значений операции скачка в точности совпадает с множеством степеней $\geq 0'$.

По операции скачка имеется довольно обширная литература. Многие из работ уточняют 3.1 в различных направлениях. Например, простая модификация доказательства 3.1 дает следующий полезный результат (см. также Спектор [1]):

3.2. Теорема. Для любой $b \geq 0'$ существует бесконечное множество $\{a_i: i \in \omega\}$ такое, что $a_i \cap a_j = 0$ для всех $i \neq j$ и $a = a_i \cup 0' = b$ для всех i .

Из других уточнений 3.1 следуют ограничения на область определения операции скачка. Так в § 6 книги Сакса [1] показано, что

$$\{a': 0 < a < 0' \text{ и } a \text{ р. п.}\} = \{b: b \geq 0' \text{ и } b \text{ р. п. относительно } 0'\}.$$

Этот замечательный результат важен также и в историческом плане, потому что при его доказательстве впервые применен так называемый метод приоритета «с бесконечными нарушениями». Другое поразительное уточнение 3.1, доказательство которого, как выяснилось, также требует рассуждений о бесконечных нарушениях, состоит в следующем:

3.3. Теорема (Купер [1]). Для любой $b \geq 0'$ существует минимальная степень m такая, что $m' = m \cup 0' = b$.

Теперь обсудим некоторые недавние результаты, относящиеся к определимости в логике первого порядка и к автоморфизмам системы

$$\mathcal{D} = \langle D, \cup, j \rangle.$$

Под арифметикой второго порядка мы понимаем теорию первого порядка двусортной системы

$$\mathcal{P} = \langle 2^\omega, \omega, +, \cdot, E \rangle,$$

где $+$ и $\cdot$ — обычные арифметические операции на ω , а $E: 2^\omega \times \omega \rightarrow \omega$ определяется как $E(f, n) = f(n)$. Хорошим введением в литературу по теории рекурсии в арифметике второго порядка является п. 16.2 из книги Роджерса [1] и п. 8.5 из книги Шенфилда [2]. Мы хотим обсудить некоторые переводы языка арифметики второго порядка в язык для $\mathcal{D}$. Чтобы это сделать, нам нужно специальное отображение $\Gamma: D \rightarrow 2^\omega$, определенное так:

$$\Gamma(d)(n) = \begin{cases} 1, & \text{если } 0^{(n+1)} \leq d \cup 0^{(n)}, \\ 0 & \text{в противном случае.} \end{cases}$$

3.4. Теорема (Симпсон [2]). Пусть $\varphi(f_1, \dots, f_i, n_1, \dots, n_j)$ — формула арифметики второго порядка. Тогда мы можем эффективно найти формулу $\varphi^*(x_1, \dots, x_i, y_1, \dots, y_j)$ теории степеней такую, что для всех $d_1, \dots, d_i \in D$ и $n_1, \dots, n_j \in \omega$

$$\mathcal{P} \models \varphi[\Gamma(d_1), \dots, \Gamma(d_i), n_1, \dots, n_j]$$

тогда и только тогда, когда

$$\mathcal{D} \models \varphi^*[d_1, \dots, d_i, 0^{(n_1)}, \dots, 0^{(n_j)}].$$

Доказательство (набросок). Для формул арифметики первого порядка достаточно показать, что множество $\Omega = \{0^{(n)}: n \in \omega\}$ и предикаты $\{\langle 0^{(m)}, 0^{(n)}, 0^{(p)} \rangle: m+n=p\}$ и $\{\langle 0^{(m)}, 0^{(n)}, 0^{(p)} \rangle: m \cdot n=p\}$ «сложения» и «умножения» на Ω определимы в $\mathcal{D}$ с помощью формул логики первого порядка. Для функциональных кванторов достаточно показать, что Γ отображает D на 2^ω . □

Чтобы вывести некоторые следствия об автоморфизмах и определимости в $\mathcal{D}$, нам нужно следующее довольно легкое утверждение. Напомним, что степень $0^{(\omega)}$ — каноническая верхняя грань для $\{0^{(n)}: n \in \omega\}$.

3.5. Утверждение (Симпсон [2]). Предикат $\{\langle a, b \rangle: 0^{(\omega)} \leq b = \deg(\Gamma(a))\}$ определим в $\mathcal{D}$ формулой логики первого порядка.

3.6. Следствие (Соловей). Каждая степень $\geq 0^{(\omega)}$ неподвижна относительно всех автоморфизмов $\mathcal{D}$.

3.7. Следствие (Симпсон [2]). n -местный предикат $R \equiv \{d: 0^{(\omega)} \leq d\}^n$ определим в $\mathcal{D}$ тогда и только тогда, когда

$$R^* = \{(f_1, \dots, f_n): R(\deg(f_1), \dots, \deg(f_n))\}$$

определим в арифметике второго порядка.

3.8. Следствие (Симпсон [2]). Подсистема системы $\mathcal{D}$, имеющая основное множество $\{d: 0^{(\omega)} \leq d\}$, не является элементарно эквивалентной $\mathcal{D}$.

Следствия 3.6, 3.7 и 3.8 легко и непосредственно следуют из 3.4 и 3.5. Другое доказательство 3.6 нашел ранее Р. М. Соловей, который использовал наблюдения из § 5 статьи Ейтса [3]. Джокуш заметил, что те же самые рассуждения показывают, что в 3.6 $0^{(\omega)}$ может быть заменено $0^{(b)}$. Остается открытым вопрос: имеет ли $\mathcal{D}$ автоморфизмы, отличные от тождественного.

§ 4. $V = L$ против PD

В этом параграфе мы обсудим некоторые аспекты соотношения между теорией степеней и аксиоматической теорией множеств. Начнем с некоторых исторических замечаний.

С самых первых дней, когда возник козновский метод вынуждения (форсинга), специалисты по теории степеней заметили сильное сходство между этим методом и хорошо развитой техникой конечных приближений в теории степеней. Несколько позднее Сакс использовал аналогии с теорией степеней для формулировки новых результатов и проблем в аксиоматической теории множеств («степени неконструктивности», Сакс [4]). Однако на прямые связи между степенями и аксиоматической теорией множеств пролит свет лишь совсем недавно. Как мне известно, литература до 1968 г. не содержит никаких намеков на такие прямые связи (хотя у Сакса [1] встречаются некоторые использования теории меры и дескриптивной теории множеств).

Первыми статьями, в которых понятия аксиоматической теории множеств прямо применяются к степеням, являются статьи Булоса и Патнема [1] и Мартина [2]. Впоследствии неожиданно была найдена тесная и детализированная связь. Например, из 3.7 следует, что существует выражаемая в логике первого порядка формула $\psi(x)$ теории степеней такая, что для всех степеней d имеем $\mathcal{D} \models \psi(d)$ тогда и только тогда, когда d конструктивна в смысле Гёделя [1].

С нашей точки зрения, аксиоматическая теория множеств является наиболее интересной областью проблем для будущих исследований по степеням. (Справедливо будет сказать, что

многие наши коллеги — специалисты по степеням — не разделяют эту точку зрения.) Мы хотим здесь предложить некоторые из известных результатов, показывающие, что различные теоретико-множественные гипотезы такие, как $V = L$ («аксиома» конструктивности) или PD («аксиома» проективной определимости), имеют поразительные следствия для изучения структуры степеней.

Множество степеней $X \subseteq D$ называется *определенным*, если существует степень a такая, что либо $\{d: d \geq a\} \subseteq X$, либо $\{d: d \geq a\} \cap X = \emptyset$. Не каждое множество степеней определенное. Однако существует много нетривиальных идей в литературе, говорящих о том, что некоторые конкретные множества степеней являются определенными тем или другим способом. Например, каждая из теорем 2.4, 2.5, 2.6, 3.1 служит некоторым примером определенности.

Многие известные подмножества множества D оказываются определенными, но читатель (даже специалист по теории степеней), вероятно, не сможет определить в ZFC такого множества степеней и доказать в ZFC, что это множество не определенное. Это эвристическое явление приводит к формулировке следующего эвристического принципа:

4.1. Эвристический принцип. Пусть X — имеющее «простую природу» подмножество множества D . Тогда X определено.

Существует тесная связь между определенностью и играми Гейла — Стюарта. Общую информацию об этих играх читатель может получить из главы 8 «Теории множеств». Эта специфическая связь состоит в следующем. Пусть X — подмножество множества D . Пусть два игрока I и II играют в бесконечную игру с полной информацией, приводящей к определению некоторой функции $f \in 2^\omega$. По правилам этой игры I указывает $f(0)$, затем II указывает $f(1)$, ..., затем I указывает $f(2n)$, затем II указывает $f(2n+1)$, ... В итоге I выигрывает, если $\deg(f) \in X$, в противном случае выигрывает II. Можно показать, что X определено тогда и только тогда, когда один из игроков имеет выигрышную стратегию. (Более того, степень a , участвующая в определении определенности, может быть выбрана как степень выигрышной стратегии.) Это замечание принадлежит Мартину [2].

Многие примеры, подтверждающие принцип 4.1, могут быть получены, если использовать замечание из предыдущего параграфа и недавние результаты по играм Гейла — Стюарта. Для $X \subseteq D$ будем писать $X^* = \{f: \deg(f) \in X\}$. Тогда имеет место

4.2. Теорема (Мартин [2]—[4]). Множество $X \subseteq D$ является определенным при любом из следующих обстоятельств:

- (i) X^* борелевское (т. е. Δ_1^1 -множество).
- (ii) X^* аналитическое (т. е. Σ_1^1 -множество) и существует некоторый кардинал Рамсея.
- (iii) X проективное (т. е. Σ_n^1 -множество для некоторого $n \in \omega$) и PD выполняется.

Из аксиоматической теории множеств мы знаем, что невозможно доказать совместность ZFC с существованием кардинала Рамсея или с PD. Однако несовместность ZFC с этими гипотезами не доказана.

Для того чтобы получить интересное следствие из 4.2 (i), обозначим через $\{\varphi_n\}_{n \in \omega}$ нумерацию всех предложений языка первого порядка для верхних полурешеток. Так как каждый главный идеал $I(b) = \{d: d \leq b\}$ является верхней полурешеткой, мы можем определить множества $X_n = \{b \in D: I(b) \models \varphi_n\}$. В силу 4.2 (i) X_n являются определенными. Пусть

$$\psi_n = \begin{cases} \varphi_n, & \text{если } \exists a \{b: b \geq a\} \subseteq X_n, \\ \neg \varphi_n, & \text{если } \exists a \{b: b \geq a\} \cap X_n = \emptyset. \end{cases}$$

Тогда $\{\psi_n\}_{n \in \omega}$ — теория «типичного» главного идеала, т. е. существует степень a такая, что $I(b) \models \psi_n$ для всех $b \geq a$, $n \in \omega$.

Скажем, что множество $X \subseteq D$ (слабо) *определимо*, если оно определимо в системе $\mathcal{D} = \langle D, \cup, j \rangle$ с помощью формулы логики первого порядка (допускаются параметры из D). Учитывая 4.1, естественно спросить: будет ли каждое слабо определенное множество определенным? Если PD выполняется, то это как раз случай 4.2 (iii). (В действительности 3.7 и недавний результат Харрингтона делают вероятным то, что PD эквивалентно утверждению, что каждое слабо определенное подмножество множества D является определенным.) Однако известно, что для некоторых широких классов моделей теории ZFC справедлив отрицательный результат. В частности, пусть $Y = \{d \in D: \text{гиперстепень для } d \text{ является минимальной}\}$. Тогда в силу 3.7 или из результата Джокуша и Симпсона [1] Y определимо, но, согласно Симпсону [1], Y не определено, если справедливо $V = L$ или V есть генерическое расширение L .

Мы уже заметили, что несколько результатов о $\mathcal{D}$ получаются, если допустить PD. Теперь нам хочется сказать, что при диаметрально противоположном предположении, т. е. при $V = L$, картина $\mathcal{D}$ также очень привлекательна.

Без каких-либо дополнительных предположений можно показать, что существует трансфинитная возрастающая последовательность степеней $0^{(\alpha)}, \alpha < \aleph_1^L$ (см. также Булос и Патнем [1] и Йенсен [1]).

Степени из этой последовательности естественно считать трансфинитными итерациями операции скачка, т. е. имеем:

- (i) $0^{(0)} = 0$;
- (ii) $0^{(\alpha+1)}$ — скачок $0^{(\alpha)}$ для всех α ;
- (iii) $0^{(\alpha)} < 0^{(\beta)}$ для $\alpha < \beta$;

(iv) для каждого предельного ординала $\lambda < \aleph_1^L$ $0^{(\lambda)}$ есть «наименьшая естественная» верхняя грань для $\{0^{(\alpha)}: \alpha < \lambda\}$ в D .

Кроме того, если $V = L$, то степени $0^{(\alpha)}, \alpha < \aleph_1^L$, составляют полную систему в том смысле, что идеал, ими порожденный, совпадает со всем D . В частности, эти степени образуют естественный пример неопределенного множества.

Чтобы объяснить утверждение (iv), написанное выше, напомним, что, согласно 2.3, степени $0^{(\alpha)}, \alpha < \lambda$, не могут иметь наименьшей верхней грани. Утверждение (iv) говорит, что $0^{(\lambda)}$ — специфическая верхняя грань, естественно возникающая в терминах алгебраической системы $\mathcal{D} = \langle D, \cup, j \rangle$. Обозначим через I_λ счетный идеал, порожденный $\{0^{(\alpha)}: \alpha < \lambda\}$. Опишем теперь (в специальном случае) точную природу теоретико-степенной зависимости $0^{(\lambda)}$ от I_λ . (См. также Бойд, Хензел и Патнем [1] и Джокуш и Симпсон [1]). Если I — любой счетный идеал в D , то степень d назовем κ -точной над I (где κ — некоторое положительное число), если d — единственная наименьшая степень вида $(a \cup b)^{(\kappa)}$, где a, b — точная пара над I . Пусть β_0 — ординал разветвленного анализа, который также может быть определен как наименьший ординал β такой, что L_β — модель теории ZFC без аксиомы степени. Хорошо известно, что β_0 — довольно большой, хотя и счетный ординал.

4.3. Теорема. Для любого предельного ординала $\lambda < \beta_0$ можно найти наименьшее положительное число $n = n_\lambda$ такое, что существует степень, n -точная над I_λ . Более того, $0^{(\lambda)}$ — именно эта единственная степень.

В то время как λ пробегает все предельные ординалы, меньшие β_0 , можно показать, что n_λ пробегает все числа $n \geq 2$. При этом, если λ — само β_0 , то n_λ неопределенно. Можно обобщить 4.3 и за β_0 , рассмотрев понятие ν -точности, где ν — некоторый ординал. Чтобы выйти за $\aleph_1^L$, необходимо применить «тонкую структуру L » Йенсена (Йенсен [1]) вместе с «тонкой структурой $L(\mu)$ » Соловея (не опубликовано).

§ 5. Между 0 и 0'

Результаты, о которых говорилось в предыдущих параграфах, принадлежат к тому, что можно назвать «глобальной теорией степеней», т. е. они имеют дело с общими свойствами систем $\langle D, \cup \rangle$ и $\langle D, \cup, j \rangle$. Теперь обратимся к «локальной теории степеней», т. е. к теории степеней $\leq 0'$.

Подмножество множества ω называется *рекурсивно перечислимым* (р.п.), если оно пусто или есть область значения некоторой рекурсивной функции из ω в ω . Назовем степень *р. п.*, если она есть степень некоторого рекурсивно перечислимого множества из ω . Легко видеть, что 0 и $0'$ — р. п. степени и что каждая р. п. степень $\leq 0'$. Р. п. степени были введены Постом [1], который поставил следующую проблему: доказать, что существует р. п. степень между 0 и $0'$. Пост добился сам некоторого прогресса в этой проблеме, хотя она оставалась нерешенной до работ Фридберга [1] и Мучника [1]. Идеи, вытекающие из проблемы Поста и ее решения, играют доминирующую роль в локальной теории степеней вплоть до настоящего времени.

Методы доказательств в локальной теории степеней очень сложны. Для каждой из теорем этого параграфа действует следующая общая схема доказательства. Совершается некая рекурсивная конструкция из бесконечно многих шагов. Имеется бесконечное число требований, которые надо удовлетворить. По ходу конструкции время от времени некоторые из этих требований вступают в конфликт с другими. Конфликты разрешаются, когда они возникают, согласно некоторой рекурсивной схеме приоритетов. Так как требования могут нарушаться на различных шагах, необходимы тонкие методы доказательства того, что каждое требование в конце концов будет удовлетворено.

Доказательство, следующее этой описанной схеме, называется доказательством *методом приоритета*. Впервые такой метод был использован при решении проблемы Поста Фридбергом и Мучником. Обобщения метода Фридберга — Мучника были развиты для других задач более поздними авторами; среди них Лахлан, Сакс и Ейтс. В соответствии с нашей общей установкой говорить о результатах больше, чем о методах, не будем больше ничего говорить здесь о методе приоритета. Интересующийся читатель может обратиться к мастерски изложенным работам Лахлана [5], Шенфилда [3] и Соара [3].

Окончательным решением проблемы Поста могло бы стать полное описание структуры $\mathcal{R}$ — счетного частично упорядоченного множества р. п. степеней. Не видно никакого решения этого, и даже нет разумной гипотезы. Небольшое число известных результатов носят разрозненный характер. Некоторой вехой является установленная Саксом [2] *теорема плотности*: если $a < b$ — р. п. степени, то существует р. п. степень c такая, что $a < c < b$.

Другие результаты про $\mathcal{R}$ относятся к его решеточной структуре. Тривиально, что $\mathcal{R}$ — верхняя полурешетка. Каждая счетная дистрибутивная решетка решеточно вложима в $\mathcal{R}$ (Тома-

сон [2], Лахлан [4]). Само $\mathcal{R}$ не является решеткой (Лахлан [1], Ейтс [1]). Каждая ненулевая р. п. степень является наименьшей верхней гранью двух меньших р. п. степеней (Сакс [1]). Не каждая р. п. степень $< 0'$ является наибольшей нижней гранью двух больших р. п. степеней (Лахлан [1]). Существует пара ненулевых р. п. степеней, у которых 0 является наибольшей нижней гранью (Лахлан [1], Ейтс [1]). Не существует пары ненулевых р. п. степеней с наибольшей нижней гранью 0 и наименьшей верхней гранью $0'$ (Лахлан [1]). Имеется еще небольшое число результатов в этом направлении, значительное большинство из которых принадлежит Лахлану, Ейтсу и Р. В. Робинсону. Хорошим обзором известных результатов является статья Купера [2]. Но не ясно, к чему ведут эти результаты.

Ничего не известно об автоморфизмах $\mathcal{R}$ и о сложности теории первого порядка для $\mathcal{R}$. Сакс [1] предположил, что теория первого порядка для $\mathcal{R}$ разрешима.

Часто специалисты бросаются на поиски разумных подклассов р. п. степеней. Наиболее полезной находкой пока является следующая классификация, использующая конечные скачки. Для $n \in \omega$ определим

$$H_n = \{d: d \leq 0' \text{ и } d^{(n)} = 0^{(n+1)}\},$$

$$L_n = \{d: d \leq 0' \text{ и } d^{(n)} = 0^{(n)}\}.$$

Степени из $H_1(L_1)$ иногда называются *высокими* (*низкими*). Известно, что иерархия $\{H_n, L_n\}_{n \in \omega}$ является собственной, но не исчерпывающей: каждое из $H_{n+1} - H_n$ и $L_{n+1} - L_n$ содержит р. п. степени, но существуют и такие р. п. степени, которые не попадают ни в одно H_n и L_n (Сакс [3]).

Известно несколько замечательных приложений иерархии $\{H_n, L_n\}$. Укажем здесь лишь только один тип такого приложения. Скажем, что рекурсивно перечислимое множество $A \subseteq \omega$ *максимально*, если $\omega - A$ бесконечно, но не существует рекурсивно перечислимого множества $B \equiv A$ такого, что и $\omega - B$ и $B - A$ бесконечны.

5.1. Теорема (Мартин [1]). *Р. п. степень содержит максимальное множество тогда и только тогда, когда она лежит в H_1 .*

5.2. Теорема (Лахлан [3], Шенфилд [4]). *Р. п. степень содержит бесконечное рекурсивно перечислимое множество, не имеющее максимальных надмножеств, тогда и только тогда, когда она не лежит в L_2 .*

Теоремы 5.1 и 5.2 имеют отношение к общей проблеме поведения степени рекурсивно перечислимого множества в зависимости от его положения в решетке $\mathcal{R}$ рекурсивно перечисли-

мых множеств, упорядоченных по включению. Эта проблема возвращает нас к работе Поста [1]. Дальнейшие результаты по этой проблеме имеются у Соара [1], [2], где, в частности, показано, что H_n и L_n не инвариантны относительно автоморфизмов решетки $\mathcal{E}$.

В последние годы возрос интерес к степеням $\leq 0'$, но отличным от р. п. степеней. Одним из главных здесь является результат Сакса [1]: существует минимальная степень, меньшая $0'$. (По теореме плотности для р. п. степеней никакая р. п. степень не может быть минимальной.) Замечательные уточнения теоремы Сакса получены Купером, Ейтсом, Р. Эпштейном и А. Сасо. Свежий обзор этой развивающейся области можно найти у Ейтса [4] и в аннотированной библиографии Купера [2]*).

Ейтс [2], [3] объявил, что каждая конечная дистрибутивная решетка порядково изоморфна некоторому главному идеалу $I(a) = \{d: d \leq a\}$ такому, что $a < 0'$. Из этого следует, что теория первого порядка для верхней полурешетки $I(0')$ неразрешима (см. также Лахлан [2], Томасон [1]). Мы предполагаем, что теория первого порядка для $I(0')$ рекурсивно изоморфна множеству истинных формул арифметики первого порядка (ср. 2.7).

По-видимому, трудной открытой проблемой является следующая: будет ли для каждой степени $a \leq 0'$ существовать *относительное дополнение*, т. е. степень c такая, что $a \cup c = 0'$ и $a \cap c = 0$. Замечательным результатом в этом направлении является

5.3. Теорема (Робинсон [1]). Если a и b — ненулевые степени $\leq 0'$, то существует степень c такая, что $a \cup c = 0'$, и неверно, что $b \leq c$.

§ 6. Степени полных теорий

Множество $C \subseteq 2^\omega$ называется *кореккурсивно перечислимым* (к. р. п.), если $2^\omega - C$ есть область определения частично рекурсивного функционала из 2^ω в ω (см. главу 1). Основной проблемой является проблема эффективного выбора элемента из непустого к. р. п. подмножества множества 2^ω . В данном параграфе будет представлено некоторое число результатов по этой основной проблеме.

Причиной, по которой основная проблема очень интересна, является то, что к. р. п. множества часто и естественно возникают в математической практике. Мы остановимся здесь на

*) Укажем в этой связи новую книгу: Эпштейн (R. L. Epstein). Degrees of unsolvability: structure and theory. — Berlin: Springer, 1979. — Прим. ред.

нескольких частных примерах, взятых из математической логики. Пусть T — конечно аксиоматизируемая теория языка первого порядка конечной сигнатуры. Зафиксируем гёделеву нумерацию предложений языка теории T . Полная теория в этом языке будет отождествляться с характеристической функцией множества гёделевых номеров ее теорем. Таким образом, множество всех полных расширений теории T отождествляется с множеством $C_T \subseteq 2^\omega$. Как абстрактное топологическое пространство, C_T является стоуновским пространством булевой алгебры предложений языка теории T по модулю эквивалентности, связанной с доказуемостью в T . Как подмножество множества 2^ω , C_T является, как легко видеть, к. р. п.

Несколько отвлекаясь, укажем следующую теорему, которая показывает, что класс только что рассмотренных примеров охватывает все к. р. п. подмножества множества 2^ω . (Таким образом, когда мы изучаем основную проблему в терминах степеней, мы в действительности изучаем степени полных расширений конечно аксиоматизируемых теорий.) Скажем, что два множества $C_1, C_2 \subseteq 2^\omega$ *рекурсивно гомеоморфны*, если существует частично рекурсивный функционал из 2^ω в 2^ω , который одно-однозначно отображает C_1 на C_2 .

6.1. Теорема (Ханф [2]). Пусть C — любое к. р. п. подмножество множества 2^ω . Тогда существует конечно аксиоматизируемая теория T языка первого порядка с равенством и одним двуместным предикатным символом такая, что C рекурсивно гомеоморфно множеству полных расширений теории T .

В статье Джокуша и Соара [1] используется метод приоритета для доказательства существования к. р. п. множеств $C \subseteq 2^\omega$ с различными патологическими свойствами. Тогда можно применить теорему 6.1 для вывода следствий о существовании конечно аксиоматизируемых теорий T с соответствующими патологическими свойствами. Для дополнительной информации по данному поводу см. Ханф [1], Мартин и Пур-Эль [1].

Наши результаты, касающиеся основной проблемы, будут для краткости сформулированы в терминах предиката $\ll$ на степенях, который мы теперь определим. Говорим, что множество $C \subseteq 2^\omega$ к. р. п. *относительно степени a* , если $2^\omega - C$ является областью определения частичного функционала из 2^ω в ω , который рекурсивен относительно a . Полагаем $a \ll b$, если каждое непустое подмножество для 2^ω , являющееся к. р. п. относительно a , содержит функцию степени $\leq b$. В следующей теореме собраны простые факты о $\ll$, источники которых трудно проследить.

6.2. Теорема. (i) Из $a \ll b$ следует $a < b$.

- (ii) Из $a \leq b \leq c \leq d$ следует $a \leq d$.
- (iii) Из $a \leq b, b \leq c$ следует $a \leq c$.
- (iv) $a \leq a'$ для всех a .

Следующая теорема объясняет выбор обозначения $\leq$.

6.3. Теорема (Джокуш и Соар [1]). Если $a \leq b$, то каждое счетное частично упорядоченное множество вложимо в $\{d: a < d < b\}$.

В следующей теореме говорится, что не существует никакой позитивной связи между $\leq$ и относительной рекурсивной перечислимостью, за исключением той, что указана в 6.2 (iv).

6.4. Теорема (Джокуш и Соар [1]). (i) Если $a \leq b$ и b р. н. в a , то $a' = b$.

(ii) Для всякой a существует b такая, что $a \leq b$ и $a' = b'$.

Следующая теорема говорит о двух замечательных структурных свойствах $\leq$.

6.5. Теорема. (i) Если $a \leq b$, то существует c такая, что $a \leq c, c \leq b$.

(ii) Для всяких a и $b \geq a$ существует $c \geq a$ такая, что $a = b \cap c$.

Заканчивая, мы указываем несколько результатов об отношении $\leq$ к более известным понятиям. Для удобства приведем эти результаты в нерелятивизованной форме. Следующая теорема может быть выведена из результатов Скотта [1], Джокуша и Соара [1] и одного неопубликованного результата Р. М. Соловья (см. также Роджерс [1], с. 94 (с. 126, 127 русского перевода)).

6.6. Теорема. Для любой степени b следующие утверждения эквивалентны между собой:

- (i) $b \geq 0$;
- (ii) b — степень полного расширения арифметики Пеано (или ZFC при условии непротиворечивости ZFC);
- (iii) b — степень множества, разделяющего эффективно неотделимую пару непересекающихся рекурсивно перечислимых множеств.

6.7. Теорема (Джокуш [1]). Для любой степени b следующие утверждения эквивалентны:

- (i) либо $b \geq 0$, либо $b' \geq 0''$;
- (ii) b — степень последовательности функций, содержащей все рекурсивные элементы из 2^{ω} .

Степень b называется почти рекурсивной, если для каждой функции $p: \omega \rightarrow \omega$, которая рекурсивна в b , существует рекурсивная функция $q: \omega \rightarrow \omega$ такая, что $p(n) \leq q(n)$ для всех $n \in \omega$. (См. также Мартин и Миллер [1].)

6.8. Теорема (Джокуш и Соар [1]). Существует степень b такая, что $b \geq 0$ и b почти рекурсивна.

ЛИТЕРАТУРА

- Бойд, Хензел и Патнем (Boyd R., Hensel G., Putnam H.)
1. A recursion-theoretical characterization of the ramified analytical hierarchy. — Trans. Amer. Math. Soc., 1969, **141**, p. 37—62.
- Булос и Патнем (Boolos G., Putnam H.)
1. Degrees of unsolvability of constructible sets of integers. — J. Symbolic Logic, 1968, **33**, p. 497—513.
- Гёдель (Gödel K.)
1. Consistency proof for the generalized continuum hypothesis. — Proc. Nat. Acad. Sci. USA, 1939, **25**, p. 220—224.
- Дейвис (Davis M. ed.)
1. The Undecidable. — N. Y.: Raven Press, 1965.
- Джокуш (Jockusch C. G., Jr.)
1. Degrees in which the recursive sets are uniformly recursive. — Canad. J. Math., 1972, **24**, p. 1092—1099.
- Джокуш и Симпсон (Jockusch C. G., Jr., Simpson S. G.)
1. A degree-theoretic definition of the ramified analytical hierarchy. — Ann. Math. Logic, 1976, **10**, p. 1—32.
- Джокуш и Соар (Jockusch C. G., Jr., Soare R. I.)
1. π_1^0 classes and degrees of theories. — Trans. Amer. Math. Soc., 1972, **173**, p. 33—56.
- Ейтс (Yates C. E. M.)
1. A minimal pair of recursively enumerable degrees. — J. Symbolic Logic, 1966, **31**, p. 159—168.
2. Initial segments of the degrees of unsolvability, Part I: A survey. — In: Mathematical Logic and the Foundations of Set Theory/Ed. I. Bar-Hillel. Amsterdam: North-Holland, 1970, p. 63—83.
3. Initial segments and implications for the structure of degrees. — In: Conference in Mathematical Logic. — London 1970. Berlin: Springer, 1972, p. 305—335.
4. Prioric games and minimal degrees below $0'$. — Fundam. math., 1974, **82**, p. 217—237.
5. Banach-Mazur games, comeager sets and degrees of unsolvability. — Math. Proc. Camb. Phil. Soc., 1976, **79**, p. 195—220.
- Йенсен (Jensen R. B.)
1. The fine structure of the constructible hierarchy. — Ann. Math. Logic, 1972, **4**, p. 229—308.
- Клини и Пост (Kleene S. C., Post E. L.)
1. The upper semilattice of degrees of recursive unsolvability. — Ann. Math., 1954, **59**, p. 379—407.
- Купер (Cooper S. B.)
1. Minimal degrees and the jump operator. — J. Symbolic Logic, 1973, **38**, p. 249—271.
2. An annotated bibliography for the structure of the degrees below $0'$ with special reference to that of the recursively enumerable degrees. — Recursive Function Theory Newsl., 1974, **5**, p. 1—15.
- Лаклан (Lachlan A. H.)
1. Lower bounds for pairs of recursively enumerable degrees. — Proc. London Math. Soc., 1966, **16**, p. 537—569.
2. Distributive initial segments of the degrees of unsolvability. — Z. math. Logik Grundl. Math., 1968, **14**, p. 457—472.
3. Degrees of recursively enumerable sets which have no maximal super-set. — J. Symbolic Logic, 1968, **33**, p. 431—443.
4. Embedding nondistributive lattices in the recursively enumerable degrees. — In: Conference in Mathematical Logic — London 1970. Berlin: Springer, 1972, p. 149—177.

5. The priority method for the construction of recursively enumerable sets. — In: Cambridge Summer School in Mathematical Logic. Berlin: Springer, 1973, p. 299—310.
- Лаклан и Лебеф (Lachlan A. H., Lebeuf R.)
1. Countable initial segments of the degrees of unsolvability. — J. Symbolic Logic, 1976, **41**, p. 289—300.
- Лерман (Lerman M.)
1. Initial segments of the degrees of unsolvability. — Ann. Math., 1971, **93**, p. 365—389.
- Мартин (Martin D. A.)
1. Classes of recursively enumerable sets and degrees of unsolvability. — Z. math. Logik Grundle Math., 1966, **12**, p. 295—310.
 2. The axiom of determinateness and reduction principles in the analytical hierarchy. — Bull. Amer. Math. Soc., 1968, **74**, p. 687—689.
 3. Measurable cardinals and analytic games. — Fundam. math., 1970, **66**, p. 287—291.
 4. Borel determinacy. — Ann. Math., 1975, **102**, p. 363—371.
- Мартин и Миллер (Martin D. A., Miller W.)
1. The degrees of hyperimmune sets. — Z. math. Logik Grundle Math., 1968, **14**, p. 159—166.
- Мартин и Пур-Эль (Martin D. A., Pour-El M. B.)
1. Axiomatizable theories with few axiomatizable extensions. — J. Symbolic Logic, 1970, **35**, p. 205—209.
- Мучник А. А.
1. Неразрешимость проблемы сводимости теории алгоритмов. — ДАН СССР, 1956, **108**, с. 194—197.
- Пост (Post E. L.)
1. Recursively enumerable sets of positive integers and their decision problems. — Bull. Amer. Math. Soc., 1944, **50**, p. 284—316.
 2. Degrees of recursive unsolvability Preliminary report. — Bull. Amer. Math. Soc., 1948, **54**, p. 641—642.
- Робинсон (Robinson R. W.)
1. Degrees joining to $0'$. — 1972.
- Роджерс (Rogers H., Jr.)
1. Theory of Recursive Functions and Effective Computability. — N. Y.: McGraw-Hill, 1967. [Русский перевод: Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. — М.: Мир., 1972.]
 2. Some problems of definability in recursive function theory. — In: Sets, Models and Recursion Theory/Ed J. N. Crossley. Amsterdam: North-Holland, 1967, p. 183—201.
- Сакс (Sacks G. E.)
1. Degrees of Unsolvability. — Ann. Math. Studies, 1963, **55**.
 2. The recursively enumerable degrees are dense. — Ann. Math., 1964, **80**, p. 300—312.
 3. On a theorem of Lachlan and Martin. — Proc. Amer. Math. Soc., 1967, **18**, p. 140—141.
 4. Forcing with perfect closed sets. — In: Axiomatic Set Theory/Ed. D. Scott. Providence (Rhode Island): Amer. Math. Soc., 1971, p. 331—355.
- Симпсон (Simpson S. G.)
1. Minimal covers and hyperdegrees. — Trans. Amer. Math. Soc., 1975, **209**, p. 45—64.
 2. First-order theory of the degrees of recursive unsolvability. — Ann. Math., 1977, **105**, p. 121—139.
- Скотт (Scott D.)
1. Algebras of sets binumerable in complete extensions of arithmetic. In: Recursive Function Theory/Ed. J. Dekker. Providence (Rhode Island): Amer. Math. Soc., 1962, p. 117—121.

- Соар (Soare R. I.)
1. Automorphisms of the lattice of recursively enumerable sets. — Bull. Amer. Math. Soc., 1974, **80**, p. 53—58.
 2. Incomplete recursively enumerable sets. — Notices Amer. Math. Soc., 1975, **22**, p. A-24.
 3. The infinite injury priority method. — J. Symbolic Logic, 1976, **41**, p. 513—530.
- Спектор (Spector C.)
1. On degrees of recursive unsolvability. — Ann. Math., 1956, **64**, p. 581—592.
- Томасон (Thomason S. K.)
1. On initial segments of hyperdegrees. — J. Symbolic Logic, 1970, **35**, p. 189—197.
 2. Sublattices of the recursively enumerable degrees. — Z. math. Logik Grundle Math., 1971, **17**, p. 273—280.
- Фридберг (Friedberg R. M.)
1. Two recursively enumerable sets of incomparable degrees of unsolvability (solution of Post's problem 1944). — Proc. Nat. Acad. Sci. USA, 1957, **43**, p. 236—238.
 2. A criterion for completeness of degrees of unsolvability. — J. Symbolic Logic, 1957, **22**, p. 159—160.
- Ханф (Hani W.)
1. Model theoretic methods in the study of elementary logic. — In: The Theory of Models/Ed. J. W. Addison et al. Amsterdam: North-Holland, 1965, p. 132—145.
 2. The Boolean algebra of logic. — Bull. Amer. Math. Soc., 1975, **81**, p. 587—589.
- Шенфилд (Shoenfield J. R.)
1. Applications of model theory to degrees of unsolvability. — In: The Theory of Models/Ed. J. W. Addison et al. Amsterdam: North-Holland, 1965, p. 359—363.
 2. Mathematical Logic. — Reading (Mass.): Addison-Wesley, 1967. [Русский перевод: Шенфилд Дж. Математическая логика. — М.: Наука, 1975.]
 3. Degrees of Unsolvability. — Amsterdam: North-Holland, 1971. [Русский перевод: Шенфилд Дж. Степени неразрешимости. — М.: Наука, 1977.]
 4. Degrees of classes of r.e. sets. — J. Symbolic Logic, 1976, **41**, p. 695—696.

ТЕОРИЯ α -РЕКУРСИИ

Ричард А. Шор

СОДЕРЖАНИЕ

Введение	134
§ 1. Идеи и определения	136
§ 2. Вопросы и ответы	140
§ 3. Пример	144
§ 4. Связи и применения	150
§ 5. Библиографические указания	153
Аннотированная библиография	154

Введение

В этой главе нашей целью является представление для неспециалиста грубой картины современного состояния теории α -рекурсии (т. е. теории рекурсии на допустимых ординалах). Мы надеемся сначала (в § 1) объяснить основные идеи, лежащие в основе предмета, и затем (в § 2) представить важные вопросы и главные области, в которых ведутся исследования в настоящее время. Мы также опишем достигнутые успехи и технику, разрабатываемую и применяемую при этом. Для того чтобы проиллюстрировать идеи, мы дадим (в § 3) одно довольно полное доказательство типичной теоремы в теории α -рекурсии и затем (в § 4) рассмотрим связи и применения этих методов к другим областям исследований. По необходимости наше рассмотрение предыстории, так же как и самого материала, будет и схематично, и поверхностно. Чтобы помочь заполнить пробелы, мы попытались включить довольно полную и частично аннотированную библиографию.

Исторически побуждения для обобщения теории рекурсии на бесконечные ординалы шли из нескольких различных ветвей математической логики: теории доказательств, теории моделей и теории множеств, так же как, конечно, и самой теории рекурсии. Так, например, Такеути [1], [2] интересовался задачей сведения непротиворечивости теории множеств к непротиворечивости теории ординальных чисел. В работе [3] он ввел теорию рекурсии на ординалах, чтобы показать, что требуемая теория и доказательство относительной непротиворечивости могут быть сделаны эффективными в некотором обобщенном смысле.

По существу он показал, что гёделевое построение L (класса конструктивных множеств) может быть имитировано (ординально) эффективным образом для получения (рекурсивно) изоморфной копии L внутри его теории ординальных чисел (Такеути [4]). Во многих отношениях эта работа явилась предзнаменованием тесной взаимосвязи между теорией рекурсии и теорией множеств, возникшей при изучении тонкой структуры L . Позже мы обсудим эту взаимосвязь довольно подробно.

Укажем два примера из теории моделей. Махвер [1] (который также сотрудничал с Леви) хотел обобщить теоретико-модельные идеи и результаты, включающие понятия теории рекурсии, на бесконечные языки $L_{\kappa, \kappa}$. Поэтому он развил теорию рекурсии на бесконечных регулярных кардиналах, чтобы формулировать и доказывать теоремы вроде теоремы о том, что выполнимость не является «арифметически» определимой. Имеются работы Крайзела [1], [2] (позже сотрудничавшего с Саксом; см. Крайзел и Сакс [1], [2]) в несколько ином духе. По-видимому, здесь основным интересующим вопросом является теория определимости и ее отношение к различным логикам и языкам высших порядков. Эти исследования развивались как в теоретико-рекурсивном направлении (о чем свидетельствуют статьи, совместные с Саксом), которое мы еще обсудим, так и в более теоретико-модельном направлении (хотя также и с некоторым теоретико-доказательным оттенком). Последнее происходит из настойчивых пожеланий Крайзела об ограничении бесконечного языка и соответствующем обобщении понятия конечности, основанном на соображениях определимости, а не мощности.

В руках Барвайса и других все это разрослось в обширный предмет допустимых структур и связанных с ними бесконечных языков. Поскольку эта область лежит вне темы этой главы, мы только отошлем читателя к библиографии и к главе 7 «Теории моделей».

Теоретико-множественная точка зрения представлена работой Йенсена (Йенсен и Карп [1]). (Карп, однако, пришла к нашему предмету от теоретико-модельного подхода, подобно Махверу.) Поскольку этот подход тесно связан с теоретико-рекурсивным, представленным работами Крипке [1], [2] и Платека [1] (а также упомянутыми ранее работами Крайзела и Сакса), которые образуют сердцевину нашего предмета, мы попытаемся следовать изложению с обеих точек зрения.

Кроме частных проблем из других областей, мотивировавших ранние работы по теории рекурсии на ординалах, были привлечены также и общие принципы. Специалисты по теории рекурсии имели в виду многие из обычных целей обобщений. Они надеются построить абстрактные структуры не только по-

вые и интересные, но и такие, которые разъяснили бы обычную теорию рекурсии и, возможно, оказались бы также полезными в приложениях. Дальнейшие надежды состоят в том, что такая работа может привести к аксиоматическому подходу к теории рекурсии. С другой стороны, специалист по теории множеств приходит к предмету скорее с целью эффективизации, чем обобщения. Посредством введения понятия эффективности он надеется получить более тонкое и глубокое знание структуры множеств и в итоге использовать эту дополнительную информацию для решения уже поставленных задач в теории множеств.

§ 1. Идеи и определения

Вопрос теперь состоит в том, с чего начать обобщение теории рекурсии. Сначала нужно решить, каковы те основные объекты и понятия обычной теории рекурсии, которые желательно обобщить или абстрагировать. Конечно, натуральные числа $0, 1, 2, 3, \dots$ являются первичными элементами нашего универсума, а интересующими нас основными понятиями являются, по-видимому, рекурсивность и рекурсивная перечислимость. Одним естественным обобщением натуральных чисел являются, конечно, ординалы. Просто счет продолжается и за ω . Имеется, тем не менее, две возможности, соответствующие, может быть, двум различным точкам зрения на натуральные числа. В качестве базисных объектов можно взять все ординалы (ON) или только некоторый начальный сегмент ординалов, скажем, до α . Мы будем рассматривать второй подход, хотя почти все, что мы скажем, применимо одинаково хорошо к обоим. Что касается определений рекурсивности и рекурсивной перечислимости, специалисту по теории рекурсии известно несколько стандартных подходов, которые можно рассмотреть (хотя в обычной теории рекурсии все они определяют один и тот же класс функций). Многие из них были опробованы ранними исследованиями в этой области. В качестве примера отметим, что Такеути [3] ввел схемы для порождения полурекурсивных функций и совместно с Кино (Кино и Такеути [1]) выдвинул другой подход, согласно которому сначала порождаются примитивно рекурсивные функции и затем применяется μ -оператор (оператор наименьшего числа). Среди других предложений встречаются аналоги машин Тьюринга (Леви [1]), критерии определимости (Крайзел [2]) и различные типы исчислений равенств (Маховер [1], Туге [1] и Крипке [1]).

По-видимому, наиболее полезным является подход, основанный на исчислении равенств, как у Крипке [1]. Берется обычное исчисление равенств Клини и добавляется бесконеч-

ное правило, выражающее основную идею обобщения: разрешено по крайней мере α шагов в вычислении и дана возможность обозреть α единиц информации, произведенной к каждому из этих шагов (технические детали и дальнейшее обсуждение см. в работах Крипке [3] или Сакса [4])¹⁾. Затем определяются рекурсивные функции, как обычно, это те функции, значения которых могут быть последовательно выведены из некоторого конечного множества уравнений в соответствии с правилами. Рекурсивно перечислимыми (р. п.) множествами являются, конечно, те, которые могут быть рекурсивно перечислены. (Мы будем указывать обобщенные понятия, добавляя префикс α -, как в словах « α -рекурсивный» и « α -рекурсивно перечислимый».)

Одна проблема немедленно обращает на себя внимание в связи с этой процедурой. Не все ординалы α будут удовлетворительными областями для этой теории рекурсии. Так, например, $\omega + 17$ не замкнут относительно сложения и, несомненно, не должен быть допустимым. Какую мы процедуру мы ни использовали для определения рекурсивности, мы хотим, по меньшей мере, гарантировать, что α замкнут относительно рекурсивных функций. Имея в виду исчисление равенств, в частности, мы также хотели бы потребовать, чтобы любое отдельное вычисление, т. е. выведение значения некоторой рекурсивной функции, могло быть закончено за менее чем α шагов. Оба эти требования выполнены, если мы примем, что для любого конечного множества равенств все возможные следствия могут быть выведены менее чем за α шагов. Такие ординалы называются *допустимыми* (Крипке [1]) и составляют подходящие области для наших теорий рекурсии. Нужно заметить, что до работ Крипке [1] и Платека [1] подходящие области для теории рекурсии на ординалах не были выделены. Большинство других исследователей (например, Маховер [1], Леви [1] и Туге [1]) ограничивались очевидно удобным классом регулярных кардиналов. Возможность других областей была осознана в работе Такеути [3], где было показано, что сингулярные кардиналы также замкнуты относительно рекурсивных функций. Кроме этого, Крайзел и Сакс [2], подходя к делу совсем с другой стороны, работали на $\omega_1^{СК}$, наименьшем

¹⁾ Нужно заметить, что выбор исчисления равенств должен быть сделан с некоторой осторожностью. Крипке сообщил от имени А. Леви (см. AvoI, 6, № 6), что в системе Маховера [1] возникают трудности, если $V \neq L$, потому что используется бесконечно много переменных и оператор точной верхней грани. Действительно, даже если использовать только конечное число переменных и принять $V = L$, то формулировки, использующие операторы $\sup$ и $\inf$ из работ Туге [1] и Стилуэлла [1], обладают всеми желаемыми свойствами только для регулярных кардиналов.

нерекурсивном ординале, который является также наименьшим допустимым после ω .

Хотя это может быть и не очевидным, но имеется еще одно основное понятие, требующее обобщения: конечность. В ранних работах наблюдается склонность оставлять его неизменным или (особенно в бесконечных языках) использовать мощностные условия (множества величины $< \alpha$ были α -конечными). Потребность в более тонком подходе была впервые подчеркнута Крайзелом [1]. При теперешнем положении могло бы, наверное, показаться, что разумно потребовать, чтобы каждое из наших чисел (ординалов, меньших α) считалось α -конечным. Этого, однако, было бы недостаточно. Что бы мы сказали о множествах, которые имеют ту же величину, что и некоторый $\beta < \alpha$? Несомненно, если соответствие между элементами эффективно, то оно также должно быть α -конечным. Достаточно ли этого? Как оказалось, полезно обратиться к теоретико-множественной точке зрения, чтобы ответить на этот вопрос. Поэтому давайте на время вообразим, как специалист по теории множеств мог бы обобщить теорию рекурсии на бесконечное.

Естественной отправной точкой для интересующихся эффективизацией теории множеств является конструктивный универсуум Гёделя (см. главу 5 «Теории множеств»). Он состоит в конечном счете из множеств, построенных наиболее эффективным методом обычной теории множеств — определением. Опять мы имеем две возможности для выбора нашей области исследований. Мы можем работать со всем L или с некоторым его начальным сегментом L_α (это множества, построенные к уровню α). Как и раньше, мы будем заниматься второй альтернативой в основном ради удобства обозначений. Если дана такая область L_α , построенная при помощи определений, то кажется целесообразным рассмотреть сложность определения как руководство к решению вопроса о том, какие подмножества множества L_α или какие функции на L_α должны считаться простыми или эффективными. Сочетая это с той идеей, что рекурсивно перечислимые множества задаются оператором поиска или перечислением, в качестве хорошего кандидата на рекурсивную перечислимость мы получаем Σ_1 -множества над L_α (т. е. определимые посредством формулы с параметрами из L_α с одним начальным квантором существования, который единственный из кванторов не ограничен в области действия каким-либо элементом из L_α). Идея, конечно, заключается в том, что элемент принадлежит Σ_1 -множеству, если мы найдем при поисках внутри L_α элемент, подтверждающий истинность квантора существования. (Проверка истинности такого предложения включает только поиски в пределах единственного элемента (например, L_β для $\beta < \alpha$) из L_α и поэтому несомненно эффективна.)

Имея определение рекурсивной перечислимости, мы можем называть подмножество множества L_α рекурсивным, если оно само и его дополнение р. п. (т. е. оно есть Δ_1 -множество).

Мы опять сталкиваемся с проблемой, что не все ординалы α соответствуют L_α , удобным для нашей теории рекурсии. Рассуждая теперь как специалисты по теории множеств, мы могли бы попытаться исправить эту ситуацию, потребовав, чтобы L_λ удовлетворяло аксиомам теории множеств в некоторой эффективной форме. Это значит, в частности, что в дополнение к обычным тривиальным аксиомам (объемности, пустого множества, пары и объединения), которые верны в любом L_λ с предельным λ , мы могли бы потребовать, чтобы аксиома замены (или, эквивалентно, аксиома Aussonderung) выполнялась для эффективных функций ($= \Delta_1$ -функций $= \Sigma_1$ -функций с областью определения — элементом L_α). Мы, однако, полностью отказываемся от аксиомы степени. Оказывается, наше условие Σ_1 -замены эквивалентно условию допустимости, определенному теоретико-рекурсивно (фактические детали доказательства эквивалентности см. в работах Крипке [1] или Фукуямы [1]). Таким образом, мы видим начало взаимоотношений между этими двумя подходами.

На самом деле связь между этими двумя формулировками значительно более всеобъемлюща, чем одно это совпадение. В действительности они по существу совпадают. Для допустимого α существует α -рекурсивный предикат на α , который изоморфен предикату $\in$ на L_α . Более того, все основные понятия переносятся с помощью этого перевода. Так, множество является α -рекурсивным или α -р. п., если и только если его образ является Δ_1 -множеством или Σ_1 -множеством над L_α соответственно. Эта эквивалентность может быть использована, чтобы навести нас на хороший ответ на вопрос о правильном определении α -конечности. Для специалиста по теории множеств вполне осмысленным является естественное обобщение конечного до элемента из L_α . При обратном переводе этого понятия на язык теории рекурсии мы обнаруживаем, что оно эквивалентно такому: быть рекурсивным образом ординала, меньшего α . Эта эквивалентность является хорошим подтверждением адекватности нашего определения α -конечности.

Нужно отметить, что когда проблема обобщенной конечности была впервые поднята Крайзелом, особое ударение делалось на аналогии между Π_1^1 и р. п. в обычной теории рекурсии. Предложение (Крайзел [1]) состояло в том, чтобы Δ_1^1 соответствовало конечному, а не рекурсивному, для того чтобы улучшить аналогию. Когда Крайзел и Сакс [1], [2] сформулировали эти идеи на языке теории рекурсии на ω_1^{CK} , они

соответственно обобщили конечное до рекурсивного и ограниченного. (Π_1^1 -множества и в действительности становятся $\omega_1^{\text{СК}}$ -р. п. и потому Δ_1^1 -подмножества ω становятся $\omega_1^{\text{СК}}$ -рекурсивными и ограниченными). Легко видеть, что это определение также эквивалентно α -конечности.

§ 2. Вопросы и ответы

Теперь, когда мы договорились об основных понятиях теории α -рекурсии, мы должны рассмотреть, проблемы какого сорта нужно решать. После установления основных фактов обычной теории рекурсии таких, как теоремы о перечислении, об итерации и теорема о рекурсии, специалист по теории рекурсии естественно приходит к традиционным областям исследования обычной теории рекурсии: относительной сложности (т. е. теории степеней), особенно р. п. множеств, и структурным (т. е. теоретико-решеточным) свойствам множеств, опять-таки обычно р. п. множеств. В настоящее время эти области составляют главный интерес теории α -рекурсии. Кроме установления основных структурных теорем (как для степеней, так и для множеств), целью большего числа современных работ является анализ и разъяснение методов, используемых в этих областях. В частности, различные типы доказательств методом приоритета, являющегося ключом к большинству глубоких результатов обычной теории рекурсии, широко изучались и были приспособлены к более общей ситуации, имеющейся в теории α -рекурсии. Мы упомянем некоторые из таких результатов в каждой из областей, но сначала должны прервать изложение для того, чтобы объяснить, что мы имеем в виду под α -степенями и α -сводимостями.

В обычной теории рекурсии существует несколько интересных сводимостей. Некоторые из них, такие, как много-односводимость и одно-односводимость, имеют полезные прямые обобщения в теории α -рекурсии: $A \leq_{\text{та}} B$ ($A \leq_{1\alpha} B$), если и только если существует одно-однозначная α -рекурсивная функция f такая, что $\beta \in A \Leftrightarrow f(\beta) \in B$. С другой стороны, ситуация с тьюринговой сводимостью (которая, конечно, является наиболее важной в обычной теории рекурсии) несколько более сложна.

Сейчас, вероятно, наиболее общепринятым подходом к тьюринговой сводимости является подход, связанный с оракулом. Вычисления относительно некоторой функции f (множества рассматриваются как их характеристические функции) считаются протекающими, как обычно, но с добавлением условия, что в любой момент у оракула можно получить значение f на данном

числе n . На языке исчисления равенств можно было бы включить всю функцию f в начальное множество уравнений, и тогда на любом шаге было бы доступно значение $f(n)$ для любого n . Тогда можно было бы сказать, что g вычислима относительно f , если все ее значения могут быть последовательно выведены из конечного множества уравнений плюс полный график f . В теории α -рекурсии это определяет сводимость, называемую α -вычислимостью. (Пишем $g \leq_{\alpha} f$ ($A \leq_{\alpha} B$) для обозначения того, что $g(A)$ вычислима относительно $f(B)$.)

Хотя α -вычислимость является важной и полезной сводимостью (для счетных α она соответствует понятию неявной инвариантной определимости, введенному Крайзелем [2]), мы не считаем ее подходящей с теоретико-рекурсивной точки зрения. Главный ее концептуальный недостаток состоит в том, что одно-единственное вычисление значения g может потребовать α -много информации об f и может занять больше чем α шагов для своего выполнения. Обе эти возможности серьезно противоречат нашим интуитивным идеям из обычной теории рекурсии о том, как должны протекать относительные вычисления.

Для того чтобы увидеть, как преодолеть эти трудности, мы обратимся к другому взгляду на относительную рекурсивность в обычной теории рекурсии, который согласуется с нашей интуицией. Идея состоит в том, что мы должны быть в состоянии эффективно отделить процедуру вычисления от вопросов, которые она задает оракулу в каждом данном вычислении, т. е. описание процедуры как целого не зависит от конкретных ответов, данных во время вычисления. Можно вообразить процедуру вычисления заданной посредством структуры эффективного дерева, ветвящегося на различных вопросах. Информация, использованная на любом заканчивающемся пути, и является тогда конечным количеством, нужным для вычисления. Для дальнейшего обсуждения мы рекомендуем книгу Роджерса [1], с. 128—132 (с. 168—172 русского перевода), где принимается этот подход в качестве основного в обычной теории рекурсии. Мы считаем процедуру вычисления закодированной р. п. множеством. Это множество перечисляет элементы, соответствующие выходам заканчивающихся ветвей, спаренные с конечным множеством ответов, необходимых для того, чтобы произвести эти выходы. Эта точка зрения приводит нас к приемлемому формальному определению: A α -рекурсивно относительно B , что обозначается как $A \leq_{\alpha} B$, если и только если существует α -р. п. множество W_e такое, что для каждого α -конечного множества K имеем

$$K \subseteq A \Leftrightarrow \exists \langle K, 1, M, N \rangle \in W_e (M \subseteq B \ \& \ N \subseteq \bar{B}),$$

$$K \subseteq \bar{A} \Leftrightarrow \exists \langle K, 0, M, N \rangle \in W_e (M \subseteq B \ \& \ N \subseteq \bar{B}),$$

где M и N пробегают все α -конечные множества, и мы используем некоторый эффективный способ кодирования для таких множеств и четверок. Заметим, что в соответствии с нашим обобщением понятия конечности и наши входы (M, N) и выходы $(K \sqsubseteq A$ или $K \sqsubseteq \bar{A})$ должны быть α -конечными. (В исторически более ранней попытке определения требовался только один выход (или, эквивалентно, действительно конечное множество выходов). Это теперь называется слабой α -рекурсивностью: $A \leq_{w\alpha} B$. Этому понятию не только не удалось уловить верный дух обобщения, но оно оказалось не в состоянии работать как сводимость технически — оно не транзитивно, см. Дрисколл [2].)

Естественно, мы имеем понятие α -степени, ассоциированное со сводимостью $\leq_{\alpha}$ (классы эквивалентности по $\leq_{\alpha}$ обычно обозначаются буквами $a, b, c, \dots$ полужирного шрифта). На степенях задается структура верхней полурешетки посредством упорядочения, индуцированного $\leq_{\alpha}$, и оператора объединения $\vee$, определяемого, как и в обычной теории рекурсии. Как мы сказали раньше, исследование структуры этой полурешетки является одной из основных областей исследования в теории α -рекурсии (главным образом Саксом и его учениками). Наиболее успешная работа по методологии приоритетных доказательств*), а также получения самих структурных результатов относятся к α -степеням α -р.п. множеств (называемым α -рекурсивно перечислимыми степенями). Хотя значительная работа была проделана первоначально для конкретных ординалов (особенно ω_1^{CK}), первый действительный успех метода приоритета для допустимых ординалов пришел, когда Сакс и Симпсон [1] установили аналог решения проблемы Поста, полученного Фридбергом и Мучником: существуют несравнимые α -р.п. степени, т. е. степени a и b такие, что $a \not\leq_{\alpha} b$ и $b \not\leq_{\alpha} a$. Они, однако, достигли большего, чем просто решили эту проблему. Их методы достаточны для перенесения всех типов доказательств простым методом приоритета — с конечными нарушениями — на все допустимые ординалы.

После этого был достигнут значительный прогресс с более трудными приоритетными доказательствами. Методы, развитые Шором [5] для доказательства теоремы о разложении (для каждой не α -рекурсивной α -р.п. степени c существуют α -р.п. степени a и b такие, что $a \leq_{\alpha} c$, $b \leq_{\alpha} c$ и $a \vee b = c$), по-видимому, достаточны для приоритетных доказательств с неограниченными сохранениями (подробнее см. ниже, в § 3). Статус

*) Здесь и в дальнейшем ради удобства вместо «доказательство методом приоритета» иногда будем говорить «приоритетное доказательство». — Прим. ред.

доказательств с бесконечными нарушениями в теории α -рекурсии в настоящее время несколько менее ясен. Первый пример из обычной теории рекурсии был успешно обобщен — α -р.п. степени плотны (Шор [8]), однако не со всеми доказанными теоремами получилось так гладко. Так, например, Лерман и Сакс [1] показали, что существует минимальная пара α -р.п. степеней (т. е. не α -рекурсивные α -р.п. степени a и b такие, что если $c \leq_{\alpha} a$ и $c \leq_{\alpha} b$, то c есть степень α -рекурсивных множеств) для большинства, но не для всех допустимых α . (Небольшое улучшение получено Шором [6], но наиболее трудный случай остался открытым.)

В этом направлении главным открытым вопросом, по-видимому, является нахождение выразимого в языке первого порядка различия между теориями р.п. степеней и α -р.п. степеней для некоторых α . В действительности этот вопрос открыт даже для теории всех α -степеней. Единственный ответ (на оба вопроса), имеющийся в настоящее время, использует оператор скачка: так, например, если $\alpha = \aleph_{\omega}^L$ и $A <_{\alpha} 0'$, то $A \equiv_{\alpha} 0'$ (Шор [9]), в то время как в обычной теории рекурсии существуют даже р.п. множества $A < 0'$ со свойством $A' \equiv 0'$ (Сакс [1], § 7). Конечно, вопрос состоит в нахождении различия в теориях только со знаком $\leq$ в языке¹⁾. Мы должны мириться с тем, что вообще очень мало известно о структуре α -степеней в целом. Даже на первый же вопрос, который можно задать, нет полного ответа: известно, что существуют минимальные α -степени для всех счетных α (Макинтайр [3]) и всех Σ_2 -допустимых α (Шор [2]), но, вообще говоря, не для всех α . Простейшим примером нерешенного случая является $\alpha = \aleph_{\omega}^L$.

Другой главной областью современных исследований является изучение строения решетки α -р.п. множеств $\mathcal{E}(\alpha)$ (в основном Лерманом и его учениками). Кроме выяснения структуры α -р.п. множеств ответами на конкретные естественные вопросы об этой решетке (например, существуют ли максимальные элементы), общей целью этой деятельности является установление того, разрешимы ли эти решетки. Хотя это является главной открытой проблемой даже в обычной теории рекурсии, есть надежда, что можно справиться с ней по частям для различных α , которые имеют особенно простые структуры решеток.

Точнее, внимание в действительности сосредоточено, как и в обычной теории рекурсии, на решетке $\mathcal{E}^*(\alpha)$ α -р.п. множеств по модулю «конечных» множеств. Что должно быть плодотворным аналогом конечности при таких обстоятельствах,

¹⁾ Такое различие теперь найдено, см. Шор [10].

явилось в свою очередь предметом некоторых исследований, как в статьях Лермана [6], [7]. По-видимому, для теоретико-решеточных целей лучшим выбором является то, что Лерман называет α^* -конечным (множество и все его α -р. п. подмножества являются α -конечными). Это понятие является единственным приводящим к обобщенно конечным множествам, образующим идеал, определяемый над $\mathcal{E}(\alpha)$. Более того, теория $\mathcal{E}(\alpha)$ и теория фактор-решетки $\mathcal{E}^*(\alpha)$ одновременно или разрешимы, или неразрешимы (Лерман [6]).

В соответствии с общей целью выяснения разрешимости $\mathcal{E}^*(\alpha)$ для различных α , исследования направлены не только на доказательство общих теорем для всех допустимых ординалов, но также на углубленный анализ для некоторых многообещающих ординалов таких, как $\aleph_1^L$ и $\aleph_\omega^L$. Лучшим результатом первого типа является характеристика Лерманом [3] тех допустимых ординалов, которые имеют максимальные элементы в $\mathcal{E}^*(\alpha)$. По существу он показал, что α таков, если и только если α счетен относительно функции с определенным типом рекурсивной аппроксимации. (Необходимость некоторых условий счетности была впервые показана Лерманом и Симпсоном [1].) В качестве примера второго типа мы отметим работы Чона и Лермана [1] о гипергиперпростых множествах (надмножества которых в $\mathcal{E}^*(\alpha)$ образуют булеву алгебру), Лермана [5] и Леджета и Шора [1] о возможных 1-типах простых множеств (дополнения которых, хотя и α -бесконечны, не содержат α -бесконечных α -р. п. подмножеств). Нечего и говорить, что большую часть работы в этой области осталось проделать¹⁾.

§ 3. Пример

Работы по теории α -рекурсии пролили свет на общую природу приоритетных доказательств и породили применения к теории рекурсии на объектах высших типов (Харрингтон [1]) и к аксиоматической теории рекурсии (Симпсон [3]). Они также сильно связаны с работами по теории множеств. Наверное, лучше всего объяснить и эти взаимоотношения и сами работы по теории α -рекурсии на примере. Мы дадим слегка модифицированное доказательство теоремы о разложении из работы Шора [5]. Сначала мы опишем в общих чертах доказательство этой теоремы в обычной теории рекурсии (см. Сакс [1], § 5 или Шенфилд [1], § 14).

Теорема. Пусть функция с перечисляет р. п. множество C данной нерекурсивной р. п. степени c . Существуют р. п. мно-

жества A и B такие, что $A \cup B = C$, $A \cap B = \emptyset$, $A \leq_T C$, $B \leq_T C$, $C \not\leq_T A$ и $C \not\leq_T B$.

(Заметьте, что $A \cup B = C$ влечет $A \vee B \equiv_T C$, и потому мы разложили степень c множества C , что и требовалось.) Основной план состоит в том, чтобы на каждом шаге σ построения помещать $c(\sigma)$ в одно и только в одно из множеств A или B (позитивные требования). Это сразу обеспечивает, что $A \cup B = C$, $A \cap B = \emptyset$, $A \leq_T C$ и $B \leq_T C$ (чтобы узнать, например, будет ли $x \in A$, спросите, верно ли, что $x \in C$, и если это так, то ждите, пока x не будет перечислен, и тогда проверьте, помещен ли он в A или нет). Таким образом, мы должны лишь удостовериться в том, что нельзя вычислить C относительно A или B . Наш (несколько окольный) подход (принадлежащий Саксу) состоит в том, что для каждого e мы пытаемся (с приоритетом e) сохранять вычисления функций $\{e\}^A$ (и соответственно $\{e\}^B$) на начальных сегментах до тех пор, пока они кажутся совпадающими с C (т. е. с его характеристической функцией). Идея состоит в том, что как только e имеет наивысший приоритет (это объяснено ниже), мы сохраняем первое имеющееся вычисление $\{e\}^A(x)$ для каждого x до тех пор, пока оно согласуется с C . Если бы $\{e\}^A = C$, то мы бы тогда сохраняли эти вычисления для каждого x . Конечно, $\{e\}^A$ была бы тогда рекурсивной. (Просто ждите до тех пор, пока не начнем сохранять вычисления для $\{e\}^A(x)$. Поскольку e имеет наивысший приоритет, оно никогда не будет нарушено, и потому мы получаем правильное значение для $\{e\}^A(x)$.) Тогда мы пришли бы к противоречию с нерекурсивностью C .

Точнее, построение и одновременное определение терминологии протекает следующим образом: пусть A^σ и C^σ обозначают множества элементов, перечисленные в A и в C до этапа σ соответственно. Мы используем обозначение $\{e\}_\sigma^{A^\sigma}(x) = C^\sigma(x)$ для выражения того, что существует вычисление (подходящая четверка), меньшее чем σ , которое показывает, что вычисление по процедуре e относительно A^σ на аргументе x дает значение характеристической функции C^σ на аргументе x . На этапе σ для каждого e -активного числа $x < \sigma$ мы находим наименьшее вычисление $\{e\}_\sigma^{A^\sigma}(x) = C^\sigma(x)$ (если такое существует) и создаем отрицательное e -требование для A с аргументом x , состоящее из тех элементов, которые считались вне A в этом вычислении (здесь x — наименьшее число y , для которого нет отрицательных e -требований с аргументом y). Если на каком-либо более позднем этапе мы поместим элемент этого требования в A , то говорим, что мы разрушили его. Мы говорим, что процедура сведения $e < \sigma$ является e -активной на этапе σ , если нет отрицательного e -требования (пока еще не разрушенного) с аргу-

¹⁾ Дальнейшие значительные продвижения см. в работе Лермана [8].

ментом y такого, что $\{e\}_0^{A^0}(y) \neq C^0(y)$, в противном случае она неактивна (заметьте, что это может случиться, если только y был перечислен в C после того, как требование было создано). Конечно, все это проделывается также и для B .

Наконец, мы помещаем $c(\sigma)$ в A или B так, чтобы сохранить максимум возможного, т. е. полагаем $e_A(e_B)$ равным наименьшему числу e такому, что $c(\sigma)$ принадлежит отрицательному e -требованию для $A(B)$ (пусть, например, -1 , если такого числа e нет). Если $e_A \leq e_B$, то помещаем $c(\sigma)$ в B , в противном случае — в A . Таким образом, мы даем e -требованиям для A приоритет перед e' -требованиями для B , если и только если $e \leq e'$.

Для того чтобы убедиться, что построение удалось (т. е. $C \leq_T A$ и $C \leq_T B$), сначала индукцией по e доказывается, что создается только конечное число отрицательных e -требований.

Для проведения индукции предположим, что к этапу σ_0 мы уже создали все отрицательные e' -требования для $e' < e$, которые вообще будут созданы. Все вместе они образуют конечное множество, скажем N . К некоторому этапу $\sigma_1 \geq \sigma_0$ все элементы из $C \cap N$ будут перечислены в C . Приоритетное упорядочение теперь гарантирует, что никакое e -требование для A , созданное после этапа σ_1 , не будет разрушено. (Мы называем такие требования *постоянными*, а остальные — *временными*.) Сначала заметим, что если e неактивно на каком-то этапе $\sigma > \sigma_1$, то оно неактивно навсегда, поскольку соответствующее требование постоянно. Тогда по правилам построения для A впоследствии не может быть создано никакое e -требование. Если же e не будет неактивным ни на каком этапе $\sigma > \sigma_1$, то по определению каждое e -требование для A связано с вычислением $\{e\}^A(x)$, дающим правильное значение $C(x)$. Поскольку такие требования создаются для начальных сегментов аргументов x , то их может быть бесконечно много, только если мы создаем их по одному для каждого x . Но если бы это было так, то мы могли бы вычислить $C(x)$, просто посмотрев на значение первого e -требования для A с аргументом x , созданного после этапа σ_1 . Поскольку это противоречило бы нерекурсивности C , мы заключаем, что для A создается только конечное число e -требований. Затем мы рассуждаем таким же образом для B .

Теперь достаточно легко убедиться в том, что $C \leq_T A$. Предположим, что $\{e\}^A = C$, и пусть σ_1 будет такое, как в предыдущем рассуждении. e не может быть неактивным ни на каком этапе $\sigma > \sigma_1$, потому что тогда бы $\{e\}^{A^0}(x) \neq C^0(x)$ (для $x \in C$, в действительности), и постоянность требования влечет то, что это вычисление относительно A правильно, а это противоречит $\{e\}^A = C$. Таким образом, ничто не мешает нам создавать e -тре-

бования для A с аргументом x для каждого x , когда действительно происходит правильное вычисление $\{e\}^A(x) = C(x)$. Это, конечно, противоречит предыдущему результату о конечности числа требований и потому $C \not\leq_T A$. Конечно, $C \leq_T B$ по тем же соображениям.

Попытаемся теперь следовать тому же образцу в теории α -рекурсии. Трудности появляются только при индуктивном доказательстве того, что существует только α -конечное количество e -требований для каждого e . Здесь-то и кроется наибольшая трудность, вообще свойственная теории α -рекурсии. Даже если мы доказали это для всех $e' < e$, мы не знаем, что множество N всех таких требований α -конечно. Поэтому мы не можем предполагать существование требуемого этапа σ_0 . Дело в том, что объединение менее чем α α -конечных множеств не обязано быть α -конечным. Например, если $\alpha = \aleph_\omega$, ничто не мешает образованию e -требований для каждого $x < \aleph_e$ для каждого $e < \omega$. Тогда мы имели бы α e' -требований для $e' < \omega$ и никакого этапа вроде σ_0 не существовало бы. (Заметьте, что если N является α -конечным, то все же σ_0 существует, поскольку отображение, дающее по элементу из N этап, на котором он создан, является α -рекурсивным и потому ограниченным на α -конечных множествах в силу допустимости.)

Единственная другая явная трудность состоит в том, что даже если N является α -конечным, $C \cap N$ таким быть не обязано, и потому может не быть этапа σ_1 такого, как в оригинальном доказательстве. (Снова заметьте, что если $C \cap N$ является α -конечным, то оно перечисляется за α -конечное число шагов в силу допустимости.) Хотя это также является общей трудностью в теории α -рекурсии, Сакс [3] дал простое средство. Назовем множество C *регулярным*, если $C \cap N$ является α -конечным для каждого α -конечного N . Работа Сакса [3] говорит, что каждая α -р. п. степень содержит регулярное α -р. п. множество. Тогда без потери общности можно предполагать, что C регулярна, и тем самым устранить вторую трудность.

Способ решения первой проблемы указан Шором [5], [8]. Идея состоит в том, чтобы сделать список отрицательных требований столь коротким, чтобы проблема никогда не смогла возникнуть. Например, если $\alpha = \aleph_\omega$, то мы хотели бы ограничиться ω -списками. В целом граница на создание e -требований (если она существует) задается Σ_2 -функцией. Тогда мы хотим организовать приоритетное упорядочение процедур сведения e в список длины γ такой, что не существует Σ_2 -отображения, определенного на $\delta < \gamma$ и неограниченного в α . Наибольшее такое γ (и потому наиболее подходящий выбор) называется Σ_2 -кофинальностью α ($\sigma_2 \text{ cf}(\alpha)$). Теперь разбиваем процедуры

сведения на $\gamma = \sigma_2 \text{cf}(\alpha)$ блоков $\{B_e\}_{e < \gamma}$, каждый из которых является собственным начальным сегментом обычного списка процедур сведения (так, для $\alpha = \aleph_\omega$ мы могли бы взять $B_e = \aleph_e$ для $e < \omega$). Идея состоит в том, чтобы для каждого x допускать вычисления $\{\delta\}^{\alpha^\sigma}(x) = C^\sigma(x)$ для любого $\delta \in B_e$. Нужно также заметить, что можно порождать эти блоки при помощи рекурсивной аппроксимации, которая будет правильной на каждом начальном сегменте γ , начиная с некоторого момента. (Мы используем обычную аппроксимацию для всюду определенных Σ_2 - (и также Δ_2 -) функций из обычной теории рекурсии. Допустимость α заставляет аппроксимацию сходиться поточно, а сходимость на начальных сегментах обеспечивается тем, что γ является Σ_2 -кофинальностью α .)

Осталось проверить только то, что наше разбиение не вступает в противоречие с вычислением C в случае, если существует α -бесконечное количество e -требований для некоторого $e < \gamma$. Это, однако, ставит еще одну важную проблему, с которой нужно справиться прежде, чем мы сможем точно сформулировать наше построение. Рассмотрим некоторое B_e и предположим, что, как и в обычном доказательстве, имеется этап σ_1 такой, что ни одно e -требование для A не разрушается после σ_1 . Для вычисления C в предположении, что имеется α -бесконечное количество e -требований, мы должны устранить те $\delta \in B_e$, которые неактивны на некотором этапе после σ_1 (и тогда уже навсегда). Они будут давать неправильные ответы, т. е. $\{\delta\}^A(x) \neq C(x)$ для некоторого x , в то время как все остальные дают только правильные значения C . Поэтому если бы мы могли ограничить, скажем, посредством σ_2 этапы, на которых δ из B_e становятся неактивными, мы могли бы вычислять C , как и раньше, находя для каждого x первое вычисление $\{\delta\}_{\sigma_2}^{\alpha^\sigma}(x) = C^\sigma(x)$ для любого $\sigma > \sigma_2$.

Опять, если бы множество W тех $\delta \in B_e$, которые становятся неактивными, было α -конечным, то нужная граница существовала бы ввиду допустимости. Проблема, однако, состоит в том, что W всего лишь α -р. п. и могут существовать α -р. п. подмножества α -конечных множеств (B_e здесь), которые не α -конечны. (Это, конечно, было причиной нашей первой трудности — $C \cap N$ могло бы быть α -р. п., но не α -конечным.) Решение здесь также состоит в том, чтобы сделать список процедур сведения (в отличие от приоритетного упорядочения блоков процедур) столь коротким, что ни одно ограниченное α -р. п. подмножество не могло бы быть α -бесконечным. Таким образом, нам нужен короткий список ординалов, меньших α , и мы должны быть способны порождать его рекурсивным образом. Ключевым понятием здесь является понятие *проекции* α^* орди-

нала α : α^* является наименьшим β таким, что существует α -рекурсивная функция f , одно-однозначно отображающая α в β . Причина, по которой эта идея дает решение нашей проблемы, заключается в следующем:

Теорема. *Всякое α -р. п. подмножество любого $\delta < \alpha^*$ является α -конечным.*

(Доказательство просто с теоретико-рекурсивной точки зрения: обычное рекурсивное перечисление без повторений α -бесконечного α -р. п. подмножества ординала δ даст отображение из α в δ .) Таким образом, нам нужно только использовать список наших процедур сведения длины α^* , чтобы сделать W α -конечным и решить нашу последнюю проблему.

Остается только скомбинировать наши решения — разделить α^* на γ блоков. Пусть $f: \alpha \rightarrow \alpha^*$ будет одно-однозначным α -рекурсивным проектированием, и пусть $h: \gamma \rightarrow \alpha$ будет Σ_2 -отображением, неограниченным в α . Наши блоки задаются теперь равенством $B_e = fh(e)$ для $e < \gamma$. Заметим, что в силу допустимости область значений f^{-1} ограничена на каждом собственном начальном сегменте α^* . Итак, область значений функции γ проектируется на неограниченную последовательность в α^* , и потому мы включили каждую процедуру сведения в эти блоки. Более того, по нашим предыдущим замечаниям мы можем α -рекурсивно аппроксимировать эти блоки, например посредством $B_e(\sigma)$, таким образом, что для каждого $e \in B_e(\delta)$ совпадает с B_e , начиная с некоторого момента. Мы можем также находить приближения к $f^{-1}(\delta)$ для любого $\delta < \alpha^*$ α -рекурсивным образом при помощи обычной процедуры (например, вычислите $f(\eta)$ для каждого $\eta < \sigma$ и посмотрите, попали ли вы в δ). Комбинируя различные аппроксимации, мы можем теперь точно описать нашу конструкцию; соглашения об обозначениях — как ранее.

На этапе σ мы находим для каждого $e < \gamma$ наименьшее вычисление $\{f^{-1}(\delta)\}_{\sigma}^{\alpha^\sigma}(x) = C^\sigma(x)$ для некоторого e -активного $\delta \in B_e(\sigma)$ (где x — наименьший y , который не является аргументом некоторого отрицательного e -требования). Затем мы создаем отрицательное e -требование и действуем с оставшейся частью построения в точности так, как и раньше.

Проверка того, что построение достигает успеха, протекает, как в обычной теории рекурсии, а с новыми трудностями справляемся, как описано. По предположению индукции существует только α -конечное количество e' -требований для $e' < e$; тогда существует граница на их образование, даваемая Σ_2 -функцией. Поскольку $e < \gamma$, они образуют одно α -конечное множество N , и мы имеем границу σ_0 на этапы, на которых они создаются. В силу регулярности C существует этап $\sigma_1 \geq \sigma_0$, к которому все

элементы N перечислены в C . Мы можем также взять σ_1 достаточно большим, чтобы $B_e(\sigma_1)$ и $f^{-1}(\delta)$ для $\delta \in B_e$ достигли своих окончательных значений. Опять-таки, все создаваемые e -требования постоянны. Поскольку $B_e < \alpha^*$, те $\delta \in B_e$, которые становятся неактивными, образуют α -конечное множество, и потому их вклад ограничен. Таким образом, если бы было α -бесконечное количество e -требований для A , мы снова могли бы вычислить C α -рекурсивно для получения нашего противоречия. Итак, существует только α -конечное количество e -требований для A . Часть рассуждения, относящаяся к B , точно такая же, и индукция продолжается.

Наконец, для доказательства того, что $C \not\leq_\alpha A$ (или $C \not\leq_\alpha B$), предполагаем, что $C \leq_\alpha A$ с e' , дающим процедуру сведения, как в определении сводимости $\leq_\alpha$. Пусть $f(e') = \delta \in B_e$ для некоторого e . Мы можем теперь доказывать (начиная с этапа σ_1), что должно быть создано α -конечное количество e -требований. По выбору δ существуют правильные вычисления $\{f^{-1}(\delta)\}^A(x) = C(x)$ для всех x , поэтому требования должны создаваться для каждого x . Поскольку это противоречит нашему последнему результату, мы имеем $C \not\leq_\alpha A$ (и аналогично $C \not\leq_\alpha B$), что и требовалось.

Этим кончается доказательство теоремы о разложении. (Детали см. у Шора [5].) Теперь мы рассмотрим, как идеи, использованные для преодоления специфических трудностей в теории рекурсии, связаны с некоторыми другими областями исследований.

§ 4. Связи и применения

Начнем с понятия проекции, которое играло ключевую роль в нашем доказательстве и тесно связано с некоторыми важными теоретико-множественными результатами о тонкой структуре L . При изучении конструктивной иерархии встает очевидный вопрос: когда именно строятся множества. Так, например, все (конструктивные) подмножества ω строятся к уровню $\aleph_1$ (в L), но хочется знать, на каком точно уровне они появляются. Ответ на этот конкретный вопрос был дан Булосом и Патнемом [1] (которые, между прочим, работали над иерархиями степеней в обычной теории рекурсии). Эти результаты обобщены Крипке [1] и Платеком [1], тогда как наилучшие (и наиболее общие) результаты содержатся в статье Йенсена [1]:

Теорема. *В $L_{\alpha+1} - L_\alpha$ существует подмножество ординала δ , задаваемое определением, являющимся Σ_n -(Δ_n -) определением над L_α , тогда и только тогда, когда существует одно-одно-*

значная функция $f: \alpha \rightarrow \delta$, являющаяся Σ_n -функцией над L_α (и отображающая α на δ).

Например, при $\delta = \omega$ теорема говорит, что новое подмножество ординала ω строится на уровне α точно в том случае, если все становится счетным на этом уровне.

Рассматривая допустимый α при $n = 1$ и применяя подходящий перевод, мы видим, что получили в точности ключевой факт об α^* -проекции α : Если нельзя одно-однозначно отобразить α в δ при помощи α -рекурсивной функции (= всюду определенной Σ_1 -функции = Δ_1 -функции), то не существует новых α -р.п. (= Σ_1 -) подмножеств ординала δ (потому что они все α -конечны). Общий результат Йенсена играет ключевую роль и в более поздних теоретико-рекурсивных результатах.

При работе в теории α -рекурсии часто необходимо использовать более сложные проектирования, чем Σ_1 -проектирование, для получения еще более коротких списков. Сошлемся в качестве примера на построение минимальной пары Лерманом и Саксом [1] и Шором [6] (а также Леджетом и Шором [1]), где Σ_2 -проекция используется для упорядочения процедур сведения и требований. В несколько ином духе используется релятивизированный вариант теоремы для α -р.п. множеств и $n = 1$ у Шора [8] для доказательства плотности α -р.п. степеней. Конечно, такие проекции высокого уровня могут быть введены в α -рекурсивные конструкции только ценою усложнения аппроксимирующих процедур и ослабления свойств сходимости, нужных в доказательствах.

Основные теоретико-множественные применения проекций вытекают из замечательной теоремы Йенсена об униформизации.

Теорема (Йенсен [1]). *Каждый Σ_n -предикат над L_α может быть униформизован посредством функции, являющейся Σ_n -функцией над L_α .*

Хотя этот результат имеет, очевидно, теоретико-рекурсивный оттенок, он явился ключевой составной частью многих чисто теоретико-множественных результатов Йенсена. В качестве простейшего примера укажем результаты из работы Йенсена [1] о том, что гипотеза Суслина неверна в L . (Имеется также много других результатов комбинаторного и теоретико-модельного характера, родственных по используемым методам.) Нужно также отметить, что йенсеновские доказательства этих результатов имеют дополнительный теоретико-рекурсивный оттенок. Они в значительной степени опираются на идею равномерности. Именно благодаря всегда предписанной равномерности конструкции могут быть осуществлены на предельных шагах.

В качестве последнего применения этих понятий укажем недавнюю работу Джокуша и Симпсона [1]. В ней идея

обобщенных проекций и соответствующее кодирование L_α как подмножества проекции возвращается к источнику, вызвавшему ее, — к иерархиям степеней в обычной теории рекурсии. Эти идеи (вместе с методом вынуждения на совершенных множествах, принадлежащем Саксу) используются для доказательства результатов об определмости в теории тьюринговых степеней с оператором скачка. Например, показано, что разветвленная аналитическая иерархия определма уровень за уровнем в теории степеней с операцией скачка.

Другое важное нововведение, потребовавшееся для доказательства в § 3 (блочная техника), имело некоторые следствия для аксиоматической теории рекурсии. Вопрос о том, что же необходимо для выполнения приоритетных доказательств, является ключевым для этого направления, поскольку эти доказательства являются, вероятно, наиболее глубокими и наиболее характерными методами обычной теории рекурсии. При одном типичном подходе к аксиоматической теории рекурсии (как у Московакиса [1]) основной структурной потерей (с точки зрения теории α -рекурсии) является отсутствие рекурсивного вполне упорядочения универсума. Вместо него имеется только некоторое хорошее предвполнеупорядочение. Хотя, по-видимому, этого не вполне достаточно для проведения приоритетных доказательств (см. Симпсон [3], которому, однако, потребовалась аксиома определмости для построения контрпримера), блочная техника позволила дать некоторые ответы. Можно действительно разбить на блоки все элементы одного уровня в предвполнеупорядочении (предполагая, что они «конечны»), но, по-видимому, требуется понятие проектирования для доказательства того, что с блоками все в порядке. Так, можно дать расширенную аксиоматизацию, которая позволяет использовать эту технику для выполнения многих приоритетных доказательств. (Это также отмечено Симпсоном [3].)

Наконец, мы хотели бы упомянуть два применения результатов и методов приоритетных доказательств в теории α -рекурсии в целом. Первое позволяет проделывать некоторые построения при помощи вынуждения над несчетными системами. Эта идея используется, например, Шором [4], где приоритетное доказательство совмещается с конструкцией вынуждения. Частным случаем результатов, доказанных здесь, является то, что в каждой модели теории множеств, обладающей глобальной Σ_n -функцией выбора, существуют Σ_n -классы A и B такие, что ни один из них не является Δ_n -классом относительно другого. Другой пример соединения вынуждения и теории α -рекурсии имеется у Симпсона [2]. Там он используется для доказательства аналога теоремы Фридберга об операторе скачка для α -степеней.

Последним применением этих методов, которое мы рассмотрим, является применение к рекурсии на объектах высших типов. Харрингтон [1] дал метод для прямого перенесения некоторых результатов теории α -рекурсии в результаты об объектах высших типов. Единственным дополнительным условием является то, что конструкция в теории α -рекурсии должна быть равномерной в том смысле, что никаких бесконечных параметров не используется для ее описания. Хотя мы здесь не заботились об этом (мы использовали и γ , и α^*), но это может быть сделано. (Теорему о разложении см. у Шора [3] и Мааса [3], а решение Фридбергом и Мучником проблемы Поста — у Шора [4].) Таким образом, в теории объектов высших типов мы «автоматически» имеем аналоги этих доказательств методом приоритета из теории α -рекурсии.

§ 5. Библиографические указания

Мы постарались дать полный список статей, посвященных теории α -рекурсии, с очень краткими резюме их содержания. Как правило, мы указываем рефераты и резюмируем диссертации, только если не знаем, где еще появился этот материал. Значительное число статей, касающихся теории α -рекурсии только периферийно или в связи с другими предметами, также указано, но без аннотаций.

Для читателя, интересующегося теорией α -рекурсии, мы рекомендуем книгу Сакса [6] в качестве отправной точки. Для первоначального знакомства подходят статьи Симпсона [2] и Шора [5]. По поводу дальнейшей информации о приоритетных доказательствах и α -р.п. степенях, а также других подходов к ним см. Сакс и Симпсон [1], Лерман [1] и Шор [8]. Изучение решетки α -р.п. множеств можно начать с работы Лермана и Симпсона [1] и продолжить работами Лермана [3] о максимальных множествах и Лермана [4], [6] об общих теоретико-решеточных проблемах.

Имеется также несколько важных тем, которые мы вообще здесь не упомянули. Оператор скачка рассматривается Симпсоном [2] и Шором [9]. Явления нерегулярности и негиперрегулярности исследуются Симпсоном [1], и структура таких степеней анализируется Шором [6].

Обращаясь к более широкой точке зрения, упомянем некоторые отправные точки для работы в других областях, имеющих отношение к теории α -рекурсии. Теорию моделей и общую точку зрения на допустимость см. в главе 7 «Теории моделей» и в книге Барвайса [2]. С точки зрения истории вопроса наиболее значительными работами являются Барвайс [1] и Карп [1]. Основным источником по индуктивным определе-

ниям является книга Московакиса [2]; связь с теорией α -рекурсии появляется в главе 9, содержащей результаты из статьи Барвайса, Ганди и Московакиса [1]. Более глубокие связи с допустимыми ординалами см. в работе Цензера [1]. Аксиоматическая теория рекурсии представлена работами Московакиса [1] и Х. Фридмана [1]. Статья Симпсона [3] также имеет отношение к этому. Применения теории α -рекурсии к объектам высших типов даны в работах Харрингтона [1] и Левентала [2]. Тонкая структура L лучше всего излагается в главе 5 «Теории множеств» или в статье Йенсена [1]. К более ранним работам в этой области, связанным с теорией рекурсии, относятся Йенсен и Карп [1] и Ганди [2].

АННОТИРОВАННАЯ ВИБЛИОГРАФИЯ*)

- Аддисон, Генкин и Тарский (Addison J. W., Henkin L., Tarski A., ed.)
1. The Theory of Models: Proceedings of the 1963 International Symposium at Berkeley. — Amsterdam: North-Holland, 1965.
- Барвайс (Barwise J. K.)
1. Infinitary logic and admissible sets. — J. Symbolic Logic, 1969, 34, p. 226—252.
2. Admissible Sets and Structures. — Berlin: Springer, 1975.
- Барвайс, Ганди и Московакис (Barwise J. K., Gandy R. O., Moschovakis Y. N.)
1. The next admissible set. — J. Symbolic Logic, 1971, 36, p. 108—120.
- Бар-Хиллел (Bar-Hillel Y., ed.)
1. Logic, Methodology and Philosophy of Science: Proceedings of the 1964 International Congress. — Amsterdam: North-Holland, 1965.
- Булос и Патнем (Boolos G., Putnam H.)
1. Degrees of unsolvability of constructible sets of integers. — J. Symbolic Logic, 1968, 33, p. 497—513.
- Ганди (Gandy R. O.)
1. Review #4677. — Math. Rev., 1965, 29, p. 882.
2. Set theoretic functions for elementary syntax. — In: Axiomatic Set Theory: The UCLA 1967 Set Theory Conference/Ed. T. J. Jech. Providence (Rhode Island): Amer. Math. Soc., 1974, p. 103—126.
- Ганди и Ейтс (Gandy R. O., Yates C. M. E., ed.)
1. Logic Colloquium '69: Proceedings of the Summer School and Colloquium in Mathematical Logic, Manchester, August, 1969. — Amsterdam: North-Holland, 1971.
- Джекобс (Jacobs B. E.)
1*. α -computational complexity: Thesis. — N. Y.: New York University, Courant Institute of Mathematical Sciences, 1975.
2*. On generalized computational complexity. — J. Symbolic Logic, 1977, 42, № 1, p. 47—58.
Основные понятия абстрактной теории сложности обобщаются в теории α -рекурсии. Аналогии теорем о сжатии и о пробеле.
3*. α -naming and α -speedup theorems — 1977.
Доказываются аналоги теорем об α -наименовании и α -ускорении.

*) Звездочкой отмечены работы, добавленные при корректуре английского издания. — Прим. ред.

- 4*. The α -union theorem and generalized primitive recursion. — Trans. Amer. Math. Soc., 1978, 237, p. 63—82.
Доказывается аналог теоремы об объединении и рассматриваются два аналога примитивной рекурсии на допустимом α .
- Джокуш и Симпсон (Jockusch C. G., Jr., Simpson S. G.)
1. A degree theoretic definition of the ramified analytical hierarchy. — Ann. Math. Logic, 1976, 1, p. 1—32.
- Джу (Jhu R.)
1. Contributions to axiomatic recursion theory and related aspects of alpha-recursion theory: Thesis. — Toronto (Ont.): University of Toronto, 1973.
Некоторые категорные (в топологическом смысле) результаты: если $0 < \alpha^B$, то $\{x | x \in B\}$ является множеством первой категории для счетных α .
- Дрисколл (Driscoll G. C., Jr.)
1. Contributions to metarecursion theory: Thesis. — Ithaca (N. Y.): Cornell University, 1965.
2. Metarecursively enumerable sets and their meta-degrees. — J. Symbolic Logic, 1968, 33, p. 389—411.
Два важных результата из теории ω_1^{CK} -рекурсии: отношение $\geq_w \omega_1^{CK}$ не является транзитивным и ω_1^{CK} -р.п. степени плотны.
- Йенсен (Jensen R. B.)
1. The fine structure of the constructible hierarchy. — Ann. Math. Logic, 1972, 4, p. 229—308.
- Йенсен и Карп (Jensen R. B., Karp C.)
1. Primitive recursive set functions. — In: Axiomatic Set Theory: The UCLA 1967 Set Theory Conference/Ed. D. Scott. Providence (Rhode Island): Amer. Math. Soc., 1971, p. 143—176.
- Йех (Jech T. J., ed.)
1. Axiomatic Set Theory: The UCLA 1967 Set Theory Conference. Providence (Rhode Island): Amer. Math. Soc., 1974.
- Карп (Karp C.)
1. Languages with Expressions of Infinite Length. — Amsterdam: North-Holland, 1964.
- Кино и Такеути (Kino A., Takeuti G.)
1. On hierarchies of predicates of ordinal numbers. — J. Math. Soc. Japan, 1962, 14, p. 199—232.
(В предположении $V = L$.) Определяется рекурсивность (на $\aleph_1$) при помощи конструкции примитивно рекурсивных функций и μ -оператора, подобно Клини. Эквивалентно Такеути [3]. Даются основные теоремы теории рекурсии. Исследуются связи с моделями теории множеств и аналитической иерархией (то, что здесь обозначено Δ_n , обычно обозначается Δ_{n+1}^1).
- Крайзел (Kreisel G.)
1. Set theoretic problems suggested by the notion of potential totality. — In: Infinitistic Methods: Proceedings of the Symposium on Foundations of Mathematics, Warsaw, 2—9 September 1959. Oxford: Pergamon Press, 1961, p. 103—140.
Начало изучения ω -моделей и теории рекурсии. Π_1^1 является аналогом р.п. и Δ_1^1 — аналогом конечности (первое использование обозначения понятия конечности такого сорта). Используются обозначения для НУР-подмножеств ω в качестве области рассмотрения теории.
2. Model theoretic invariants: Applications to recursive and hyperarithmetical operations. — In: The Theory of Models: Proceedings of the 1963 International Symposium at Berkeley/Ed. J. W. Addison, L. Henkin and A. Tarski. Amsterdam: North-Holland, 1965, p. 190—205.

Теоретико-модельный подход к обобщенной теории рекурсии, основанный на понятии жестко содержащихся структур. Рекурсия на ω_1^{CK} и ω -логика в качестве примеров.

3. Relative recursiveness in metarecursion theory (Abstracts). — J. Symbolic Logic, 1967, 32, p. 442.

Связи между рекурсией на ω_1^{CK} и (равномерными) неявными ин-

вариантными определениями. См. также Кюннен [1].

4. Some reasons for generalizing recursion theory. — In: Logic Colloquium' 69: Proceedings of the Summer School and Colloquium in Mathematical Logic, Manchester, August 1969/Ed. R. O. Gandy, C. E. M. Yates. Amsterdam: North-Holland, 1971, p. 139—198.

Фундаментальная работа, посвященная математическим и философским вопросам обобщения теории рекурсии.

Крайзел и Сакс (Kreisel G., Sacks G. E.)

1. Metarecursive sets, I, II (Abstracts). — J. Symbolic Logic, 1963, 28, p. 304—305.

I. Изложение абстрактной теории рекурсии на языке теоретико-модельных инвариантов.

II. Теоретико-рекурсивные результаты на ω_1^{CK} . Существует ма-

ксимальное простое ω_1^{CK} -р. п. множество и ω_1^{CK} -неполное множество.

2. Metarecursive sets. — J. Symbolic Logic, 1965, 30, p. 318—338.

Даются действительные доказательства результатов предыдущих рефератов. Основной вводный текст по теории метарекурсии, т. е. $\alpha = \omega_1^{CK}$.

Крипке (Kripke S.)

1. Transfinite recursion on admissible ordinals, I, II (Abstracts). — J. Symbolic Logic, 1964, 29, p. 161—162.

I. Дается исчисление равенств для рекурсии на ординалах, определяется допустимость и отмечается, что основные теоремы выполняются.

II. Кардиналы допустимы, как и многие другие ординалы. α -конечность эквивалентна принадлежности L_α . Допустимость эквивалентна удовлетворению аксиом слабой теории множеств. Понятие проекции.

Теорема Фридберга — Мучника для случая, когда α^* — кардинал.

2. Admissible ordinals and the analytic hierarchy (Abstract). — J. Symbolic Logic, 1964, 29, p. 162.

Связь между допустимыми ординалами, аналитической иерархией и ординалами.

3. Transfinite recursion, constructible sets and analogs of large cardinals. — Unpublished lecture notes from UCLA 1967 Conference in Axiomatic Set Theory, 1967.

Общее описание и эвристическое объяснение теории рекурсии на ординалах через исчисление равенств. Описание эквивалентности понятий в терминах L_α и аксиом слабой теории множеств. Проекция и ключевая теорема. Обсуждаются рекурсивные аналоги чисел Мало и отношение α -рекурсии к δ_α^1 , Π_2^1 и Δ_2^1 .

Кроссли (Crossley J. N.)

1. Sets, Models and Recursion Theory: Proceedings of the Summer School in Mathematical Logic and Tenth Logic Colloquium, Leicester, August-September 1965. — Amsterdam: North-Holland, 1967.

Кюннен (Kunen K.)

1. Implicit definability and infinitary languages. — J. Symbolic Logic, 1968, 33, p. 446—451.

Левенталь (Löwenenthal F. D.)

1. Some results on measure and category in α -recursion theory. — Notices Amer. Math. Soc., 1973, 20, p. A-450.

Для счетного α : множества над (относительно $\leq_\alpha$ или $\leq_{ca}$) дан-

ным не α -рекурсивным множеством образуют множество меры 0 и первой категории. Множество всех точных верхних граней двух степеней имеет меру 1.

2. The minimal pair problem for higher type objects: Thesis. — Cambridge (Mass.): M. I. T., 1974.

Рассматривается применение методов из работы Харрингтона [1] к построению минимальной пары из работы Лермана и Сакса [1] для получения результата об объектах высших типов.

Левин (Levy A.)

1. Transfinite computability. — Notices Amer. Math. Soc., 1963, 10, p. 286.

Определение рекурсии на регулярных кардиналах с помощью машин Тьюринга, эквивалентное подходу Такеути [3] и близкое подходу Маховеца [2].

Леджет (Leggett A.)

1. Maximal α -r. e. sets and their complements: Thesis. — New Haven (Conn.): Yale University, 1973.

2. Maximal α -r. e. sets and their complements. — Ann. Math. Logic, 1974, 6, p. 293—357.

Расширяет работу Лермана [3]. Даются необходимые и достаточные условия для возможных порядковых типов дополнений максимальных множеств. Выясняется экстенциональная эквивалентность различных определений максимальных α -р. п. множеств.

Леджет и Шор (Leggett A., Shore R. A.)

1. Types of simple α -recursively enumerable sets. — J. Symbolic Logic, 1976, 41, p. 681—694.

Расширение работы Лермана [5]. Используются идеи главного подмножества и гипергиперпростого множества для различения 1-типов простых α -р. п. множеств для всех α . Вводятся метод использования Σ_2 -проектирования в приоритетных доказательствах, когда оно меньше чем $\sigma 2cf(\alpha)$.

Лерман (Lerman M.)

1. On suborderings of the α -recursively enumerable α -degrees. — Ann. Math. Logic, 1972, 4, p. 369—392.

Всякая α -конечная верхняя полурешетка вкладывается в α -степени. Вводится важное понятие ручного (tame) Σ_2 -проектирования, чтобы дать новый вариант метода приоритета с конечными нарушениями.

2. Admissible ordinals and priority arguments. — In: Cambridge Summer School in Mathematical Logic, held in Cambridge/England, August 1—21, 1971/Ed. A. R. D. Mathias and H. Rogers. Berlin: Springer, 1973, p. 311—344.

Дается эвристическое описание конструкции минимальной пары р. п. степеней в обычной и α -теории рекурсии. Вводится метафора «китайский бильярд».

3. Maximal α -r. e. sets. — Trans. Amer. Math. Soc., 1974, 188, p. 341—386.

Рассматриваются различные возможные определения максимальных α -р. п. множеств. Доказываются, что они существуют (для разумных определений), если $s3p(\alpha) = \omega$. Вводится это новое ($s3$) проектирование, задаваемое при помощи рекурсивной аппроксимации с двумя дополнительными переменными.

4. Least upper bounds for pairs of α -r. e. α -degrees. — J. Symbolic Logic, 1974, 39, p. 49—56.

$0'$ не является точной верхней гранью ни одной минимальной пары α -р. п. степеней.

5. Types of simple α -recursively enumerable sets. — J. Symbolic Logic, 1976, 41, p. 419—426.

Существуют различные $\{$ -типы простых множеств в $\mathcal{E}(\alpha)$ для многих α . Используется главное подмножество (каждое α -р. п. множество таким обладает) и гипергиперпростота. См. также Леджет и Шор [1].

6. Ideals of generalized finite sets in the lattice of α -recursively enumerable sets. — Z. Math. Logik Grundl. Math., 1976, 22, № 4, p. 347—352.

Существует единственный идеал обобщенно конечных множеств, определимый над $\mathcal{E}(\alpha)$. Для этих множеств разрешимость $\mathcal{E}(\alpha)$ и $\mathcal{E}^*(\alpha)$ эквивалентны.

7. Congruence relations, filters, ideals and definability in lattices of α -recursively enumerable sets. — J. Symbolic Logic, 1976, 41, p. 405—418.

Существуют наибольшие идеал, фильтр и отношение эквивалентности, определяемые на $\mathcal{E}(\alpha)$. Классифицируются все идеалы для некоторых α и оставляются только две возможности для других α . В любом случае их существует только конечное число. Замечается, что основной результат Мачти [3] справедлив только для предложений, не являющихся $\forall\exists$ предложениями.

- 8*. On elementary theories of some lattices of α -recursively enumerable sets. — Ann. Math. Logic, 1978, 14, № 3, p. 227—272.

Доказывается разрешимость $\forall\exists$ -теории решетки $\mathcal{E}^*(\alpha)$ для двух различных классов ординалов. Если $\sigma 2cf(\alpha) = \iota\sigma 2p(\alpha) = \omega$ и $\alpha^* = \alpha$, то эта теория совпадает с теорией $\mathcal{E}^*(\omega)$. Если $\sigma 3cf(\alpha) = \sigma 3p(\alpha) = \alpha$ (т. е. регулярный кардинал из L), то это другая разрешимая $\forall\exists$ -теория.

Лерман и Сакс (Lerman M., Sacks G. E.)

1. Some minimal pairs of α -recursively enumerable degrees. — Ann. Math. Logic, 1972, 4, p. 415—442.

Если наибольший кардинал из $L_\alpha = \sigma 2p(\alpha) < \iota\sigma 2p(\alpha) \leq \alpha$, то существует минимальная пара α -р. п. степеней. См. также Шор [8].

Лерман и Симпсон (Lerman M., Simpson S. G.)

1. Maximal sets in α -recursion theory. — Israel J. Math., 1973, 4, p. 236—247.

Некоторые необходимые и некоторые достаточные условия для существования максимальных α -р. п. множеств, особенно необходимость счетности. См. также Лерман [3]. Также имеются разрозненные результаты о γ -максимальных множествах.

Маас (Maass W.)

- 1*. On minimal pairs and minimal degrees in higher recursion theory. — Arch. math. Logik Grundlagenforsch., 1977, 18, № 3/4, p. 169—186.

Строятся гиперрегулярные минимальные α -р. п. пары для многих α . Методы из работы Мааса [2] применяются для построения минимальных степеней при условии $\sigma 2cf(\alpha) = \sigma 2p(\alpha) < \alpha$.

- 2*. Inadmissibility, tame r.e. sets and the admissible collaps. — Ann. Math. Logic, 1978, 13, № 2, p. 149—170.

Вводится понятие допустимого коллапса и изучается этот и другие объекты в теории рекурсии на недопустимых ординалах.

- 3*. The uniform regular set theorem in α -recursion theory. — J. Symbolic Logic, 1978, 43, № 2, p. 270—279.

Отвечает на вопрос Сакса [3], давая равномерную конструкцию регулярного α -р. п. множества той же α -степени, что и любое данное α -р. п. множество.

Майерс (Myers D. L.)

1. Meta-arithmetical hierarchies: Thesis. — Cambridge (Mass.): M. I. T., 1970.

Рассматривается релятивизация в теории рекурсии на ω_1^{CK} и изучаются возможные понятия скачка и арифметической иерархии с частичными результатами.

Макинтайр (Macintyre J. M.)

1. Contributions to metarecursion theory: Thesis. — Cambridge (Mass.): M. I. T., 1968.

В дополнение к следующим двум темам изучаются подмножества множества ω , генерические над $L_{\omega_1^{CK}}$ и структура α -степеней под

таким множеством.

2. Minimal α -recursion theoretic degrees. — J. Symbolic Logic, 1973, 38, p. 18—28.

Существуют минимальные α -степени для счетных α и регулярных кардиналов из L .

3. Non-initial segments of the α -degrees. — J. Symbolic Logic, 1973, 38, p. 368—388.

Для всех $\alpha < \aleph_1$ существует $A \subseteq \alpha$ такое, что каждая счетная дистрибутивная решетка с 0 и 1 изоморфна начальному сегменту α -степеней над A . Таким образом, эти теории α -степеней неразрешимы.

Матхас и Роджерс (Mathias A. R. D., Rogers H., ed.)

1. Cambridge Summer School in Mathematical Logic, held in Cambridge/England, August 1—21, 1971. — Berlin: Springer, 1973.

Маховер (Machover M.)

1. The theory of transfinite recursion. — Bull. Amer. Math. Soc., 1961, 67, p. 575—578.

Вводится исчисление равенств для теории рекурсии на регулярных кардиналах, используя оператор sub и функции с бесконечным числом аргументов. В предположении $V = L$ рекурсивно гёделевски нумеруется процесс и отмечаются аналоги основных теоретико-рекурсивных фактов. Дается типичное применение к бесконечным языкам. Для кардиналов-последователей α множество выполнимых формул языка $L_{\alpha, \alpha}$ не является α -арифметическим.

2. The theory of transfinite recursion (in Hebrew): Thesis. — Jerusalem: Hebrew University of Jerusalem, 1962.

Мачти (Machtey M.)

1. Intrinsic consistency results and lattices of recursively enumerable sets in abstract recursion theory: Thesis. — Cambridge (Mass.), M. I. T., 1969.

2. Admissible ordinals and intrinsic consistency. — J. Symbolic Logic, 1970, 35, p. 389—400.

В общем случае нельзя найти внутренне непротиворечивую (т. е. применимую ко всем множествам) процедуру сведения, которая может заменить данную, если α не есть кардинал. Это можно сделать, если α — кардинал и $V = L$.

3. Admissible ordinals and lattices of α -r.e. sets. — Ann. Math. Logic, 1971, 2, p. 379—417.

Утверждается, что разрешающая процедура Лахлана для $\forall\exists$ -формул на $\mathcal{E}^*$ работает для α при $\alpha^* = \omega$, но см. у Лермана [7] контрпример для второго уровня квантификации.

4. Minimal degrees in generalized recursion theory. — Z. math. Logik Grundl. Math., 1974, 20, p. 133—148.

Модифицирует работу Макинтайра [2] для доказательства того, что существует $2^{\aleph_0}$ минимальных α -степеней для счетных α . Основной результат состоит в том, что для $\alpha^* = \omega$ существует минимальная α -степень под каждой α -р. п. степенью.

Метакидес (Metakides G.)

1. α -degrees of α -theories. — J. Symbolic Logic, 1972, 37, p. 667—682.

Для каждого $\omega_1^{\text{СК}}$ -р.п. $X \subseteq \omega$ существует $\omega_1^{\text{СК}}$ -теория $T(X)$ с ограниченным $\omega_1^{\text{СК}}$ -р.п. множеством аксиом той же степени, что и X . Для всех $X \subseteq \beta < \omega_1^{\text{СК}}$ существует $T(X)$ той же степени. То же доказательство работает для всех α .

Московакис (Moschovakis Y. N.)

1. Axioms for computation theories — first draft. — In: Logic Colloquium '69: Proceedings of the Summer School and Colloquium in Mathematical Logic, Manchester, August 1969/Ed. R. O. Gandy and C. E. M. Yates. Amsterdam: North-Holland, 1971, p. 199—255.
2. Elementary Induction on Abstract Structures. — Amsterdam: North-Holland, 1974.

Оуингс (Owings J. C., Jr.)

1. Topics in metarecursion theory: Thesis. — Ithaca (N. Y.): Cornell University, 1966.
2. Recursion, metarecursion and inclusion. — J. Symbolic Logic, 1967, 32, p. 173—179.

Множество A называется множеством типа 1, если для каждого B , максимального в A , существует максимальное C такое, что $A \cap C = B$. В противном случае A называется множеством типа 2. Максимальные $\omega_1^{\text{СК}}$ -р.п. множества A с неограниченным $\bar{A}$ имеют тип 1, а с ограниченным $\bar{A}$ — тип 2. И те, и другие существуют.

3. Π_1^1 -sets, ω -sets and metacompleteness. — J. Symbolic Logic, 1969, 34, p. 194—204.

Каждая $\omega_1^{\text{СК}}$ -степень нерегулярного $\omega_1^{\text{СК}}$ -р.п. множества (или, эквивалентно, Π_1^1 — Σ_1^1 -подмножества множества ω) содержит такое же множество, дополнение которого имеет порядковый тип ω . Для каждого нерегулярного $\omega_1^{\text{СК}}$ -р.п. множества существует некоторое полное р.п. множество, слабо рекурсивное относительно его, так что отношение $\leq_{\omega_1^{\text{СК}}}$ интранзитивно на Π_1^1 -множествах.

4. The metarecursively enumerable sets but not the Π_1^1 sets can be enumerated without repetitions. — J. Symbolic Logic, 1970, 35, p. 223—229. Доказывается теорема, указанная в заглавии.
5. A splitting theorem for simple Π_1^1 sets. — J. Symbolic Logic, 1971, 36, p. 433—438.

Каждое простое Π_1^1 -множество ($\equiv$ простое $\omega_1^{\text{СК}}$ -р.п. не $\omega_1^{\text{СК}}$ -рекурсивное подмножество множества ω) может быть разложено на непересекающиеся Π_1^1 -множества строго меньших $\omega_1^{\text{СК}}$ -степеней.

Охаси (Ohashi K.)

1. On a question of G. E. Sacks. — J. Symbolic Logic, 1970, 35, p. 46—50. Внутренние непротиворечивые процедуры сведения недостаточны. См. также Маччи [2].

Платек (Platek R.)

1. Foundations of recursion theory: Thesis — Stanford (Calif.): Stanford University, 1966.

Развивается теория α -рекурсии как частный случай обобщенной теории рекурсии. Подход — через определимость при помощи (примитивной) рекурсии. Затем добавляется оператор поиска. Выделяются правильные основные понятия (допустимость, α -конечность, проекция и т. д.) и устанавливаются основные теоретико-рекурсивные факты и эквивалентность с теоретико-множественным подходом.

Роджерс (Rogers H., Jr.)

1. Theory of Recursive Functions and Effective Computability. — N. Y.: McGraw-Hill, 1967. [Русский перевод: Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. — М.: Мир, 1972.]

Сакс (Sacks G. E.)

1. Degrees of Unsolvability. — 2nd ed. — Princeton (N. J.): Princeton University Press, 1966.
2. Metarecursively enumerable sets and admissible ordinals. — Bull. Amer. Math. Soc., 1966, 72, p. 59—64.

Описывается мета ($= \omega_1^{\text{СК}}$)-рекурсия на языке $\Pi_1^1 = \text{р.п.}$ и также через исчисление равенств. Существуют два Π_1^1 -множества, которые $\omega_1^{\text{СК}}$ -несравнимы. Объявляются результаты из работы Сакса [3].

3. Post's problem, admissible ordinals and regularity. — Trans. Amer. Math. Soc., 1966, 124, p. 1—23.

Каждая α -р.п. степень содержит регулярное α -р.п. множество. Используется слабое приоритетное доказательство для того, чтобы показать, что существует (по отношению ко всем сводимостям) неполное не α -рекурсивное α -р.п. множество. Вводится понятие регулярности и гиперрегулярности. Существует счетный α без максимального α -р.п. множества.

4. Metarecursion theory — In: Sets, Models and Recursion Theory: Proceedings of the Summer School in Mathematical Logic and Tenth Logic Colloquium, Leicester, August-September 1965/Ed. J. N. Crossley. Amsterdam: North-Holland, 1967, p. 243—263.

Рецензия и изложение работы Крайзела и Сакса [1] и основных результатов теории рекурсии на $\omega_1^{\text{СК}}$, но с использованием исчисления равенств вместо системы обозначений $\mathcal{O}$ и Π_1^1 . Показывается также, что каждое нерегулярное $\omega_1^{\text{СК}}$ -р.п. множество имеет ту же степень, что и некоторое Π_1^1 -подмножество множества ω . Объявляются результаты из работы Сакса [5].

5. On the reducibility of Π_1^1 sets. — Advances in Math., 1971, 7, p. 57—82.

Используются $\omega_1^{\text{СК}}$ -бесконечные, кобесконечные вынуждающие условия для построения Π_1^1 -множеств, которые $\omega_1^{\text{СК}}$ -подгенеричны ($\equiv$ гиперрегулярны) и несравнимы по отношению к произвольному вычислению длины менее, чем $\omega_1^{\text{СК}}$ шагов. Аналогичные результаты для $\alpha^* = \omega$.

6. Higher Recursion Theory. — Berlin: Springer, 1980.

Введение в теорию α -рекурсии (главы V, VI). Включает частный случай $\alpha = \omega_1^{\text{СК}}$ и некоторые приоритетные доказательства для всех α . Содержит большинство основных фактов и определений.

Сакс и Симпсон (Sacks G. E., Simpson S. G.)

1. The α -finite injury method. — Ann. Math. Logic, 1972, 4, p. 323—367.

Первое действительно приоритетное доказательство для всех α , показывающее, что существуют гиперрегулярные α -несравнимые α -р.п. множества. Рассуждение в наиболее трудном случае проводится внутри последовательности Σ_1 -подструктур L_α .

Симпсон (Simpson S. G.)

1. Admissible ordinals and recursion theory: Thesis. — Cambridge (Mass.): M. I. T., 1971.

В дополнение к материалу, включенному в работы Лермана и Симпсона [1] и Симпсона [2], содержит много информации

о негиперрегулярных α -р.п. степенях, простых подмножествах α^* и много интересных контрпримеров.

2. Degree theory on admissible ordinals. — In: Generalized Recursion Theory: Proceedings of the 1972 Oslo Symposium/Ed. J. E. Fenstad, P. G. Hinman. Amsterdam: North-Holland, 1974, p. 165—194.

$b > \alpha_0'$ регулярна тогда и только тогда, когда она является скачком регулярной гиперрегулярной степени. Даются необходимые и достаточные условия существования конуса регулярных степеней. Существуют несравнимые α -р.п. a и b такие, что $(a \vee b)' = 0'$. Дается обзор других результатов по α -степеням и рассматриваются связи с йенсенской тонкой структурой L .

3. Post's problem for admissible sets. — In: Generalized Recursion Theory: Proceedings of the 1972 Oslo Symposium/Ed. J. E. Fenstad, P. G. Hinman. Amsterdam: North-Holland, 1974, p. 437—441.

Используя проективную определимость, строится допустимое множество, для которого нет несравнимых р.п. множеств. Отмечается, что можно использовать блочную технику для получения положительного ответа, если имеется аналог α^* (такие множества называются «тонкими»).

Скотт (Scott D., ed.)

1. Axiomatic Set Theory: The UCLA 1967 Set Theory Conference. — Providence (Rhode Island): Amer. Math. Soc., 1971.

Стилуэлл (Stillwell J.)

1. Reducibility in generalized recursion theory: Thesis. — Cambridge (Mass.): M. I. T., 1970.

Пытается провести приоритетные доказательства для всех допустимых α . Осознание того, что жизнь не так проста, как представляется в этой работе, привело к действительному решению в статье Сакса и Симпсона [1].

Суконик (Sukonick J.)

1. Lower bounds for pairs of metarecursively enumerable degrees: Thesis. — Cambridge (Mass.): M. I. T., 1969.

Существует минимальная пара ω_1^{CK} -р.п. степеней.

Такахаси (Takahashi M.)

1. Recursive functions of ordinal numbers and Levy's hierarchy. — Comment. Math. Univ. St. Paul, 1968, 17, p. 21—29.

Рекурсивность на ON эквивалентна Δ_1 , если $V = L$.

Такеути (Takeuti G.)

1. Construction of the set theory from the theory of ordinal numbers. — J. Math. Soc. Japan, 1954, 6, p. 196—220.
2. On the theory of ordinal numbers. — J. Math. Soc. Japan, 1957, 9, p. 93—113.
3. On the recursive functions of ordinal numbers. — J. Math. Soc. Japan, 1960, 12, p. 119—128.

Вводится рекурсия на ординалах, порождая полурекурсивные функции из базисных при помощи рекурсии и оператора минимизации. Рекурсивные функции получаются, когда $\min$ применяется в случаях ограниченности и всюду определенности. Основной результат состоит в том, что кардиналы (в частности, сингулярные кардиналы) замкнуты относительно рекурсивных функций (индукции по сложности). Эта теория используется для доказательства того, что аксиомы из работы Такеути [2] могут быть эффективизированы. Мотивировка этого дана в статье Такеути [1].

4. A formalization of the theory of ordinal numbers. — J. Symbolic Logic, 1965, 30, p. 295—317.

Результаты из доклада, прочитанного на Симпозиуме по основаниям математики, Катада. Япония, в октябре 1962 г. Излагается тео-

рия рекурсии на ординалах и дается «эффективное» доказательство непротиворечивости теории множеств, показывая, что существует рекурсивный предикат, изоморфный $\in$ на L .

5. Recursive functions and arithmetic functions of ordinal numbers. — In: Logic, Methodology and Philosophy of Science: Proceedings of the 1964 International Congress/Ed. Y. Bar-Hillel. Amsterdam: North-Holland, 1965, p. 179—196.

Рассматриваются некоторые аксиомы бесконечности, основанные на понятии арифметической недостижимости.

Туге (Tugué T.)

1. On the partial recursive functions of ordinal numbers. — J. Math. Soc. Japan, 1964, 16, p. 1—31.

Дается исчисление равенств для рекурсии на регулярных кардиналах, используя $\sup$ -оператор. Показывается, что оно эквивалентно системам Такеути, и доказываются некоторые основные факты такие, как теоремы о рекурсии и об иерархии.

Фенстад и Хинмен (Fenstad J. E., Hinman P. G.)

1. Generalized Recursion Theory: Proceedings of the 1972 Oslo Symposium. — Amsterdam: North-Holland, 1974.

Фридман С. (Friedman S.)

- 1*. Recursion on inadmissible ordinals: Thesis. — Cambridge (Mass.), M. I. T., 1976.

Первая работа по теории рекурсии на недопустимых ординалах. Основные факты и определения. Простые множества существуют. Решение проблемы Поста для многих недопустимых β .

Фридман Х. (Friedman H.)

1. Axiomatic recursive function theory. — In: Logic Colloquium '69: Proceedings of the Summer School and Colloquium in Mathematical Logic, Manchester, August, 1969/Ed. R. O. Gandy, C. E. M. Yates. Amsterdam: North-Holland, 1971, p. 113—137.

Фукуяма (Fukuyama M.)

1. Some concepts of recursiveness on admissible ordinals. — J. Math. Soc. Japan, 1971, 23, p. 435—451.

Детальные доказательства эквивалентности различных определений допустимых ординалов и рекурсивности на них.

Харрингтон (Harrington L.)

1. Contributions to recursion theory in higher types: Thesis. — Cambridge (Mass.): M. I. T., 1973.

Хирано (Hirano M.)

1. Some definitions for recursive functions of ordinal numbers. — Sci. Rep. Tokyo Kyoiku Daigaku, Sect. A, 1969, 10, p. 135—141.

Эквивалентность определений Крипке [1] и Туге [1].

Цензер (Cenzer D.)

1. Ordinal recursion and inductive definitions. — In: Generalized Recursion Theory: Proceedings of the 1972 Oslo Symposium/Ed. J. E. Fenstad, P. G. Hinman. Amsterdam: North-Holland, 1974, p. 221—264.

Чон (Chong C. T.)

1. Tame Σ_2 functions in α -recursion theory: Thesis. — New Haven (Conn.): Yale University, 1973.
2. Almost local non α -recursiveness. — J. Symbolic Logic, 1974, 39, p. 552—562.

Изучается вопрос: когда для не α -рекурсивного α -р.п. множества A $A \cap \Pi_\gamma$ не γ -рекурсивно для $\gamma < \alpha$.

3. An α -finite injury method of the unbounded type. — J. Symbolic Logic, 1976, 41, p. 1—17.

- Две теоремы: 1. Для всякой α -р.п. $a \neq 0$ существует α -р.п. $b <_\alpha a$ такая, что $b|c$ (доказательство использует $is2p$). 2. Для всякой α -р.п. $a \neq 0$ существует α -р.п. $b <_\alpha a$, которая не является наибольшей нижней гранью двух α -р.п. степеней.
4. Minimal upper bounds for ascending sequences of α -recursively enumerable degrees. — J. Symbolic Logic, 1976, 41, p. 250—260.
- Частичные результаты о предмете, указанном в названии.
- 5*. Σ_n -cofinalities in L_α . — 1977.
- Некоторые результаты о возможных значениях $o_1 cf(\alpha)$ и отношении этой функции к $hpr(\alpha)$.
- Чон и Лерман (Chong C. T., Lerman M.)
1. Hyperhypersimple α -r.e. sets. — Ann. Math. Logic, 1976, 9, p. 1—48.
- Г.г.п. множества определяются как те, надмножества которых в $\mathcal{E}^*(\alpha)$ образуют булеву алгебру. Связь с обычным определением через последовательности и смесь результатов о существовании и несуществовании.
- Шенфилд (Shoenfield J. R.)
1. Degrees of Unsolvability. — Amsterdam: North-Holland, 1971.
- [Русский перевод: Шенфилд Дж. Степени неразрешимости. — М.: Наука, 1977.]
- Шор (Shore R. A.)
1. Priority arguments in α -recursion theory: Thesis. — Cambridge (Mass.): M. I. T., 1972.
2. Minimal α -degrees. — Ann. Math. Logic, 1972, 4, p. 393—414.
- Доказывается, что существуют минимальные α - (и $\alpha\alpha$ -) степени, если α является Σ_2 -допустимым, при этом используется метод приоритета из работы Сакса и Симпсона [1]. Также и для некоторых других ординалов.
3. Cohesive sets: countable and uncountable. — Proc. Amer. Math. Soc., 1974, 44, p. 442—445.
- Многие несчетные α имеют сжатые подмножества. То, что делается, не зависит от ZFC.
4. Σ_n sets which are Δ_n incomparable (uniformly). — J. Symbolic Logic, 1974, 39, p. 295—304.
- Комбинируется вынуждение и приоритетное доказательство для доказательства того, что для каждого n существуют индексы $k, l < \omega$ для Σ_n -множеств, которые Δ_n -несравнимы для каждого Σ_n -допустимого α .
5. Splitting an α -recursively enumerable set. — Trans. Amer. Math. Soc., 1975, 204, p. 65—78.
- Для данных не α -рекурсивного α -р.п. D и регулярного α -р.п. C существуют A, B такие, что $A \cup B = C$, $A \cap B = \emptyset$, $A, B \leq_\alpha C$, $D \not\leq_\alpha A$, $D \not\leq_\alpha B$. Та же теорема для $\leq_{\alpha\alpha}$ и обычные следствия для степеней. Вводится блочная техника для приоритетных доказательств.
6. Some more minimal pairs of α -r.e. degrees. — Notices Amer. Math. Soc., 1975, 22, p. A-524—A-525.
- Разрешается один из двух случаев, оставленных открытыми Лерманом и Саксом [1]: если $o_2 cf(\alpha) = \alpha$, то существует минимальная пара α -р.п. степеней.
7. The irregular and non-hyperregular α -r.e. degrees. — Israel J. Math., 1975, 22, p. 28—41.
- Характеризуются ординалы α , для которых существует единственная α -р.п. степень нерегулярного и негиперрегулярного α -р.п. множества. В противном случае доказывается теорема о разложении для таких степеней. Отношение $\leq_{\omega\alpha}$ интранзитивно на α -р.п. множествах в том и только в том случае, когда существует более одной негиперрегулярной α -р.п. степени.

8. The recursively enumerable α -degrees are dense. — Ann. Math. Logic, 1976, 9, p. 123—155.
- Продолжает идеи из статьи Шора [5] для доказательства плотности α -р.п., α - и $\alpha\alpha$ -степеней. Первое доказательство методом приоритета с бесконечными нарушениями в теории α -рекурсии.
9. On the jump of the recursively enumerable α -degrees. — Trans. Amer. Math. Soc., 1976, 217, p. 351—363.
- Рассматриваются различные возможные определения оператора скачка. Изучается одно; показывается, что нет неполных α -р.п. A таких, что $A' = 0''$, если существует единственная не гиперрегулярная α -р.п. степень. Такое A существует, если $o_2 cf(\alpha) = \alpha$.
- Данное доказательство того, что если A негиперрегулярно, то $A' \neq_\alpha 0''$, в действительности показывает лишь то, что $0'' \leq_{\omega\alpha} A'$.
- 10*. Combining the density and splitting theorems for α -r.e. degrees. — Notices Amer. Math. Soc., 1976, 23, p. A-598.
- Если $A' \equiv_\alpha 0'$ и $A <_\alpha D$ являются α -р.п., то существуют α -р.п. B, C такие, что $A <_\alpha B$, $C <_\alpha D$ и $B \vee C \equiv_\alpha D$. Согласно Шору [9], существуют α (например, $\aleph_\omega^L$), для которых $A' \equiv_\alpha 0'$ для каждого неполного α -р.п. A . Тогда по результату Лахлана элементарные теории α -р.п. степеней с $\leq_\alpha$ различны для $\alpha = \omega$ и $\alpha = \aleph_\omega^L$.

РЕКУРСИЯ В ВЫСШИХ ТИПАХ

Александр С. Кекрис
Яннис Н. Московакис

СОДЕРЖАНИЕ

Введение	166
Функциональная индукция	167
§ 1. Монотонные операторы на частичных функциях	167
§ 2. Подходящие классы функционалов	168
§ 3. Основные конструкции	172
§ 4. Связь с обычной теорией рекурсии	176
§ 5. Рекурсия относительно объектов типа 2 и кванторов	177
§ 6. Теорема о пошаговом сравнении	181
§ 7. Полурекурсивные предикаты	185
§ 8. Теорема о перечислении	187
§ 9. Следствия перечислимости	190
Рекурсия в высших типах	193
§ 10. Объекты высших типов над ω	193
§ 11. Клиниевские классы функционалов на T^*	194
§ 12. Рекурсия по Клини относительно объектов высших типов и кванторов	196
§ 13. Нормальность и перечислимость в рекурсии в высших типах	199
§ 14. Определение, данное Клини	201
§ 15. Эквивалентность определения, данного Клини, и нашего	203
§ 16. Теоремы Клини о подстановках	208
§ 17. Сечения и оболочки	214
§ 18. Индуктивный анализ полурекурсивных множеств	216
§ 19. Замкнутость относительно высшей экзистенциальной квантификации	218
§ 20. Указания к литературе	220
Литература	221

Введение

Рекурсия в высших типах была введена Клини [1], [2] и вскоре была признана глубоким и значительным расширением теории рекурсивных функций на натуральных числах. Нашей целью является изложение основных понятий и фактов этой теории методом, делающим их доступными для математика, знакомого с обычной теорией рекурсии.

С самого создания рекурсия в высших типах считалась трудной и доступной лишь посвященным. Хотя она достигла значительной степени зрелости благодаря работам многих исследователей за последние пятнадцать лет, она не была понята таким широким кругом математиков, какого она заслуживает. Час-

точно это произошло вследствие технической трудности основных статей на эту тему. Более того, основные понятия этой теории считались трудными для понимания и проблематичными с точки зрения оснований математики.

Мы будем развивать теорию рекурсии в высших типах в контексте общей теории индуктивной определимости. Клини [2] и сам видел эту возможность и обсудил ее в конце § 10. Позже Платек [1] дал вполне удовлетворительные обоснования для нашего предмета в рамках теории индукции. Его работа, тем не менее, была также технически трудна и ее применение к рекурсии по Клини не просто.

Излагаемый подход принадлежит Московакису. В работе Московакиса [4] обсуждается, как этот подход укладывается в общую теорию индукции, но знание указанной работы не является необходимым для чтения этой главы.

Нужно подчеркнуть, что мы излагаем элементарные части теории рекурсии в высших типах. В последнем параграфе мы сделаем некоторые замечания о том, что читать дальше, для тех, кто желает стать специалистами.

ФУНКЦИОНАЛЬНАЯ ИНДУКЦИЯ

§ 1. Монотонные операторы на частичных функциях

Фиксируем бесконечное множество A такое, что $\omega = \{0, 1, 2, \dots\} \subseteq A$. Под n -арной *частичной функцией* (из A в ω) мы понимаем любое отображение из подмножества множества A^n в ω . Они объединяются в множество

$$\mathcal{PF}_n(A) = \mathcal{PF}_n = \{f: f \text{ есть } n\text{-арная частичная функция}\}.$$

Оператор $\Theta: \mathcal{PF}_n \rightarrow \mathcal{PF}_n$ называется *монотонным*, если для любых $f, g \in \mathcal{PF}_n$

$$f \subseteq g \Rightarrow \Theta(f) \subseteq \Theta(g).$$

Каждый такой монотонный оператор определяет трансфинитную последовательность $\{f_\Theta^\xi\}$ частичных функций посредством рекурсии

$$f_\Theta^\xi = \Theta(f_\Theta^{<\xi}),$$

где $f_\Theta^{<\xi} = \bigcup_{\eta < \xi} f_\Theta^\eta$, т. е.

$$f_\Theta^{<\xi}(\bar{x}) = \omega \Leftrightarrow f_\Theta^\eta(\bar{x}) = \omega \text{ для некоторого } \eta < \xi.$$

В частности, $f_\Theta^0 = \Theta(\emptyset)$, где $\emptyset$ — нигде не определенная n -арная частичная функция.

Простая индукция дает, что

$$\zeta \leq \xi \Rightarrow f_{\Theta}^{\zeta} \subseteq f_{\Theta}^{\xi},$$

так что из мощностных соображений существуют наименьший ординал κ такой, что

$$f_{\Theta}^{\kappa} = f_{\Theta}^{<\kappa} = \bigcup_{\xi} f_{\Theta}^{\xi}.$$

Мы называем f_{Θ}^{κ} частичной функцией, индуктивно определенной при помощи Θ , и обозначаем ее

$$f_{\Theta}^{\infty} = \bigcup_{\xi} f_{\Theta}^{\xi}.$$

Легко проверить, что f_{Θ}^{∞} является также наименьшей неподвижной точкой оператора Θ , т. е.

$$\Theta(f_{\Theta}^{\infty}) = f_{\Theta}^{\infty} \quad \text{и} \quad \Theta(f) \subseteq f \Rightarrow f_{\Theta}^{\infty} \subseteq f.$$

§ 2. Подходящие классы функционалов

2.1. Функционал (на A со значениями в ω) — это частичное отображение

$$\Phi: A^n \times \mathcal{PF}_{k_1} \times \dots \times \mathcal{PF}_{k_m} \rightarrow \omega$$

из декартова произведения нескольких экземпляров A и некоторых пространств $\mathcal{PF}_k$ в ω , которое монотонно, т. е.

$$f_1 \subseteq g_1, \dots, f_m \subseteq g_m, \Phi(\bar{x}, f_1, \dots, f_m) = \omega \\ \Rightarrow \Phi(\bar{x}, g_1, \dots, g_m) = \omega.$$

Мы здесь допускаем, что n или m могут равняться нулю, в частности, все частичные функции являются функционалами.

Сигнатурой функционала

$$\Phi(\bar{x}, \bar{f}) = \Phi(x_1, \dots, x_n, f_1, \dots, f_m)$$

называется $(n, k_1, \dots, k_m)$, если f_i является k_i -арной функцией. Существует естественное одно-однозначное соответствие между функционалами сигнатуры $(n, k_1, \dots, k_m)$ и монотонными операторами $\Theta: \mathcal{PF}_{k_1} \times \dots \times \mathcal{PF}_{k_m} \rightarrow \mathcal{PF}_n$, которое ставит в соответствие каждому $\Phi(\bar{x}, f_1, \dots, f_m)$ отображение

$$\Theta(f_1, \dots, f_m) = \lambda \bar{x} \Phi(\bar{x}, f_1, \dots, f_m)$$

и каждому $\Theta(f_1, \dots, f_m)$ — функционал

$$\Phi(\bar{x}, f_1, \dots, f_m) = \Theta(f_1, \dots, f_m)(\bar{x}).$$

В частности, если Φ имеет сигнатуру (n, n) , то ассоциированный с ним Θ является монотонным оператором на $\mathcal{PF}_n$. Будет удобно обозначать ξ -ю итерацию Θ через Φ^{ξ} , так что

$$\Phi^{\xi}(\bar{x}) = \Phi(\bar{x}, \Phi^{<\xi}),$$

где $\Phi^{<\xi} = \bigcup_{\eta < \xi} \Phi^{\eta}$. Пусть также $\Phi^{\infty} = \bigcup_{\xi} \Phi^{\xi}$ будет наименьшей неподвижной точкой (оператора, ассоциированного с) Φ , или частичной функцией, индуктивно определенной функционалом Φ .

Это определение непосредственно релятивизируется относительно любой конечной последовательности частичных функций: для данного $\Phi(\bar{x}, \bar{f}, \bar{g})$ сигнатуры $(n, n, k_1, \dots, k_m)$ положим

$$\Phi^{\xi}(\bar{x}, \bar{g}) = \Phi(\bar{x}, \lambda \bar{x}' \Phi^{<\xi}(\bar{x}', \bar{g}), \bar{g}),$$

$$\Phi^{\infty}(\bar{x}, \bar{g}) = \omega \Leftrightarrow \exists \xi \Phi^{\xi}(\bar{x}, \bar{g}) = \omega,$$

где, естественно,

$$\Phi^{<\xi}(\bar{x}, \bar{g}) = \omega \Leftrightarrow \exists \eta < \xi \Phi^{\eta}(\bar{x}, \bar{g}) = \omega.$$

Такие функционалы $\Phi(\bar{x}, \bar{f}, \bar{g})$ сигнатуры $(n, n, k_1, \dots, k_m)$ называются *оперативными*, а $\Phi^{\infty}(\bar{x}, \bar{g})$ — функционалом, индуктивно определенным функционалом Φ . Он имеет следующее свойство минимальности: если $\Psi(\bar{x}, \bar{g})$ удовлетворяет соотношению

$$\lambda \bar{x} \Phi(\bar{x}, \lambda \bar{x}' \Psi(\bar{x}', \bar{g}), \bar{g}) \subseteq \lambda \bar{x} \Psi(\bar{x}, \bar{g})$$

для всех $\bar{g}$, то $\Phi^{\infty} \subseteq \Psi$.

2.2. Пусть $\mathcal{F}$ будет классом функционалов на A . $\mathcal{F}$ -неподвижными точками называются все функционалы $\Phi^{\infty}(\bar{x}, \bar{g})$, которые индуктивно определены оперативными функционалами $\Phi(\bar{x}, \bar{f}, \bar{g})$ из $\mathcal{F}$. Говорим, что $\Psi(\bar{x}, \bar{g})$ $\mathcal{F}$ -рекурсивен, если существует $\mathcal{F}$ -неподвижная точка $\Phi^{\infty}(\bar{u}, \bar{x}, \bar{g})$ и конечная последовательность констант $\bar{n} = (n_1, \dots, n_k)$ из ω такая, что $\Psi(\bar{x}, \bar{g}) = \Phi^{\infty}(\bar{n}, \bar{x}, \bar{g})$. В частности, частичная функция $\varphi(\bar{x})$ будет $\mathcal{F}$ -рекурсивной, если существует оперативный функционал $\Phi(\bar{u}, \bar{x}, \bar{f})$ из $\mathcal{F}$ и константы $\bar{n}$ из ω такие, что

$$\varphi(\bar{x}) = \Phi^{\infty}(\bar{n}, \bar{x}).$$

Нашей главной целью является изучение этих $\mathcal{F}$ -рекурсивных частичных функций для различных $\mathcal{F}$. Для получения интересной теории $\mathcal{F}$ -рекурсии нужно наложить некоторые минимальные условия замкнутости на класс $\mathcal{F}$.

2.3. Определение. Класс функционалов $\mathcal{F}$ называется подходящим, если $\mathcal{F}$ содержит следующие начальные частич-

ные функции и функционалы (i)–(v) и замкнут относительно правил (vi)–(x):

(i) *Характеристическая функция множества ω :*

$$\varphi(a) = \chi_{\omega}(a) = \begin{cases} 0, & \text{если } a \in \omega, \\ 1, & \text{если } a \notin \omega. \end{cases}$$

(ii) *Тождественная функция на ω :*

$$\varphi(a) = \begin{cases} a, & \text{если } a \in \omega, \\ 0, & \text{если } a \notin \omega. \end{cases}$$

(iii) *Функция следования:*

$$\varphi(a) = \begin{cases} a + 1, & \text{если } a \in \omega, \\ 0, & \text{если } a \notin \omega. \end{cases}$$

(iv) *Характеристическая функция равенства на ω :*

$$\varphi(a, b) = \begin{cases} 0, & \text{если } a = b \in \omega, \\ 1, & \text{если } a \neq b \text{ и } a, b \in \omega, \\ 0 & \text{в остальных случаях.} \end{cases}$$

(v) *Вычисление значения функции:*

$$\Phi(\bar{x}, f) = f(\bar{x}).$$

Понятно, что здесь Φ имеет сигнатуру (n, n) , так что $f(\bar{x})$ имеет смысл. В последующем мы будем опускать условия такого тривиального сорта.

(vi) *Добавление переменных:* если $\Phi(\bar{x}, f)$ лежит в $\mathcal{F}$, то

$$\Psi(\bar{z}, \bar{x}, \bar{y}, \bar{h}, \bar{f}, \bar{g}) = \Phi(\bar{x}, \bar{f})$$

также лежит в $\mathcal{F}$.

(vii) *Композиция:* если $\Phi(a, \bar{x}, \bar{f})$ и $X(\bar{x}, \bar{f})$ лежат в $\mathcal{F}$, то

$$\Psi(\bar{x}, \bar{f}) = \Phi(X(\bar{x}, \bar{f}), \bar{x}, \bar{f})$$

также лежит в $\mathcal{F}$.

(viii) *Определение разбором случаев:* если $\Phi(\bar{x}, \bar{f})$ и $X(\bar{x}, \bar{f})$ лежат в $\mathcal{F}$, то

$$\Psi(a, \bar{x}, \bar{f}) = \begin{cases} \Phi(\bar{x}, \bar{f}), & \text{если } a = 0, \\ X(\bar{x}, \bar{f}), & \text{если } a \neq 0 \text{ и } a \in \omega, \\ 0, & \text{если } a \notin \omega, \end{cases}$$

также лежит в $\mathcal{F}$.

(ix) *Подстановка проектирований:* проектированием называется отображение вида

$$\pi(x_1, \dots, x_n) = x_i,$$

где $1 \leq i \leq n$. Тогда (ix) утверждает, что если $\Phi(y_1, \dots, y_m, \bar{f})$ лежит в $\mathcal{F}$, а $\pi_1, \dots, \pi_m$ — проектирования, то

$$\Psi(\bar{x}, \bar{f}) = \Phi(\pi_1(\bar{x}), \dots, \pi_m(\bar{x}), \bar{f})$$

также лежит в $\mathcal{F}$.

(x) *Функциональные подстановки:* если $\Phi(\bar{x}, g_1, \dots, g_m)$ лежит в $\mathcal{F}$ и $X_1, \dots, X_m$ также лежат в $\mathcal{F}$, то

$$\Psi(\bar{x}, \bar{f}) = \Phi(\bar{x}, \lambda \bar{y}_1 X_1(\bar{y}_1, \bar{x}, \bar{f}), \dots, \lambda \bar{y}_m X_m(\bar{y}_m, \bar{x}, \bar{f}))$$

также лежит в $\mathcal{F}$.

Мы будем использовать тривиальные следствия этих свойств замкнутости без явных оговорок. Например, из (vii) и (viii) следует, что если Φ_0, Φ_1 и X лежат в $\mathcal{F}$, то

$$\Psi(\bar{x}, \bar{f}) = \begin{cases} \Phi_0(\bar{x}, \bar{f}), & \text{если } X(\bar{x}, \bar{f}) = 0, \\ \Phi_1(\bar{x}, \bar{f}), & \text{если } X(\bar{x}, \bar{f}) \neq 0, \end{cases}$$

также лежит в $\mathcal{F}$, где $X(\bar{x}, \bar{f}) \neq 0$ — сокращение для « $X(\bar{x}, \bar{f})$ определено и имеет значение $\neq 0$ ».

Из (v), (vi), (ix) и (x) также следует, что если $\Phi(x_1, \dots, x_n, f_1, \dots, f_m) \in \mathcal{F}$ и π, ρ являются перестановками $\{1, \dots, n\}$ и $\{1, \dots, m\}$ соответственно, то

$$\Psi(x_1, \dots, x_n, f_1, \dots, f_m) = \Phi(x_{\pi(1)}, \dots, x_{\pi(n)}, f_{\rho(1)}, \dots, f_{\rho(m)})$$

также лежит в $\mathcal{F}$. Наконец, поскольку $f = \lambda \bar{x} f(\bar{x})$, то из (v), (ix) и (x) следует, что если $\Phi(\bar{x}, g_1, g_2, g_3)$ лежит в $\mathcal{F}$, то

$$\Psi(\bar{x}, f, g) = \Phi(\bar{x}, f, f, \lambda y g(y, \bar{x}, y))$$

также лежит в $\mathcal{F}$.

2.4. Теперь мы дадим два примера нетривиальных функционалов, которые $\mathcal{F}$ -рекурсивны для любого подходящего $\mathcal{F}$.

Минимизация. Пусть

$$\begin{aligned} \Phi_{\mu}(\bar{x}, f) &= \mu i (f(i, \bar{x}) = 0) \\ &= \text{наименьшему } i \in \omega \text{ (если хоть одно существует)} \\ &\text{такому, что } f(i, \bar{x}) = 0 \text{ и для всех } j < i \text{ } f(j, \bar{x}) \\ &\text{определено и } f(j, \bar{x}) \neq 0. \end{aligned}$$

Чтобы понять, что Φ_{μ} является $\mathcal{F}$ -рекурсивным, положим

$$\Psi(a, \bar{x}, g, f) = \begin{cases} f(a, \bar{x}), & \text{если } f(a, \bar{x}) = 0, \\ g(a + 1, \bar{x}) + 1, & \text{если } f(a, \bar{x}) \neq 0. \end{cases}$$

Ясно, что $\Psi \in \mathcal{F}$, и легко проверить, что $\Phi_{\mu}(\bar{x}, f) = \Psi^{\infty}(0, \bar{x}, f)$, так что Φ_{μ} является $\mathcal{F}$ -рекурсивным.

Примитивная рекурсия. Рассмотрим функционал $\Phi_p(a, f_1, f_2)$, определенный так:

$$\begin{aligned}\Phi_p(a, \bar{x}, f_1, f_2) &= 0, \quad \text{если } a \notin \omega, \\ \Phi_p(0, \bar{x}, f_1, f_2) &= f_1(\bar{x}), \\ \Phi_p(i+1, \bar{x}, f_1, f_2) &= f_2(\Phi_p(i, \bar{x}, f_1, f_2), i, \bar{x}),\end{aligned}$$

и предположим, что $\mathcal{F}$ является подходящим классом, содержащим функцию предшествования

$$a \div 1 = \begin{cases} a-1, & \text{если } a \in \omega, a \geq 1, \\ 0, & \text{если } a \notin \omega \text{ или } a = 0. \end{cases}$$

Положим

$$\Psi(a, \bar{x}, g, f_1, f_2) = \begin{cases} f_1(\bar{x}), & \text{если } a = 0, \\ f_2(g(a \div 1, \bar{x}), a, \bar{x}), & \text{если } a \in \omega, a \neq 0, \\ 0, & \text{если } a \notin \omega. \end{cases}$$

Тогда $\Psi \in \mathcal{F}$ и легко проверить, что $\Phi_p = \Psi^\infty$, так что Φ_p является $\mathcal{F}$ -рекурсивным. В следующем параграфе мы увидим, что на самом деле нет необходимости предполагать, что $a \div 1$ лежит в $\mathcal{F}$.

2.5. Пусть $\mathcal{F}_0 = \mathcal{F}_0(A)$ будет наименьшим подходящим классом функционалов на A . Более общо, если $\bar{\Phi} = (\Phi_1, \dots, \Phi_n)$ есть конечная последовательность функционалов, то пусть

$$\mathcal{F}_0[\bar{\Phi}]$$

будет наименьшим подходящим классом функционалов, содержащим $\Phi_1, \dots, \Phi_n$. Обычно мы будем называть $\mathcal{F}_0[\bar{\Phi}]$ -рекурсивные функционалы просто рекурсивными относительно $\bar{\Phi}$.

§ 3. Основные конструкции

Нашим основным инструментом для проведения сложных индукций является следующая

3.1. Лемма о совместной индукции. Пусть $\mathcal{F}$ — подходящий класс функционалов на A , $\Phi_0(\bar{x}, f_1, f_2, \bar{g})$ и $\Phi_1(\bar{y}, f_1, f_2, \bar{g})$ — два функционала из $\mathcal{F}$ и определим индуктивно

$$\begin{aligned}\Psi_0^\xi(\bar{x}, \bar{g}) &= \Phi_0(\bar{x}, \lambda \bar{x}' \Psi_0^{<\xi}(\bar{x}', \bar{g}), \lambda \bar{y}' \Psi_1^{<\xi}(\bar{y}', \bar{g}), \bar{g}), \\ \Psi_1^\xi(\bar{y}, \bar{g}) &= \Phi_1(\bar{y}, \lambda \bar{x}' \Psi_0^{<\xi}(\bar{x}', \bar{g}), \lambda \bar{y}' \Psi_1^{<\xi}(\bar{y}', \bar{g}), \bar{g}).\end{aligned}$$

Тогда Ψ_0^∞ и Ψ_1^∞ являются $\mathcal{F}$ -рекурсивными.

Доказательство. Пусть $\bar{0}$ будет последовательностью нулей подходящей длины, так что выражения, написанные ниже,

имеют смысл, и аналогично для $\bar{1}$. Положим

$$X(a, \bar{x}, \bar{y}, \bar{f}, \bar{g}) = \begin{cases} \Phi_0(\bar{x}, \lambda \bar{x}' f(0, \bar{x}', \bar{0}), \lambda \bar{y}' f(1, \bar{1}, \bar{y}'), \bar{g}), & \text{если } a = 0, \\ \Phi_1(\bar{y}, \lambda \bar{x}' f(0, \bar{x}', \bar{0}), \lambda \bar{y}' f(1, \bar{1}, \bar{y}'), \bar{g}), & \text{если } a \in \omega, a \neq 0, \\ 0, & \text{если } a \notin \omega. \end{cases}$$

Тогда $X \in \mathcal{F}$ и тривиальная индукция по ξ показывает, что

$$\Psi_0^\xi(\bar{x}, \bar{g}) = X^\xi(0, \bar{x}, \bar{0}, \bar{g}), \quad \Psi_1^\xi(\bar{y}, \bar{g}) = X^\xi(1, \bar{1}, \bar{y}, \bar{g}),$$

так что Ψ_0^∞ и Ψ_1^∞ являются $\mathcal{F}$ -рекурсивными. (Точнее говоря, мы имеем $\Psi_0^\infty(\bar{x}, \bar{g}) = X^\infty(0, \bar{x}, \bar{0}, \bar{g})$, что не имеет нужного вида, но очевидно, что

$$\Psi_0^\infty(\bar{x}, \bar{g}) = \bar{X}^\infty(0, \bar{0}, \bar{x}, \bar{g}),$$

где $\bar{X}(a, \bar{x}, \bar{y}, \bar{f}, \bar{g}) = X(a, \bar{y}, \bar{x}, \lambda a' \bar{y}' \bar{x}' f(a', \bar{y}', \bar{x}'), \bar{g})$.) $\square$

Непосредственным следствием предыдущего результата является важная

3.2. Теорема о функциональной подстановке. Пусть $\mathcal{F}$ — подходящий класс функционалов на A . Тогда класс $\mathcal{F}$ -рекурсивных функционалов замкнут относительно функциональных подстановок, т. е. если $\Phi(\bar{x}, g_1, \dots, g_m)$, $X_1, \dots, X_m$ являются $\mathcal{F}$ -рекурсивными, то таким же является и

$$\Psi(\bar{x}, \bar{f}) = \Phi(\bar{x}, \lambda \bar{y}_1 X_1(\bar{y}_1, \bar{x}, \bar{f}), \dots, \lambda \bar{y}_m X_m(\bar{y}_m, \bar{x}, \bar{f})).$$

Доказательство. Для простоты положим $m=1$ и рассмотрим $\Phi(\bar{x}, g)$, $X(\bar{y}, \bar{x}, \bar{f})$. В $\mathcal{F}$ найдутся функционалы $\Phi_0(\bar{u}, \bar{y}, \bar{x}, h, \bar{f})$, $\Phi_1(\bar{v}, \bar{x}, h', g)$ такие, что для некоторых $\bar{n}$, $\bar{m}$

$$X(\bar{y}, \bar{x}, \bar{f}) = \Phi_0^\infty(\bar{n}, \bar{y}, \bar{x}, \bar{f}), \quad \Phi(\bar{x}, g) = \Phi_1^\infty(\bar{m}, \bar{x}, g).$$

Теперь рассмотрим совместную индукцию

$$\begin{aligned}\Psi_0^\xi(\bar{u}, \bar{y}, \bar{x}, \bar{f}) &= \Phi_0(\bar{u}, \bar{y}, \bar{x}, \lambda \bar{u}' \bar{y}' \bar{x}' \Psi_0^{<\xi}(\bar{u}', \bar{y}', \bar{x}', \bar{f}), \bar{f}), \\ \Psi_1^\xi(\bar{v}, \bar{x}, \bar{f}) &= \Phi_1(\bar{v}, \bar{x}, \lambda \bar{v}' \bar{x}' \Psi_1^{<\xi}(\bar{v}', \bar{x}', \bar{f}), \lambda \bar{y}' \Psi_0^{<\xi}(\bar{n}, \bar{y}', \bar{x}, \bar{f})).\end{aligned}$$

По лемме о совместной индукции $\Psi_1^\infty(\bar{v}, \bar{x}, \bar{f})$ является $\mathcal{F}$ -рекурсивным. Мы утверждаем, что

$$\Psi(\bar{x}, \bar{f}) = \Psi_1^\infty(\bar{m}, \bar{x}, \bar{f}), \quad (*)$$

чем заканчивается доказательство. Чтобы убедиться, что (*) выполняется, сначала проверим, что $\Psi_0^\xi = \Phi_0^\xi$ для всех ξ . Из этого простой индукцией по ξ , используя монотонность функ-

ционалов на их функциональных аргументах, получаем (для любой $\bar{f}$)

$$\lambda \bar{x} \Psi_1^{\bar{f}}(\bar{v}, \bar{x}, \bar{f}) \subseteq \lambda \bar{x} \Phi_1^{\infty}(\bar{v}, \bar{x}, \lambda \bar{y} X(\bar{y}, \bar{x}, \bar{f})),$$

так что

$$\lambda \bar{x} \Psi_1^{\infty}(\bar{m}, \bar{x}, \bar{f}) \subseteq \lambda \bar{x} \Psi(\bar{x}, \bar{f}).$$

Для обратного включения мы доказываем индукцией по ξ , опять используя монотонность, что

$$\lambda \bar{x} \Phi_1^{\bar{f}}(\bar{v}, \bar{x}, \lambda \bar{y} \Phi_0^{<\xi}(\bar{n}, \bar{y}, \bar{x}, \bar{f})) \subseteq \lambda \bar{x} \Psi_1^{\bar{f}}(\bar{v}, \bar{x}, \bar{f}),$$

так что

$$\lambda \bar{x} \Phi_1^{\infty}(\bar{v}, \bar{x}, \lambda \bar{y} X(\bar{y}, \bar{x}, \bar{f})) \subseteq \lambda \bar{x} \Psi_1^{\infty}(\bar{v}, \bar{x}, \bar{f}),$$

и тогда

$$\lambda \bar{x} \Psi(\bar{x}, \bar{f}) \subseteq \lambda \bar{x} \Psi_1^{\infty}(\bar{m}, \bar{x}, \bar{f}),$$

что и требовалось. $\square$

Этот результат принимает особенно простую форму, если мы подставляем частичную функцию: если $\Phi(\bar{x}, g, \bar{f})$ и Ψ являются $\mathcal{F}$ -рекурсивными, то такой же является $\Psi(\bar{x}, \bar{f}) = \Phi(\bar{x}, \Phi, \bar{f})$.

Используя теорему о функциональной подстановке и тот тривиальный факт, что каждый функционал из $\mathcal{F}$ является $\mathcal{F}$ -рекурсивным, мы сразу получаем, что класс $\mathcal{F}$ -рекурсивных функционалов обладает всеми теми свойствами замкнутости, что и $\mathcal{F}$, так что, в частности, и сам является подходящим классом. Например, для доказательства того, что он замкнут относительно композиции, рассмотрим функционал

$$\Phi_C(\bar{x}, f_1, f_2) = f_2(f_1(\bar{x}), \bar{x}).$$

Ясно, что $\Phi_C \in \mathcal{F}$ ввиду 2.3 (v), (vii). Поэтому, если $\Phi(a, \bar{x}, \bar{f})$ и $X(\bar{x}, \bar{f})$ являются $\mathcal{F}$ -рекурсивными, то из теоремы о функциональной подстановке следует, что

$$\Psi(\bar{x}, \bar{f}) = \Phi(X(\bar{x}, \bar{f}), \bar{x}, \bar{f}) = \Phi_C(\bar{x}, \lambda \bar{x}' X(\bar{x}', \bar{f}), \lambda \bar{x}' \Phi(a, \bar{x}', \bar{f}))$$

также является $\mathcal{F}$ -рекурсивным. Аналогично, используя 2.4, устанавливаем, что класс $\mathcal{F}$ -рекурсивных функционалов замкнут относительно минимизации и примитивной рекурсии, по крайней мере если $a \div 1$ лежит в $\mathcal{F}$.

Наш последний результат в этом параграфе является, вероятно, наиболее важным свойством замкнутости класса $\mathcal{F}$ -рекурсивных функционалов для подходящих $\mathcal{F}$. Он позволяет свободно использовать $\mathcal{F}$ -рекурсивные функционалы в построении сложных индукций и будет часто использоваться впоследствии. Он называется также *первой теоремой о рекурсии* для функциональной индукции.

3.3. Теорема об индукционной полноте (Московакис [4]). Пусть $\mathcal{F}$ будет подходящим классом функционалов на A . Если $\Phi(\bar{x}, g, \bar{f})$ является оперативным $\mathcal{F}$ -рекурсивным функционалом, то его неподвижная точка $\Phi^{\infty}(\bar{x}, \bar{f})$ также $\mathcal{F}$ -рекурсивна.

Доказательство. Пусть $\Phi(\bar{x}, g, \bar{f}) = \Psi^{\infty}(\bar{n}, \bar{x}, g, \bar{f})$, где $\Psi(\bar{u}, \bar{x}, h, g, \bar{f}) \in \mathcal{F}$ и $\bar{n}$ является некоторой последовательностью констант. Положим

$$X(\bar{u}, \bar{x}, h, \bar{f}) = \Psi(\bar{u}, \bar{x}, h, \lambda \bar{x}' h(\bar{n}, \bar{x}', \bar{f}), \bar{f});$$

ясно, что $X \in \mathcal{F}$. Мы утверждаем, что

$$\Phi^{\infty}(\bar{x}, \bar{f}) = X^{\infty}(\bar{n}, \bar{x}, \bar{f}), \quad (**)$$

чем будет закончено доказательство.

Для доказательства (**) покажем сначала простой трансфинитной индукцией по ξ (используя монотонность), что

$$X^{\xi}(\bar{u}, \bar{x}, \bar{f}) = \omega \Rightarrow \Psi^{\xi}(\bar{u}, \bar{x}, \lambda \bar{x}' \Phi^{<\xi}(\bar{x}', \bar{f}), \bar{f}) = \omega,$$

так что

$$\begin{aligned} \lambda \bar{x} X^{\infty}(\bar{n}, \bar{x}, \bar{f}) &\subseteq \lambda \bar{x} \Psi^{\infty}(\bar{n}, \bar{x}, \lambda \bar{x}' \Phi^{\infty}(\bar{x}', \bar{f}), \bar{f}) \\ &= \lambda \bar{x} \Phi(\bar{x}, \lambda \bar{x}' \Phi^{\infty}(\bar{x}', \bar{f}), \bar{f}) \\ &= \lambda \bar{x} \Phi^{\infty}(\bar{x}, \bar{f}). \end{aligned}$$

Для доказательства обратного включения покажем индукцией по ξ (опять используя монотонность), что

$$\Psi^{\xi}(\bar{u}, \bar{x}, \lambda \bar{x}' X^{\infty}(\bar{n}, \bar{x}', \bar{f}), \bar{f}) = \omega \Rightarrow X^{\infty}(\bar{u}, \bar{x}, \bar{f}) = \omega,$$

так что

$$\begin{aligned} \lambda \bar{y} \Psi^{\infty}(\bar{n}, \bar{x}, \lambda \bar{x}' X^{\infty}(\bar{n}, \bar{x}', \bar{f}), \bar{f}) \\ = \lambda \bar{x} \Phi(\bar{x}, \lambda \bar{x}' X^{\infty}(\bar{n}, \bar{x}', \bar{f}), \bar{f}) \subseteq \lambda \bar{x}' X^{\infty}(\bar{n}, \bar{x}', \bar{f}); \end{aligned}$$

тогда ввиду минимальности Φ^{∞} (см. 2.1)

$$\lambda \bar{x} \Phi^{\infty}(\bar{x}, \bar{f}) \subseteq \lambda \bar{x} X^{\infty}(\bar{n}, \bar{x}, \bar{f}),$$

что и требовалось. $\square$

Теперь в качестве простого применения этой теоремы мы можем элиминировать предположение, что $\Phi(a) = a \div 1$ принадлежит $\mathcal{F}$, из доказательства того, что класс $\mathcal{F}$ -рекурсивных функционалов замкнут относительно примитивной рекурсии (см. 2.4). Действительно, теорема об индукционной полноте

говорит нам, что достаточно показать, что $a \div 1$ является $\mathcal{F}$ -рекурсивной. Но

$$a \div 1 = \begin{cases} 0, & \text{если } a = 0, \\ \mu i [i + 1 = a], & \text{если } a \in \omega, a \neq 0, \\ 0, & \text{если } a \notin \omega, \end{cases}$$

так что $a \div 1$ является $\mathcal{F}$ -рекурсивной.

§ 4. Связь с обычной теорией рекурсии

Прежде чем приступить к дальнейшему развитию теории функциональной индукции, в этом и следующем параграфах мы рассмотрим некоторые интересные примеры и установим связь с некоторыми классическими аспектами теории рекурсии.

4.1. Пусть A будет бесконечным множеством и предположим, что $\omega \subseteq B \subseteq A$. Функционал $\Phi(\bar{x}, \bar{f})$ на A сосредоточен на B , если для каждого $\bar{x} \in B^n$ и каждой $\bar{f} = (f_1, \dots, f_m) \in \mathcal{PF}_{k_1}(A) \times \dots \times \mathcal{PF}_{k_m}(A)$ имеем

$$\Phi(\bar{x}, \bar{f}) = \Phi(\bar{x}, \bar{f} \upharpoonright B),$$

где $\bar{f} \upharpoonright B = (f_1 \upharpoonright B^{k_1}, \dots, f_m \upharpoonright B^{k_m})$. Если $\mathcal{F}$ — класс функционалов на A , то пусть $\mathcal{F} \upharpoonright B$ будет классом тех функционалов на B , которые являются сужениями на B функционалов из $\mathcal{F}$, сосредоточенных на B . Здесь сужение $\Phi \upharpoonright B$ функционала $\Phi(\bar{x}, \bar{f})$ на A — это функционал на B , определенный равенством

$$\Phi \upharpoonright B(\bar{x}, \bar{f}) = \Phi(\bar{x}, \bar{f})$$

для $\bar{x} \in B^n$, $\bar{f} \in \mathcal{PF}_{k_1}(B) \times \dots \times \mathcal{PF}_{k_m}(B)$, и мы имеем

$$\mathcal{F} \upharpoonright B = \{\Phi \upharpoonright B: \Phi \in \mathcal{F}, \Phi \text{ сосредоточен на } B\}.$$

Заметим, что если $\mathcal{F}$ — подходящий класс функционалов на A , то $\mathcal{F} \upharpoonright B$ является подходящим классом функционалов на B .

Например, каждый функционал из $\mathcal{F}_0(A)$ — наименьшего подходящего класса функционалов на A — является сосредоточенным на B , так что

$$\mathcal{F}_0(A) \upharpoonright B = \mathcal{F}_0(B)$$

Более общо, если $\mathcal{F} = \mathcal{F}_0(A)[\bar{\Phi}]$, где каждый функционал из $\bar{\Phi}$ сосредоточен на B , то $\mathcal{F}_0(A)[\bar{\Phi}] \upharpoonright B = \mathcal{F}_0(B)[\bar{\Phi} \upharpoonright B]$, где $\bar{\Phi} \upharpoonright B = (\Phi_1 \upharpoonright B, \dots, \Phi_n \upharpoonright B)$, если $\bar{\Phi} = (\Phi_1, \dots, \Phi_n)$. Заметим здесь также, что если каждый функционал из $\mathcal{F}$ сосредоточен на B , то $\mathcal{F} \upharpoonright B$ -рекурсивные функционалы — это в точности ограничения на B $\mathcal{F}$ -рекурсивных функционалов.

Конкретизируя это на случай $B = \omega$, получаем, что для каждого $A \in \mathcal{F}_0(A)$ ω -рекурсивные функции — это в точности $\mathcal{F}_0(\omega)$ -рекурсивные функции. Теперь легко охарактеризовать их следующим образом:

4.2. Теорема. Частичная функция $f: \omega^n \rightarrow \omega$ является $\mathcal{F}_0$ -рекурсивной, если и только если она является рекурсивной.

Доказательство. То, что каждая частично рекурсивная функция на ω является $\mathcal{F}_0$ -рекурсивной, очевидно из свойств замкнутости класса $\mathcal{F}_0$ -рекурсивных частичных функций. В обратную сторону заметим, что если $\Phi(\bar{x}, f)$ является оперативным функционалом в $\mathcal{F}_0$, то соответствующий оператор $\Theta(f) = \lambda \bar{x} \Phi(\bar{x}, f)$ является рекурсивным оператором в смысле обычной теории рекурсии, поэтому его наименьшая неподвижная точка $\Phi^\infty(\bar{x})$ также рекурсивна по первой теореме Клини о рекурсии (см. Роджерс [1]). $\square$

§ 5. Рекурсия относительно объектов типа 2 и кванторов

В этом параграфе мы дадим некоторое число важных типов функционалов, рекурсию относительно которых мы хотим изучать.

5.1. Пусть A будет бесконечным множеством и $\omega \subseteq A$. Объектом типа 2 на A называется всюду определенное отображение

$$F: \omega^A \rightarrow \omega,$$

где ω^A — множество всех всюду определенных функций из A в ω . Каждый объект F типа 2 может быть естественным образом отождествлен с функционалом сигнатуры $(0, 1)$ на A , а именно;

$$F(f) = \begin{cases} F(f), & \text{если } f: A \rightarrow \omega \text{ всюду определена,} \\ \text{не определено в противном случае.} \end{cases}$$

Ясно, что полученный функционал монотонен, поскольку если $f \subseteq g$ и $F(f) = \omega$, то f всюду определена и тогда g также всюду определена, откуда $f = g$, следовательно, $F(g) = \omega$.

Особый интерес представляет объект $E = E_A$ типа 2, реализующий экзистенциальную квантификацию на A :

$$E(f) = \begin{cases} 0, & \text{если } \exists x (f(x) = 0), \\ 1, & \text{если } \forall x (f(x) \neq 0). \end{cases}$$

Другим интересным объектом типа 2 является объект Туге E_1 . Он определяется в зависимости от кодирования кортежей на A , т. е. одно-однозначного отображения $\langle \rangle: \bigcup_n A^n \rightarrow A$.

Для каждой всюду определенной /

$$E_1(f) = \begin{cases} 0, & \text{если } \exists a_0 a_1 \dots \forall n (f(\langle a_0, \dots, a_n \rangle) = 0), \\ 1, & \text{если } \forall a_0 a_1 \dots \exists n (f(\langle a_0, \dots, a_n \rangle) \neq 0). \end{cases}$$

Для иллюстрации этих идей и установления дальнейших связей с классическими понятиями теории рекурсии рассмотрим несколько подробнее рекурсию относительно $E = E_\omega$. Сначала дадим определение.

5.2. Определение. Пусть $\mathcal{F}$ будет подходящим классом функционалов на A . Предикат $R \subseteq A^n$ называется $\mathcal{F}$ -полурекурсивным, если существует $\mathcal{F}$ -рекурсивная частичная функция $f: A^n \rightarrow \omega$ такая, что

$$R = \text{domain}(f),$$

т. е.

$$\begin{aligned} R(\bar{x}) &\Leftrightarrow f(\bar{x}) \downarrow \\ &\Leftrightarrow f(\bar{x}) \text{ определено.} \end{aligned}$$

В случае $\mathcal{F} = \mathcal{F}_0[\bar{\Phi}]$ мы будем называть $\mathcal{F}$ -полурекурсивные предикаты просто *полурекурсивными относительно $\bar{\Phi}$* . В случае $A = \omega$, $\bar{\Phi} = \emptyset$ эта терминология согласуется с классической в силу 4.2. Теперь имеет место

5.3. Теорема (Клини [1]). Пусть E будет объектом типа 2, реализующим экзистенциальную квантификацию на ω . Предикат на ω полурекурсивен относительно E тогда и только тогда, когда он является Π_1^1 -предикатом.

Доказательство. Пусть $R(\bar{x})$ полурекурсивен относительно E и $\Phi(\bar{u}, \bar{x}, f) \in \mathcal{F}_0[E]$ таков, что для некоторого фиксированного $\bar{n}$

$$R(\bar{x}) \Leftrightarrow \Phi^\infty(\bar{n}, \bar{x}) \downarrow.$$

Тогда

$$\begin{aligned} R(\bar{x}) &\Leftrightarrow \exists k (\Phi^\infty(\bar{n}, \bar{x}) = k) \\ &\Leftrightarrow \exists k \forall f [\forall \bar{u}' \bar{x}' (\Phi(\bar{u}', \bar{x}', f) = f(\bar{u}', \bar{x}')) \Rightarrow f(\bar{n}, \bar{x}) = k]. \end{aligned}$$

Отождествляя частичные функции на ω с их графиками, мы легко вычисляем, что R является Π_1^1 -предикатом.

Наоборот, предположим, что $R(\bar{x})$ есть Π_1^1 -предикат, скажем

$$R(\bar{x}) \Leftrightarrow \forall \alpha \exists n P(\bar{x}, \bar{\alpha}(n)).$$

Здесь α пробегает ω^ω , $\bar{\alpha}(n) = \langle \alpha(0), \dots, \alpha(n-1) \rangle$ и

$$\langle k_0, \dots, k_{n-1} \rangle = p_0^{k_0+1} \cdot p_1^{k_1+1} \cdot \dots \cdot p_{n-1}^{k_{n-1}+1},$$

где p_i равно i -му простому числу и $P(\bar{x}, u)$ является рекурсивным предикатом, обладающим тем свойством, что если

$P(\bar{x}, \bar{\alpha}(n)) \& m \geq n$, то $P(\bar{x}, \bar{\alpha}(m))$. Определим

$$\Psi(u, \bar{x}, f) = \begin{cases} 0, & \text{если } P(\bar{x}, u) \& \text{Seq}(u), \\ 1 \div E(M(1 - f(u * t, \bar{x}))), & \text{если } \neg P(\bar{x}, u) \vee \neg \text{Seq}(u), \end{cases}$$

где $\text{Seq}(u) \Leftrightarrow \exists k_0 \dots k_{n-1} (u = \langle k_0, \dots, k_{n-1} \rangle)$ и

$$u * t = \begin{cases} \langle k_0, \dots, k_{n-1}, t \rangle, & \text{если } u = \langle k_0, \dots, k_{n-1} \rangle \\ & \text{для некоторых } k_0, \dots, k_{n-1}, \\ 0, & \text{если } \neg \text{Seq}(u). \end{cases}$$

По соглашению $1 = \langle \rangle$ — код пустой последовательности, так что $\text{Seq}(1)$. Поскольку Seq , $*$ рекурсивны, Ψ рекурсивен относительно E , так что по теореме 3.3 об индукционной полноте $\Psi^\infty(u, \bar{x})$ также рекурсивен относительно E . Теперь легко проверить индукцией по ξ , что если $\text{Seq}(u)$, то

$$\Psi^\xi(u, \bar{x}) = 0 \Rightarrow \forall \alpha \ni u \exists n P(\bar{x}, \bar{\alpha}(n)),$$

где $\alpha \ni u \Leftrightarrow \exists t (\bar{\alpha}(t) = u)$. С другой стороны, если $\Psi^\infty(u, \bar{x})$ не определено или определено и $\neq 0$, то выполнено $\neg P(\bar{x}, u)$, так что для некоторого t $\Psi^\infty(u * t, \bar{x})$ не определено или $\neq 0$. Повторяя это, находим $\alpha \ni u$ такое, что $\neg P(\bar{x}, \bar{\alpha}(n))$ для всех n , так что для $\text{Seq}(u)$ имеем

$$\Psi^\infty(u, \bar{x}) = 0 \Leftrightarrow \forall \alpha \ni u \exists n P(\bar{x}, \bar{\alpha}(n)),$$

следовательно, $R(\bar{x}) \Leftrightarrow \Psi^\infty(1, \bar{x}) = 0$. Таким образом, $R = \text{domain}(\Phi)$, где

$$\Phi(\bar{x}) = \begin{cases} 0, & \text{если } \Psi^\infty(1, \bar{x}) = 0, \\ \text{не определено,} & \text{если } \Psi^\infty(1, \bar{x}) \neq 0, \end{cases}$$

так что R полурекурсивен относительно E . $\square$

В § 9 мы докажем, что функция Φ рекурсивна относительно E в точности тогда, когда ее график является Π_1^1 -множеством.

5.4. Второй тип функционалов, который мы собираемся рассмотреть, происходит от понятия квантора.

Квантором на множестве A называется семейство Q подмножеств множества A со свойством монотонности:

$$X \subseteq Y \subseteq A \wedge X \in Q \Rightarrow Y \in Q.$$

Для исключения тривиальных случаев мы предполагаем также, что $\emptyset \subsetneq Q \subsetneq$ множество-степень множества A . Обычно при работе с кванторами употребляются эквивалентные друг другу обозначения:

$$\{x: R(x)\} \in Q \Leftrightarrow Q(\{x: R(x)\}) \Leftrightarrow QxR(x).$$

Квантор, дуальный к квантору Q , определяется так:

$$\check{Q}xR(x) \Leftrightarrow \neg Qx \neg R(x),$$

т. е.

$$X \in \check{Q} \Leftrightarrow (A - X) \notin Q.$$

Конечно, стандартными примерами кванторов являются квантор существования $\exists = \exists_A = \{X \subseteq A: X \neq \emptyset\}$ и дуальный к нему квантор всеобщности $\forall = \forall_A = \{A\}$. Другим интересным квантором является квантор Суслина (зависящий от кодирования кортежей на A),

$$\mathcal{C}xR(x) \Leftrightarrow \forall x_0 \forall x_1 \dots \exists kR(\langle x_0, \dots, x_k \rangle).$$

Каждый квантор Q может быть естественным образом отождествлен с объектом F_Q типа 2, определенным следующим образом: для всюду определенной $f: A \rightarrow \omega$

$$F_Q(f) = \begin{cases} 0, & \text{если } Qx(f(x) = 0), \\ 1, & \text{если } \check{Q}x(f(x) \neq 0). \end{cases}$$

При этом отождествлении E соответствует $\exists$ и E_1 соответствует $\mathcal{C}$. Конечно, существует много объектов типа 2, которые не соответствуют никаким кванторам.

Каждый квантор Q приводит также к другому функционалу $F_Q^\#$ сигнатуры $(0, 1)$:

$$F_Q^\#(f) = \begin{cases} 0, & \text{если } Qx(f(x) = 0), \\ 1, & \text{если } \check{Q}x(f(x) \neq 0), \\ \text{не определено} & \text{в остальных случаях.} \end{cases}$$

Например (напомним, что $F_\exists = E$),

$$E^\#(f) = \begin{cases} 0, & \text{если } \exists x(f(x) = 0), \\ 1, & \text{если } \forall x(f(x) \neq 0), \\ \text{не определено} & \text{в остальных случаях.} \end{cases}$$

Ясно, что F_Q является ограничением $F_Q^\#$ на всюду определенные $f: A \rightarrow \omega$, и нетрудно убедиться, что F_Q рекурсивен относительно $F_Q^\#, E^\#$. Действительно,

$$F_Q(f) = F_Q^\#(f) \cdot \Psi(f),$$

где

$$\Psi(f) = \begin{cases} 1, & \text{если } f \text{ всюду определена,} \\ \text{не определено} & \text{в противном случае.} \end{cases}$$

Далее, Ψ рекурсивен относительно $E^\#$, поскольку $\Psi(f) = E^\#(\lambda x(f(x) + 1))$. В частности, E рекурсивен относительно $E^\#$, так что каждая функция, рекурсивная относительно E , рекурсивна также относительно $E^\#$. В общем, для большинства множеств A существуют функции, рекурсивные относительно $E^\#$, которые не рекурсивны относительно E . Исключением является $A = \omega$, в этом случае классы функций, рекурсивных относительно E и $E^\#$, совпадают с классом функций, имеющих Π_1^1 -график; см. 5.3 и 9.5.

Для знакомых с теорией индуктивной определимости упомянем, что если $\mathfrak{A} = \langle A, R_1, \dots, R_l \rangle$ является допустимой структурой, то предикат на A полурекурсивен относительно $F_Q^\#, E^\#$ и характеристических функций для $=, R_1, \dots, R_l$ в том и только в том случае, когда он абсолютно $\mathcal{L}^{\mathfrak{A}}(Q)$ -индуктивен. Определения см. у Московского [2].

Рекурсия относительно F_Q и $F_Q^\#$ для кванторов Q на ω была введена Хинненом [1], где также установлены их основные свойства (включая соответствующий вариант теоремы 7.2 в контексте рекурсии относительно $F_Q^\#$). См. также Ацел [1].

§ 6. Теорема о пошаговом сравнении

6.1. Пусть $\Phi(\bar{x}, f)$ будет оперативным функционалом на A . Рассмотрим $\Phi^\infty(\bar{x})$ и свяжем с каждым $\bar{x}$, для которого $\Phi^\infty(\bar{x})$ определено, ординал

$$|\bar{x}|_\Phi = \text{наименьшему } \xi \text{ такому, что } \Phi^\xi(\bar{x}) \downarrow.$$

Условимся также полагать

$$|\bar{x}|_\Phi = \infty = \text{card}(A)^+,$$

если $\Phi^\infty(\bar{x}) \uparrow$, где

$$f(\bar{x}) \uparrow \Leftrightarrow f(\bar{x}) \text{ не определено.}$$

Таким образом,

$$|\bar{x}|_\Phi < \infty \Leftrightarrow \Phi^\infty(\bar{x}) \downarrow.$$

Теперь для двух данных оперативных функционалов положим

$$\bar{x} \leq_{\Phi, \Psi}^* \bar{y} \Leftrightarrow \Phi^\infty(\bar{x}) \downarrow \wedge |\bar{x}|_\Phi \leq |\bar{y}|_\Psi,$$

$$\bar{x} <_{\Phi, \Psi}^* \bar{y} \Leftrightarrow \Phi^\infty(\bar{x}) \downarrow \wedge |\bar{x}|_\Phi < |\bar{y}|_\Psi \Leftrightarrow |\bar{x}|_\Phi < |\bar{y}|_\Psi,$$

и пусть

$$\chi(\bar{x}, \bar{y}) = \begin{cases} 0, & \text{если } \bar{x} \leq_{\Phi, \Psi}^* \bar{y}, \\ 1, & \text{если } \bar{y} <_{\Psi, \Phi}^* \bar{x}; \end{cases}$$

мы называем χ частичной функцией *пошагового сравнения* для Φ и Ψ .

Если Φ, Ψ принадлежат некоторому подходящему классу $\mathcal{F}$, то естественно спросить, является ли соответствующая χ $\mathcal{F}$ -рекурсивной. Это не так в общем случае, но выполняется, если Φ и Ψ являются нормальными в соответствии со следующим определением, данным Московакисом [4].

6.2. Определение. Пусть $\mathcal{F}$ будет классом функционалов на A и $\Phi(\bar{x}, \bar{f})$ — функционал из $\mathcal{F}$. Мы называем Φ *нормальным* относительно $\mathcal{F}$, если существует $\mathcal{F}$ -рекурсивный функционал $\Delta_\Phi(\bar{x}, \bar{f}, \bar{\delta})$, принимающий только значения 0 и 1, такой, что:

- (i) если $\Phi(\bar{x}, \bar{f} \upharpoonright \{\bar{y}: \bar{\delta}(\bar{y})=0\}) \downarrow$, то $\Delta_\Phi(\bar{x}, \bar{f}, \bar{\delta})=0$,
- (ii) если $\bar{\delta}$ всюду определена, $\{\bar{y}: \bar{\delta}(\bar{y})=0\} \subseteq \text{domain}(\bar{f})$ и $\Phi(\bar{x}, \bar{f} \upharpoonright \{\bar{y}: \bar{\delta}(\bar{y})=0\}) \uparrow$, то $\Delta_\Phi(\bar{x}, \bar{f}, \bar{\delta})=1$.

Здесь векторные обозначения используются с очевидным смыслом: если $\bar{f}=(f_1, \dots, f_m) \in \mathcal{PF}_{k_1} \times \dots \times \mathcal{PF}_{k_m}$, то $\bar{\delta}=(\delta_1, \dots, \delta_m)$ также пробегает $\mathcal{PF}_{k_1} \times \dots \times \mathcal{PF}_{k_m}$,

$\bar{f} \upharpoonright \{\bar{y}: \bar{\delta}(\bar{y})=0\}=(f_1 \upharpoonright \{\bar{y}_1: \delta_1(\bar{y}_1)=0\}, \dots, f_m \upharpoonright \{\bar{y}_m: \delta_m(\bar{y}_m)=0\})$ и $\{\bar{y}: \bar{\delta}(\bar{y})=0\} \subseteq \text{domain}(\bar{f})$ означает, что для всех $1 \leq i \leq m$ $\{\bar{y}_i: \delta_i(\bar{y}_i)=0\} \subseteq \text{domain}(f_i)$.

Мы называем класс функционалов $\mathcal{F}$ *нормальным*, если каждый функционал из $\mathcal{F}$ нормален относительно $\mathcal{F}$.

Следующий результат принадлежит Московакису [4] и доказывается по образцу доказательства Ацелом и Кюненом аналогичного результата в теории позитивной элементарной индуктивной определенности, см. Московакис [2].

6.3. Теорема о пошаговом сравнении. Пусть $\mathcal{F}$ будет подходящим классом функционалов на A , а $\Phi(\bar{x}, \bar{f})$ и $\Psi(\bar{y}, \bar{g})$ — два функционала из $\mathcal{F}$, которые нормальны относительно $\mathcal{F}$, тогда функция пошагового сравнения для Φ и Ψ является $\mathcal{F}$ -рекурсивной.

Доказательство. Пусть $\Delta_\Phi(\bar{x}, \bar{f}, \bar{\delta})$ и $\Delta_\Psi(\bar{y}, \bar{g}, \bar{\epsilon})$ будут функционалами, связанными с Φ и Ψ в определении нормальности 6.2. Мы найдем функционал $X(\bar{x}, \bar{y}, h)$ со значениями 0 и 1, неподвижная точка $X^\infty(\bar{x}, \bar{y})$ которого будет иметь то свойство, что если $\bar{x} \leq_{\Phi, \Psi}^* \bar{y}$, то $X^\infty(\bar{x}, \bar{y})=0$, а если $\bar{y} <_{\Psi, \Phi}^* \bar{x}$, то $X^\infty(\bar{x}, \bar{y})=1$. Из этого мы можем легко получить функцию пошагового сравнения

$$\chi(\bar{x}, \bar{y}) = \begin{cases} \Phi^\infty(\bar{x}) \cdot 0, & \text{если } X^\infty(\bar{x}, \bar{y})=0, \\ \Phi(\Psi^\infty(\bar{y})), & \text{если } X^\infty(\bar{x}, \bar{y})=1, \end{cases}$$

где $\phi(a)=1$ для всех a .

Эвристически χ находится следующим образом: опуская индексы для упрощения обозначений, имеем

$$\begin{aligned} \bar{x} \leq_{\Phi, \Psi}^* \bar{y} &\Leftrightarrow \Phi^{\upharpoonright \bar{y}}(\bar{x}) \downarrow \Leftrightarrow \Phi(\bar{x}, \Phi^{< \upharpoonright \bar{y}}) \downarrow \\ &\Leftrightarrow \Phi(\bar{x}, \Phi^\infty \upharpoonright \{\bar{x}': |\bar{x}'| < |\bar{y}|\}) \downarrow. \end{aligned}$$

Теперь

$$|\bar{x}'| < |\bar{y}| \Rightarrow \Psi^{\upharpoonright \bar{x}'}(\bar{y}) \uparrow \Leftrightarrow \Psi(\bar{y}, \Psi^{< \upharpoonright \bar{x}'}) \uparrow.$$

Таким образом, полагая

$$\neg h(\bar{z}) = \begin{cases} 1, & \text{если } h(\bar{z})=0, \\ 0, & \text{если } h(\bar{z})=1, \end{cases}$$

мы имеем

$$\begin{aligned} \chi(\bar{x}, \bar{y})=0 &\Rightarrow \Phi(\bar{x}, \Phi^\infty \upharpoonright \{\bar{x}': \Psi(\bar{y}, \Psi^\infty \upharpoonright \{\bar{y}': |\bar{y}'| < |\bar{x}'|\}) \uparrow\}) \downarrow \\ &\Rightarrow \Delta_\Phi(\bar{x}, \Phi^\infty, \lambda \bar{x}' \neg \Delta_\Psi(\bar{y}, \Psi^\infty, \lambda \bar{y}' \neg \chi(\bar{x}', \bar{y}')))=0. \end{aligned}$$

Аналогично

$$\chi(\bar{x}, \bar{y})=1 \Rightarrow \Delta_\Phi(\bar{x}, \Phi^\infty, \lambda \bar{x}' \neg \Delta_\Psi(\bar{y}, \Psi^\infty, \lambda \bar{y}' \neg \chi(\bar{x}', \bar{y}')))=1.$$

Поэтому, если $\Phi^\infty(\bar{x}) \downarrow$ или $\Psi^\infty(\bar{y}) \downarrow$, имеем

$$\chi(\bar{x}, \bar{y})=\Delta_\Phi(\bar{x}, \Phi^\infty, \lambda \bar{x}' \neg \Delta_\Psi(\bar{y}, \Psi^\infty, \lambda \bar{y}' \neg \chi(\bar{x}', \bar{y}'))).$$

Это подсказывает определение

$$X(\bar{x}, \bar{y}, h)=\Delta_\Phi(\bar{x}, \Phi^\infty, \lambda \bar{x}' \neg \Delta_\Psi(\bar{y}, \Psi^\infty, \lambda \bar{y}' \neg h(\bar{x}', \bar{y}'))).$$

Ясно, что X является $\mathcal{F}$ -рекурсивным функционалом по теореме 3.2 о подстановке, поэтому по теореме 3.3 о полноте $X^\infty(\bar{x}, \bar{y})$ также $\mathcal{F}$ -рекурсивен. Для доказательства того, что X^∞ обладает требуемыми свойствами, доказываем сначала индукцией по ξ , что

$$\bar{x} \leq_{\Phi, \Psi}^* \bar{y} \wedge |\bar{x}|_\Phi = \xi \Rightarrow X^\xi(\bar{x}, \bar{y})=0,$$

и затем снова индукцией по ξ , что

$$\bar{y} <_{\Psi, \Phi}^* \bar{x} \wedge |\bar{y}|_\Psi = \xi \Rightarrow X^\xi(\bar{x}, \bar{y})=1.$$

Детали мы оставляем читателю. $\square$

Мы сейчас увидим, что все примеры функционалов, которые мы обсуждали в § 5, приводят к нормальным классам, но сначала установим следующий простой критерий нормальности.

6.4. Предложение. Пусть $\bar{\Phi}$ будет конечной последовательностью функционалов на A ; если каждый функционал в списке $\bar{\Phi}$ нормален относительно $\mathcal{F}_0[\bar{\Phi}]$, то $\mathcal{F}_0[\bar{\Phi}]$ является нормальным.

Доказательство. Предположим, что каждый функционал из $\bar{\Phi}$ нормален относительно $\mathcal{F}_0[\bar{\Phi}]$. Мы докажем, что

каждый функционал из $\mathcal{F}_0[\bar{\Phi}]$ нормален относительно $\mathcal{F}_0[\bar{\Phi}]$, индукцией по построению $\mathcal{F}_0[\bar{\Phi}]$.

Случай 2.3 (i)–(v), т. е. случаи начальных функционалов, тривиальны. Например, если $\Phi(\bar{x}, f) = f(\bar{x})$, то полагаем

$$\Delta_{\Phi}(\bar{x}, f, \delta) = \begin{cases} 0, & \text{если } \delta(\bar{x}) = 0, \\ 1, & \text{если } \delta(\bar{x}) \neq 0. \end{cases}$$

Случай 2.3 (vi), (viii), (ix) и (x) также рассматриваются непосредственно. Наконец, в случае 2.3 (vii), предполагая, что для $\Phi(a, \bar{x}, \bar{f})$ и $X(\bar{x}, \bar{f})$ мы уже нашли Δ_{Φ} , Δ_X с требуемыми свойствами, и полагая $\Psi(\bar{x}, \bar{f}) = \Phi(X(\bar{x}, \bar{f}), \bar{x}, \bar{f})$, определяем

$$\Delta_{\Psi}(\bar{x}, \bar{f}, \bar{\delta}) = \begin{cases} \Delta_{\Phi}(X(\bar{x}, \bar{f}), \bar{x}, \bar{f}, \bar{\delta}), & \text{если } \Delta_X(\bar{x}, \bar{f}, \bar{\delta}) = 0, \\ \Delta_X(\bar{x}, \bar{f}, \bar{\delta}), & \text{если } \Delta_X(\bar{x}, \bar{f}, \bar{\delta}) \neq 0. \quad \square \end{cases}$$

Назовем конечную последовательность $\bar{\Phi}$ функционалов на A *нормальной*, если каждый функционал из $\bar{\Phi}$ нормален относительно $\mathcal{F}_0[\bar{\Phi}]$.

6.5. Теорема. (i) Для каждой конечной последовательности $\bar{F}$ объектов типа 2 на A расширенная последовательность $\bar{F}, E$ является нормальной.

(ii) Пусть Q будет квантором на A ; тогда $F_Q^{\#}$ нормален.

Доказательство. (i) С каждым объектом F типа 2 из $\bar{F}$ свяжем один и тот же

$$\Delta_F(f, \delta) = 1 \div E(\lambda x(1 \div \delta(x))),$$

где

$$1 \div a = \begin{cases} 1, & \text{если } a = 0, \\ 0, & \text{если } a \neq 0 \text{ или } a \notin \omega. \end{cases}$$

(ii) Пусть Q будет квантором на A , а $\Phi = F_Q^{\#}$ — соответствующий функционал. Положим сначала

$$\Psi(x, f, \delta) = \begin{cases} 1, & \text{если } \delta(x) \neq 0, \\ 1, & \text{если } \delta(x) = 0, \quad f(x) \neq 0, \\ 0, & \text{если } \delta(x) = 0, \quad f(x) = 0, \end{cases}$$

и

$$X(x, f, \delta) = \begin{cases} 0, & \text{если } \delta(x) \neq 0, \\ 1, & \text{если } \delta(x) = 0, \quad f(x) \neq 0, \\ 0, & \text{если } \delta(x) = 0, \quad f(x) = 0. \end{cases}$$

Теперь положим

$$\Delta_{\Phi}(f, \delta) = \begin{cases} 0, & \text{если } F_Q^{\#}(\lambda x \Psi(x, f, \delta)) = 0, \\ 0, & \text{если } F_Q^{\#}(\lambda x \Psi(x, f, \delta)) = 1 \text{ \& } F_Q^{\#}(\lambda x X(x, f, \delta)) = 1, \\ 1, & \text{если } F_Q^{\#}(\lambda x \Psi(x, f, \delta)) = 1 \text{ \& } F_Q^{\#}(\lambda x X(x, f, \delta)) = 0. \end{cases}$$

Чтобы доказать, что Δ_{Φ} годится, предположим сначала, что $F_Q^{\#}(f \upharpoonright \{x: \delta(x) = 0\}) \downarrow$. Тогда $Qx(f(x) = 0 \wedge \delta(x) = 0)$ либо $Qx(f(x) \neq 0 \wedge \delta(x) = 0)$. В первом случае $F_Q^{\#}(\lambda x \Psi(x, f, \delta)) = 0$, а во втором $F_Q^{\#}(\lambda x \Psi(x, f, \delta)) = 1$ и $F_Q^{\#}(\lambda x X(x, f, \delta)) = 1$, так что в обоих случаях $\Delta_{\Phi}(f, \delta) = 0$. Теперь, если δ всюду определена, $\{x: \delta(x) = 0\} \subseteq \text{domain}(f)$ и $F_Q^{\#}(f \upharpoonright \{x: \delta(x) = 0\}) \uparrow$, то обязательно не имеют места ни $Qx(f(x) = 0 \wedge \delta(x) = 0)$, ни $Qx(f(x) \neq 0 \wedge \delta(x) = 0)$, так что выполняются $Qx(f(x) \neq 0 \vee f(x) \uparrow \vee \delta(x) \neq 0)$ и $Qx(f(x) = 0 \vee f(x) \uparrow \vee \delta(x) \neq 0)$. Замечая, что $f(x) \uparrow \Rightarrow \delta(x) \neq 0$, мы получаем, что $Qx(f(x) \neq 0 \vee \delta(x) \neq 0)$ и $Qx(f(x) = 0 \vee \delta(x) \neq 0)$, так что $F_Q^{\#}(\lambda x \Psi(x, f, \delta)) = 1$ и $F_Q^{\#}(\lambda x X(x, f, \delta)) = 0$, т. е. $\Delta_{\Phi}(f, \delta) = 1$. $\square$

§ 7. Полурекурсивные предикаты

7.1. Пусть $\mathcal{F}$ будет классом функционалов на A . Напомним, что в 5.2 предикат $R \subseteq A^n$ был назван $\mathcal{F}$ -полурекурсивным, если он является областью определения $\mathcal{F}$ -рекурсивной частичной функции $\varphi: A^n \rightarrow \omega$. Назовем предикат $R \subseteq A^n$ $\mathcal{F}$ -рекурсивным, если его характеристическая функция

$$\chi_R(\bar{x}) = \begin{cases} 0, & \text{если } R(\bar{x}), \\ 1, & \text{если } \neg R(\bar{x}), \end{cases}$$

является $\mathcal{F}$ -рекурсивной, где $\neg R = A^n - R$.

В этом параграфе мы обсудим некоторые структурные свойства и свойства замкнутости класса $\mathcal{F}$ -полурекурсивных предикатов для подходящего нормального $\mathcal{F}$. Это изучение будет продолжено в § 9, после того как мы докажем свойство пересисимости.

Для данного предиката $R \subseteq A^n$ *нормой* на R называется отображение $\sigma: R \rightarrow$ ординалы. Мы условимся также полагать $\sigma(\bar{x}) = \infty =$ ординалу, большему чем все $\sigma(\bar{y})$ для тех $\bar{y}$, для которых $R(\bar{y})$, если выполняется $\neg R(\bar{x})$. С каждой нормой σ на R мы связываем предикаты

$$\bar{x} \leq_o^* \bar{y} \Leftrightarrow R(\bar{x}) \wedge \sigma(\bar{x}) \leq \sigma(\bar{y}),$$

$$\bar{x} <_o^* \bar{y} \Leftrightarrow R(\bar{x}) \wedge \sigma(\bar{x}) < \sigma(\bar{y}) \Leftrightarrow \sigma(\bar{x}) < \sigma(\bar{y}).$$

Если Γ — совокупность предикатов на A и σ — норма на R , то мы называем σ Γ -нормой, если $\leq^*_\sigma$ и $<^*_\sigma$ лежат в Γ . Говорим, что Γ является *нормированным*, или обладает *свойством предвполнеупорядоченности*, если каждый предикат из Γ обладает Γ -нормой.

7.2. Теорема о предвполнеупорядоченности. Пусть $\mathcal{F}$ будет подходящим нормальным классом функционалов на A . Тогда класс $\mathcal{F}$ -полурекурсивных предикатов является нормированным.

Доказательство. Пусть $R(\bar{x}) \Leftrightarrow \varphi(\bar{x}) \downarrow$, где φ является $\mathcal{F}$ -рекурсивной, и пусть $\varphi(\bar{x}) = \Phi^\infty(\bar{n}, \bar{x})$, где $\Phi \in \mathcal{F}$. Положим $\sigma(\bar{x}) = |\bar{n}, \bar{x}|_\Phi$ (см. 6.1). Тогда σ является $\mathcal{F}$ -полурекурсивной нормой на R по теореме 6.3 о пошаговом сравнении. $\square$

Класс Γ предикатов на A замкнут относительно $\bigvee$, если для любых $R, S \in A^n$ из Γ предикат

$$(R \vee S)(\bar{x}) \Leftrightarrow R(\bar{x}) \vee S(\bar{x})$$

также принадлежит Γ . Аналогично для $\wedge$ и $\neg$.

7.3. Теорема. Пусть $\mathcal{F}$ будет подходящим нормальным классом функционалов на A . Тогда:

(i) Класс $\mathcal{F}$ -полурекурсивных предикатов замкнут относительно $\wedge$ и $\vee$.

(ii) Предикат R является $\mathcal{F}$ -рекурсивным тогда и только тогда, когда R и $\neg R$ являются $\mathcal{F}$ -полурекурсивными.

Доказательство. (i) Замкнутость относительно $\wedge$ тривиальна и не требует нормальности, потому что

$$\varphi(\bar{x}) \downarrow \wedge \psi(\bar{x}) \downarrow \Leftrightarrow (\varphi(\bar{x}) + \psi(\bar{x})) \downarrow.$$

Для $\vee$ положим

$$R(\bar{x}) \Leftrightarrow \varphi(\bar{x}) \downarrow, \quad S(\bar{x}) \Leftrightarrow \psi(\bar{x}) \downarrow,$$

где φ и ψ являются $\mathcal{F}$ -рекурсивными. По теореме о пошаговом сравнении получаем функцию $\chi(\bar{x}_1, \bar{x}_2)$, где $\bar{x}_1, \bar{x}_2 \in A^n$, которая определена в точности тогда, когда либо $\varphi(\bar{x}_1) \downarrow$, либо $\psi(\bar{x}_2) \downarrow$. Тогда

$$R(\bar{x}) \vee S(\bar{x}) \Leftrightarrow \chi(\bar{x}, \bar{x}) \downarrow,$$

и все готово.

(ii) Предположим, что R и $\neg R$ являются $\mathcal{F}$ -полурекурсивными. Пусть $R(\bar{x}) \Leftrightarrow \varphi(\bar{x}) \downarrow$ и $\neg R(\bar{x}) \Leftrightarrow \psi(\bar{x}) \downarrow$, и снова найдем $\mathcal{F}$ -рекурсивную $\chi(\bar{x}_1, \bar{x}_2)$ такую, что если $\varphi(\bar{x}_1) \downarrow$ и $\psi(\bar{x}_2) \uparrow$, то $\chi(\bar{x}_1, \bar{x}_2) = 0$, а если $\psi(\bar{x}_2) \downarrow$ и $\varphi(\bar{x}_1) \uparrow$, то $\chi(\bar{x}_1, \bar{x}_2) = 1$. Тогда мы имеем $\chi_R(\bar{x}) = \chi(\bar{x}, \bar{x})$, так что R является $\mathcal{F}$ -рекурсивным. $\square$

Например, в силу 6.5 и 5.3 получаем, что предикат на ω рекурсивен относительно E тогда и только тогда, когда он есть Δ_1 -предикат, т. е. гиперарифметический (Клини [1]).

§ 8. Теорема о перечислении

В этом параграфе нашей целью является доказательство существования универсальных $\mathcal{F}$ -рекурсивных частичных функций для соответствующих $\mathcal{F}$. Сначала напомним определение.

8.1. Пусть $\mathcal{F}$ будет классом частичных функций (нескольких переменных) на множестве A таком, что $\omega \subseteq A$. Говорим, что $\mathcal{F}$ обладает *свойством перечисления*, или $\mathcal{F}$ является ω -*параметризуемым*, если для каждого $n \geq 1$ существует некоторая функция $\varphi(a, x_1, \dots, x_n)$ в $\mathcal{F}$ такая, что класс всех n -местных частичных функций из $\mathcal{F}$ совпадает с $\{\varphi_e: e \in \omega\}$, где для каждой частичной функции f

$$f_e(x_1, \dots, x_n) = f(e, x_1, \dots, x_n).$$

Если $f = \varphi_e$, то мы называем e *кодом* или *индексом* функции f (относительно φ). Такая частичная функция φ называется *универсальной* (для n -местных частичных функций из $\mathcal{F}$).

В 8.4 мы докажем, что класс $\mathcal{F}$ -рекурсивных частичных функций обладает свойством перечисления в предположении, что $\mathcal{F}$ является подходящим, конечно порожденным и допускает кодирование кортежей. Теперь объясним эти понятия.

8.2. Пусть дано множество A такое, что $\omega \subseteq A$. *Кодирование кортежей на A* — это одно-однозначная функция $\mathcal{C} = \langle \rangle$ из множества всех конечных последовательностей элементов из A (включая пустую последовательность) в A . С каждым таким кодированием мы связываем следующие всюду определенные функции (из A в ω) и (всюду определенные) отображения из A^2 или A в A :

$$(i) \chi_{\text{Seq}}(x) = \chi_{\text{Seq}}^{\mathcal{C}}(x) = \begin{cases} 0, & \text{если } \exists x_0 \dots \exists x_{n-1} (x = \langle x_0, \dots, x_{n-1} \rangle), \\ 1 & \text{в противном случае.} \end{cases}$$

$$(ii) \text{lh}(x) = \text{lh}^{\mathcal{C}}(x) = \begin{cases} n, & \text{если } \exists x_0 \dots \exists x_{n-1} (x = \langle x_0, \dots, x_{n-1} \rangle), \\ 0 & \text{в противном случае.} \end{cases}$$

$$(iii) (x)_i = (x)_i^{\mathcal{C}} = q^{\mathcal{C}}(x, i) = \begin{cases} x_i, & \text{если } \exists x_0 \dots \exists x_{n-1} (x = \langle x_0, \dots, x_{n-1} \rangle), \\ 0 & \text{в противном случае.} \end{cases}$$

$$(iv) x * y = x *^{\mathcal{E}} y$$

$$= \begin{cases} \langle x_0, \dots, x_{n-1}, y_0, \dots, y_{m-1} \rangle, \\ \text{если } \exists x_0 \dots \exists x_{n-1} (x = \langle x_0, \dots, x_{n-1} \rangle) \\ \quad \& \exists y_0 \dots \exists y_{m-1} (y = \langle y_0, \dots, y_{m-1} \rangle), \\ 0 & \text{в противном случае.} \end{cases}$$

$$(v) s(x) = s^{\mathcal{E}}(x) = \langle x \rangle.$$

Теперь для данного класса функционалов $\mathcal{F}$ на A говорим, что $\mathcal{F}$ допускает кодирование кортежей $\mathcal{E}$, если $\chi_{\text{Seq}}^{\mathcal{E}}$, lh $\mathcal{E}$ являются $\mathcal{F}$ -рекурсивными и класс $\mathcal{F}$ -рекурсивных функционалов замкнут относительно подстановок функций $(x)_i^{\mathcal{E}}$, $x *^{\mathcal{E}} y$, $s^{\mathcal{E}}$. Это означает, что если $\Phi(x, \bar{y}, \bar{f})$ является $\mathcal{F}$ -рекурсивным и t является любым из этих отображений, то $\Psi(\bar{z}, \bar{y}, \bar{f}) = \Phi(t(\bar{z}), \bar{y}, \bar{f})$ также является $\mathcal{F}$ -рекурсивным.

Теперь заметим, что если подходящий класс $\mathcal{F}$ допускает кодирование кортежей $\mathcal{E}$, то можно без потери общности предполагать, что $\mathcal{E} = \langle \rangle$ совпадает со стандартным кодированием

$$\langle k_0, \dots, k_{n-1} \rangle = p_0^{k_0+1} \cdot \dots \cdot p_{n-1}^{k_{n-1}+1}$$

на ω . Действительно, если мы определим $\mathcal{E}' = \langle \rangle$ посредством $\langle x_0, \dots, x_{n-1} \rangle$

$$= \begin{cases} r(\langle x_0, \dots, x_{n-1} \rangle), & \text{если хотя бы один из } x_0, \dots, x_{n-1} \\ & \text{не принадлежит } \omega \text{ и } \langle x_0, \dots, x_{n-1} \rangle \in \omega, \\ \langle x_0, \dots, x_{n-1} \rangle, & \text{если хотя бы один из } x_0, \dots, x_{n-1} \\ & \text{не принадлежит } \omega \text{ и } \langle x_0, \dots, x_{n-1} \rangle \notin \omega, \\ p_0^{x_0+1} \cdot \dots \cdot p_{n-1}^{x_{n-1}+1}, & \text{если все } x_i \text{ лежат в } \omega, \end{cases}$$

где $r: \omega \rightarrow \omega$ — рекурсивная одно-однозначная функция, область значений которой рекурсивна и не пересекается с множеством $\{p_0^{k_0+1} \cdot \dots \cdot p_{n-1}^{k_{n-1}+1} : n, k_0, \dots, k_{n-1} \in \omega\}$, то $\mathcal{F}$ допускает также и $\mathcal{E}'$. Единственным нетривиальным из того, что нужно проверить, является то, что предикат

$$P(x) \Leftrightarrow \chi_{\text{Seq}}^{\mathcal{E}}(x) = 0 \wedge \forall i < \text{lh}^{\mathcal{E}}(x) ((x)_i^{\mathcal{E}} \in \omega)$$

является рекурсивным. Для этого заметим, что

$$\neg P(x) \Leftrightarrow \chi_{\text{Seq}}^{\mathcal{E}}(x) = 1 \vee \mu i [\chi_{\omega}((x)_i^{\mathcal{E}}) = 1] < \text{lh}^{\mathcal{E}}(x).$$

В дальнейшем будем считать, что любое кодирование согла-

суется со стандартным на ω , так что обозначения вроде $\langle e_0, \dots, e_{n-1} \rangle$, $(e)_i$ и т. д. понимаются однозначно, если $e_i, e \in \omega$. Условимся также, что

$$\langle \emptyset \rangle = \text{код пустой последовательности} = 1.$$

Заметим, что если $\mathcal{F}$ допускает кодирование $\mathcal{E}$, то для каждого фиксированного $n \geq 1$ класс $\mathcal{F}$ -рекурсивных функционалов замкнут относительно отображения $p_n(x_0, \dots, x_{n-1}) = \langle x_0, \dots, x_{n-1} \rangle$. Класс $\mathcal{F}$ -рекурсивных функционалов замкнут также относительно подстановок отображений

$$t(x, i, j) = \begin{cases} \langle (x)_i, \dots, (x)_j \rangle, & \text{если } 0 \leq i \leq j \in \omega, \\ 0 & \text{в противном случае.} \end{cases}$$

Для этого сначала примитивной рекурсией по j доказывают, что если $\Phi(x, \bar{y}, \bar{f})$ является $\mathcal{F}$ -рекурсивным, то таков же и

$$\Psi(x, i, j, z, \bar{y}, \bar{f}) = \Phi(t(x, i, j) * z, \bar{y}, \bar{f}),$$

и затем полагают $z = 1 = \langle \emptyset \rangle$.

Мы завершаем предварительные сведения для доказательства теоремы о перечислении следующим определением.

8.3. Пусть $\mathcal{F}$ является подходящим классом функционалов. Говорим, что $\mathcal{F}$ конечно порожден, если существует конечная последовательность функционалов $\bar{\Phi}$ и конечная последовательность всюду определенных отображений $\bar{t} = (t_1, \dots, t_k)$, где $t_i: A^{k_i} \rightarrow A$ такие, что $\mathcal{F}$ является наименьшим подходящим классом функционалов, содержащим $\bar{\Phi}$ и замкнутым относительно подстановок отображений из $\bar{t}$.

8.4. Теорема о перечислении. Пусть $\mathcal{F}$ — подходящий класс функционалов на A . Если $\mathcal{F}$ конечно порожден и допускает кодирование кортежей, то класс $\mathcal{F}$ -рекурсивных частичных функций обладает свойством перечисления.

Доказательство. Понятно, что достаточно найти $\mathcal{F}$ -рекурсивную универсальную частичную функцию $\Phi(e, x)$ для одноместных $\mathcal{F}$ -рекурсивных функций. Наш план таков: припишем некоторым каноническим образом код (гёделев номер) $\ulcorner \Phi \urcorner \in \omega$ каждому функционалу Φ из $\mathcal{F}$; затем построим $\mathcal{F}$ -рекурсивный функционал $U(e, x, f)$ с одноместной f такой, что если $\ulcorner \Phi(x_1, \dots, x_n, f_1, \dots, f_m) \urcorner = e$, то

$$\Phi(x_1, \dots, x_n, f_1, \dots, f_m) = U(e, \langle x_1, \dots, x_n \rangle, \langle f_1, \dots, f_m \rangle),$$

где $\langle f_1, \dots, f_m \rangle = \lambda x \langle \bar{f}_1(x), \dots, \bar{f}_m(x) \rangle$ и $\bar{f}_i(x) = f_i(\langle x \rangle_0, \dots, \langle x \rangle_{k_i-1})$, если $f_i: A^{k_i} \rightarrow \omega$. Мы организуем все таким образом, что $p(\ulcorner \Phi(x_1, \dots, x_n, \bar{f}) \urcorner) = n$ для некоторой рекурсивной $p: \omega \rightarrow \omega$.

Затем, полагая (для $g: A^2 \rightarrow \omega$)

$$V(e, x, g) = U(e, x, \lambda x \langle g(e, \langle (x)_0, \dots, (x)_{p(e)-1} \rangle) \rangle),$$

получаем для каждого оперативного $\Phi(x_1, \dots, x_n, f)$ такого, что $\ulcorner \Phi \urcorner = e$ и $p(e) = n$,

$$\begin{aligned} \Phi(x_1, \dots, x_n, \lambda x'_1 \dots x'_n g(e, \langle x'_1, \dots, x'_n \rangle)) &= \\ &= U(e, \langle x_1, \dots, x_n \rangle, \langle \lambda x'_1 \dots x'_n g(e, \langle x'_1, \dots, x'_n \rangle) \rangle) \\ &= U(e, \langle x_1, \dots, x_n \rangle, \lambda x \langle g(e, \langle (x)_0, \dots, (x)_{n-1} \rangle) \rangle) \\ &= V(e, \langle x_1, \dots, x_n \rangle, g), \end{aligned}$$

так что индукцией по ξ можно доказать, что

$$V^\xi(e, \langle x_1, \dots, x_n \rangle) = \Phi^\xi(x_1, \dots, x_n),$$

следовательно,

$$V^\infty(e, \langle x_1, \dots, x_n \rangle) = \Phi^\infty(x_1, \dots, x_n).$$

Тогда

$$\varphi(e, x) = V^\infty((e)_0, \langle (e)_1, \dots, (e)_{\text{lh}(e)-1} \rangle, x)$$

является требуемой универсальной функцией.

Способ определения $\ulcorner \Phi \urcorner$ индукцией по построению $\mathcal{F}$ более или менее очевиден. Затем мы определяем $\tilde{U}(e, x, g, f)$, рассматривая различные случаи $e = \ulcorner \Phi \urcorner$, так, чтобы $\tilde{U}^\infty(e, x, f) = V(e, x, f)$ обладал требуемыми свойствами. Здесь полезно заметить, что поскольку $\mathcal{F}$ конечно порожден, существует конечное число функционалов $\Phi_1, \dots, \Phi_n$ из $\mathcal{F}$ и всюду определенных функций $t_1, \dots, t_k$ таких, что $\mathcal{F}$ является наименьшим классом функционалов, содержащим $\Phi_1, \dots, \Phi_n$, который замкнут относительно подстановок $t_1, \dots, t_k$ и удовлетворяет (i) — (ix) из 2.3 и (x) только для $\Phi_1, \dots, \Phi_n$. Действительные детали построения ясны, но несколько неприятны, и мы их опускаем. $\square$

§ 9. Следствия перечислимости

Имеется несколько следствий теоремы о перечислимости, которые мы рассмотрим в первую очередь. В конце этого параграфа мы обратимся также к некоторым следствиям теоремы о перечислимости, касающимся структуры полурекурсивных предикатов.

9.1. Пусть $\mathcal{F}$ — класс частичных функций на A . Универсальная система для $\mathcal{F}$ состоит из последовательности $\{\varphi^n\}_{n \geq 1}$ частичных функций из $\mathcal{F}$ такой, что для каждого n φ^n является $n+1$ -местной и универсальной для n -местных ча-

стичных функций из $\mathcal{F}$. Мы называем $\{\varphi^n\}$ хорошей, если для каждого $n, m \geq 1$ существует всюду определенная рекурсивная функция $S_n^m(e, k_1, \dots, k_m)$ на ω такая, что для любых $k_1, \dots, k_m \in \omega, x_1, \dots, x_n \in A$

$$\begin{aligned} \varphi^{m+n}(e, k_1, \dots, k_m, x_1, \dots, x_n) \\ = \varphi^n(S_n^m(e, k_1, \dots, k_m), x_1, \dots, x_n). \end{aligned}$$

Такие функции называем s - m - n -функциями для $\{\varphi^n\}$. Теперь имеет место

9.2. s - m - n -теорема. Пусть $\mathcal{F}$ — подходящий класс функционалов на A , который конечно порожден и допускает кодирование кортежей. Тогда класс $\mathcal{F}$ -рекурсивных частичных функций допускает хорошую универсальную систему.

Доказательство. По 8.4 пусть $\varphi(e, x, y)$ будет $\mathcal{F}$ -рекурсивной частичной функцией, которая универсальна для двухместных $\mathcal{F}$ -рекурсивных частичных функций. Тогда полагаем

$$\varphi^k(e, x_1, \dots, x_k) = \varphi((e)_0, (e)_1, \langle x_1, \dots, x_k \rangle),$$

если $\mathcal{F}$ допускает кодирование кортежей $\langle \rangle$. Пусть

$$f(x, y) = \varphi^{m+n}((x)_0, \dots, (x)_m, (y)_0, \dots, (y)_{n-1})$$

и найдем e_0 такое, что

$$f(x, y) = \varphi(e_0, x, y).$$

Тогда

$$S_n^m(e, k_1, \dots, k_m) = \langle e_0, \langle e, k_1, \dots, k_m \rangle \rangle$$

является требуемой s - m - n -функцией. $\square$

Основным следствием s - m - n -теоремы является 9.3. (Вторая) теорема о рекурсии. Пусть $\mathcal{F}$ — подходящий, конечно порожденный класс функционалов на A , допускающий кодирование кортежей. Если $\{\varphi^n\}$ является хорошей универсальной системой для класса $\mathcal{F}$ -рекурсивных частичных функций, то для каждой $\mathcal{F}$ -рекурсивной частичной функции $\psi(a, \bar{x})$ найдется некоторое $e \in \omega$ такое, что

$$\varphi_e(\bar{x}) = \psi(e, \bar{x}).$$

Доказательство. Пусть e_0 будет таким, что $\varphi_{e_0}(a, \bar{x}) = \psi(S_n^1(a, a), \bar{x})$, и положим $e = S_n^1(e_0, e_0)$. $\square$

Теперь мы можем закончить изучение общих структурных свойств $\mathcal{F}$ -полурекурсивных предикатов, которое мы начали в § 7. Говорим, что класс предикатов $\mathfrak{R}$ на A замкнут относительно $\exists^\omega$, если для каждого $P(\bar{x}, a)$ из $\mathfrak{R}$ предикат

$$\exists^\omega P(\bar{x}) \iff \exists n P(\bar{x}, n) \iff \exists n (n \in \omega \wedge P(\bar{x}, n))$$

также принадлежит $\mathfrak{R}$.

9.4. Теорема. Пусть $\mathcal{F}$ — подходящий, конечно порожденный класс функционалов на A , который нормален и допускает кодирование кортежей. Тогда:

(i) Класс $\mathcal{F}$ -полурекурсивных предикатов замкнут относительно $\exists^0$.

(ii) Частичная функция $\varphi: A^n \rightarrow \omega$ $\mathcal{F}$ -рекурсивна тогда и только тогда, когда ее график является $\mathcal{F}$ -полурекурсивным. $\square$

Оба эти результата являются непосредственными следствиями следующей основной леммы.

9.5. Лемма о числовом селекторе. Если $\mathcal{F}$ — подходящий, конечно порожденный класс функционалов на A , который нормален и допускает кодирование кортежей, то для каждого $\mathcal{F}$ -полурекурсивного предиката $P(\bar{x}, a)$ существует некоторая $\mathcal{F}$ -рекурсивная функция ψ такая, что

$$\exists n P(\bar{x}, n) \Rightarrow \psi(\bar{x}) \downarrow \wedge P(\bar{x}, \psi(\bar{x})).$$

Доказательство. Пусть $\varphi(e, \bar{x}, a)$ будет универсальной $\mathcal{F}$ -рекурсивной частичной функцией в силу 8.4. Пусть σ будет $\mathcal{F}$ -полурекурсивной нормой на $W = \{(e, \bar{x}, a): \varphi(e, \bar{x}, a) \downarrow\}$, и пусть $\chi(e, \bar{x}, a, e', \bar{x}', a')$ будет $\mathcal{F}$ -рекурсивной функцией такой, что

$$(e, \bar{x}, a) \leq_{\sigma}^* (e', \bar{x}', a') \Leftrightarrow \chi(e, \bar{x}, a, e', \bar{x}', a') = 0,$$

$$(e', \bar{x}', a') <_{\sigma}^* (e, \bar{x}, a) \Leftrightarrow \chi(e, \bar{x}, a, e', \bar{x}', a') = 1$$

согласно 6.3. Тогда, используя теорему 9.3 о рекурсии, мы можем найти $e \in \omega$ такое, что если

$$P(\bar{x}, a) \Leftrightarrow \varphi(e_0, \bar{x}, a) \downarrow,$$

то

$$\varphi_e(\bar{x}, a)$$

$$= \begin{cases} 0, & \text{если } a \in \omega \text{ \& } \chi(e_0, \bar{x}, a, e, \bar{x}, a+1) = 0, \\ \varphi(e, \bar{x}, a+1) + 1, & \text{если } a \in \omega \text{ \& } \chi(e_0, \bar{x}, a, e, \bar{x}, a+1) = 1, \\ 0, & \text{если } a \notin \omega. \end{cases}$$

Наконец, положим

$$\psi(\bar{x}) = \varphi_e(\bar{x}, 0).$$

Для доказательства того, что ψ годится, заметим сначала, что если $\varphi(e_0, \bar{x}, a) \downarrow$, то $\varphi_e(\bar{x}, a) \downarrow$ или $\varphi_e(\bar{x}, a+1) \downarrow$. Более того, если $\varphi_e(\bar{x}, b) \downarrow$, то $\varphi_e(\bar{x}, c) \downarrow$ для всех $c \leq b$. Тогда ясно, что если $\exists a \varphi(e_0, \bar{x}, a) \downarrow$, то $\varphi_e(\bar{x}, 0) \downarrow$. Пусть a будет наименьшим таким, что $\varphi_e(\bar{x}, a)$ определено согласно первому случаю в определении; такое a существует, поскольку в противном случае $\varphi_e(\bar{x}, 0) = \varphi_e(\bar{x}, 1) + 1 = \varphi_e(\bar{x}, 2) + 2 = \dots$ Поскольку $\varphi_e(\bar{x}, b-1) =$

$= \varphi_e(\bar{x}, b)$ для любого $1 \leq b \leq a$, мы имеем $\varphi_e(\bar{x}, 0) = \varphi_e(\bar{x}, a) + 1 = a + 1$ и $\varphi(e_0, \bar{x}, a) \downarrow$, чем заканчивается доказательство. $\square$

В качестве простого применения мы получаем, что функция на ω полурекурсивна относительно E тогда и только тогда, когда ее график является Π_1^1 -множеством (см. 5.3). Аналогично для $E^\#$.

Фундаментальная идея доказательства теорем о селекторе для получения структурных результатов принадлежит Ганди [1].

РЕКУРСИЯ В ВЫСШИХ ТИПАХ

§ 10. Объекты высших типов над ω

10.1. Для каждого натурального j определим множество $T^{(j)}$ объектов типа j (над ω) индукцией:

$$T^{(0)} = \omega,$$

$T^{(j+1)}$ = множеству всех всюду определенных функций из $T^{(j)}$ в ω .

Мы часто будем использовать переменные $\alpha^j, \beta^j, \gamma^j$ с верхними индексами для элементов $T^{(j)}$ с указанием их типов, когда это не ясно из контекста. Элементы множества

$$T = \bigcup_j T^{(j)}$$

называются объектами высших типов над ω .

Точкой называется конечная последовательность $x = (x_1, \dots, x_n)$ объектов высших типов; **типом** $\text{type}(x_1, \dots, x_n)$ точки $(x_1, \dots, x_n)$ является максимум из типов входящих в нее x_i . **Сцеплением** двух точек $x = (x_1, \dots, x_n)$ и $y = (y_1, \dots, y_m)$ является точка

$$x \frown y = x, y = (x_1, \dots, x_n, y_1, \dots, y_m).$$

Мы будем изучать рекурсию в высших типах, применяя уже развитую теорию к множеству

$$A = T^* = \text{множеству всех точек}$$

относительно соответствующих классов функционалов на T^* . Как обычно, мы будем отождествлять одноэлементную последовательность (α^j) с самим α^j , так что имеем $T \subseteq T^*$; в частности, $\omega \subseteq T^*$.

Более того, каждое произведение вида $\mathcal{X} = T^{(j_1)} \times \dots \times T^{(j_n)}$ также содержится в T^* , так что можно представлять частичные функции

$$f: \mathcal{X} \rightarrow \omega$$

как частичные функции на T^* , область определения которых содержится в $\mathcal{X}$. В конечном счете мы интересуемся изучением рекурсивных частичных функций на таких пространствах. По определению, если $\mathcal{X} = X_1 \times \dots \times X_n$ и $\mathcal{Y} = Y \times \dots \times Y_m$, то

$$\mathcal{X} \times \mathcal{Y} = X_1 \times \dots \times X_n \times Y_1 \times \dots \times Y_m,$$

так что набор таких пространств, содержащийся в T^* , замкнут относительно декартовых произведений.

10.2. Нам потребуются некоторые простые отображения, вкладывающие $T^{(j)}$ в $T^{(k)}$ при $j \leq k$ (функции повышения типа) и обратные к ним (функции понижения типа). Сначала положим

$$u^1(n) = \lambda m(n), \quad d_0(\alpha^1) = \alpha^1(0);$$

ясно, что

$$u^1: T^{(0)} \rightarrow T^{(1)}, \quad d_0: T^{(1)} \rightarrow T^{(0)},$$

u^1 является одно-однозначной функцией и для всех n

$$d_0(u^1(n)) = n.$$

Теперь по индукции полагаем

$$u^{j+2}(\alpha^{j+1}) = \lambda \beta^{j+1} \alpha^{j+1}(d_j(\beta^{j+1})),$$

$$d_{j+1}(\sigma^{j+2}) = \lambda \beta^j \alpha^{j+2}(u^{j+1}(\beta^j)),$$

и легко проверяется, что u^{j+2} является инъективным вложением $T^{(j+1)}$ в $T^{(j+2)}$ и для всех $\alpha^{j+1} \in T^{(j+1)}$

$$d_{j+1}(u^{j+2}(\alpha^{j+1})) = \alpha^{j+1}.$$

Отображения

$$u^{j,k}: T^{(j)} \rightarrow T^{(k)} \quad (j < k),$$

$$d_{j,k}: T^{(k)} \rightarrow T^{(j)} \quad (j < k)$$

определяются при помощи итерирования этой процедуры, т. е.

$$u^{j,j+1} = u^{j+1}, \quad d_{j,j+1} = d_j,$$

$$u^{j,j+2} = u^{j+2} \circ u^{j+1}, \quad d_{j,j+2} = d_j \circ d_{j+1},$$

и т. д. Удобно также положить

$$u^{j,j} = d_{j,j} = \text{функции, тождественной на } T^{(j)}.$$

Теперь все $u^{j,k}$ одно-однозначны и $d_{j,k}(u^{j,k}(\alpha^j)) = \alpha^j$ ($j \leq k$, $\alpha^j \in T^{(j)}$).

§ 11. Клиниевские классы функционалов на T^*

Теперь мы переходим к главным понятиям, лежащим в основе теории рекурсии в высших типах.

11.1. Определение. Класс $\mathcal{X}$ функционалов на $A = T^*$ называется клиниевским классом, если он является подходя-

щим, содержит функции (i) — (iii) и замкнут относительно правил (iv), (v). Мы используем переменные $x, y, z, \dots$ для элементов из T^* и σ, τ для конечных последовательностей элементов из T^* (включая пустую последовательность).

(i) Функция распознавания типа:

$$\chi(j, x) = \begin{cases} 0, & \text{если } j \in \omega, x \in T^{(j)}, \\ 1 & \text{в противном случае.} \end{cases}$$

(ii) Функция длины:

$$\text{length}(x) = n, \quad \text{если } x = (x_1, \dots, x_n).$$

(iii) Вычисление значения объекта типа 1:

$$\varphi(x, n) = \begin{cases} x(n), & \text{если } x \in T^{(1)}, n \in \omega, \\ 0 & \text{в противном случае.} \end{cases}$$

(iv) Вычисление значения объекта типа > 1 : Если $\Phi(x, y, \sigma, \bar{f})$ лежит в $\mathcal{X}$, то для каждого j

$$\Psi_j(y, \sigma, \bar{f}) = \Psi(y, \sigma, \bar{f}) = \begin{cases} y(\lambda \alpha^j \Phi(\alpha^j, y, \sigma, \bar{f})), & \text{если } y \in T^{(j+2)}, \\ 0, & \text{если } y \notin T^{(j+2)}, \end{cases}$$

также принадлежит $\mathcal{X}$. Понятно, что поскольку $y \in T^{(j+2)}$, то $\Psi(y, \sigma, \bar{f})$ не определено, если $\lambda \alpha^j \Phi(\alpha^j, y, \sigma, \bar{f})$ не является всюду определенной.

(v) Подстановки сцеплений и точечных проектирований: Напомним, что отображением сцепления называется всюду определенное отображение (из $T^* \times T^*$ в T^*)

$$t(x, y) = x \wedge y = x, y.$$

Точечным проектированием называется всюду определенное отображение из $T^* \times T^*$ в T^* , задаваемое так:

$$p(x, i) = \begin{cases} x_i, & \text{если } x = (x_0, \dots, x_{n-1}), i \in \omega \text{ и } i < n, \\ 0 & \text{в противном случае.} \end{cases}$$

Используя (iii) и (iv), мы можем доказать индукцией по $j \geq 1$, что

$$\varphi(x, y) = \begin{cases} x(y), & \text{если } x \in T^{(j)}, y \in T^{(j-1)}, \\ 0 & \text{в противном случае} \end{cases}$$

также принадлежит $\mathcal{X}$.

Предположим теперь, что $\mathcal{X}$ — клиниевский класс и

$$\varphi: \mathcal{X} \rightarrow \omega$$

— частичная функция на некотором пространстве $\mathcal{X} = X_1 \times \dots \times X_n \subseteq T^*$. Говорим, что φ является $\mathcal{X}$ -рекурсивной, если

она $\mathcal{K}$ -рекурсивна (в смысле 2.2), когда мы рассматриваем ее как частичную функцию на T^* , область определения которой оказалась содержащейся в $\mathcal{X}$; это, очевидно, эквивалентно тому, что существует $\mathcal{K}$ -рекурсивная функция $\varphi^*: T^* \rightarrow \omega$, ограничение которой на $\mathcal{X}$ есть φ . По определению это означает, что существует оперативный функционал $\Phi(\sigma, x, f)$ в $\mathcal{K}$ и натуральные числа $n_1, \dots, n_k$ такие, что

$$\varphi(x) = \Phi^\infty(n_1, \dots, n_k, x) \quad (x \in \mathcal{X}).$$

Эти частичные функции являются основным объектом нашего изучения.

Естественно назвать также частичное отображение

$$\theta: \mathcal{X} \rightarrow T^{(j+1)}$$

$\mathcal{K}$ -рекурсивным, если существует $\mathcal{K}$ -рекурсивная частичная функция

$$\varphi: T^{(j)} \times \mathcal{X} \rightarrow \omega$$

такая, что

$$\theta(x) = \lambda \alpha^j \varphi(\alpha^j, x);$$

аналогично

$$\theta: \mathcal{X} \rightarrow \mathcal{Y} = T^{(j_1)} \times \dots \times T^{(j_n)}$$

является $\mathcal{K}$ -рекурсивным, если

$$\theta(x) = (\theta_1(x), \dots, \theta_n(x)),$$

с $\mathcal{K}$ -рекурсивными $\theta_1, \dots, \theta_n$.

11.2. Пусть $\mathcal{K}_0$ будет наименьшим клиниевским классом на T^* . Более общо, для данного конечного списка функционалов $\bar{\Phi} = (\Phi_1, \dots, \Phi_n)$ на T^* пусть $\mathcal{K}_0[\bar{\Phi}]$ будет наименьшим клиниевским классом функционалов, содержащим $\Phi_1, \dots, \Phi_n$. Вместо $\mathcal{K}_0$ -рекурсивный мы говорим *рекурсивный по Клини* и вместо $\mathcal{K}_0[\bar{\Phi}]$ -рекурсивный говорим *рекурсивный по Клини относительно $\bar{\Phi}$* .

Например, все отображения $u^{j,k}, d_{j,k}$, данные в 10.2, являются рекурсивными по Клини.

§ 12. Рекурсия по Клини относительно объектов высших типов и кванторов

Для иллюстрации основных понятий рассмотрим некоторые интересные примеры рекурсии в высших типах. Здесь наше обсуждение параллельно проведенному в §§ 4 и 5.

12.1. Каждый объект высшего типа

$$F = {}^i F \in T^{(j)} \quad (j \geq 1)$$

может быть рассмотрен как функционал на T^* , где для $j \geq 2$

$$F(f) = \begin{cases} F(f \upharpoonright T^{(j-2)}), & \text{если } f \upharpoonright T^{(j-2)} \text{ всюду определено,} \\ \text{не определено в противном случае} \end{cases}$$

и для $j = 1$

$$F(x) = \begin{cases} F(x), & \text{если } x \in \omega, \\ 0, & \text{если } x \notin \omega. \end{cases}$$

Поэтому мы можем изучать рекурсию относительно фиксированного объекта высшего типа F , т. е. $\mathcal{K}_0[F]$ -рекурсию. Особую важность имеют объекты ${}^i E$ ($j \geq 2$), которые реализуют экзистенциальную квантификацию на $T^{(j-2)}$,

$${}^i E(\alpha^{j-1}) = \begin{cases} 0, & \text{если } \exists \alpha^{j-2} (\alpha^{j-1}(\alpha^{j-2}) = 0), \\ 1, & \text{если } \forall \alpha^{j-2} (\alpha^{j-1}(\alpha^{j-2}) \neq 0). \end{cases}$$

Наш первый результат здесь очень полезен — он показывает, что рекурсия по Клини относительно объекта высшего типа может быть определена в терминах (абсолютной) рекурсии по Клини при помощи подстановки.

12.2. Теорема (Клини [1]). Пусть $F = {}^i F$ — объект типа $j \geq 1$. Частичная функция $\varphi: \mathcal{X} \rightarrow \omega$ является рекурсивной по Клини относительно F тогда и только тогда, когда существует рекурсивная по Клини частичная функция $\psi: T^{(j)} \times \mathcal{X} \rightarrow \omega$ такая, что для всех $x \in \mathcal{X}$

$$\varphi(x) = \psi(F, x).$$

Доказательство. В одну сторону достаточно связать с каждым $\Phi(\sigma, y, \sigma', g)$ из $\mathcal{K}_0$ функционал $\Phi^*(\sigma, \sigma', f, g)$ из $\mathcal{K}_0[F]$ такой, что

$$\Phi(\sigma, F, \sigma', g) = \Phi^*(\sigma, \sigma', \lambda \tau' g(\tau, F, \tau'), g).$$

Действительно, если Φ — оперативный функционал, то мы можем легко доказать индукцией по ξ , что $\Phi^\xi(\sigma, F, \sigma') = \omega \Rightarrow \Phi^{\xi+1}(\sigma, \sigma', \Phi^\infty) = \omega$ и $\Phi^\xi(\sigma, \sigma', \Phi^\infty) = \omega \Rightarrow \Phi^\infty(\sigma, F, \sigma') = \omega$, так что $\Phi^\infty(\sigma, F, \sigma') = \Phi^{*\infty}(\sigma, \sigma', \Phi^\infty)$ и, следовательно, $\Phi^\infty(\sigma, F, \sigma')$ рекурсивен относительно F . Построение Φ^* непосредственно осуществляется индукцией по построению $\mathcal{K}_0$. Например, если

$$\Phi(\sigma, y, \sigma', g) = g(\sigma, y, \sigma'),$$

то полагаем

$$\Phi^*(\sigma, \sigma', f, g) = f(\sigma, \sigma'),$$

а если

$$\Phi(\sigma, y, \sigma', g) = g(\sigma, \sigma')$$

(так что y не входит в g), то полагаем

$$\Phi^*(\sigma, y, \sigma', f, g) = g(\sigma, \sigma').$$

Если же (как в 11.1 (v))

$$\Psi(\sigma, y, \sigma', g) = y(\lambda \alpha^{j-2} \Phi(\alpha^{j-2}, \sigma, y, \sigma', g)),$$

то полагаем

$$\Psi^*(\sigma, \sigma', f, g) = F(\lambda z \Phi^*(z, \sigma, \sigma', f, g)).$$

В обратную сторону покажем, что если $\Phi(\sigma, f)$ — функционал из $\mathcal{X}_0[F]$, то существует функционал $\Phi^*(y, \sigma, g)$ из $\mathcal{X}_0$ такой, что

$$\Phi(\sigma, \lambda \tau g(F, \tau)) = \Phi^*(F, \sigma, g).$$

Тогда для оперативного Φ индукцией по ξ получаем, что $\Phi^{\xi}(\sigma) = \Phi^{\xi}(F, \sigma)$, так что $\Phi^{\infty}(\sigma) = \Phi^{\infty}(F, \sigma)$, и все сделано. Построение Φ^* снова ведется индукцией по построению $\mathcal{X}_0[F]$. Единственный интересный случай — это когда $\Phi = F$; полагаем при $j \geq 2$

$$\Phi^*(y, g) = \begin{cases} y(\lambda \alpha^{j-2} g(y, \alpha^{j-2})), & \text{если } y \in T^{(j)}, \\ 0, & \text{если } y \notin T^{(j)}. \end{cases}$$

При $j = 1$

$$\Phi^*(y, x) = \begin{cases} y(x), & \text{если } y \in T^{(1)}, x \in \omega, \\ 0 & \text{в противном случае. } \square \end{cases}$$

12.3. Свяжем с данным квантором Q на некотором $T^{(j)}$ объект типа $j+2$:

$${}^{j+2}F_Q(\alpha^{j+1}) = \begin{cases} 0, & \text{если } Q\alpha^j(\alpha^{j+1}(\alpha^j) = 0), \\ 1, & \text{если } Q\alpha^j(\alpha^{j+1}(\alpha^j) \neq 0), \end{cases}$$

и функционал на T^*

$${}^{j+2}F_Q^{\#}(f) = \begin{cases} 0, & \text{если } Q\alpha^j(f(\alpha^j) = 0), \\ 1, & \text{если } Q\alpha^j(f(\alpha^j) \neq 0), \\ \text{не определено в противном случае.} \end{cases}$$

В частности, если $Q = \exists^j$ — квантор существования на объектах типа j , то получаем ${}^{j+2}E$ и ${}^{j+2}E^{\#}$ соответственно. Ясно, что, как и в 5.4, ${}^{j+2}F_Q$ рекурсивен по Клини относительно ${}^{j+2}F_Q^{\#}$, ${}^{j+2}E^{\#}$.

12.4. Нас в основном интересует изучение рекурсии по Клини относительно функционалов, которые сосредоточены (в смысле п. 4.1) на

$$T_m^* = \text{множеству всех точек типа } \leq m$$

для некоторого m . Все примеры, которые мы привели, включаются сюда.

Предположим, что $\bar{\Phi} = (\Phi_1, \dots, \Phi_n)$ — конечный список таких функционалов. Тогда легко показать, что все функционалы из $\mathcal{X}_0[\bar{\Phi}]$ сосредоточены на T_m^* и, более того,

$$\mathcal{X}_0[\bar{\Phi}] \upharpoonright T_m^* = \mathcal{X}_0(T_m^*)[\bar{\Phi} \upharpoonright T_m^*],$$

где $\mathcal{X}_0(T_m^*)[\bar{\Psi}]$ — наименьший подходящий класс функционалов на T_m^* , содержащий все функционалы из $\bar{\Psi}$, который удовлетворяет также условиям (i) — (vi) из 11.1 (ограниченным соответствующим образом до T_m^*).

Как в 4.2, можно легко проверить, что если $\text{type}(\mathcal{R}) = 0$, то частичная функция $f: \mathcal{R} \rightarrow \omega$ рекурсивна по Клини (или рекурсивна по Клини относительно некоторого фиксированного $\alpha \in T^{(1)}$) в точности тогда, когда она рекурсивна (или рекурсивна относительно α) в смысле обычной теории рекурсии. Снова, как в 5.3, легко проверить, что если $\text{type}(\mathcal{R}) \leq 1$ и $R \subseteq \mathcal{R}$, то R является полурекурсивным по Клини относительно ${}^2E$ (или ${}^2E^{\#}$) в точности тогда, когда R есть Π_1^1 -множество.

§ 13. Нормальность и перечислимость в рекурсии в высших типах

При изучении рекурсии относительно функционалов $\bar{\Phi}$, сосредоточенных на некотором T_m^* , мы не ожидаем нормальности на всем T^* в смысле § 6. Поэтому мы вводим простую модификацию этого понятия, соответствующую этой ситуации.

13.1. Пусть $\mathcal{F}$ — класс функционалов на множестве A , пусть $\omega \subseteq B \subseteq A$ и пусть Φ — функционал. Говорим, что Φ *нормален относительно $\mathcal{F}$ на B* , если существует $\mathcal{F}$ -рекурсивный функционал Δ_{Φ} такой, что $\Phi \upharpoonright B, \Delta_{\Phi} \upharpoonright B$ удовлетворяют условиям (i) и (ii) из 6.2 (где A заменено на B). Говорим, что $\mathcal{F}$ *нормален на B* , если каждый $\Phi \in \mathcal{F}$ нормален относительно $\mathcal{F}$ на B . Аналогично предложению 6.4 имеем

13.2. Предложение. Пусть $\bar{\Phi} = (\Phi_1, \dots, \Phi_n)$ — конечный список функционалов на T^* , сосредоточенных на T_m^* . Если каждый Φ_i нормален относительно $\mathcal{X}_0[\bar{\Phi}, {}^2E, \dots, {}^mE]$ на T_m^* , то $\mathcal{X}_0[\bar{\Phi}, {}^2E, \dots, {}^mE]$ нормален на T_m^* . (Если $m \leq 1$, то имеем просто $\mathcal{X}_0[\bar{\Phi}]$.)

Доказательство. Оно подобно доказательству 6.4. Нужно рассмотреть добавочные случаи, проистекающие из 11.1, из которых единственным интересным является 11.1 (iv). Поэтому рассмотрим $\Phi(x, y, \sigma, f)$ и предположим, что мы нашли Δ_{Φ} , удовлетворяющий 6.2, конечно, работающий на T_m^* . Далее, пусть j таково, что $j+2 \leq m$, и положим

$$\Psi(y, \sigma, \bar{f}) = \begin{cases} y(\lambda \alpha^j \Phi(\alpha^j, y, \sigma, \bar{f})), & \text{если } y \in T^{(j+2)}, \\ 0 & \text{в противном случае.} \end{cases}$$

Поскольку $\Psi(y, \sigma, \bar{f}) \downarrow \Leftrightarrow \forall \alpha^l (\Phi(\alpha^l, y, \sigma, \bar{f}) \downarrow)$ или $y \notin T^{(l+2)}$, полагаем

$$\Delta_{\Psi}(y, \sigma, \bar{f}, \bar{\delta}) = \begin{cases} 1 \div {}^{l+2}E(\lambda \alpha^l (1 \div \Delta_{\Phi}(\alpha^l, y, \sigma, \bar{f}, \bar{\delta}))), & \text{если } y \in T^{(l+2)}, \\ 0, & \text{если } y \notin T^{(l+2)}. \quad \square \end{cases}$$

Назовем конечную последовательность функционалов $\bar{\Phi}$ нормальной на T_m^* , если каждый функционал из $\bar{\Phi}$ нормален относительно $\mathcal{K}_0[\bar{\Phi}]$ на T_m^* . Замечая, что каждый объект $F = {}^{l+2}F$ сосредоточен на T_j^l и аналогично для кванторов на $T^{(l)}$, имеем следующий аналог теоремы 6.5:

13.3. Теорема. (i) Пусть $F = {}^{l+2}F$ — объект типа ≥ 2 ; тогда $F, {}^2E, \dots, {}^{l+2}E$ нормальна на T_{j+2}^* .

(ii) Пусть Q — квантор на $T^{(l)}$, тогда $F_Q^{\#}, {}^2E, \dots, {}^{l+2}E$ нормальна на T_{j+2}^* .

Мы рассмотрим, как влияет нормальность на структуру полурекурсивных предикатов, особенно в случае рекурсии относительно объектов высших типов, в § 17.

Теперь мы переходим к доказательству свойства перечисления в нашей теперешней ситуации. Основным является следующее

13.4. Предложение. Пусть $\mathcal{K}$ — клиниевский класс функционалов на T^* . Тогда $\mathcal{K}$ допускает кодирование кортежей на T^* .

Доказательство. Положим

$$\langle x_1, \dots, x_n \rangle = 2^n \cdot 3^{\text{length}(x_1)+1} \cdot \dots \cdot p_n^{\text{length}(x_n)+1}, \quad x_1, x_2, \dots, x_n,$$

где, как обычно,

$$y, x_1, \dots, x_n = \text{сцеплению } y, x_1, \dots, x_n = y \hat{\ } x_1 \hat{\ } \dots \hat{\ } x_n.$$

Рутинная проверка показывает, что $\mathcal{K}$ допускает это кодирование. $\square$

Из этого предложения и 8.4 следует, что для каждого конечного списка функционалов $\bar{\Phi}$ на T^* класс частичных функций на T^* , рекурсивных по Клини относительно $\bar{\Phi}$, обладает свойством перечисления. В свою очередь отсюда и из результатов § 9 мы немедленно получаем следующие теоремы.

13.5. Теорема о перечислении и s-m-n-теорема. Для любого конечного списка $\bar{\Phi} = (\Phi_1, \dots, \Phi_n)$ функционалов на T^* и каждого пространства $\mathcal{X}$ можно определить частичную функцию

$$\varphi^{\mathcal{X}}: \omega \times \mathcal{X} \rightarrow \omega,$$

которая рекурсивна по Клини относительно $\bar{\Phi}$, причем выполнены следующие условия:

(i) Частичная функция $\psi: \mathcal{X} \rightarrow \omega$ рекурсивна по Клини относительно $\bar{\Phi}$ в точности тогда, когда для некоторого $e \in \omega$ и всех $x \in \mathcal{X}$

$$\psi(x) = \varphi_e^{\mathcal{X}}(x) = \varphi^{\mathcal{X}}(e, x)$$

(т. е. каждая $\varphi^{\mathcal{X}}$ универсальна для рекурсии по Клини относительно $\bar{\Phi}$ на $\mathcal{X}$).

(ii) Для каждого пространства $\mathcal{X}$ типа 0 и каждого $\mathcal{Y}$ существует всюду определенная рекурсивная функция

$$S_{\mathcal{Y}}^{\mathcal{X}}: \omega \times \mathcal{X} \rightarrow \omega$$

такая, что

$$\begin{aligned} \varphi^{\mathcal{X} \times \mathcal{Y}}(e, x_1, \dots, x_m, y_1, \dots, y_n) \\ = \varphi^{\mathcal{Y}}(S_{\mathcal{Y}}^{\mathcal{X}}(e, x_1, \dots, x_m), y_1, \dots, y_n). \end{aligned}$$

Будем называть систему универсальных частичных функций $\{\varphi^{\mathcal{X}}\}$ с этими свойствами хорошей.

13.6. (Вторая) теорема о рекурсии. Если $\{\varphi^{\mathcal{X}}\}$ — хорошая универсальная система, то для любой рекурсивной по Клини относительно $\bar{\Phi}$ частичной функции $\psi: \omega \times \mathcal{X} \rightarrow \omega$ существует $e \in \omega$ такое, что

$$\varphi_e^{\mathcal{X}}(x) = \varphi_e(x) = \psi(e, x).$$

§ 14. Определение, данное Клини

В этом параграфе мы приведем первоначальное определение рекурсии в высших типах, данное Клини [1]. В следующем параграфе мы установим эквивалентность этого первоначального определения с нашим.

14.1. В нашей терминологии Клини определяет конкретный оперативный функционал $\Theta(e, x, f)$, где e пробегает ω , x пробегает T^* и f пробегает частичные функции на $\omega \times T^*$. Затем он называет частичную функцию $\varphi: \mathcal{X} \rightarrow \omega$ рекурсивной, если для некоторого фиксированного $e \in \omega$ (индекса для φ) и всех $x \in \mathcal{X}$

$$\varphi(x) = \Theta^{\infty}(e, x).$$

Таким образом, он в действительности дает одну сводную рекурсию (master recursion) и считает рекурсивными все частичные функции (на пространствах), сводимые к ней, вместо уточнения тех форм индукции, которые разрешены.

Неподвижная точка Θ обозначается так:

$$\{e\}(x) = \Theta^{\infty}(e, x).$$

Далее, легче описывать $\Theta(e, x, f)$, если писать $\{e\}(x)$ вместо

$\Theta(e, x, f)$ в левой части последующих уравнений и снова $\{e\}(x)$ вместо $f(e, x)$ в правой части тех же уравнений. Поскольку Клини отождествляет всякие две точки, которые содержат одни и те же объекты в одном и том же порядке для каждого фиксированного типа (как $(n, \alpha, m, \alpha^2, \beta)$ и $(n, \alpha, \beta, \alpha^2, m)$), в последующих (i)–(ix) будем предполагать, что все точки находятся в упрощенной форме, т. е. объекты типа 0 предшествуют объектам типа 1 и т. д. Таким образом, выражение вроде (α', x) , где x — упрощенная точка, является сокращенной записью упрощенной точки, у которой первый объект типа j есть α^j и которая в остальном совпадает с x . Теперь полагаем $\{e\}(x) = \{e\}(x^*)$, где x^* — единственная точка в упрощенной форме, эквивалентная x (например, $(n, \alpha, m, \alpha^2, \beta)^* = (n, m, \alpha, \beta, \alpha^2)$). Определение дается в зависимости от формы e как кода последовательности и местности $\text{arity}(x)$, где

$$\text{arity}(x) = \langle n_0, n_1, \dots, n_r \rangle;$$

здесь $r = \text{type}(x)$ и для $0 \leq i \leq r$ n_i — числу объектов типа i , входящих в x :

- (i) $\{e\}(n, x) = n + 1$, если $e = \langle 1, \text{arity}(n, x) \rangle$;
- (ii) $\{e\}(x) = q$, если $e = \langle 2, \text{arity}(x), q \rangle$;
- (iii) $\{e\}(n, x) = n$, если $e = \langle 3, \text{arity}(n, x) \rangle$;
- (iv) $\{e\}(x) = \{e_2\}(\{e_1\}(x), x)$, если $e = \langle 4, \text{arity}(x), e_1, e_2 \rangle$;
- (v) $\{e\}(k, t, l, m, n, x) = \begin{cases} k^t, & \text{если } m = n, \\ l \cdot t, & \text{если } m \neq n, \end{cases}$ если $e = \langle 5, \text{arity}(k, t, l, m, n, x) \rangle$;

- (vi) $\{e\}(x) = \{e_1\}(x_1)$, если $e = \langle 6, \text{arity}(x), j, k, e_1 \rangle$,

где x_1 содержит по меньшей мере $k + 1$ объект типа j и x получается из x_1 передвижением $(k + 1)$ -го объекта типа j из x_1 к началу списка;

- (vii) $\{e\}(n, \alpha, x) = \alpha(n)$, если $e = \langle 7, \text{arity}(n, \alpha, x) \rangle$;
- (viii) $\{e\}(\alpha^j, x) = \alpha^j(\lambda \alpha^{j-2} \{e_1\}(\alpha^j, \alpha^{j-2}, x))$, если $e = \langle 8, \text{arity}(\alpha^j, x), j, e_1 \rangle$ и $j \geq 2$;
- (ix) $\{e\}(n, x, y) = \{n\}(x)$, если $e = \langle 9, \text{arity}(n, x, y), \text{arity}(x) \rangle$.

Как обычно, со всеми e, x такими, что $\{e\}(x) = \Theta^\infty(e, x)$ определено, мы связываем ординал

$|e, x|$ — наименьшему ξ такому, что $\Theta^\xi(e, x)$ определено.

14.2. Читатель, знакомый с работой Клини [1], конечно, заметил, что определение, данное там, не совпадает в точности с данным в 14.1. Схема Клини S5 для введения примитивной рекурсии была заменена первичной функцией (v). Соответственно нумерация Клини отличается от данной в 14.1. Тем не

менее хорошо известно (и по существу упомянуто Клини [1]), что оба способа представления определения фактически совпадают в следующем сильном смысле; если $\{e\}'(x)$ относится к варианту Клини [1], то существуют общерекурсивные функции $p, q: \omega \rightarrow \omega$ такие, что $\{e\}(x) = \{p(e)\}'(x)$ и $\{e\}'(x) = \{q(e)\}(x)$. Доказательство совершенно просто для всякого, знакомого с работой Клини [1], и мы его опускаем. Мы дали здесь упрощенный вариант определения Клини, потому что его легче использовать как технический инструмент, что мы собираемся делать в следующем параграфе.

14.3. Клини разъяснял свое индуктивное определение как ведущее к процедуре вычисления для $\{e\}(x)$, которую мы можем пояснить на примере, следуя Клини [1] (рис. 2).

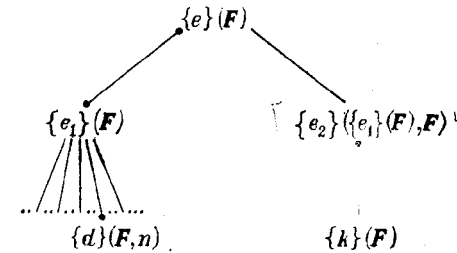


Рис. 2.

Пусть $e = \langle 4, \langle 0, 0, 1 \rangle, e_1, e_2 \rangle$ и предположим, что $F = {}^2F$ — фиксированный объект типа 2. Для вычисления $\{e\}(F)$ мы должны вычислить $\{e_1\}(F)$ и затем, если это определено, $\{e_2\}(\{e_1\}(F), F)$. Пусть $e_1 = \langle 8, \langle 0, 0, 1 \rangle, 2, d \rangle$. Тогда для вычисления $\{e_1\}(F)$ мы должны вычислить $\{d\}(F, n)$ для всех $n \in \omega$. Возьмем, например, $d = \langle 2, \langle 1, 0, 1 \rangle, 3 \rangle$. Тогда $\{d\}(F, n) = 3$ для всех n . Двигаясь назад по этим шагам, получаем, что

$$\{e_1\}(F) = F(\lambda n \{d\}(F, n)) = F(\lambda n (3)) = k.$$

Поэтому мы должны теперь вычислить $\{e_2\}(k, F)$. Пусть $e_2 = \langle 9, \langle 1, 0, 1 \rangle, \langle 0, 0, 1 \rangle \rangle$. Тогда для вычисления $\{e_2\}(k, F)$ нужно вычислить $\{k\}(F)$. Если это не определено, то не определено и $\{e\}(F)$. С другой стороны, если, например, $k = \langle 2, \langle 0, 0, 1 \rangle, 5 \rangle$, то $\{k\}(F) = 5$, и, двигаясь назад по этим шагам, мы имеем $\{e\}(F) = 5$.

§ 15. Эквивалентность определения, данного Клини, и нашего

Непосредственно из определения § 14 имеем, что каждая частичная функция

$$f: \mathcal{X} \rightarrow \omega,$$

которая рекурсивна в первоначальном смысле Клини [1], является также рекурсивной по Клини в смысле нашего п. 11.2. Теперь мы докажем обратное.

15.1. Характером каждой точки

$$x \in \mathcal{X} = T^{(j_1)} \times \dots \times T^{(j_m)}$$

назовем

$$\text{ch}(x) = \text{ch}(\mathcal{X}) = \langle j_1, \dots, j_m \rangle$$

и для каждой конечной последовательности $\sigma = (x_1, \dots, x_n)$ из T^* положим

$$\text{ch}(\sigma) = \langle n, \text{ch}(x_1), \dots, \text{ch}(x_n) \rangle.$$

Положим также

$$\hat{\sigma} = x_1, \dots, x_n = x_1 \hat{\cap} x_2 \hat{\cap} \dots \hat{\cap} x_n = \text{сцеплению точек } x_1, \dots, x_n.$$

Наш план состоит в том, чтобы каждому функционалу $\Phi(\sigma, f)$ из $\mathcal{H}_0$ сопоставить общерекурсивную функцию $p_\Phi = p: \omega \rightarrow \omega$ такую, что

$$\Phi^\infty(\sigma) = \{p(\text{ch}(\sigma))\}(\hat{\sigma}).$$

Этого, конечно, достаточно, потому что если $\varphi: \mathcal{X} \rightarrow \omega$ рекурсивна по Клини в нашем смысле, то для некоторого $\Phi(\tau, x, f) \in \mathcal{H}_0$ имеем $\varphi(x) = \Phi^\infty(\bar{n}, x)$, где $\bar{n} \in \omega^k$, так что

$$\varphi(x) = \{e\}(\bar{n}, x),$$

где

$$e = p(\text{ch}(\omega^k \times \mathcal{X})).$$

Для определения p_Φ мы должны будем определить одновременно p_Ψ для всех «подфункционалов» Ψ функционала Φ (которых конечное число).

15.2. Заметим сначала, что из определения клиниевского класса получаем, что функционал вида $\Phi(\sigma, f)$ лежит в $\mathcal{H}_0$, если он есть один из функционалов (i)–(vii) или порожден в соответствии с правилами (viii)–(xii) (неопределяемые обозначения таковы, как в 2.3 и 11.1).

$$(i) \quad \Phi(j, x, \sigma, f) = \begin{cases} 0, & \text{если } j \in \omega, \quad x \in T^{(j)}, \\ 1 & \text{в противном случае.} \end{cases}$$

$$(ii) \quad \Phi(x, \sigma, f) = \begin{cases} x, & \text{если } x \in \omega, \\ 0, & \text{если } x \notin \omega. \end{cases}$$

$$(iii) \quad \Phi(x, \sigma, f) = \begin{cases} x + 1, & \text{если } x \in \omega, \\ 0, & \text{если } x \notin \omega. \end{cases}$$

$$(iv) \quad \Phi(x, y, \sigma, f) = \begin{cases} 0, & \text{если } x = y \in \omega, \\ 1, & \text{если } x, y \in \omega, \quad x \neq y, \\ 0 & \text{в остальных случаях.} \end{cases}$$

$$(v) \quad \Phi(\tau, \sigma, f) = f(\tau).$$

$$(vi) \quad \Phi(x, \sigma, f) = \text{length}(x).$$

$$(vii) \quad \Phi(x, y, \sigma, f) = \begin{cases} y(x), & \text{если } y \in T^{(1)}, \quad x \in \omega, \\ 0 & \text{в противном случае.} \end{cases}$$

$$(viii) \quad \Psi(\sigma, f) = \Phi(X(\sigma, f), \sigma, f).$$

$$(ix) \quad \Psi(x, \sigma, f) = \begin{cases} \Phi(\sigma, f), & \text{если } x = 0, \\ X(\sigma, f), & \text{если } x \neq 0, \quad x \in \omega, \\ 0 & \text{в остальных случаях.} \end{cases}$$

$$(x) \quad \Psi(y, \sigma, f) = \begin{cases} y(\lambda \alpha^i \Phi(\alpha^i, y, \sigma, f)), & \text{если } y \in T^{(i+2)}, \\ 0 & \text{в противном случае.} \end{cases}$$

$$(xi) \quad \Psi(\sigma, f) = \Phi(\pi_1(\sigma), \dots, \pi_k(\sigma), f).$$

$$(xii) \quad \Psi(x, y, \sigma, f) = \Phi(t(x, y), \sigma, f),$$

где t — сцепление или точечное проектирование.

Определим множество $\text{Sub}(\Phi)$ подфункционалов функционала $\Phi(\sigma, f)$ следующим образом:

(a) Если Φ получается по (i)–(vii), то $\text{Sub}(\Phi) = \{\Phi\}$.

(b) Если Ψ получается из Φ, X , как в (viii)–(xii), то $\text{Sub}\{\Psi\} = \{\Psi\} \cup \text{Sub}(\Phi) \cup \text{Sub}(X)$.

Наконец, положим $\Phi < X$, если $\Phi \in \text{Sub}(X) \& \Phi \neq X$.

15.3. Предложение. Пусть $\Phi(\sigma, f)$ — оперативный функционал из $\mathcal{H}_0$, и пусть $\Phi_0, \dots, \Phi_c$ — перечисление всех его подфункционалов такое, что если $\Phi_i < \Phi_j$, то $i < j$, и $\Phi_c = \Phi$. Существует общерекурсивная функция $p(i, t)$ на ω такая, что для всех $i \leq c$

$$\Phi_i(\tau, \Phi^\infty) = \{p(i, \text{ch}(\tau))\}(\hat{\tau}).$$

Доказательство. Будем временно называть частичную функцию $\varphi: \mathcal{X} \rightarrow \omega$ рекурсивной по Клини₀, если она рекурсивна в смысле первоначального определения Клини. Нам далее потребуются два простых утверждения о рекурсии по Клини₀, которые могут быть легко установлены из определений (или см. Клини [1]):

(i) Если

$$\varphi^{\mathcal{X}}(e, x) = \{e\}(x) \quad (x \in \mathcal{X}),$$

то $\{\varphi^{\mathcal{X}}\}$ является хорошей системой универсальных частичных функций для рекурсии по Клини₀. В частности, имеем вторую теорему о рекурсии для рекурсии по Клини₀.

(ii) Каждая частичная функция на ω , рекурсивная в смысле обычной теории рекурсии, является также рекурсивной по Клини₀. Обратное также верно, что следует из 12.4 и замечаний в начале этого параграфа.

Мы определим

$$p(i, t) = \{\beta\}(i, t)$$

при помощи второй теоремы о рекурсии для рекурсии по Клини₀. Мы рассматриваем несколько случаев в зависимости от того, что есть Φ_i .

Сначала положим $p(i, t) = 0$, если $i > c$.

Для $i \leq c$ определение $p(i, t)$ тривиально, за исключением случая, когда Φ_i получается по 15.2 (v), т. е. вычислением значения. В остальных случаях функция $p(i, t)$ определяется либо явно, либо рекурсивно через $p(j, t')$, где $j < i$. Например, в случае 15.2 (viii) имеем

$$\Phi_i(\tau, f) = \Phi_j(\Phi_k(\tau, f), \tau, f),$$

где $j, k < i$. Тогда имеем

$$\Phi_i(\tau, \Phi^\infty) = \Phi_j(\Phi_k(\tau, \Phi^\infty), \tau, \Phi^\infty)$$

$$= \{p(j, \text{ch}(0, \tau))\}(\{p(k, \text{ch}(\tau))\}(\hat{\tau}), \hat{\tau})$$

$$= \{\langle 4, \text{arity}(\hat{\tau}), p(k, \text{ch}(\tau)), p(j, \text{ch}(0, \tau)) \rangle\}(\hat{\tau}).$$

Поэтому полагаем $p(i, t) = \langle 4, q_1(t), p(k, t), p(j, q_2(t)) \rangle$, где q_1, q_2 — рекурсивные функции такие, что

$$q_1(\text{ch}(\tau)) = \text{arity}(\hat{\tau}), \quad q_2(\text{ch}(\tau)) = \text{ch}(0, \tau).$$

Предположим теперь, что Φ_i получается по 15.2 (v) и для упрощения обозначений возьмем σ пустым, так что

$$\Phi_i(\tau, f) = f(\tau).$$

Тогда имеем

$$\Phi_i(\tau, \Phi^\infty) = \Phi^\infty(\tau) = \Phi(\tau, \Phi^\infty)$$

$$= \Phi_c(\tau, \Phi^\infty) = \{p(c, \text{ch}(\tau))\}(\hat{\tau}).$$

Могло бы показаться целесообразным положить $p(i, t) = p(c, t)$, но поскольку $c > i$, мы не можем ожидать, что $p(i, t)$ будет корректно определено таким путем. Тем не менее, если β — индекс p , мы имеем также

$$\{p(c, \text{ch}(\tau))\}(\hat{\tau}) = \{\{\beta\}(c, \text{ch}(\tau))\}(\hat{\tau})$$

$$= \{\langle 9, \text{arity}(0, \hat{\tau}), \text{arity}(\hat{\tau}) \rangle\}(\{\beta\}(c, \text{ch}(\hat{\tau})), \hat{\tau})$$

$$= \{q(\beta, \text{ch}(\tau))\}(\hat{\tau})$$

с рекурсивной функцией q , которую нетрудно вычислить; затем положим

$$p(i, t) = q(\beta, t)$$

в этом случае. Доказательство будет зависеть от некоторого дополнительного свойства этой функции q , которое мы ниже объясним.

По второй теореме о рекурсии для рекурсии по Клини₀ существует индекс β такой, что функция $p(i, t) = \{\beta\}(i, t)$ удовлетворяет всем вышеизложенным требованиям. Ясно, что p всюду определена.

Чтобы показать, что p годится, докажем сначала индукцией по ξ , что

$$\Phi_i(\tau, \Phi^{<\xi}) = w \Rightarrow \{p(i, \text{ch}(\tau))\}(\hat{\tau}) = w.$$

Для этого для каждого фиксированного ξ мы используем индукцию по i . Детали, которые тривиальны, мы оставляем читателю. В другую сторону, мы покажем

$$\{p(i, \text{ch}(\tau))\}(\hat{\tau}) = w \Rightarrow \Phi_i(\tau, \Phi^\infty) = w,$$

проводя индукцию по ординалу

$$|p(i, \text{ch}(\tau)), \hat{\tau}| = \xi$$

(см. 14.1) и для каждого ξ рассматривая случаи по i .

Единственный трудный случай — когда Φ_i получается по 15.2 (v). Тогда по определению $p(i, \text{ch}(\tau))$ имеем

$$\{p(i, \text{ch}(\tau))\}(\hat{\tau}) = \{q(\beta, \text{ch}(\tau))\}(\hat{\tau})$$

$$= \{p(c, \text{ch}(\tau))\}(\hat{\tau}).$$

Более того, всякий естественный выбор функции q обладает дополнительным свойством — она *увеличивает* ординал вычисления, т. е.

$$|p(i, \text{ch}(\tau)), \hat{\tau}| = |q(\beta, \text{ch}(\tau)), \hat{\tau}|$$

$$\geq |\langle g, \text{arity}(0, \hat{\tau}), \text{arity}(\hat{\tau}), p(c, \text{ch}(\tau)), \hat{\tau} \rangle|$$

$$> |p(c, \text{ch}(\tau)), \hat{\tau}|.$$

Здесь требуется проверка, но она нетрудна и является ключом к этой части доказательства. Поэтому можно воспользоваться индукционным предположением, по которому

$$\Phi_c(\tau, \Phi^\infty) = w,$$

так что

$$\Phi_i(\tau, \Phi^\infty) = \Phi_c(\tau, \Phi^\infty) = w. \quad \square$$

§ 16. Теоремы Клини о подстановках

16.1. Пусть $\varphi(y, z)$ — рекурсивная по Клини частичная функция, и пусть $\theta: \mathcal{X} \rightarrow \mathcal{Y}$ — рекурсивное по Клини частичное отображение в смысле п. 11.1. Рассмотрим вопрос: является ли

$$\chi(x, z) = \varphi(\theta(x), z)$$

рекурсивной по Клини? Без потери общности можно предполагать, что $\mathcal{Y} = T^{(j+1)}$, так что

$$\chi(x, z) = \varphi(\lambda \alpha^j \psi(\alpha^j, x), z)$$

для некоторой рекурсивной по Клини частичной функции ψ .

Контрпример из Клини [1] показывает, что нельзя ожидать, что χ рекурсивна по Клини при $j > 0$, даже если θ всюду определено. Действительно, пусть $T(m, n)$ — рекурсивный предикат на ω такой, что $\forall n T(m, n)$ не является полурекурсивным (т. е. рекурсивно перечислимым). Положим

$$\varphi'(\alpha^2, n, m) = \begin{cases} 0, & \text{если } T(m, n), \\ \text{не определено, если } \neg T(m, n), \end{cases}$$

и затем

$$\varphi(\alpha^2, m) = \alpha^2 (\lambda n \varphi'(\alpha^2, n, m)).$$

Тогда φ рекурсивна по Клини. Пусть

$$\theta: \omega \rightarrow T^{(2)}$$

— любое *всюду определенное* рекурсивное по Клини отображение. Тогда

$$\varphi(\theta(0), m)$$

не может быть рекурсивной по Клини, так как в этом случае она была бы рекурсивной (в смысле обычной теории рекурсии), поэтому

$$P(m) \Leftrightarrow \varphi(\theta(0), m) \downarrow \Leftrightarrow \forall n T(m, n)$$

был бы полурекурсивным, а он таким не является.

Следующая теорема о частичных подстановках очень важна.

16.2. Теорема (Клини [1]). Пусть $\varphi: \mathcal{Y} \times \mathcal{Z} \rightarrow \omega$ будет рекурсивной по Клини частичной функцией, пусть $\theta: \mathcal{X} \rightarrow \mathcal{Y}$ будет рекурсивным по Клини частичным отображением и положим

$$\chi(x, z) = \varphi(\theta(x), z);$$

тогда χ имеет рекурсивное по Клини расширение.

Более подробно, существует рекурсивная по Клини частичная функция $\chi^*(x, z)$ такая, что если $\theta(x)$ и $\varphi(\theta(x), z)$ определены, то $\chi^*(x, z)$ определено и

$$\chi^*(x, z) = \varphi(\theta(x), z).$$

В частности, если и φ , и θ всюду определены, то χ рекурсивна по Клини.

Доказательство (схема). Достаточно предполагать, что $\mathcal{Y} = T^{(j+1)}$, так что

$$\chi(x, z) = \varphi(\lambda \alpha^j \psi(\alpha^j, x), z).$$

Доказательство является типичным примером «метода переноса индексов», который мы использовали также при установлении 15.3. В этих рассуждениях одним из наиболее важных шагов является формулировка желаемого результата в сильной форме, допускающей доказательство «эффективной трансфинитной индукцией». В нашем случае мы свяжем с каждым j рекурсивную функцию $p_j(e_1, e_2, t)$ такую, что для каждой пары кодов e_1, e_2 и точек x, y, z

$$\{e_1\}(y, \lambda \alpha^j \{\{e_2\}(\alpha^j, x, y, z), z\}) = \{p_j(e_1, e_2, \text{ch}(x, y, z))\}(x, y, z), \quad (*)$$

как только левая часть равенства определена.

Построение p_j проводим индукцией по j , так что фиксируем некоторое $j > 0$ и предположим, что $p_0, \dots, p_{j-1}$ уже определены и $(*)$ выполнена для каждого из них. (Построение p_0 аналогично построению p_j ($j > 0$) и мы опускаем его.)

Определим

$$p(e_1, e_2, t) = p_j(e_1, e_2, t)$$

через ее индекс β с помощью теоремы о рекурсии. Определение дается в зависимости от индекса e_1 соответственно случаям 14.1 (i) — (ix). Все случаи, кроме (viii), (ix), очевидны, поскольку $p(e_1, e_2, t)$ определяется в них явно (и рекурсивно) и либо абсолютно, либо через $p(e'_1, e'_2, t')$ для $e'_1 < e_1$.

Рассмотрим теперь случай 14.1 (viii). Если $t = \text{ch}(x, y, z)$ для точек x, y, z , где y содержит некоторые объекты типа $j+1$, то определение $p(e_1, e_2, t)$ снова тривиально. В противном случае можно объединить y, z в новую последовательность, так что без потери общности можно предполагать, что y пуста и

$$e_1 = \langle 8, \text{arity}(\alpha^{j+1}, z), j+1, (e_1)_3 \rangle,$$

так что

$$\{e_1\}(\alpha^{j+1}, z) = \alpha^{j+1} (\lambda \alpha^{j-1} \{\{e_1\}_3\}(\alpha^{j+1}, \alpha^{j-1}, z)).$$

Фиксируем x и z , и пусть

$$\beta^{j+1} = \lambda \alpha^j \{e_2\}(\alpha^j, x, z);$$

тогда ясно, что

$$\{e_1\}(\beta^{j+1}, z) = \{e_2\}(\lambda\alpha^{j-1}\{(e_1)_3\}(\beta^{j+1}, \alpha^{j-1}, z), x, z).$$

Теперь

$$\beta^{j+1} = \lambda\alpha^j\{q(e_2)\}(\alpha^j, x, \alpha^{j-1}, z),$$

где q рекурсивна, так что

$$\begin{aligned} \{(e_1)_3\}(\beta^{j+1}, \alpha^{j-1}, z) &= \{(e_1)_3\}(\lambda\alpha^j\{q(e_2)\}(\alpha^j, x, \alpha^{j-1}, z), \alpha^{j-1}, z) \\ &= \{p((e_1)_3, q(e_2), \text{ch}(x, \alpha^{j-1}, z))\}(x, \alpha^{j-1}, z) \end{aligned}$$

в предположении, что p определена и обладает требуемыми свойствами на $(e_1)_3, q(e_2), \text{ch}(x, \alpha^{j-1}, z)$; мы докажем это, когда подойдем к доказательству того, что наше определение годится, но заметьте, что $|(e_1)_3, \lambda\alpha^j\{q(e_2)\}(\alpha^j, x, \alpha^{j-1}, z), \alpha^{j-1}, z| < |e_1, \beta^{j+1}, z|$.

Для упрощения обозначений положим

$$d = p((e_1)_3, q(e_2), \text{ch}(x, \alpha^{j-1}, z)),$$

так что имеем

$$\{e_1\}(\beta^{j+1}, z) = \{e_2\}(\lambda\alpha^{j-1}\{d\}(x, \alpha^{j-1}, z), x, z).$$

Теперь мы уже свели задачу вычисления $\{e_1\}(\beta^{j+1}, z)$ к подстановке меньшего типа, именно, вставке $\lambda\alpha^{j-1}\{d\}(x, \alpha^{j-1}, z)$ в $\{e_2\}(\alpha^j, x, z)$. Это не является вполне корректной формой применения p_{j-1} , но, вводя рекурсивную r (как мы делали раньше с q), положим

$$\{d\}(x, \alpha^{j-1}, z) = \{r(d)\}(\alpha^{j-1}, x, z)$$

и имеем

$$\begin{aligned} \{e_1\}(\beta^{j+1}, z) &= \{e_2\}(\lambda\alpha^{j-1}\{r(d)\}(\alpha^{j-1}, x, z), x, z) \\ &= \{p_{j-1}(e_2, r(d), \text{ch}(x, z))\}(x, z). \end{aligned}$$

Наконец, мы устанавливаем

$$p(e_1, e_2, t) = p_{j-1}(e_2, r(d), \text{ch}(x, z)),$$

где, конечно, $\text{ch}(x, z) = t$.

В случае 14.1 (ix) мы определяем $p(e_1, e_2, t)$ через индекс p функции p , как в доказательстве 15.3. Детали мы опускаем. Доказательство того, что p всюду определена, точно то же, что и в 15.3.

Чтобы показать, что p удовлетворяет (*), индукцией по

$$|e_1, y, \lambda\alpha^j\{e_2\}(\alpha^j, x, y, z), z| = \xi$$

и для каждого ξ рассмотрением случаев по e_1 проверяем, что

$$\begin{aligned} \{e_1\}(y, \lambda\alpha^j\{e_2\}(\alpha^j, x, y, z), z) &= w \\ \Rightarrow \{p(e_1, e_2, \text{ch}(x, y, z))\}(x, y, z) &= w. \quad (**) \end{aligned}$$

Опять единственным трудным случаем является 14.1 (viii), и доказательство в этом случае может быть легко извлечено из анализа, который мы проделали выше. $\square$

Обращение (**) для $j > 0$ нельзя доказать, даже предполагая, что $\lambda\alpha^j\{e_2\}(\alpha^j, x, y, z)$ всюду определена, в силу контр-примера, который мы дали в 16.1. Для $j = 0$ можно проверить, что

$$\{p(e_1, e_2, \text{ch}(x, y, z))\}(x, y, z) = w \Rightarrow \{e_1\}(y, \lambda n\{e_2\}(n, x, y, z), z) = w,$$

индукцией по $|p(e_1, e_2, \text{ch}(x, y, z)), x, y, z|$, так что имеет место

16.3. Теорема (Клини [1]). Если $\text{type}(\mathcal{Y}) = 1$, $\varphi: \mathcal{Y} \times \mathcal{Z} \rightarrow \omega$ — рекурсивная по Клини частичная функция и $\theta: \mathcal{Z} \rightarrow \mathcal{Y}$ — рекурсивное по Клини частичное отображение, то существует рекурсивная по Клини функция $\chi^*(x, z)$ такая, что как только $\theta(x)$ определено, то

$$\chi^*(x, z) = \varphi(\theta(x), z).$$

В частности, если θ всюду определено, то $\varphi(\theta(x), z)$ рекурсивна по Клини.

Снова контрпример, подобный приведенному в 16.1, показывает, что предположение, что $\theta(x)$ определено, необходимо.

Наш последний результат в этом параграфе показывает, что полная подстановка такая, как в 16.3, допустима в любом типе, если есть объект достаточно высокого типа. Этот факт будет весьма полезным впоследствии.

16.4. Теорема (Клини). Пусть $\varphi: \mathcal{Y} \times \mathcal{Z} \rightarrow \omega$ — рекурсивная по Клини частичная функция, $\theta: \mathcal{Z} \rightarrow \mathcal{Y}$ — рекурсивное по Клини частичное отображение и положим

$$\chi(x, z) = \varphi(\theta(x), z).$$

Для каждого $m \geq \text{type}(\mathcal{Y})$ существует рекурсивная по Клини частичная функция $\chi^*(\alpha^m, x, z)$ такая, что для всех объектов α^m типа m и всех x таких, что $\theta(x)$ определено, имеем

$$\chi(x, z) = \chi^*(\alpha^m, x, z).$$

В частности, если θ всюду определено, то χ рекурсивна относительно каждого объекта типа $\geq \text{type}(\mathcal{Y})$.

Доказательство (схема). Предположим без потери общности, что $\mathcal{Y} = T^{(j+1)}$, так что $\theta(x) = \lambda\alpha^j\psi(\alpha^j, x)$. Сначала рассмотрим случай $m = j + 1$.

Снова используя «метод переноса индексов», показываем, что существует всюду определенная рекурсивная функция p такая, что если $\lambda\alpha^j\psi(\alpha^j, x)$ всюду определена, то для любого α^m

$$\{e\}(y, \lambda\alpha^j\psi(\alpha^j, x), z) = \{p(e, \text{ch}(x, y, z))\}(\alpha^m, x, y, z). \quad (*)$$

Определение p проходит по образцу доказательства 16.2. но нам не нужна индукция по j , поскольку мы можем теперь использовать 16.2.

Как и в доказательстве того результата, рассмотрим только интересный подслучай случая 14.1 (viii), когда e таково, что

$$\{e\}(\lambda\alpha^j\psi(\alpha^j, x), z) = \psi(\lambda\alpha^{j-1}\{(e_1)_3\}(\lambda\alpha^j\psi(\alpha^j, x), \alpha^{j-1}, z), x);$$

если p определена и имеет требуемое свойство на $(e_1)_3$, то это выражение равно

$$\begin{aligned} \psi(\lambda\alpha^{j-1}\{p((e_1)_3, \text{ch}(\alpha^{j-1}, z, x))\}(\alpha^m, \alpha^{j-1}, z, x), x) \\ = \psi(\lambda\alpha^{j-1}\{d\}(\alpha^m, \alpha^{j-1}, z, x), x), \end{aligned}$$

где

$$d = p((e_1)_3, \text{ch}(\alpha^{j-1}, z, x)).$$

Используя 16.2, можно найти всюду определенную рекурсивную функцию h такую, что

$$\psi(\lambda\alpha^{j-1}\{d\}(\alpha^m, \alpha^{j-1}, z, x), x) = \{h(d, \text{ch}(x, z))\}(\alpha^m, x, z), \quad (**)$$

как только

$$f = \lambda\alpha^{j-1}\{d\}(\alpha^m, \alpha^{j-1}, z, x)$$

всюду определена и левая часть равенства (**) определена. Теперь осталось видоизменить правую часть (**) так, чтобы она была определена, только когда f есть всюду определенная функция, и именно в этом месте используется наличие аргумента α^m .

Найдем всюду определенную рекурсивную функцию h' такую, что

$$\begin{aligned} \{h'(d, \text{ch}(x, z))\}(\alpha^m, x, z) \\ = \begin{cases} \{h(d, \text{ch}(x, z))\}(\alpha^m, x, z), & \text{если } \alpha^m(f) \downarrow, \\ \text{не определено} & \text{в противном случае,} \end{cases} \end{aligned}$$

и положим в этом случае

$$p(e, t) = h'(p((e_1)_3, q(t)), t),$$

где q рекурсивна и такова, что

$$q(\text{ch}(x, z)) = \text{ch}(\alpha^{j-1}, z, x).$$

Заметим здесь, что h' может быть выбрана так, что

$$|h'(d, \text{ch}(x, z)), \alpha^m, x, z| > |d, \alpha^m, \alpha^{j-1}, z, x| \quad \text{для всех } \alpha^{j-1}.$$

При таком определении нетрудно проверить, что

$$\{e\}(y, \lambda\alpha^j\psi(\alpha^j, x), z) = w \Rightarrow \{p(e, \text{ch}(x, y, z))\}(\alpha^m, x, y, z) = w,$$

индукцией по $|e, y, \lambda\alpha^j\psi(\alpha^j, x), z|$ и обратную импликацию индукцией по $|p(e, \text{ch}(x, y, z)), \alpha^m, x, y, z|$; обе при условии, что $\lambda\alpha^j\psi(\alpha^j, x)$ всюду определена.

Для доказательства общего случая, когда

$$m \geq j + 1,$$

достаточно установить следующее утверждение:

Лемма. Для любой рекурсивной по Клини частичной функции $\varphi(\alpha^j, x)$ частичная функция

$$\psi(\alpha^{j+1}, x) = \varphi(d_j(\alpha^{j+1}), x)$$

также рекурсивна по Клини. (Здесь d_j — это функция понижения типа из 10.2.)

Доказательство. Используем индукцию по j . Для каждого фиксированного j снова применяем «метод переноса индексов». Затруднительный случай 14.1 (viii) рассматриваем просто, заметив, что если

$$\varphi(\alpha^j, x) = \alpha^j(\lambda\alpha^{j-2}\chi(\alpha^j, \alpha^{j-2}, x)),$$

то

$$\begin{aligned} \varphi(d_j(\alpha^{j+1}), x) &= d_j(\alpha^{j+1})(\lambda\alpha^{j-2}\chi(\alpha^j, \alpha^{j-2}, x)) \\ &= \alpha^{j+1}(u^j(\lambda\alpha^{j-2}\chi(\alpha^j, \alpha^{j-2}, x))) \\ &= \alpha^{j+1}(\lambda\beta^{j-1}\chi(\alpha^j, d_{j-2}(\beta^{j-1}), x)), \end{aligned}$$

так что можно использовать индукционное предположение о j .

Это завершает доказательство леммы и нашу схему доказательства теоремы 16.4. $\square$

16.5. Как простое следствие этих теорем о подстановках мы теперь можем получить следующие факты об относительной рекурсии по Клини. Пусть $F \leq G$ для любых двух объектов F, G означает, что F рекурсивен по Клини относительно G , т. е. для некоторой рекурсивной по Клини частичной функции φ и всех α^j

$$F(\alpha^j) = \varphi(G, \alpha^j).$$

В силу 16.2 $\leq$ является транзитивным отношением. Это позволяет определить отношение эквивалентности

$$F \equiv G \Leftrightarrow F \leq G \wedge G \leq F.$$

Если $F \equiv G$, то говорим, что F и G имеют одну и ту же клиниевскую степень. Если $F \leq G$, то каждая всюду определенная рекурсивная по Клини относительно F функция также рекурсивна по Клини относительно G . Это также выполняется для частичных функций (по 16.4) при условии, что $\text{type}(F) \leq \text{type}(G)$.

§ 17. Сечения и оболочки

17.1. Точечным множеством типа $k > 0$ называется подмножество $R \subseteq \mathcal{X}$ пространства типа $k-1$. Например, точечные множества типа 1 — это подмножества ω^n для некоторого n . Если $R \subseteq \mathcal{X}$ является точечным множеством, то пишем взаимозаменяемо

$$x \in R \Leftrightarrow R(x).$$

Точечным k -классом называется семейство точечных множеств типов $\leq k$. Для данного конечного списка функционалов $\bar{\Phi}$ k -оболочкой $\bar{\Phi}$, символически

$${}_k \text{ep}(\bar{\Phi}),$$

называется точечный k -класс, состоящий из тех точечных множеств типов $\leq k$, которые полурекурсивны по Клини относительно $\bar{\Phi}$, т. е. являются областями определения рекурсивных по Клини относительно $\bar{\Phi}$ частичных функций. k -сечением $\bar{\Phi}$, символически

$${}_k \text{sc}(\bar{\Phi}),$$

называется точечный k -класс, состоящий из тех точечных множеств типов $\leq k$, которые рекурсивны по Клини относительно $\bar{\Phi}$, т. е. их характеристические функции рекурсивны по Клини относительно $\bar{\Phi}$. Например, из 12.4 следует, что для $k = 1, 2$

${}_k \text{ep}(^2 E)$ — все точечные Π_1^1 -множества типа $\leq k$,

${}_k \text{sc}(^2 E)$ — все точечные Δ_1^1 -множества типа $\leq k$.

Остаток этой главы мы посвятим изучению свойств оболочек и сечений объектов высших типов. В общем случае нельзя утверждать никаких интересных результатов о структуре ${}_k \text{ep}(\bar{F})$, если только $\bar{F}$ не является нормальным на T_{k-1}^* . По теореме 13.3 (i), если $\bar{F} = (F_1, \dots, F_n)$ и $m = \max\{\text{type}(F_i) : i = 1, \dots, n\} \geq 2$, то $\bar{F}, {}^2 E, \dots, {}^m E$ нормальна на T_m^* , поэтому мы ограничимся изучением ${}_k \text{ep}(\bar{F}, {}^2 E, \dots, {}^m E)$ для $k \leq m+1$. Заметим здесь, что если $j \leq m$, то ${}^j E \leq {}^m E$, поскольку ${}^j E = d_{j,m}({}^m E)$ (в обозначениях 10.2), так что ${}_k \text{ep}(\bar{F}, {}^2 E, \dots, {}^m E) = {}_k \text{ep}(\bar{F}, {}^m E)$. Более того, мы можем закодировать все объекты из $\bar{F}$ единственным объектом G типа m так, что ${}_k \text{ep}(\bar{F}, {}^m E) = {}_k \text{ep}(G, {}^m E)$. Это осуществляем, поднимая до m тип всех объектов $\bar{F}$ (при помощи $u^{1,m}$) и затем используя простую спаривающую функцию для объектов типа m , например $\langle F_1, F_2 \rangle (\alpha^{m-1}) =$

$= \langle F_1(\alpha^{m-1}), F_2(\alpha^{m-1}) \rangle$. Поэтому мы будем отныне изучать только ${}_k \text{ep}(F, {}^m E)$

для $\text{type}(F) = m \geq 2$ и $k \leq m+1$. Ниже мы суммируем основные свойства этих оболочек, которые вытекают более или менее непосредственно из того, что мы уже доказали.

17.2. Пусть Γ — точечный k -класс. Говорим, что Γ замкнут относительно $\exists^!$, если для каждого $R \subseteq \mathcal{X} \times T^{(1)}$ из Γ точечное множество

$$P(x) \Leftrightarrow \exists \alpha^1 R(x, \alpha^1)$$

также принадлежит Γ . Замкнутость относительно $\forall^!$ и $\neg, \vee, \wedge$ определяется таким же образом. Говорим, что Γ замкнут относительно подстановки всюду определенных рекурсивных по Клини отображений, если он содержит все рекурсивные по Клини точечные множества типов $\leq k$, и как только $\theta: \mathcal{X} \rightarrow \mathcal{Y}$ всюду определена и рекурсивна по Клини при условии $\text{type}(\mathcal{X})$, $\text{type}(\mathcal{Y}) < k$ и $R(y, z)$ принадлежит Γ , то

$$P(x, z) \Leftrightarrow R(\theta(x), z)$$

также принадлежит Γ . Говорим, что Γ обладает свойством перечисления, или является ω -параметризованным, если для каждого $\mathcal{X}$ типа $\leq k$ существует некоторое $W \subseteq \omega \times \mathcal{X}$ такое, что для всякого $R \subseteq \mathcal{X}$

$$R \in \Gamma \Leftrightarrow \exists e (R = W_e),$$

где $W_e = \{x: W(e, x)\}$. Наконец, говорим, что Γ нормирован, или обладает свойством предвполнеупорядоченности, если каждое $R \in \Gamma$ допускает Γ -норму (определение см. в 7.1).

Теперь мы имеем следующий результат, наиболее важное утверждение которого, а именно предвполнеупорядоченность и замкнутость относительно $\exists^0$, принадлежит Ганди [1] для $m = 2$, Платеку [1] и Московакису [1] для $m \geq 3$ (доказательство у Московакиса [1] дается только для $m = 3$, Грийо [1] расширил его на все m).

17.3. Теорема. Пусть $F = {}^m F$ — объект типа $m \geq 2$. Пусть $\Gamma = {}_k \text{ep}(F, {}^m E)$ для $1 \leq k \leq m+1$. Тогда:

(i) Γ замкнут относительно подстановки всюду определенных рекурсивных по Клини отображений, $\wedge, \vee, \exists^0, \forall^!$ ($j \leq m-2$), нормирован и обладает свойством перечисления.

(ii) Функция $f: \mathcal{X} \rightarrow \omega$, где $\text{type}(\mathcal{X}) < k$, рекурсивна по Клини относительно $F, {}^m E$ тогда и только тогда, когда график f принадлежит Γ . В частности, точечное множество $R \subseteq \mathcal{X}$ типа $\leq k$ рекурсивно по Клини относительно $F, {}^m E$ тогда и только тогда, когда и R и $\mathcal{X} - R$ принадлежат Γ .

Доказательство. Замкнутость относительно подстановки всюду определенных рекурсивных по Клини отображений следует из 16.4. Замкнутость относительно $\wedge, \vee, \exists^0$ вытекает из 13.3, 13.4, 9.4 и 7.3. Для замкнутости относительно $\forall^j$ ($j \leq m-2$) заметьте, что если $\varphi(x, \alpha^j)$ — частичная функция, то

$$\forall \alpha^j (\varphi(x, \alpha^j) \downarrow) \Leftrightarrow {}^{j+2}E(\lambda \alpha^j \varphi(x, \alpha^j)) \downarrow.$$

Нормальность и перечислимость следуют из 13.3 и 13.5. Наконец, (ii) получается, как в 9.4. $\square$

§ 18. Индуктивный анализ полурекурсивных множеств

Здесь мы дадим индуктивный анализ точечных множеств из $\text{Kep}(^mF, ^mE)$, который оказывается ключом ко многим дальнейшим структурным свойствам оболочек. Некоторые его непосредственные применения к проблеме замкнутости оболочек относительно высшей экзистенциальной квантификации будут даны в следующем параграфе.

18.1. Оператор

$$\Omega: \text{Pow}(\mathcal{X}) \rightarrow \text{Pow}(\mathcal{X})^*$$

на $\mathcal{X}$ называется *монотонным*, если

$$A \subseteq B \subseteq \mathcal{X} \Rightarrow \Omega(A) \subseteq \Omega(B).$$

Для таких операторов индуктивно определяем:

$$\Omega^i = \Omega(\Omega^{<i}), \quad \text{где } \Omega^{<i} = \bigcup_{\eta < i} \Omega^\eta,$$

и полагаем $\Omega^\infty = \bigcup_i \Omega^i$ — наименьшей неподвижной точке Ω .

Если $R \subseteq \mathcal{X}$ и $S \subseteq \mathcal{Y}$ — два точечных множества, то говорим, что R сводится к S , если существует всюду определенная рекурсивная по Клини функция $\theta: \mathcal{X} \rightarrow \mathcal{Y}$ такая, что $R(x) \Leftrightarrow \Leftrightarrow S(\theta(x))$.

18.2. Теорема (Московакис [1]). Пусть $F = ^mF$ — объект типа $m \geq 2$ и $m-1 \leq k \leq m+1$. Каждый $P \in \text{Kep}(F, ^mE)$ сводится к неподвижной точке Ω^∞ некоторого монотонного оператора Ω на пространстве типа $<k$, имеющего вид

$$x \in \Omega(S) \Leftrightarrow \forall y (R(x, y) \Rightarrow y \in S),$$

где $R \in \text{Kep}(F, ^mE)$.

Доказательство (набросок). Для упрощения обозначений положим $G = \langle F, ^mE \rangle$. Тогда $\text{Kep}(G) = \text{Kep}(F, ^mE)$, так

*) Символом $\text{Pow}(X)$ обозначается множество всех подмножеств множества X . — Прим. ред.

что дальше работаем с G . Рассмотрим только случай $k = m-1$, так как остальные случаи подобны и несколько проще. Будет также удобно работать с единственным стандартным пространством $\mathcal{X} = T^{(m-2)}$ типа $m-2$, и для этого мы кодируем конечные последовательности объектов типа $\leq m-2$ при помощи объектов типа $m-2$ следующим образом: если α^j — объект типа $\leq m-2$, то полагаем

$$\tilde{\alpha}^j = u^{j, m-2}(\alpha^j).$$

Если $\alpha_0, \dots, \alpha_{n-1}$ — конечная последовательность объектов типа $\leq m-2$, то полагаем

$$\langle \alpha_0, \dots, \alpha_{n-1} \rangle = \lambda \alpha^{m-3} (\langle \tilde{\alpha}_0(\sigma^{m-3}), \dots, \tilde{\alpha}_{n-1}(\sigma^{m-3}) \rangle).$$

Декодирующие функции определяются теперь следующим образом: для любого объекта α^{m-2} полагаем

$$(\alpha^{m-2})_i = \lambda \alpha^{m-3} ((\alpha^{m-2}(\alpha^{m-3}))_i)$$

и для любого $j \leq m-2$ полагаем

$$(\alpha^{m-2})_i^j = d_{j, m-2}((\alpha^{m-2})_i).$$

Далее, если $j = \text{type}(\alpha_i)$, то имеем

$$\langle \langle \alpha_0, \dots, \alpha_{n-1} \rangle \rangle_i^j = \alpha_i.$$

Ясно, что все эти кодирующие и декодирующие функции всюду определены и рекурсивны по Клини. (Эти определения были даны для $m > 2$. Мы оставляем читателю сделать тривиальные модификации, необходимые для $m = 2$.) Следуя Клини [1] и Грийо [1], будем сокращать

$$\begin{aligned} \{e\} [\alpha^{m-2}, \alpha^m] &= \{e\} ((\sigma^{m-2})_0^0, \dots, (\alpha^{m-2})_{k_0-1}^0, \\ &\dots, (\alpha^{m-2})_{k_0}^1, \dots, (\alpha^{m-2})_{k_0+k_1-1}^1, \dots, (\alpha^{m-2})_{k_0+\dots+k_{m-3}}^{m-3}, \\ &\dots, (\alpha^{m-2})_{k_0+k_1+\dots+k_{m-2}-1}^{m-2}, \alpha^m), \end{aligned}$$

если e является индексом частичной функции, имеющей k_i аргументов типа $i \leq m-2$ и один аргумент типа m . Легко видеть, что для подходящей рекурсивной по Клини функции φ

$$\{e\} [\alpha^{m-2}, \alpha^m] = \varphi(e, \alpha^{m-2}, \alpha^m).$$

Положим

$$W = \{(e, \alpha^{m-2}): \{e\} [\alpha^{m-2}, G] \text{ определено}\}.$$

Ясно, что достаточно показать, что $W = \Omega^\infty$ для Ω такого, как в формулировке теоремы.

Будем считать, что каждая пара (e, α^{m-2}) кодирует вычисление $\{e\} [\alpha^{m-2}, G]$ в соответствии с определением Клини из

§ 14. Как в 14.3, для вычисления $\{e\}[\alpha^{m-2}, G]$ нужно вычислить его подвычисления, которые все имеют вид $\{e'\}[\beta^{m-2}, G]$ и, следовательно, кодируются различными парами (e', β^{m-2}) . Например, если e — индекс и $(e)_0 = 4$, то подвычислениями (e, α^{m-2}) являются $((e)_2, \alpha^{m-2})$ и (полагая $l = k_0 + k_1 + \dots + k_{m-3}$)

$$((e)_3, \langle \{(e)_2\}[\alpha^{m-2}, G], (\alpha^{m-2})_0^0, \dots, (\alpha^{m-2})_{k_0-1}^0, \dots, (\alpha^{m-2})_l^{m-2}, \dots, (\alpha^{m-2})_{l+k_{m-2}-1}^{m-2} \rangle)$$

при условии, что $\{(e)_2\}[\alpha^{m-2}, G]$ определено.

Положим

$$R((e, \alpha^{m-2}), (d, \beta^{m-2}))$$

$$\Leftrightarrow (e \text{ не является индексом требуемой формы}$$

$$\text{и } e = d, \alpha^{m-2} = \beta^{m-2}) \vee ((d, \beta^{m-2}) \text{ является}$$

$$\text{подвычислением вычисления } (e, \alpha^{m-2})).$$

Тогда R полурекурсивен по Клини относительно G . В этом можно убедиться, заметив, что R определяется разбором случаев в зависимости от индекса e . Во всех случаях, кроме $(e)_0 = 4$, R в действительности рекурсивен относительно G . В случае, когда $(e)_0 = 4$ и e допускает требуемые типы аргументов,

$$\begin{aligned} R((e, \alpha^{m-2}), (d, \beta^{m-2})) &\Leftrightarrow (d = (e)_2 \wedge \beta^{m-2} = \alpha^{m-2}) \\ &\vee (d = (e)_3 \wedge \exists n (\{(e)_2\}[\alpha^{m-2}, G] = n \\ &\wedge \beta^{m-2} = \langle n, (\alpha^{m-2})_0^0, \dots, (\alpha^{m-2})_{k_0-1}^0, \\ &\dots, (\alpha^{m-2})_l^{m-2}, \dots, (\alpha^{m-2})_{l+k_{m-2}-1}^{m-2} \rangle)). \end{aligned}$$

так что R полурекурсивен по Клини относительно G . Теперь, полагая

$$(e, \alpha^{m-2}) \in \Omega(S) \Leftrightarrow \forall d \beta^{m-2} [R((e, \alpha^{m-2}), (d, \beta^{m-2})) \Rightarrow (d, \beta^{m-2}) \in S],$$

получаем, что $W = \Omega^\infty$, что и требовалось. $\square$

§ 19. Замкнутость относительно высшей экзистенциальной квантификации

В качестве простого следствия теоремы о представлении 18.2 получается

19.1. Теорема (Московакис [1]). Пусть $F = {}^m F$ — объект типа $m \geq 3$. Если $R \in {}_{m-1} \text{ep}(F, {}^m E)$, то найдется P из

${}_{m-1} \text{ep}(F, {}^m E)$ такой, что

$$\neg R(x) \Leftrightarrow \exists \alpha^{m-2} P(x, \alpha^{m-2}).$$

Доказательство. Пусть $\theta: \mathcal{X} \rightarrow \mathcal{Y}$ — функция, всюду определенная и рекурсивная по Клини, а Ω — оператор на $\mathcal{Y}$ такие, что, как в 18.2, $R(x) \Leftrightarrow \Omega^\infty(\theta(x))$. Пусть

$$y \in \Omega(S) \Leftrightarrow \forall z (Q(y, z) \Rightarrow z \in S),$$

где $Q \in {}_{m-1} \text{ep}(F, {}^m E)$. Заметим тогда, что

$$\neg \Omega^\infty(y) \Leftrightarrow \exists y_0 y_1 y_2 \dots (y_0 = y \wedge \forall i Q(y_i, y_{i+1})),$$

так что

$$\neg R(x) \Leftrightarrow \exists y_0 y_1 \dots (y_0 = \theta(x) \wedge \forall i Q(y_i, y_{i+1})).$$

Для завершения доказательства нужно только закодировать $y_0, y_1, \dots$ единственным элементом из $\mathcal{Y}$. Для этого предположим без потери общности, что

$$\mathcal{Y} = T^{(m-2)},$$

и положим

$$\varphi(\alpha^{m-2}, i) = [\alpha^{m-2}]_i = \lambda \alpha^{m-3} \alpha^{m-2} (\langle i, \alpha^{m-3} \rangle).$$

Тогда φ всюду определена и рекурсивна по Клини, и

$$\neg R(x) \Leftrightarrow \exists \alpha^{m-2} ([\alpha^{m-2}]_0 = \theta(x) \wedge \forall i Q([\alpha^{m-2}]_i, [\alpha^{m-2}]_{i+1})),$$

что и требовалось. $\square$

Предыдущий результат выполняется также для $R \in {}_{m+1} \text{ep}(F, {}^m E)$ — видоизменяем предшествующее доказательство (см. Московакис [1]), — но нам этот более сильный вариант не нужен. Заметим также, что если даже $m = 2$, приведенное доказательство показывает, что если например $R \in \omega$ и принадлежит ${}_{\text{ep}}({}^2 F, {}^2 E)$, то для некоторого $Q(m, n)$ такого, что $Q \in {}_1 \text{ep}(F, {}^2 E)$,

$$\neg R(x) \Leftrightarrow \exists \alpha (\alpha(0) = x \wedge \forall i Q(\alpha(i), \alpha(i+1))).$$

Из 19.1 мы теперь получаем

19.2. Следствие (Московакис [1]). Пусть $F = {}^m F$ — объект типа $m \geq 3$, и пусть $k \geq m-1$; тогда ${}_k \text{ep}(F, {}^m E)$ не замкнута относительно $\exists^{m-2}$.

Как применение 19.1 видим, что для любого $m \geq 3$ каждое точечное множество типа $\leq m-1$, полурекурсивное относительно ${}^m E$, является рекурсивным относительно ${}^m E^\#$, поскольку

$m-1\text{en}({}^mE^\#)$, очевидно, замкнуто относительно $\exists^{m-2}$. В частности,

$$m-1\text{en}({}^mE) \subseteq m-1\text{en}({}^mE^\#) \text{ для } m \geq 3.$$

Отрицательная верхняя граница из 19.2 для проблемы замкнутости оболочек относительно экзистенциальной квантификации оказывается наилучшей в свете следующего важного результата. Он был объявлен Грийо [3], но впервые корректно доказан Харрингтоном и Маккуином [1].

19.3. Теорема (Грийо [3], Харрингтон и Маккуин [1]). Пусть $F = {}^mF$ — объект типа $m \geq 2$. Тогда $m-1\text{en}(F, {}^mE)$ замкнуто относительно $\exists^l$ для любого $l < m-2$.

Доказательство 19.3 достаточно длинно и здесь не приводится. Одна из основных его составных частей — это опять использование теоремы 18.2 о представлении.

§ 20. Указания к литературе

Мы дали изложение элементарных частей теории рекурсии в высших типах. Для читателя, желающего продолжить изучение предмета сверх изложенного, советуем, что читать дальше. Мы попробуем покрыть в основном те аспекты рекурсии в высших типах, которые были введены в этой главе. Это заставляет нас пропустить некоторые очень интересные темы современных исследований, например теорию непрерывных объектов и функционалов.

По поводу оснований рекурсии в высших типах читатель может обратиться к работам Клини [1], [2] и Платека [1], а также Ганди [1], где в теорию вводятся фундаментальные понятия пошагового сравнения и селектора.

Большая часть ранних работ по этой теории была связана с построением и изучением различных иерархий для сечений объектов высших типов в духе гиперарифметической иерархии. Сюда относятся работы: Клини [2], Туге [1], Ганди [1], Шенфилд [1], Московакис [1], Грийо [2], Хинмен [1], и более современные — Вайнер [1], [2].

Позднее Сакс положил начало более глубокому изучению сечений, сосредоточенному особенно на влиянии типа объекта F на структуру его сечений. Он также изучал аналоги многих широко известных задач теории степеней неразрешимости, вроде проблемы Поста, для клиниевских степеней. Библиография здесь включает следующие работы: Сакс [1]—[3] (где доказывается плюс-один теорема), Маккуин [1], Харрингтон [1] и Сакс [4]. См. также Грийо [4].

Еще позже изучение структуры оболочек стало другой важной областью исследования в рекурсии в высших типах. По по-

воду этих недавних работ см. Московакис [3], Харрингтон [1] (где доказывается плюс-два теорема), Кекрис [1], Харрингтон и Кекрис [1] и Нурман [1].

В литературе имеется мало результатов об рекурсии относительно конкретных объектов высших типов, отличных от тех, которые мы уже упомянули в этой главе, например $F_Q, F_Q^\#$ для различных Q . Исключением является сверхскачок, который широко изучался; положим

$${}^3S(e, \alpha^2) = \begin{cases} 0, & \text{если } \{e\}(\alpha^2) \downarrow, \\ 1, & \text{если } \{e\}(\alpha^2) \uparrow \end{cases}$$

(Ганди [1]). Хотя ${}^3E \not\leq S$, рекурсия относительно S обладает многими интересными чертами; см. Ганди [1], Платек [2], Ацел и Хинмен [1], Харрингтон [1], [2], где изучаются также обобщения сверхскачка на более высокие чем 3 типы. Харрингтон [3], [4] ввел некоторые особенно интересные новые примеры нормальных функционалов, изучение которых выглядит многообещающим.

Возможно, наиболее важная открытая проблема этой теории является концептуальной, а именно связать рекурсию в высших типах с другими работами по основаниям и найти ей должное место внутри теории определмости. В статьях, указанных выше, имеются некоторые инициативы в этом направлении, но вопрос в целом еще широко открыт.

Благодарности

Авторы обязаны Л. Кироусису и П. Колаитису за многочисленные ценные комментарии и предложения по поводу более раннего варианта этой работы.

ЛИТЕРАТУРА

- Ацел (Aczel P.)
1. Representability in some systems of second order arithmetic. — Israel J. Math., 1970, 8, p. 309—328.
- Ацел и Хинмен (Aczel P., Hinman P. G.)
1. Recursion in the superjump. — In: Generalized Recursion Theory/Ed. J. E. Fenstad and P. G. Hinman. Amsterdam: North-Holland, 1974, p. 3—41.
- Вайнер (Wainer S.)
1. A hierarchy for the 1-section of any type-two object. — J. Symbolic Logic, 1974, 39, p. 88—95.
2. Some hierarchies based on higher type quantification. — In: Logic Colloquium '73/Ed. H. Rose and T. Shepherdson. Amsterdam: North-Holland, 1975, p. 305—316.
- Ганди (Gandy R. O.)
1. General recursive functionals of finite type and hierarchies of functionals. — Ann. Fac. Sci. Univ. Clermont-Ferrand, 1967, 35, p. 5—24.

- Грийо (Grilliot T. J.)
1. Recursive functions of finite higher types: Thesis. — Durham (North Carolina): Duke University, 1967.
 2. Hierarchies, based on objects of finite type. — J. Symbolic Logic, 1969, 34, p. 177—182.
 3. Selection functions for recursive functionals. — Notre Dame J. Formal Logic, 1969, 10, p. 225—234.
 4. On effectively discontinuous type-2 objects. — J. Symbolic Logic, 1971, 36, p. 245—248.
- Кекрис (Kechris A. S.)
1. The structure of envelopes: A survey of recursion theory in higher types. — M. I. T. Logic Seminar notes, 1973.
- Клини (Kleene S. C.)
1. Recursive functionals and quantifiers of finite type, I. — Trans. Amer. Math. Soc., 1959, 91, p. 1—52.
 2. Recursive functionals and quantifiers of finite type, II. — Trans. Amer. Math. Soc., 1963, 108, p. 106—142.
- Маккуин (MacQueen D.)
1. Post's problem for recursion in higher types: Thesis. — Cambridge (Mass.): M. I. T., 1972.
- Московакис (Moschovakis Y.)
1. Hyperanalytic predicates. — Trans. Amer. Math. Soc., 1967, 129, p. 249—282.
 2. Elementary Induction on Abstract Structures. — Amsterdam: North-Holland, 1974.
 3. Structural characterization of classes of relations. — In: Generalized Recursion Theory/Ed. J. E. Fenstad and P. G. Hinman. Amsterdam: North-Holland, 1974, p. 53—79.
 4. On the basic notions in the theory of induction. — In: Proceedings of the Fifth International Congress for Logic, Methodology and Philosophy of Science, London, Ontario, 1975. Reidel: Dordrecht, 1977, p. 207—236.
- Нурман (Normann D.)
1. Imbedding of higher type theories. — Preprint Series, 16. Oslo University, 1974.
- Платек (Platek R.)
1. Foundations of recursion theory: Thesis. — Stanford (Calif.): Stanford University, 1966.
 2. A countable hierarchy for the superjump. — In: Logic Colloquium '69/Ed. R. O. Gandy and C. E. M. Yates. Amsterdam: North-Holland, 1971, p. 257—271.
- Роджерс (Rogers H., Jr.)
1. Theory of Recursive Functions and Effective Computability. — N. Y.: McGraw-Hill, 1967. [Русский перевод: Роджерс Х. Теория рекурсивных функций и эффективная вычислимость. — М.: Мир, 1972.]
- Сакс (Sacks G. E.)
1. Recursion in objects of finite type. — In: Proceedings of the International Congress of Mathematicians. Paris: Gauthiers-Villars, 1971, p. 251—254.
 2. The 1-section of a type n object. — In: Generalized Recursion Theory/Ed. J. E. Fenstad and P. G. Hinman. Amsterdam: North-Holland, 1974, p. 81—93.
 3. The k -section of a type n object. — Amer. J. Math., 1977, 99, № 5, p. 901—918.
 4. RE Sets Higher up. — In: Proceedings of the Fifth International Congress for Logic, Methodology and Philosophy of Science, London, Ontario, 1975. Reidel: Dordrecht, 1977, p. 173—194.
- Туге (Tugué T.)

1. Predicates recursive in a type-2 object and Kleene hierarchies. — Comment. Math. Univ. St. Paul, 1960, 8, p. 97—117.
- Харрингтон (Harrington L. A.)
1. Contributions to recursion theory on higher types: Thesis. — Cambridge (Mass.): M. I. T., 1973.
 2. The superjump and the first recursively Mahlo ordinal. — In: Generalized Recursion Theory/Ed. J. E. Fenstad and P. G. Hinman. Amsterdam: North-Holland, 1974, p. 43—52.
 3. The superjump revisited. — Mimeographed notes, 1974.
 4. The Kolmogorov R -operator and the first non-projectible ordinal. — Mimeographed notes, 1975.
- Харрингтон и Кекрис (Harrington L. A., Kechris A. S.)
1. On characterizing Spector classes. — J. Symbolic Logic, 1975, 40, p. 19—24.
- Харрингтон и Маккуин (Harrington L. A., MacQueen D.)
1. Selection in abstract recursion theory. — J. Symbolic Logic, 1976, 41, p. 153—158.
- Хинмен (Hinman P. G.)
1. Hierarchies of effective descriptive set theory. — Trans. Amer. Math. Soc., 1969, 142, p. 111—140.
- Шенфилд (Shoenfield J. R.)
1. A hierarchy based on a type-2 object. — Trans. Amer. Math. Soc., 1968, 134, p. 103—108.

ВВЕДЕНИЕ В ТЕОРИЮ ИНДУКТИВНЫХ ОПРЕДЕЛЕНИЙ

Петер Ацел

СОДЕРЖАНИЕ

Введение	224
§ 1. Что такое индуктивные определения?	225
1.1. Индуктивные определения как обобщенные формальные системы (225). 1.2. Фундированная часть предиката (227). 1.3. Индуктивные определения как операторы (229). 1.4. Понятие «доказательство» для монотонной индукции (231). 1.5. Монотонная индукция и игры (233). 1.6. Ядра — объекты, дуальные к индуктивным определениям (233). 1.7. Некоторые примеры индукции в классической математике (235).	
§ 2. Индукция в теории рекурсии	236
2.1. Рекурсивно перечислимые предикаты (236). 2.2. Π^1_1 -предикаты (237). 2.3. Представимость (239).	
§ 3. Классы индуктивных определений	244
3.1. Общая схема (244). 3.2. Позитивная экзистенциальная индукция (246). 3.3. Позитивная элементарная индукция (249). 3.4. Релятивизация относительно нетривиального монотонного квантора (255). 3.5. Немонотонная индукция (257). 3.6. Индукция и допустимые множества (260).	
§ 4. Индукция в основаниях математики	264
Литература	266

Введение

Индуктивные определения множеств часто задаются неформально, при помощи некоторых правил для порождения элементов множества и добавления, что объект принадлежит множеству, если только он порождается в соответствии с этими правилами. Эквивалентной формулировкой будет характеристика указанного множества как наименьшего, замкнутого относительно этих правил.

Конечно, основным примером индуктивных определений является то, которое порождает натуральные числа. Однако индуктивные определения давно оказались полезным способом задания синтаксиса формального языка. Дальнейшие примеры их неформального использования можно найти в логике и других ветвях математики. Пост [1] осознал, что финитарные индуктивные определения, используемые при задании синтаксиса любой стандартной формальной системы, могут быть приведены к некоторой канонической форме, и общий класс таких индукций можно плодотворно изучать, абстрагируясь от каких бы то

ни было конкретных формальных систем. С того времени индуктивные определения играют важную роль в развитии обычной теории рекурсии и ее обобщений. В современных работах имеется тенденция представлять теорию индуктивных определений, абстрагируясь от исходных интуитивных мотивировок. Здесь нашей целью является дать введение в предмет, которое связало бы неформальные примеры с современными формулировками на языке итераций монотонных операторов. Мы ориентируемся на читателя, знакомого с понятием формальной системы и элементами обычной теории рекурсии.

Большая часть нашего изложения будет посвящена монотонной индукции и ее роли в расширениях теории рекурсии. Но в § 3.5 мы рассмотрим некоторые работы по немонотонной индукции и опишем независимые мотивировки, которые привели к ее развитию. В § 4 мы кратко рассмотрим индуктивные определения в более общем контексте. Детальное развитие теории позитивной индукции см. у Московакиса [1]. Несколько статей по индуктивной определимости можно найти в книге Фенстада и Хинмена [1]. Среди них есть обзор Ганди [1] и статьи Ондеро [1], Цензера [1], Рихтера и Ацела [1]. Московакис [3] дает абстрактный алгебраический подход к общей теории, который применим и к монотонной, и к немонотонной индукции, а также к рекурсии в вышних типах.

§ 1. Что такое индуктивные определения?

1.1. Индуктивные определения как обобщенные формальные системы. Индуктивные определения неоднократно используются, когда логики описывают синтаксис своих языков. Например, термы языка первого порядка определяются как наименьшее множество выражений, содержащее переменные и константы и замкнутое относительно правила образования термов:

Если $t_1, \dots, t_n$ суть термы и f есть n -арный функциональный символ языка, то выражение $f(t_1, \dots, t_n)$ есть терм.

Аналогично формулы языка первого порядка определяются как наименьшее множество выражений, содержащее атомные формулы и замкнутое относительно различных правил образования формул для логических символов $\neg, \vee, \wedge, \rightarrow, \exists x, \forall x$.

Пример, который наиболее полезно рассмотреть для наших целей — это определение класса теорем формальной системы. Рассмотрим систему $\mathbf{H}$ гильбертовского типа для логики первого порядка, использованную в главе 1 «Теории моделей». Множество $\text{Th}(\mathbf{H})$ теорем системы $\mathbf{H}$ определяется там через понятие «доказательства» в $\mathbf{H}$. Но $\text{Th}(\mathbf{H})$ может быть также охарактеризовано как наименьшее множество формул, содер-

жащее аксиомы и замкнутое относительно правил вывода. Каждый частный случай правила вывода имеет следующую форму:

(*) Из посылок θ для $\theta \in X$ следует заключение ψ .

В случае правила *modus ponens* X состоит из двух посылок φ и $(\varphi \rightarrow \psi)$. Частные случаи правила обобщения имеют только одну посылку. Удобно рассматривать схему аксиом как особую форму правила вывода, где в каждом частном случае множество посылок пусто. При помощи этого соглашения формальная система $\mathbf{H}$ определяет множество $\Phi_{\mathbf{H}}$ пар (X, ψ) таких, что (*) является частным случаем некоторого правила вывода системы $\mathbf{H}$. Тогда $\text{Th}(\mathbf{H})$ — это просто наименьшее множество, замкнутое относительно (*) для $(X, \psi) \in \Phi_{\mathbf{H}}$.

Обобщая, получаем следующие определения.

1.1.1. Определение. (i) *Правило* — это пара (X, x) , где X есть множество, называемое множеством *посылок*, и x — *заключение*. Правило обычно будет записываться как $X \rightarrow x$.

(ii) Если Φ — множество правил, то множество A называется Φ -замкнутым, если у каждого правила из Φ , посылки которого лежат в A , заключение также лежит в A . Будем писать $\Phi: X \rightarrow x$ для обозначения того, что правило $X \rightarrow x$ принадлежит Φ , так что A будет Φ -замкнуто, если $\Phi: X \rightarrow x \& X \subseteq A$ влечет $x \in A$.

(iii) Если Φ — множество правил, то $I(\Phi)$, множество, индуктивно определенное посредством Φ , — это

$$I(\Phi) = \bigcap \{A \mid A \text{ является } \Phi\text{-замкнутым}\}.$$

Замечание. Φ -замкнутые множества существуют, например множество всех заключений правил из Φ . Кроме того, пересечение любого семейства Φ -замкнутых множеств также Φ -замкнуто. В частности, $I(\Phi)$ является Φ -замкнутым, и, следовательно, $I(\Phi)$ есть наименьшее Φ -замкнутое множество.

Возвращаясь к нашему примеру, видим, что $\text{Th}(\mathbf{H}) = I(\Phi_{\mathbf{H}})$. Аналогично, легко найти множества правил для индуктивного определения множеств термов и формул языка первого порядка.

Замечание. То, что обычно называют правилом вывода или правилом образования, соответствует тому, что мы называем множеством правил, а частные случаи правил вывода или правил образования соответствуют тому, что мы назвали правилом.

По-видимому, наиболее знакомый пример индуктивного определения в математике — это характеристика множества натуральных чисел $\omega = \{0, 1, 2, \dots\}$ как наименьшего множества, содержащего 0 и замкнутого относительно функции следования, т. е. $\omega = I(\Phi_{\omega})$, где Φ_{ω} состоит из правила $0 \rightarrow 0$ и правил $\{n\} \rightarrow n+1$ для $n \in \omega$. Эта характеристика оправдывает принцип математической индукции: Если $\mathcal{P}$ есть свойство, которое

выполнено для 0 и выполнено для $n+1$, как только оно выполнено для n , то $\mathcal{P}$ выполняется для всех натуральных чисел, т. е. из того, что $\{n \in \omega \mid \mathcal{P}(n)\}$ является Φ_{ω} -замкнутым, следует, что $\omega \subseteq \{n \in \omega \mid \mathcal{P}(n)\}$.

Обобщая, видим, что для всякого множества правил Φ есть принцип Φ -индукции: Если $\mathcal{P}$ есть свойство такое, что $\mathcal{P}(x)$, как только $\Phi: X \rightarrow x$ и $\forall y \in X \mathcal{P}(y)$, то $\mathcal{P}(a)$ выполнено для всех $a \in I(\Phi)$.

Вышеописанный принцип — естественный инструмент для доказательства свойств множества $I(\Phi)$.

1.1.2. Пример. Для доказательства того, что каждая теорема из $\mathbf{H}$ универсально истинна в каждой алгебраической системе, достаточно показать, что для каждой алгебраической системы $\mathfrak{M}$

$$\{\varphi(v_1, \dots, v_n) \mid \mathfrak{M} \models \forall v_1 \dots \forall v_n \varphi(v_1, \dots, v_n)\}$$

является $\Phi_{\mathbf{H}}$ -замкнутым.

До сих пор все наши индуктивные определения были финитарны в том смысле, что каждое правило имело только конечное число посылок. Для таких Φ можно обобщить стандартное понятие «доказательства» для формальных систем таких, как $\mathbf{H}$.

1.1.3. Определение. $a_0, \dots, a_n$ есть Φ -доказательство для b (конечной длины), если:

(i) $a_n = b$,

(ii) для всех $m \leq n$ существует $X \subseteq \{a_i \mid i < m\}$ такое, что $\Phi: X \rightarrow a_m$.

1.1.4. Предложение. Для финитарных Φ

$$I(\Phi) = \{b \mid b \text{ имеет } \Phi\text{-доказательство}\}.$$

Чтобы показать, что каждый $b \in I(\Phi)$ имеет Φ -доказательство, достаточно показать, что правая часть Φ -замкнута, и использовать Φ -индукцию. Обратное, если $a_0, \dots, a_n$ есть Φ -доказательство, то достаточно показать индукцией по $m \leq n$, что $a_m \in I(\Phi)$.

1.2. Фундированная часть предиката. Пусть $<$ — бинарный предикат на множестве A . Фундированная часть $<$ — это множество $W(<)$ тех $a \in A$, что не существует бесконечной убывающей последовательности $a > a_0 > a_1 > \dots$. Предикат $<$ называется *фундированным предикатом*, если $A = W(<)$. $W(<)$ может быть определена индуктивно следующим образом: пусть $\Phi_{<} =$ множество правил $(<a) \rightarrow a$ для $a \in A$, где $(<a) = \{x \in A \mid x < a\}$.

1.2.1. Предложение. $W(<) = I(\Phi_{<})$.

Доказательство. Чтобы показать, что $I(\Phi_{<}) \subseteq W(<)$, достаточно показать, что $W(<)$ является $\Phi_{<}$ -замкнутой, и использовать $\Phi_{<}$ -индукцию. Поэтому предположим, что $(<a) \in$

$\subseteq W(<)$. Теперь если $a > a_0 > \dots$, то $a_0 \in (<a) \subseteq W(<)$. Но поскольку $a_0 > a_1 > \dots$, то $a_0 \notin W(<)$, что дает противоречие. Следовательно, $a \in W(<)$.

В обратную сторону, чтобы показать, что $W(<) \subseteq I(\Phi_{<})$, положим $a \notin I(\Phi_{<})$. Мы найдем последовательность $a > a_0 > a_1 > \dots$, показывающую, что $a \notin W(<)$. Поскольку $a \notin I(\Phi_{<})$, то $(<a) \notin I(\Phi_{<})$. Следовательно, существует $a_0 < a$ такой, что $a_0 \notin I(\Phi_{<})$. Повторяя это, можно найти $a_1 < a_0$ такой, что $a_1 \notin I(\Phi_{<})$. Продолжая до бесконечности, получаем $a > a_0 > a_1 > \dots$. $\square$

Заметьте, что здесь нужна некоторая форма аксиомы выбора (аксиома зависимого выбора).

Принцип $\Phi_{<}$ -индукции в случае фундированности $<$ становится принципом трансфинитной индукции по фундированному предикату. С трансфинитной индукцией связан метод определения по трансфинитной рекурсии. Он позволяет определить единственную функцию f на $W(<)$ такую, что для $a \in W(<)$ $f(a)$ определяется через $f(x)$ для $x < a$. Единственность и существование такой f могут быть проверены подходящими частными случаями трансфинитной индукции. В качестве примера можно приписать каждому $a \in W(<)$ ординал $|a|_{<}$ такой, что

$$|a|_{<} = \sup \{ |x|_{<} + 1 \mid x < a \}.$$

Ординал $|<|$ фундированной части предиката $<$ определяется так:

$$|<| = \sup \{ |a|_{<} + 1 \mid a \in W(<) \}.$$

Индуктивное определение часто может быть перефразировано к виду $\Phi_{<}$ для подходящего $<$.

1.2.2. Определение. Множество правил Φ называется *детерминированным*, если

$$\Phi: X_1 \rightarrow x \ \& \ \Phi: X_2 \rightarrow x \text{ влечет } X_1 = X_2.$$

1.2.3. Пример. $\Phi_{<}$ и Φ_{ω} всегда детерминированы. Таковы же множества правил, определяющие термы и формулы логики первого порядка.

Заметьте, что Φ_n не является детерминированным.

Теперь пусть Φ будет детерминированным, и пусть A будет множеством заключений всех правил из Φ . Для $x, y \in A$ пусть $x < y$, если $\Phi: X \rightarrow y$ для некоторого множества X такого, что $x \in X$ и $X \subseteq A$. Тогда $\Phi_{<}$ — это множество правил $X \rightarrow x$ из Φ таких, что $X \subseteq A$. Следовательно, получаем

1.2.4. Предложение. Для детерминированных Φ

$$I(\Phi) = I(\Phi_{<}).$$

Для детерминированных Φ функции на $I(\Phi)$ могут определяться рекурсией по способу порождения объектов из $I(\Phi)$, как при трансфинитной рекурсии. Таким примером из синтаксиса является операция подстановки. Для данных предметной переменной v и терма t естественным образом рекурсией по способу построения формулы $\varphi(v)$ определяется функция, ставящая в соответствие формуле $\varphi(v)$ формулу $\varphi(t)$, получаемую подстановкой t вместо всех свободных вхождений v в формулу $\varphi(v)$.

1.3. Индуктивные определения как операторы. Пусть $\varphi: \text{Pow}(A) \rightarrow \text{Pow}(A)$, где $\text{Pow}(A)$ обозначает множество всех подмножеств множества A . Оператор φ *монотонный*, если $X \subseteq Y \subseteq A$ влечет, что $\varphi(X) \subseteq \varphi(Y)$. Для данного φ пусть Φ_{φ} будет множеством правил $X \rightarrow x$ таких, что $X \subseteq A$ и $x \in \varphi(X)$. Для монотонных φ $X \subseteq A$ будет Φ_{φ} -замкнуто в точности тогда, когда $\varphi(X) \subseteq X$. Поэтому $I(\Phi_{\varphi}) = \bigcap \{ X \subseteq A \mid \varphi(X) \subseteq X \}$. Следовательно, естественно расширить терминологию об индуктивных определениях на монотонные операторы φ , и мы пишем $I(\varphi)$ вместо $\bigcap \{ X \subseteq A \mid \varphi(X) \subseteq X \}$ и называем это множество множеством, *индуктивно определенным посредством* φ . Все индуктивные определения можно получить, используя монотонные операторы. Действительно, если Φ — множество правил на A (т. е. $X \cup \{x\} \subseteq A$ для всех $\Phi: X \rightarrow x$), то мы можем определить монотонный оператор $\varphi: \text{Pow}(A) \rightarrow \text{Pow}(A)$ так:

$$\varphi(Y) = \{ x \in A \mid \Phi: X \rightarrow x \text{ для некоторого } X \subseteq Y \} \text{ для } Y \subseteq A.$$

Тогда $Y \subseteq A$ будет Φ -замкнуто в точности тогда, когда $\varphi(Y) \subseteq Y$ так что $I(\Phi) = I(\varphi)$.

Для монотонных операторов φ есть полезная альтернативная характеристика множества $I(\varphi)$, использующая трансфинитные итерации φ^{λ} оператора φ для ординалов λ . Определим $\varphi^{\lambda} \subseteq A$ трансфинитной рекурсией по ординалу λ так:

$$\varphi^{\lambda} = \bigcup_{\mu < \lambda} \varphi^{\mu} \cup \varphi \left(\bigcup_{\mu < \lambda} \varphi^{\mu} \right).$$

Определим также $\varphi^{\infty} = \bigcup_{\lambda} \varphi^{\lambda}$, где λ пробегает все ординалы.

Если писать $\varphi^{<\lambda}$ вместо $\bigcup_{\mu < \lambda} \varphi^{\mu}$, то

$$\varphi^{\lambda} = \varphi^{<\lambda} \cup \varphi(\varphi^{<\lambda}).$$

Множества $\varphi^{<\lambda}$ могут быть непосредственно определены трансфинитной рекурсией

$$\varphi^{<\lambda} = \bigcup_{\mu < \lambda} \varphi(\varphi^{<\mu}),$$

или иначе

$$\begin{aligned}\varphi^{<0} &= \emptyset, \quad \varphi^{<\lambda+1} = \varphi^{<\lambda} \cup \varphi(\varphi^{<\lambda}), \\ \varphi^{<\lambda} &= \bigcup_{\mu < \lambda} \varphi^{<\mu} \text{ для предельных } \lambda.\end{aligned}$$

Затем можно определить $\varphi^\lambda = \varphi^{<\lambda+1}$.

Замечание. В литературе часто используется обозначение φ^λ вместо того, что мы обозначили $\varphi^{<\lambda}$. Мы приняли обозначения, введенные Московакисом [1].

Поскольку $X \subseteq I(\varphi)$ влечет $\varphi(X) \subseteq I(\varphi)$, трансфинитная индукция показывает, что $\varphi^\lambda \subseteq I(\varphi)$ для всех ординалов λ . Следовательно, если положить $\varphi^\infty = \bigcup_\lambda \varphi^\lambda$, то $\varphi^\infty \subseteq I(\varphi)$.

Поскольку из $\mu < \lambda$ следует $\varphi^{<\mu} \subseteq \varphi^{<\lambda} \subseteq A$, и A есть множество, то существует ординал $\bar{\lambda}$ такой, что $\varphi^{<\bar{\lambda}+1} = \varphi^{<\bar{\lambda}}$. Отсюда следует, что $\varphi^\lambda = \varphi^{\bar{\lambda}} = \varphi^{<\bar{\lambda}}$ для всех $\lambda \geq \bar{\lambda}$, так что $\varphi^\infty = \varphi^{<\bar{\lambda}}$. Поэтому $\varphi(\varphi^\infty) = \varphi(\varphi^{<\bar{\lambda}}) \subseteq \varphi^{\bar{\lambda}} = \varphi^\infty$. Следовательно, по φ -индукции $I(\varphi) \subseteq \varphi^\infty$. Для монотонных φ также $\mu < \lambda$ влечет $\varphi(\varphi^{<\mu}) \subseteq \varphi(\varphi^{<\lambda})$, так что $\varphi^{<\lambda} = \bigcup_{\mu < \lambda} \varphi(\varphi^{<\mu}) \subseteq \varphi(\varphi^{<\lambda})$, и, следовательно, $\varphi^\lambda = \varphi(\varphi^{<\lambda})$. Отсюда следует, что $\varphi^\infty = \varphi(\varphi^\infty)$, φ^∞ является неподвижной точкой φ (в действительности наименьшей). Таким образом, мы доказали

1.3.1. Предложение. Для монотонных $\varphi: \text{Row}(A) \rightarrow \text{Row}(A)$:

(i) $I(\varphi) = \varphi^\infty$;

(ii) $I(\varphi)$ является наименьшей неподвижной точкой φ .

Данное определение φ^∞ не требует монотонности оператора φ . Следовательно, естественно расширить понятие индуктивного определения на немонотонные операторы, назвав φ^∞ множеством, индуктивно определенным посредством φ , для любого оператора $\varphi: \text{Row}(A) \rightarrow \text{Row}(A)$. Оказалось, возможно несколько неожиданно, что теория немонотонных индуктивных определений столь же богата и интересна, как и теория монотонных операторов, хотя естественно возникающие примеры немонотонных индукций труднее найти. Вероятно, их главная мотивировка может быть обнаружена в системах обозначений для ординалов. С каждым оператором $\varphi: \text{Row}(A) \rightarrow \text{Row}(A)$ связана функция $|\cdot|_\varphi$, отображающая φ^∞ в начальный сегмент ординалов, задаваемая так:

$|a|_\varphi$ — наименьшему λ такому, что $a \in \varphi^\lambda$ для $a \in \varphi^\infty$.

Пусть $|\varphi| = \sup\{|a|_\varphi + 1 \mid a \in \varphi^\infty\}$. Тогда φ^∞ есть система обозначений для ординалов $< |\varphi|$ посредством отображения $|\cdot|_\varphi: \varphi^\infty \rightarrow |\varphi|$. (Заметьте, что мы следуем стандартному соглаше-

нию об отождествлении ординала с множеством ему предшествующих.) Этот ординал может быть также охарактеризован как наименьший ординал $\bar{\lambda}$ такой, что $\varphi^\lambda = \varphi^{<\bar{\lambda}}$. Следовательно, $\varphi^\infty = \varphi^{|\varphi|} = \varphi^{<|\varphi|}$.

1.3.2. Пример. Пусть $<$ — бинарный предикат на множестве A , и пусть φ — монотонный оператор, соответствующий множеству правил $\Phi_{<}$, так что $W(<) = I(\varphi) = \varphi^\infty$. Тогда легко видеть, что $\varphi^\lambda = \{a \in W(<) \mid |a|_\varphi \leq \lambda\}$, так что $|a|_\varphi = |a|_{<}$ для $a \in W(<)$ и $|\varphi| = |<|$.

Интересной общей проблемой, связанной с оператором $\varphi: \text{Row}(A) \rightarrow \text{Row}(A)$, является характеристика или оценка ординала $|\varphi|$. Поскольку $|\cdot|_\varphi: \varphi^\infty \rightarrow |\varphi|$ сюръективно и $\varphi^\infty \subseteq A$, мощность $|\varphi|$ должна быть меньше или равна мощности множества A .

Для монотонных операторов часто может быть найдена лучшая оценка. Если κ — кардинал, то будем говорить, что φ является κ -базируемым, если

$x \in \varphi(X)$ влечет $x \in \varphi(Y)$ для некоторого $Y \subseteq X$ мощности $< \kappa$.

1.3.3. Пример. Если Φ — финитарное множество правил на A , то монотонный оператор, ему соответствующий, является ω -базируемым. В общем случае, если множество посылок любого правила из Φ имеет мощность $< \kappa$, то φ является κ -базируемым.

1.3.4. Предложение. Пусть φ — κ -базируемый монотонный оператор, где κ — регулярный кардинал. Тогда $|\varphi| \leq \kappa$, так что $I(\varphi) = \varphi^\kappa$.

Доказательство. Достаточно показать, что $\varphi^\kappa \subseteq \varphi^{<\kappa}$. Поэтому пусть $x \in \varphi^\kappa = \varphi(\varphi^{<\kappa})$. Тогда $x \in \varphi(X)$ для некоторого $X \subseteq \varphi^{<\kappa}$ мощности $< \kappa$. По регулярности κ $X \subseteq \varphi^{<\lambda}$ для некоторого $\lambda < \kappa$, так что $x \in \varphi(\varphi^{<\lambda}) = \varphi^\lambda \subseteq \varphi^{<\kappa}$, что и требовалось. $\square$

1.3.5. Пример. Если Φ — финитарное множество правил, которому соответствует оператор φ , то $|\varphi| \leq \omega$ и $I(\varphi) = \varphi^{<\omega} = \bigcup_{n < \omega} \varphi^{<n}$, где $\varphi^{<0} = \emptyset$ и $\varphi^{<n+1} = \varphi(\varphi^{<n})$ для $n < \omega$.

1.4. Понятие «доказательство» для монотонной индукции. В 1.3.3 мы сформулировали понятие доказательства конечной длины, соответствующее финитарным множествам правил. Теперь мы рассмотрим более общее понятие.

1.4.1. Определение. Пусть φ — монотонный оператор на A . Трансфинитная последовательность $\{a_\mu\}_{\mu < \lambda}$ называется φ -доказательством для b длины λ , если:

(i) $a_\lambda = b$;

(ii) $a_\nu \in \varphi(\{a_\mu \mid \mu < \nu\})$ для всех $\nu \leq \lambda$.

Как и в предложении 1.1.4, мы получаем

1.4.2. Предложение. (i) Для любого регулярного кардинала κ имеем

$$\varphi^{<\kappa} = \{a \in A \mid a \text{ обладает } \varphi\text{-доказательством длины } < \kappa\};$$

(ii) $I(\varphi) = \{a \in A \mid a \text{ обладает } \varphi\text{-доказательством}\}.$

Иногда удобно использовать иное понятие доказательства, использующее фундированные деревья вместо трансфинитных последовательностей. Примером является понятие вывода для системы генценовского типа **G** из главы 1 «Теории моделей». Соответствующее ей множество правил финитарно, так что фундированные деревья являются в действительности конечными.

1.4.3. Определение. (Фундированным) деревом T называется множество конечных последовательностей длины > 0 таких, что:

(i) Существует в точности одна последовательность единичной длины в T . Она называется *корнем* (a_T) этого дерева.

(ii) Если $(a_1, \dots, a_{n+1}) \in T$, то $(a_1, \dots, a_n) \in T$.

(iii) T фундировано в том смысле, что не существует бесконечной последовательности $a_1, a_2, \dots$ такой, что $(a_1, \dots, a_n) \in T$ для всех $n > 0$. Иначе говоря, предикат $<_T$ фундирован, где

$(a_1, \dots, a_n) <_T (b_1, \dots, b_m)$ тогда и только тогда, когда $n = m + 1$ и $a_i = b_i$ для $i = 1, \dots, m$.

Определим длину $|T|$ дерева T как $|a_T|_{<_T}$.

1.4.4. Определение. Если Φ — множество правил, то дерево T является Φ -доказательством для a , если $a = a_T$ и $\Phi: T_{(a_1, \dots, a_n)} \rightarrow a_n$, как только $(a_1, \dots, a_n) \in T$, где

$$T_{(a_1, \dots, a_n)} = \{a \mid (a_1, \dots, a_n, a) \in T\}.$$

1.4.5. Предложение. (i) $I(\Phi) = \{a \mid a \text{ обладает } \Phi\text{-доказательством в виде дерева}\}.$

(ii) Если Φ — множество правил на A , которому соответствует монотонный оператор $\varphi: \text{Pow}(A) \rightarrow \text{Pow}(A)$, то для всех ординалов λ

$$\varphi^\lambda = \{a \in A \mid a \text{ обладает } \Phi\text{-доказательством в виде дерева длины } \leq \lambda\}.$$

Доказательство. (i) легко вытекает из (ii). (ii) будет доказано индукцией по λ . Пусть X^λ обозначает правую часть (ii), и положим $X^{<\lambda} = \bigcup_{\mu < \lambda} X^\mu$. По индукционному предположению $\varphi^{<\lambda} = X^{<\lambda}$.

Пусть $a \in X^\lambda$. Тогда a обладает Φ -доказательством T таким, что $|T| \leq \lambda$. Для каждого $x \in T_{(a)}$ положим

$$T^x = \{(x, x_1, \dots, x_n) \mid n \geq 0 \text{ и } (a, x, x_1, \dots, x_n) \in T\}.$$

Тогда T^x является Φ -доказательством для x таким, что $|T^x| < \lambda$. Следовательно, $T_{(a)} \subseteq X^{<\lambda} = \varphi^{<\lambda}$. Из того, что $\Phi: T_{(a)} \rightarrow a$, следует, что $a \in \varphi(\varphi^{<\lambda}) = \varphi^\lambda$. Наоборот, пусть $a \in \varphi^\lambda$. Тогда $a \in \varphi(X^{<\lambda})$. Для каждого $x \in X^{<\lambda}$ пусть T^x будет Φ -доказательством для x таким, что $|T^x| < \lambda$. Положим

$$T = \{(a)\} \cup \{(a, x, x_1, \dots, x_n) \mid n \geq 0 \text{ и } x \in X^{<\lambda} \text{ и } (x, x_1, \dots, x_n) \in T^x\}.$$

Тогда T является Φ -доказательством для a таким, что $|T| \leq \lambda$, так что $a \in X^\lambda$. $\square$

1.5. Монотонная индукция и игры. Для тех, кто знаком с простейшими понятиями, связанными с играми, дадим теоретико-игровую характеристику множества $I(\Phi)$ для произвольного множества правил Φ .

Для каждого a определяем игру $G(\Phi, a)$ между двумя игроками — I и II, которые делают ходы поочередно до тех пор, пока это возможно. Игра начинается тем, что II выбирает $a_0 = a$. Если после n пар ходов игрок II выбирает a_n , то игрок I должен ответить, выбрав множество X_n такое, что $\Phi: X_n \rightarrow a_n$, и тогда II должен ответить, выбрав $a_{n+1} \in X_n$. Если какой-либо из игроков не может сделать ход, он проигрывает. Если игра длится до бесконечности, то проигрывает игрок I.

1.5.1. Предложение. $a \in I(\Phi)$ тогда и только тогда, когда игрок I имеет выигрышную стратегию в игре $G(\Phi, a)$.

Доказательство. Пусть W будет множеством тех a , для которых выполнена правая часть формулировки предложения. Пусть $\Phi: X \rightarrow a$ и $X \subseteq W$. Для каждого $x \in X$ пусть σ_x будет выигрышной стратегией для I в игре $G(\Phi, x)$. Определим следующую стратегию σ для I в игре $G(\Phi, a)$. Игрок I начинает, выбирая X , и если затем II выбирает $x \in X$, то I продолжает, используя стратегию σ_x . Ясно, что σ — выигрышная стратегия. Следовательно, $a \in W$. Таким образом, W является Φ -замкнутым, так что по Φ -индукции $I(\Phi) \subseteq W$.

Обратно, пусть $a \in W$. Пусть σ будет выигрышной стратегией для I в игре $G(\Phi, a)$. Пусть T будет множеством всех возможных конечных последовательностей ходов игрока II, когда I следует стратегии σ . Теперь заметим, что T является Φ -доказательством для a в виде дерева, так что по предложению 1.4.5 $a \in I(\Phi)$. Таким образом, $W \subseteq I(\Phi)$. $\square$

1.6. Ядра — объекты, дуальные к индуктивным определениям. Иногда индуктивные определения появляются более естественно в дуальной форме.

Если Φ — множество правил, то будем говорить, что множество X является Φ -плотным, если для каждого $x \in X$ найдется множество $Y \subseteq X$ такое, что $\Phi: Y \rightarrow x$. Определим ядро $K(\Phi) = \bigcup \{X \mid X \text{ является } \Phi\text{-плотным}\}$. $K(\Phi)$ в свою очередь является Φ -плотным и является наибольшим Φ -плотным множеством. Если Φ — множество правил на A и $\varphi: \text{Pow}(A) \rightarrow \text{Pow}(A)$ — монотонный оператор, связанный с Φ , то $X \subseteq A$ будет Φ -плотным тогда и только тогда, когда $X \subseteq \varphi(X)$. Следовательно, $K(\Phi) = \bigcup \{X \subseteq A \mid X \subseteq \varphi(X)\}$, и мы определим $K(\varphi) = \bigcup \{X \subseteq A \mid X \subseteq \varphi(X)\}$ для любого монотонного φ . Чтобы сделать явной двойственность между конструкцией ядра и индукцией, определим $\check{\varphi}$ — оператор, дуальный к оператору φ , посредством $\check{\varphi}(X) = \bigcap \varphi(\bigcap X)$, где $\bigcap X = A - X$ при $X \subseteq A$. Тогда $X \subseteq A$ будет φ -плотным в том и только в том случае, когда $\bigcap X$ является $\check{\varphi}$ -замкнутым, так что $K(\varphi) = \bigcap I(\check{\varphi})$. Следовательно, $K(\varphi)$ может быть определено при помощи трансфинитных итераций $\varphi^{[\lambda]} = \bigcap \varphi^\lambda$, поскольку $K(\varphi) = \bigcap_\lambda \varphi^{[\lambda]}$, где $\varphi^{[\lambda]} = \varphi(\bigcap_{\mu < \lambda} \varphi^{[\mu]})$.

Иллюстрацией этого является конструкция Кантора — Бендиксона в общей топологии. Пусть E будет подмножеством топологического пространства. Пусть Φ будет множеством правил $X \rightarrow x$ таких, что $X \subseteq E$, а $x \in E$ и является предельной точкой X . Соответствующий монотонный оператор $\varphi: \text{Pow}(E) \rightarrow \text{Pow}(E)$ — это операция замыкания на E . Множество $X \subseteq E$ замкнуто в E в точности в том случае, когда X Φ -замкнуто, и плотно в себе в случае, когда оно Φ -плотно. Таким образом, $K(\varphi)$ является наибольшим плотным в себе подмножеством E , называемым ядром K множества E . Если E является замкнутым подмножеством пространства со счетным базисом, то $E = K \cup S$, где K совершенно, а $S = \bigcap I(\check{\varphi})$ — счетное множество, так что ординал замыкания $|\varphi|$ должен быть счетным. Это — представление Кантора — Бендиксона замкнутых подмножеств пространства со счетным базисом.

Другой пример конструкции ядра взят из теории абелевых p -групп. Это такие группы, в которых каждый элемент имеет конечный порядок p^n для некоторого n , где p — фиксированное простое число. Пусть G будет абелевой p -группой. Определим $\varphi: \text{Pow}(G) \rightarrow \text{Pow}(G)$ так:

$$\varphi(X) = pX = \{ \underbrace{g + \dots + g}_p \mid g \in X \} \text{ для } X \subseteq G.$$

Тогда φ является монотонным оператором, отображающим подгруппы G в подгруппы G . φ -плотные подгруппы G — это в точности те, которые называются делимыми, так что $K(\varphi)$ является наибольшей делимой подгруппой G . Большая часть структурной теории абелевых p -групп связана с убывающей иерархией подгрупп $\{\varphi^{[\lambda]}\}_\lambda$.

1.7. Некоторые примеры индукции в классической математике.

(1) Если X — подмножество группы G , то существует наименьшая подгруппа H группы G , содержащая X . H индуктивно определена множеством правил $\emptyset \rightarrow x$ для $x \in X \cup \{e\}$ и $\{a, b\} \rightarrow ab^{-1}$ для $a, b \in G$. То же самое понятие используется с другими алгебраическими системами такими, как кольца, поля и векторные пространства. Несколько другим вариантом этого примера является алгебраическое замыкание подполя алгебраически замкнутого поля. Все эти примеры используют финитные множества правил.

(2) Если R является бинарным предикатом на множестве A , то транзитивное замыкание $\bar{R}$ — это наименьший транзитивный предикат, продолжающий R . Он определяется индуктивно множеством правил $\emptyset \rightarrow (a, b)$, если aRb , и $\{(a, b), (b, c)\} \rightarrow (a, c)$ для $a, b, c \in A$. Аналогично, отношение эквивалентности, порожденное R , индуктивно определяется уже написанными правилами и правилами $\emptyset \rightarrow (a, a)$ для $a \in A$ и $\{(a, b)\} \rightarrow (b, a)$ для $a, b \in A$.

(3) За примером нефинитарного индуктивного определения обратимся к σ -кольцам и борелевским множествам. Напомним, что множество $\mathcal{C} \subseteq \text{Pow}(A)$ является σ -кольцом, если оно замкнуто относительно взятия дополнений и счетных объединений подмножеств, т. е., соединяя это в одно, говорим, что $\mathcal{C}$ является σ -кольцом, если $\mathcal{C}$ является Φ -замкнутым, где Φ состоит из правил $\{A_n \mid n \in \omega\} \rightarrow \bigcup_{n < \omega} A_n$ для счетных семейств $\{A_n\}_{n < \omega}$, где $A_n \subseteq A$. Следовательно, σ -кольцо, порожденное $\mathcal{C}_0 \subseteq \text{Pow}(A)$, индуктивно определено посредством множества правил Φ' , состоящего из Φ и правил $\emptyset \rightarrow X$ для $X \in \mathcal{C}_0$. Например, борелевские множества вещественных чисел — это случай, когда $A = \mathbb{R}$ и $\mathcal{C}_0$ — семейство открытых подмножеств $\mathbb{R}$. Если $\varphi: \text{Pow}(A) \rightarrow \text{Pow}(A)$ является монотонным оператором, связанным с Φ' , то φ является $\aleph_1$ -базируемым, так что по предложению 1.3.4 $|\varphi| \leq \aleph_1$. Классы φ^λ для $\lambda < \aleph_1$ — это в точности знакомые уровни борелевской иерархии. φ^0 — множество открытых множеств и для $\lambda > 0$ множества из φ^λ — это множества, имеющие вид $\bigcup_{n < \omega} \bigcap A_n$, где все $A_n \in \varphi^{<\lambda}$.

§ 2. Индукция в теории рекурсии

2.1. Рекурсивно перечислимые предикаты Имеется два главных результата, связывающих рекурсивно перечислимые (р. п.) предикаты и конечно определенные формальные системы такие, как формальная арифметика:

(I) Теоремы конечно определенных формальных систем образуют р. п. множество при гёделевой нумерации.

(II) Каждый р. п. предикат может быть представлен в любой достаточно богатой формальной системе.

Эти результаты важны для теоремы Гёделя о неполноте. Общее понятие представимости будет рассмотрено в п. 2.3. Здесь мы хотим дать один результат об индуктивных определениях, который влечет (I).

Как мы видели, формальная система определяет множество правил, при помощи которых индуктивно определяется множество теорем. Если задать гёделеву нумерацию выражений, то на ω индуцируется множество правил, которое индуктивно определяет множество гёделевых номеров теорем. Если формальная система конечно определена, то это множество правил будет рекурсивным финитарным множеством, как определено ниже.

2.1.1. Определение. Пусть Φ будет финитарным множеством правил на ω . Φ рекурсивно (р. п.), если предикат R_Φ рекурсивен (р. п.), где R_Φ — это множество пар $\langle \langle a_1, \dots, a_n \rangle, b \rangle$ таких, что $\Phi: \{a_1, \dots, a_n\} \rightarrow b$.

Здесь $\langle \rangle: \bigcup_{n \in \omega} \omega^n \rightarrow \omega$ — это стандартная конструктивная инъективная кодирующая функция для конечных последовательностей натуральных чисел. С нею связаны рекурсивные функции $lh: \omega \rightarrow \omega$ и $q: \omega \times \omega \rightarrow \omega$, которые удовлетворяют следующим условиям:

- (i) Область значений Seq функции $\langle \rangle$ рекурсивна.
- (ii) Для каждого $n > 0$ функция $\langle \rangle \upharpoonright \omega^n: \omega^n \rightarrow \omega$ рекурсивна.
- (iii) $lh \langle x_1, \dots, x_n \rangle = n$ для $n \geq 0$.
- (iv) $q \langle x_1, \dots, x_n \rangle, i = x_i$ для $1 \leq i \leq n$.

2.1.2. Предложение. Если Φ — р. п. финитарное множество правил на ω , то $I(\Phi)$ является р. п.

Доказательство. Поскольку Φ финитарно, то по предположению 1.1.4

$$I(\Phi) = \{a \in \omega \mid \exists y \text{ Pr}_\Phi(a, y)\},$$

где $\text{Pr}_\Phi(a, b)$ тогда и только тогда, когда $b = \langle a_1, \dots, a_n \rangle$ для некоторого Φ -доказательства $a_1, \dots, a_n$ для b . Следовательно, чтобы доказать предложение, достаточно показать, что Pr_Φ

является р. п., а здесь дело сводится к кодированию:

$$\text{Pr}_\Phi(a, b) \iff \text{Seq}(b) \wedge q(b, lh(b)) = a$$

$$\wedge \forall i < lh(b) \exists z [R_\Phi(z, q(b, i + 1))$$

$$\wedge \forall i < lh(z) \exists k < i (q(z, i + 1) = q(x, k + 1)).$$

По предположению, R_Φ р. п., и, используя стандартные свойства замкнутости р. п. предикатов, видим, что правая часть эквивалентности р. п. $\square$

2.2. Π_1^1 -предикаты. Если в формальной системе допускаются бесконечные правила вывода, то требуются более общие понятия индукции; например, в статье Гжегорчика, Мостовского и Рыль-Нардзевского [1] добавляется ω -правило к формальной системе арифметики второго порядка, которая в остальном является конечно определенной. ω -правило позволяет вывести $\forall x \varphi(x)$ из бесконечного множества посылок $\varphi(0), \varphi(1), \dots$ При гёделевой нумерации такая формальная система индуцирует регулярно арифметическое множество правил Φ на ω .

2.2.1. Определение. Множество правил Φ на ω называется регулярно арифметическим, если существуют арифметические предикаты R и S такие, что Φ является множеством правил $R_a \rightarrow b$ таких, что $S(a, b)$; здесь $R_a = \{y \in \omega \mid R(a, y)\}$.

2.2.2. Предложение. (i) Если Φ — регулярно арифметическое множество правил на ω , то соответствующий монотонный оператор $\varphi: \text{Pow}(\omega) \rightarrow \text{Pow}(\omega)$ есть Π_1^1 -оператор, т. е. $\{(X, x) \in \text{Pow}(\omega) \times \omega \mid x \in \varphi(X)\}$ является Π_1^1 -множеством.

(ii) Для всякого монотонного Π_1^1 -оператора φ множество $I(\varphi)$ также является Π_1^1 -множеством.

Доказательство. (i) Пусть Φ будет множеством правил $R_a \rightarrow b$ таких, что $S(a, b)$, где R и S арифметические. Тогда соответствующий монотонный оператор φ задается посредством $\varphi(X) = \{b \in \omega \mid \exists a [S(a, b) \wedge R_a \subseteq X]\}$ для $X \subseteq A$. φ является арифметическим и, следовательно, Π_1^1 -оператором.

(ii) $I(\varphi) = \{a \in \omega \mid \forall X [\forall x [x \in \varphi(X) \rightarrow x \in X] \rightarrow a \in X]\}$, так что, если φ есть Π_1^1 -оператор, то стандартные манипуляции с кванторами показывают, что $I(\varphi)$ также является Π_1^1 -множеством. $\square$

Следовательно, это предложение подсказывает, что при рассмотрении систем ω -правилом класс всех р. п. предикатов в (I) и (II) из 2.1 должен быть заменен на класс всех Π_1^1 -предикатов.

Ниже мы даем еще два примера регулярно арифметических множеств правил.

Первый пример возникает при определении клиниевской системы обозначений для рекурсивных ординалов. Она может быть задана следующим образом. Пусть $<$ будет наименьшим транзитивным предикатом на ω таким, что:

- (i) $a < 2^a$ для $a \in \omega$,
- (ii) $\{e\}(n) < 3 \cdot 5^e$ для $e, n \in \omega$ таких, что $\{e\}(n)$ определено. (Здесь $\{e\}$ — это e -я частично рекурсивная функция при стандартной нумерации.) Тогда $<$, как легко видеть, является р. п. предикатом. Пусть теперь Φ будет множеством правил $\emptyset \rightarrow 1$, $\{a\} \rightarrow 2^a$ для $a \in \omega$, и $\{\{e\}(n) | n < \omega\} \rightarrow 3 \cdot 5^e$ для $e \in \omega$ таких, что $\{e\}(n)$ определена и $\{e\}(n) < \{e\}(n+1)$ для всех $n \in \omega$. Теперь положим $\mathcal{O} = I(\Phi)$. Пусть $a <_0 b$, если и только если $a, b \in \mathcal{O}$ & $a < b$. Поскольку Φ регулярно арифметическое, то $\mathcal{O}$ и, следовательно, $<_0$ являются Π_1^1 -множествами. Для $a \in \mathcal{O}$ положим $|a|_0 = |a|_\Phi$. Тогда $|1|_0 = 0$, $|2^a|_0 = |a|_0 + 1$ для $a \in \mathcal{O}$ и $|3 \cdot 5^e|_0 = \lim_{n \in \omega} |\{e\}(n)|_0$ для $3 \cdot 5^e \in \mathcal{O}$. Таким образом $(\mathcal{O}, <_0, |\cdot|_0)$ является клиниевским рекурсивным аналогом счетных ординалов. Ординал $|\Phi| = \text{Sup}\{|a|_0 + 1 | a \in \mathcal{O}\}$ — это ординал Чёрча — Клини ω_1 , первый допустимый ординал $> \omega$.

В качестве другого примера регулярно арифметической индукции рассмотрим гиперарифметическую иерархию, как она сформулирована в книге Московакиса [1]. Она является рекурсивным аналогом борелевской иерархии. Назовем множество $\mathcal{R} \subseteq \text{Pow}(\omega)$ *эффективным σ -кольцом*, если $\mathcal{R}$ эффективно содержит р. п. множества и эффективно замкнуто относительно дополнений и счетных объединений. А именно, существует множество $I \subseteq \omega$ и множества $B_i \subseteq \omega$ для $i \in I$ такие, что $\mathcal{R} = \{B_i | i \in I\}$ и:

- (i) Существует рекурсивная функция $\tau_1: \omega \rightarrow I$ такая, что $R_e = B_{\tau_1(e)}$ для всех $e \in \omega$. (Напомним, что R_e является e -м р. п. множеством при стандартной нумерации.)
- (ii) Существует рекурсивная функция $\tau_2: \omega \rightarrow \omega$ такая, что если $\{e\}$ является всюду определенной функцией $f: \omega \rightarrow I$, то

$$\tau_2(e) \in I \text{ и } B_{\tau_2(e)} = \bigcup_{n < \omega} \bigcap B_{f(n)}.$$

Эффективное σ -кольцо может быть построено следующим образом. Положим $\tau_1(n) = 2^n$. Пусть $\tau_2(e) = 3 \cdot 5^e$. Пусть Φ будет множеством правил $\emptyset \rightarrow \tau_1(n)$ для $n \in \omega$ и $\{f(n) | n \in \omega\} \rightarrow \tau_2(e)$ для $e \in \omega$ таких, что $\{e\}$ является всюду определенной функцией f . Положим $I = I(\Phi)$. Тогда Φ является детерминированным множеством правил (см. 1.2), так что для $e \in I$ мы

можем определить $B_e \subseteq \omega$ по рекурсии:

$$B_{\tau_1(e)} = R_e \text{ для } e \in \omega, \\ B_{\tau_2(e)} = \bigcup_{n \in \omega} \bigcap B_{f(n)}, \text{ если } \{e\} = f: \omega \rightarrow I.$$

Ясно, что $\mathcal{R} = \{B_i | i \in I\}$ является эффективным σ -кольцом.

Поскольку Φ регулярно арифметическое, $I = I(\Phi)$ является Π_1^1 -множеством. Пусть φ будет монотонным оператором, связанным с Φ . $\mathcal{R}$ может быть разложено в иерархию $\mathcal{R} = \bigcup_{\lambda < \omega_1} \mathcal{R}^\lambda$, где $\mathcal{R}^\lambda = \{B_e | e \in \varphi^\lambda\}$ для $\lambda < \omega_1 (= |\Phi|)$, так что $\mathcal{R}^0$ — это множество р. п. множеств. $\mathcal{R}^1$ — множество Σ_2^0 -множеств, $\bigcup_{n < \omega} \mathcal{R}^n$ — это множество арифметических множеств. В § 8Е книги Московакиса [1] имеется доказательство следующего результата.

2.2.3. Теорема. $\mathcal{R}$ является наименьшим эффективным σ -кольцом и совпадает с множеством Δ_1^1 -подмножеств ω .

2.3. Представимость. В этом пункте мы обобщаем подход к рекурсивно перечислимым и Π_1^1 -предикатам на ω , использующий представимость, на произвольные структуры.

Предположим, что у нас есть множество A и теория T , имеющая предметные константы для элементов из A и предметные переменные. (Будет использоваться один и тот же символ для константы и объекта, который она обозначает.)

2.3.1. Определение. $R \subseteq A^n$ называется *T -представимым формулой* $\theta(\bar{x})$, если $\bar{x} = x_1, \dots, x_n$ и

$$R(\bar{a}) \Leftrightarrow T \vdash \theta(\bar{a}) \text{ для } \bar{a} \in A^n.$$

Если $A = \omega$ и T является конечно определенной, например формальной арифметикой, то множество $\ulcorner T \urcorner$ гёделевых номеров $\ulcorner \theta \urcorner$ теорем θ теории T образует р. п. множество, и, следовательно, всякий T -представимый предикат также р. п. Действительно, если R представим формулой $\theta(\bar{x})$, то $R(\bar{a}) \Leftrightarrow \ulcorner \theta(\bar{a}) \urcorner \in \ulcorner T \urcorner$ для $\bar{a} \in \omega^n$, где f — рекурсивная функция, задаваемая так: $f(\bar{a}) = \ulcorner \theta(\bar{a}) \urcorner$ для $\bar{a} \in \omega^n$. Результат (II) из 2.1 дает обращение этого результата для достаточно богатых T . Следовательно, для подходящих теорий T T -представимые предикаты — это в точности р. п. предикаты.

Обычная теория рекурсии может быть так развита с самого начала при подходящем выборе T . Например, канонические системы Поста (см. Пост [1]) дают такую возможность; они далее усовершенствованы Смальяном [1]. Другой подход — системы равенств Клини для представления частично рекурсивных функций (см. Клини и [1]).

Гжегорчик, Мостовский и Рыль-Нардзевский [1] показали, что в формальной арифметике второго порядка с ω -правилом представимы в точности Π_1^1 -предикаты. Следовательно, понятие представимости указывает способ единообразного обращения с р. п. предикатами и Π_1^1 -предикатами. Ниже мы дадим такой единообразный подход для произвольной алгебраической системы $\mathfrak{A}$, который дает эти классы предикатов на ω , когда $\mathfrak{A}$ является системой $\mathfrak{A} = \langle \omega, S, P \rangle$ для арифметики, где S и P — графики функций сложения и умножения.

Сначала нужно дать некоторые определения. Для данного множества A мы вводим полный язык первого порядка L^A над A . В L^A имеются предметные константы для элементов из A и предикатные константы для предикатов на A . Имеются также предметные переменные и n -арные предикатные переменные для каждого $n > 0$.

Элементарные (т. е. первого порядка) формулы языка L^A строятся обычным образом при помощи связок и предметных кванторов $\forall x$, $\exists x$. Формулы второго порядка получаем, добавляя кванторы $\forall X^n$, $\exists X^n$, где X^n — это n -местная предикатная переменная. Все элементарные предложения второго порядка либо истинны, либо ложны при стандартной интерпретации. Нас будут интересовать различные подклассы формул. *Экзистенциальные* формулы строим из атомных формул и их отрицаний, используя $\vee$, $\wedge$ и $\exists x$. Если дан бинарный предикат $<$ на A , то можно ввести ограниченные кванторы $\forall x < y$, $\exists x < y$, сокращающие $\forall x (x < y \rightarrow \dots)$ и $\exists x (x < y \wedge \dots)$. Затем можно определить ограниченные элементарные формулы как построенные с использованием только ограниченных кванторов. Можно определить Σ_n^0 - и Π_n^0 -пренексные формулы обычным образом, разрешая ограниченные матрицы; например, Σ_2^0 -формулы имеют вид $\exists x_1 \dots \exists x_n \forall y_1 \dots \forall y_m \theta$, где $n, m \geq 0$ и θ является ограниченной.

Нас будет также интересовать классификация формул второго порядка. Π_1^1 -формула — это формула, имеющая вид $\forall X_1 \dots \forall X_m \theta$, где $m \geq 0$ и θ элементарна. Аналогично определяем Π_n^1 - и Σ_n^1 -формулы для $n > 0$, подсчитывая число переменных блоков предикатных кванторов.

Для данной системы $\mathfrak{A} = \langle A, R_1, \dots, R_l \rangle$ определим $L(\mathfrak{A})$ — подязык L^A , в котором допускаются предикатные константы только для равенства и предикатов $R_1, \dots, R_l$. Если $\mathcal{F}$ — семейство формул языка L^A , то $R \subseteq A^n$ называется $\mathcal{F}$ -определимым над $\mathfrak{A}$, если существует формула $\theta(\bar{x})$ языка $L(\mathfrak{A})$ в $\mathcal{F}$ такая, что $\bar{x} = x_1, \dots, x_n$ включает все свободные переменные $\theta(\bar{x})$ и $R(\bar{a}) \Leftrightarrow \theta(\bar{a})$ истинна для $\bar{a} \in A^n$.

Многие конструкции в обычной теории рекурсии используют некоторый кодирующий аппарат, например гёделеву нумерацию. Для продолжения таких конструкций на $\mathfrak{A}$ нам будет нужно, чтобы этот аппарат был определен на $\mathfrak{A}$ подходящим образом.

2.3.2. Определение. *Кодирующая схема* для A — это тройка $\mathcal{C} = \langle N, \leq, < \rangle$, где:

(i) $N \subseteq A$ и $\leq$ — бинарный предикат на N такой, что $\langle N, \leq \rangle \cong \langle \omega, \leq \rangle$. Будем отождествлять N с $\omega = \{0, 1, \dots\}$.

(ii) $< : \bigcup_{n \in \omega} A^n \rightarrow A$ является инъективной функцией.

С $\mathcal{C}$ связаны следующие множество и функции:

(iii) Seq , множество всех кодов конечных последовательностей, является областью значений $<$.

(iv) $\text{lh} : \text{Seq} \rightarrow N$ задается посредством $\text{lh}(\langle x_1, \dots, x_n \rangle) = n$.

(v) $q : \text{Seq} \times N \rightarrow A$ задается посредством

$$q(\langle x_1, \dots, x_n \rangle, i) = \begin{cases} x_i, & \text{если } 1 \leq i \leq n, \\ 0 & \text{в противном случае.} \end{cases}$$

(vi) $s : N \rightarrow N$ задается как $s(n) = n + 1$.

Если $\mathcal{F}$ — класс формул, то говорим, что $\mathcal{C}$ является $\mathcal{F}$ -определимой над $\mathfrak{A}$, если N , $\leq$, Seq и графики функций lh , q и s являются $\mathcal{F}$ -определимыми над $\mathfrak{A}$. $\mathfrak{A}$ является $\mathcal{F}$ -приемлемой, если существует кодирующая схема $\mathcal{C}$ для A , которая $\mathcal{F}$ -определима над $\mathfrak{A}$. В случае, если $\mathcal{F}$ — класс элементарных формул, мы пишем просто *приемлемая* вместо $\mathcal{F}$ -приемлемая.

Если дана кодирующая схема $\mathcal{C}$ для A и система $\mathfrak{A}$, то формулам θ языка $L(\mathfrak{A})$ могут быть присвоены «гёделевы номера» $\ulcorner \theta \urcorner \in A$ стандартным образом. Мы не будем здесь вдаваться в детали этого, но иногда нам нужно будет использовать некоторые факты о такой гёделевой нумерации.

Пусть для данной алгебраической системы $\mathfrak{A}$ $T(\mathfrak{A})$ будет формальной теорией в языке первого порядка $L(\mathfrak{A})$, имеющей стандартную систему аксиом и правил вывода логики первого порядка с равенством и диаграмму $\mathfrak{A}$ в качестве множества нелогических аксиом, так что каждое истинное предложение языка $L(\mathfrak{A})$, являющееся атомным или отрицанием атомного, есть аксиома $T(\mathfrak{A})$.

Нашим обобщением класса р. п. предикатов на ω является класс $T(\mathfrak{A})$ -представимых предикатов на A . Чтобы получить хорошее понятие, мы потребуем, чтобы $\mathfrak{A}$ была экзистенциально приемлемой с экзистенциально определимой кодирующей схемой $\mathcal{C}$.

Пусть $<$ будет предикатом на A , являющимся предикатом строгого упорядочения копии натуральных чисел в A , задаваем-

мой схемой $\mathcal{C}$. Пусть $\Sigma^0_1(\mathcal{A})$ будет классом предикатов на A , которые Σ^0_1 -определимы над $\mathcal{A}$, где указанный предикат $<$ используется при определении ограниченных формул. Как и на ω , можно показать, что финитарное множество правил, индуктивно определяющее теоремы из A , индуцирует $\Sigma^0_1(\mathcal{A})$ -финитарное множество правил на A .

2.3.3. Определение. Финитарное множество правил Φ на A является $\Sigma^0_1(\mathcal{A})$ -множеством, если R_Φ является $\Sigma^0_1(\mathcal{A})$ -множеством, где R_Φ — это множество пар $\langle \langle a_1, \dots, a_n \rangle, b \rangle$ таких, что $\Phi: \{a_1, \dots, a_n\} \rightarrow b$.

Следующее предложение доказывается в точности так же, как предложение 2.2.2.

2.3.4. Предложение. Если $\mathcal{A}$ экзистенциально приемлема и Φ является $\Sigma^0_1(\mathcal{A})$ -финитарным множеством правил, то $I(\Phi)$ тоже является $\Sigma^0_1(\mathcal{A})$ -множеством.

2.3.5. Следствие. Если $\mathcal{A}$ экзистенциально приемлема, то $\lceil T(\mathcal{A}) \rceil$ является $\Sigma^0_1(\mathcal{A})$ -множеством и, следовательно, каждый $T(\mathcal{A})$ -представимый предикат является $\Sigma^0_1(\mathcal{A})$ -предикатом.

Для доказательства последней части нам нужен тот факт, что если $\theta(\bar{x})$ — формула и $f(\bar{a}) = \lceil \theta(\bar{a}) \rceil$ для $\bar{a} \in A^n$, то график f является $\Sigma^0_1(\mathcal{A})$ -множеством. Обращение этого будет дано в следующем параграфе.

Обобщим теперь ω -правило. Теория $T_\infty(\mathcal{A})$ получается из $T(\mathcal{A})$ добавлением следующего бесконечного правила:

A-правило. Из $\theta(a)$ для $a \in A$ вытекает $\forall x \theta(x)$.

Будем называть элементарные формулы $\varphi(X_1, \dots, X_m, x_1, \dots, x_n)$ языка $L(\mathcal{A})$ универсально истинными, если Π^1_1 -предложение

$$\forall X_1 \dots \forall X_m \forall x_1 \dots \forall x_n \varphi(X_1, \dots, X_m, x_1, \dots, x_n)$$

истинно. Легко заметить, что все аксиомы $T_\infty(\mathcal{A})$ универсально истинны и все правила вывода из $T_\infty(\mathcal{A})$ сохраняют универсальную истинность. Следовательно, имеем

2.3.6. Предложение. Из $T_\infty(\mathcal{A}) \vdash \varphi$ следует, что φ универсально истинна.

Если $\mathcal{A}$ счетна, то справедлива теорема о полноте, дающая обращение предложения 2.3.6. Ее можно доказать, используя теорему об опускании типов для счетных языков первого порядка (см. Чэн и Кейслер [1]) или непосредственным построением генкинского типа, как у Грийо [1].

2.3.7. Теорема. Для счетных $\mathcal{A}$

$T_\infty(\mathcal{A}) \vdash \varphi$, если и только если φ универсально истинна.

2.3.8. Следствие. Для счетных $\mathcal{A}$ предикат на A является $T_\infty(\mathcal{A})$ -представимым тогда и только тогда, когда он является $\Pi^1_1(\mathcal{A})$ -предикатом (т. е. Π^1_1 -определимым над $\mathcal{A}$).

Доказательство. По теореме 2.3.7 $\theta(\bar{x})$ $T_\infty(\mathcal{A})$ -представляет R , если и только если $\forall X_1 \dots \forall X_m \theta(\bar{x})$ определяет R , где $X_1, \dots, X_m$ — предикатные переменные, встречающиеся в элементарной формуле $\theta(\bar{x})$. Этот результат включает частный случай арифметики при $\mathcal{A} = \mathbb{N}$. $\square$

Как и раньше, если считать заданной кодирующую схему $\mathcal{C}$ над $\mathcal{A}$, то множество правил, индуктивно определяющих теоремы теории $T_\infty(\mathcal{A})$, при гёделевой нумерации индуцирует множество правил на A , обладающее следующим свойством при $\mathcal{C}$, элементарной над $\mathcal{A}$.

2.3.9. Определение. Множество правил Φ на A называется регулярно элементарным над $\mathcal{A}$, если найдутся элементарные предикаты R, S такие, что Φ является множеством тех правил $R_a \rightarrow b$, что $S(a, b)$.

2.3.10. Предложение. Если $\mathcal{A}$ — приемлемая алгебраическая система, то существует регулярно элементарное множество правил Φ такое, что $\lceil T_\infty(\mathcal{A}) \rceil = I(\Phi)$.

Этот результат потребуется в следующем параграфе.

Наконец, рассмотрим понятие истинности для (элементарных) предложений языка $L(\mathcal{A})$. Легко видеть, что каждое истинное предложение может быть доказано в $T_\infty(\mathcal{A})$, и, следовательно, у нас есть характеристизация. Если φ есть предложение языка $L(\mathcal{A})$, то φ истинно тогда и только тогда, когда $T_\infty(\mathcal{A}) \vdash \varphi$. Альтернативной возможностью является обычное индуктивное определение истинности, ведущееся по построению φ . Оно может быть выражено следующим образом. Будем называть выражения вида $\vdash \varphi$ и $\neg \varphi$, где φ — предложение языка $L(\mathcal{A})$, маркированными предложениями. Пусть Φ будет следующим множеством правил на маркированных предложениях:

$\emptyset \rightarrow \vdash \theta$ для каждого истинного атомного предложения θ ,
 $\emptyset \rightarrow \neg \theta$ для каждого ложного атомного предложения θ ;

$\{\vdash \varphi, \vdash \psi\} \rightarrow \vdash (\varphi \wedge \psi)$ для предложений φ, ψ ,

$\{\neg \varphi\} \rightarrow \neg (\varphi \wedge \psi)$ для предложений φ, ψ ,

$\{\neg \psi\} \rightarrow \neg (\varphi \wedge \psi)$ для предложений φ, ψ ;

аналогичные правила для $\neg, \wedge, \rightarrow$;

$\{\vdash \varphi(a) \mid a \in A\} \rightarrow \vdash \forall x \varphi(x)$ для предложения $\forall x \varphi(x)$,

$\{\neg \varphi(a)\} \rightarrow \neg \forall x \varphi(x)$ для $a \in A$; аналогичные правила для $\exists x$.

Тогда, если φ — предложение, то

φ истинно тогда и только тогда, когда $\vdash \varphi \in I(\Phi)$,

φ ложно тогда и только тогда, когда $\neg \varphi \in I(\Phi)$.

Снова заметим, что при гёделевой нумерации при помощи элементарной кодирующей схемы это множество правил Φ индуцирует регулярно элементарное множество правил на A .

§ 3. Классы индуктивных определений

3.1. Общая схема. Большинство современных результатов по индуктивным определениям укладывается в следующую общую схему. Предположим, что дано бесконечное множество A . Пусть $\mathcal{E}$ будет классом операторов, имеющих вид $\varphi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ для некоторых $n > 0$.

3.1.1. Определение. (i) $R \subseteq A^n$ называется $\mathcal{E}$ -индуктивным, если существует $\varphi: \text{Pow}(A^m) \rightarrow \text{Pow}(A^m)$ из $\mathcal{E}$ такое, что $m \geq n$ и $\bar{b} \in A^{m-n}$ таково, что для $\bar{a} \in A^n$.

$$R(\bar{a}) \iff (\bar{b}, \bar{a}) \in \varphi^\infty.$$

(ii) $\text{IND}(\mathcal{E})$ — множество $\mathcal{E}$ -индуктивных предикатов.

(iii) $|\mathcal{E}| = \text{Sup} \{ |\varphi| \mid \varphi \in \mathcal{E} \}$.

Почему не определяется $\text{IND}(\mathcal{E})$ как $\{ \varphi^\infty \mid \varphi \in \mathcal{E} \}$? Это множество не оказалось естественным, так как мы хотим, чтобы $\text{IND}(\mathcal{E})$ обладало некоторыми свойствами замкнутости, например мы обычно хотим, чтобы $\text{IND}(\mathcal{E})$ было замкнуто относительно пересечений, и не видно никаких разумных условий на $\mathcal{E}$, которые обеспечивали бы это для $\{ \varphi^\infty \mid \varphi \in \mathcal{E} \}$. Ниже мы дадим общий результат о свойствах замкнутости $\text{IND}(\mathcal{E})$ при разумных предположениях об $\mathcal{E}$.

Назовем $\tau: A^n \rightarrow A^m$ сечением, если $m \geq n$ и для некоторых $\bar{b} \in A^{m-n}$

$$\tau(\bar{a}) = (\bar{b}, \bar{a}) \quad \text{для всех } \bar{a} \in A^n.$$

Тогда $\text{IND}(\mathcal{E}) = \{ \tau^{-1} \varphi^\infty \mid \varphi \in \mathcal{E} \wedge \tau \text{ является сечением} \}$.

Сечения используются при кодировании нескольких индуктивных определений в одно. Следующая лемма является ключевой.

3.1.2. Лемма. Пусть $n_1, \dots, n_k > 0$ и $m \geq \max(n_1, \dots, n_k) + 1$. Тогда существуют сечения $\tau_1: A^{n_1} \rightarrow A^m, \dots, \tau_k: A^{n_k} \rightarrow A^m$, имеющие попарно различные области значений.

Доказательство. Выберем попарно различные элементы $c_1, c_2, \dots, c_k \in A$ и определим

$$\tau_i(\bar{a}) = (\overbrace{c_1, \dots, c_i}^{m-n_i}, \bar{a}) \in A^m \quad \text{для } \bar{a} \in A^{n_i}. \quad \square$$

3.1.3. Определение. Оператор

$$\theta: \text{Pow}(A^{n_1}) \times \dots \times \text{Pow}(A^{n_k}) \rightarrow \text{Pow}(A^n)$$

допускает кодирование сечениями в $\mathcal{E}$, если для любых сечений $\tau_1: A^{n_1} \rightarrow A^m, \dots, \tau_k: A^{n_k} \rightarrow A^m, \tau: A^n \rightarrow A^m$ отображение $\varphi:$

$\text{Pow}(A^m) \rightarrow \text{Pow}(A^m)$, задаваемое равенством

$$\varphi(S) = \tau \theta(\tau_1^{-1} S, \dots, \tau_k^{-1} S) \quad \text{для } S \subseteq A^m,$$

принадлежит $\mathcal{E}$.

3.1.4. Предложение. Если (i) $\mathcal{E}$ замкнуто относительно объединений (т. е. $\varphi, \psi \in \mathcal{E}$ влечет $\varphi \cup \psi \in \mathcal{E}$, где

$$\varphi \cup \psi(S) = \varphi(S) \cup \psi(S);$$

(ii) каждый оператор из $\mathcal{E}$ допускает кодирование сечениями в $\mathcal{E}$,

то $\text{IND}(\mathcal{E})$ замкнуто относительно каждого оператора $\theta: \text{Pow}(A^{n_1}) \times \dots \times \text{Pow}(A^{n_k}) \rightarrow \text{Pow}(A^n)$, являющегося монотонным по каждому аргументу и допускающего кодирование сечениями в $\mathcal{E}$.

Доказательство. Пусть θ допускает кодирование сечениями и является монотонным по каждому аргументу. Пусть $R_i = \sigma_i^{-1} \varphi_i^\infty$, где $\sigma_i: A^{n_i} \rightarrow A^{m_i}$ является сечением и $\varphi_i: \text{Pow}(A^{m_i}) \rightarrow \text{Pow}(A^{m_i})$ лежит в $\mathcal{E}$ для $i = 1, \dots, k$. Мы хотим показать, что $\theta(R_1, \dots, R_k) = \tau^{-1} \varphi^\infty$ для некоторого сечения τ и некоторого $\varphi \in \mathcal{E}$. Положим $m = \max(m_1, \dots, m_k, n) + 1$ и выберем сечения $\tau_1: A^{m_1} \rightarrow A^m, \dots, \tau_k: A^{m_k} \rightarrow A^m, \tau: A^n \rightarrow A^m$ с попарно различными областями значений. Положим $\varphi'_i(S) = \tau_i \varphi_i(\tau_i^{-1}(S))$ для $i = 1, \dots, k$ и $S \subseteq A^m$. Положим $\theta'(S) = \tau \theta((\tau_1 \sigma_1)^{-1} S, \dots, (\tau_k \sigma_k)^{-1} S)$ для $S \subseteq A^m$. Наконец, положим $\varphi(S) = \varphi'_1(S) \cup \dots \cup \varphi'_k(S) \cup \theta'(S)$ для $S \subseteq A^m$. По предположению (ii) каждое $\varphi'_i \in \mathcal{E}$. Так как θ допускает кодирование сечениями в $\mathcal{E}$, то $\theta' \in \mathcal{E}$. Следовательно, по предположению (i) $\varphi \in \mathcal{E}$.

Теперь легко видеть, что $\varphi_i^\infty = \tau_i^{-1} \varphi^\infty$, так что $R_i = (\tau_i \sigma_i)^{-1} \varphi^\infty$ для $i = 1, \dots, k$. Аналогично, $\tau^{-1} \varphi^\infty = \theta((\tau_1 \sigma_1)^{-1} \varphi^{<\lambda}, \dots, (\tau_k \sigma_k)^{-1} \varphi^{<\lambda})$. Следовательно, поскольку θ монотонный,

$$\begin{aligned} \tau^{-1} \varphi^\infty &= \bigcup_{\lambda} \tau^{-1} \varphi^\lambda \\ &= \bigcup_{\lambda} \theta((\tau_1 \sigma_1)^{-1} \varphi^{<\lambda}, \dots, (\tau_k \sigma_k)^{-1} \varphi^{<\lambda}) \\ &= \theta((\tau_1 \sigma_1)^{-1} \varphi^\infty, \dots, (\tau_k \sigma_k)^{-1} \varphi^\infty) \\ &= \theta(R_1, \dots, R_k). \quad \square \end{aligned}$$

Замечание. В этой теореме монотонность θ существенна. В общем случае $\text{IND}(\mathcal{E})$ не замкнуто относительно дополнений.

3.1.5. Пример. Основными монотонными операторами первого порядка являются $\vee^n$, $\wedge^n$, $\exists^n$ и $\forall^n$, $n > 0$.

$$\vee^n(R, S) = R \cup S \text{ для } R, S \subseteq A^n,$$

$$\wedge^n(R, S) = R \cap S \text{ для } R, S \subseteq A^n:$$

$$\exists^n(R) = \{\bar{a} \in A^n \mid \exists x R(x, \bar{a})\} \text{ для } R \subseteq A^{n+1},$$

$$\forall^n(R) = \{\bar{a} \in A^n \mid \forall x R(x, \bar{a})\} \text{ для } R \subseteq A^{n+1}.$$

Обычно класс $\mathcal{F}$ операторов указывается некоторыми условиями определимости.

Пусть $\varphi(X, \bar{x})$ будет формулой языка L^A , в которой свободными могут быть только n -местная предикатная переменная X и предметные переменные $\bar{x} = x_1, \dots, x_n$. Говорим, что $\varphi(X, \bar{x})$ определяет оператор $\varphi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$, если

$$\varphi(S) = \{\bar{a} \in A^n \mid \varphi(S, \bar{a}) \text{ истинна}\} \text{ для } S \subseteq A^n.$$

Пусть $\mathcal{F}(\mathfrak{A})$ для данных класса формул $\mathcal{F}$ языка L^A и алгебраической системы $\mathfrak{A} = \langle A, R_1, \dots, R_l \rangle$ обозначает класс операторов, определяемых формулами из $\mathcal{F}$ в языке $L(\mathfrak{A})$. Пусть $\text{mon-}\mathcal{F}(\mathfrak{A})$ обозначает подкласс монотонных операторов в $\mathcal{F}(\mathfrak{A})$. Наконец, пусть $\text{pos-}\mathcal{F}(\mathfrak{A})$ обозначает класс операторов, определяемых посредством формул $\varphi(X, \bar{x})$ из $\mathcal{F}$ в языке $L(\mathfrak{A})$, в которые X входит только позитивно, т. е. $\varphi(X, \bar{x})$ строим из формул, не содержащих X , и атомных формул, содержащих X , используя только позитивные связки $\wedge$, $\vee$ и кванторы. Операторы из $\text{pos-}\mathcal{F}(\mathfrak{A})$ автоматически являются монотонными. Таким образом, имеем

$$\text{pos-}\mathcal{F}(\mathfrak{A}) \subseteq \text{mon-}\mathcal{F}(\mathfrak{A}) \subseteq \mathcal{F}(\mathfrak{A})$$

и, следовательно,

$$\text{IND}(\text{pos-}\mathcal{F}(\mathfrak{A})) \subseteq \text{IND}(\text{mon-}\mathcal{F}(\mathfrak{A})) \subseteq \text{IND}(\mathcal{F}(\mathfrak{A}))$$

и

$$|\text{pos-}\mathcal{F}(\mathfrak{A})| \leq |\text{mon-}\mathcal{F}(\mathfrak{A})| \leq |\mathcal{F}(\mathfrak{A})|.$$

3.2. Позитивная экзистенциальная индукция. В этом пункте мы рассмотрим, возможно, простейший пример общей схемы, именно, мы рассмотрим класс операторов $\text{pos-}\mathcal{F}(\mathfrak{A})$, где $\mathcal{F}$ является классом экзистенциальных формул. Будем писать $\text{IND}(\exists - \mathfrak{A})$ и $|\exists - \mathfrak{A}|$ вместо $\text{IND}(\text{pos-}\mathcal{F}(\mathfrak{A}))$ и $|\text{pos-}\mathcal{F}(\mathfrak{A})|$, когда $\mathcal{F}$ является этим классом. Мы увидим, что для экзистенциально приемлемых $\mathfrak{A}$ класс $\text{IND}(\exists - \mathfrak{A})$ совпадает с классом $T(\mathfrak{A})$ -представимых предикатов и дает хорошее обобщение р. п. предикатов на ω .

3.2.1. Предложение. Если $\mathfrak{A}$ бесконечна, то $|\exists - \mathfrak{A}| = \omega$.

Доказательство. $|\exists - \mathfrak{A}| \geq \omega$, так как $|\varphi_n| = n$ для каждого $n \in \omega$, где

$$\varphi_n(X) = \left\{ x \in A \mid \bigvee_{i < n} \left[\bigwedge_{j < i} X(a_j) \wedge x = a_i \right] \right\} \text{ для } X \subseteq A,$$

а $a_0, \dots, a_{n-1}$ — попарно различные элементы из A . Ясно, что каждая φ_n является позитивной экзистенциальной, $\varphi_n^i = \{a_j \mid j < i\}$ для $i < n$ и, следовательно, $I(\varphi) = \{a_j \mid j < n\}$.

Для доказательства $|\exists - \mathfrak{A}| \leq \omega$ в силу предложения 1.3.4 достаточно показать, что каждый позитивный экзистенциальный оператор φ является ω -базированным, а для этого достаточно показать, что для каждой экзистенциальной формулы $\theta(X)$, позитивной относительно предикатной переменной X и не содержащей никаких других свободных переменных, истинность $\theta(R)$ влечет истинность $\theta(S)$ для некоторого конечного $S \subseteq R$. Это легко доказывается индукцией по построению этих формул $\theta(X)$. $\square$

Следующий результат дает свойства замкнутости множества $\text{IND}(\exists - \mathfrak{A})$.

3.2.2. Предложение. (i) Если $\theta: \text{Pow}(A^{n_1}) \times \dots \times \text{Pow}(A^{n_k}) \rightarrow \text{Pow}(A^n)$ является позитивным экзистенциальным над $\mathfrak{A}$ (или, эквивалентно, допускает кодирование сечениями в классе позитивных экзистенциальных операторов), то $\text{IND}(\exists - \mathfrak{A})$ замкнуто относительно θ . Следовательно, предикаты $=, R_1, \dots, R_l$ и их дополнения принадлежат $\text{IND}(\exists - \mathfrak{A})$, поскольку подходящие постоянные операторы являются позитивными экзистенциальными над $\mathfrak{A}$. $\text{IND}(\exists - \mathfrak{A})$ замкнуто также относительно $\vee^n, \wedge^n, \exists^n$ для $n > 0$, поскольку они также позитивные экзистенциальные над $\mathfrak{A}$.

(ii) Если $N \subseteq A$, $< -$ предикат на N и $S: N \rightarrow N$ таковы, что $\langle N, <, S \rangle \cong \langle \omega, <, S \rangle$, и $N, <$ и график функции S являются экзистенциально определимыми над $\mathfrak{A}$, то $\text{IND}(\exists - \mathfrak{A})$ является $\forall^n_{<}$ -замкнутым для $n > 0$, где

$$\forall^n_{<}(R) = \{(a, \bar{b}) \in A^{n+1} \mid a \in N \wedge \forall x (x < a \rightarrow R(x, \bar{b}))\}$$

для $R \subseteq A^{n+1}$.

Доказательство. (i) Это следствие предложения 3.1.4.

(ii) Пусть $R = \tau^{-1}\varphi^\infty$, где $\tau: A^{n+1} \rightarrow A^m$ является сечением и $\varphi: \text{Pow}(A^m) \rightarrow \text{Pow}(A^m)$ позитивное экзистенциальное над $\mathfrak{A}$. Мы покажем, что $\forall^n_{<}(R)$ лежит в $\text{IND}(\exists - \mathfrak{A})$. Прежде всего, отождествим N с $\omega = \{0, 1, \dots\}$. Пусть $\tau_i: A^m \rightarrow A^{m+1}$ будут сечениями $\tau_i(\bar{x}) = (i, \bar{x})$ для $\bar{x} \in A^m$, где $i = 0, 1$. Положим $\psi(X) = \tau_0\varphi(\tau_0^{-1}X) \cup (\tau_1\tau)\theta((\tau_0\tau)^{-1}X, (\tau_1\tau)^{-1}X)$ для $X \subseteq A^m$, где

$$\theta(Y, Z) = \{(x, \bar{x}) \in A^{n+1} \mid x = 0 \vee \exists y (x = S(y)$$

$$\wedge Y(y, \bar{z}) \wedge Z(y, \bar{x}))\}$$

для $Y, Z \subseteq A^{n+1}$. Тогда ψ позитивное экзистенциальное над $\mathfrak{A}$. Ясно, что $\tau_0^{-1}\psi^\infty = \psi^\infty$. Поэтому $R = (\tau_0\tau)^{-1}\psi^\infty$. Следовательно, если $S = (\tau_1\tau)^{-1}\psi^\infty$, то $S(x, \bar{x}) \Leftrightarrow x = 0$ или $\exists y (x = S(y) \wedge \wedge R(y, \bar{x}) \wedge S(y, \bar{x}))$. Это может быть выполнено, только если $S = \bigvee_{\tau}^n (R)$. Следовательно, $\bigvee_{\tau}^n (R) = (\tau_1\tau)^{-1}\psi^\infty$ лежит в $\text{IND}(\exists - \mathfrak{A})$. $\square$

3.2.3. Предложение. Если $\varphi: \text{Pow}(A^m) \rightarrow \text{Pow}(A^m)$ позитивный экзистенциальный над $\mathfrak{A}$, то $I(\varphi)$ является $T(\mathfrak{A})$ -представимым при помощи $\psi(X) \rightarrow X(\bar{x})$, где $\psi(X)$ есть $\forall \bar{y} (\varphi(X, \bar{y}) \rightarrow X(\bar{y}))$, а $\varphi(X, \bar{x})$ — экзистенциальная формула языка $L(\mathfrak{A})$, позитивная относительно X , которая определяет оператор φ .

Доказательство. Пусть T будет предикатом, представленным формулой $\psi(X) \rightarrow X(\bar{x})$. Сначала заметим, что если $\bar{a} \in T$, то по предложению 2.3.6 $\psi(X) \rightarrow X(\bar{a})$ является универсально истинной, т. е. $a \in \bigcap \{S \subseteq A^m \mid \varphi(S) \subseteq S\} = I(\varphi)$. Таким образом, $T \subseteq I(\varphi)$. Для доказательства $I(\varphi) \subseteq T$ достаточно показать, что $\varphi(T) \subseteq T$. Нам нужно следующее

Утверждение. Пусть $\theta(X)$ будет экзистенциальной формулой языка $L(\mathfrak{A})$, содержащей X только позитивно и не содержащей других свободных переменных. Тогда

$$\theta(T) \text{ истинно влечет } T(\mathfrak{A}) \vdash \psi(X) \rightarrow \theta(X).$$

Это утверждение доказывается легкой индукцией по числу логических символов в $\theta(X)$.

Теперь, если $\bar{a} \in \varphi(T)$, то $\varphi(T, \bar{a})$ истинна, и, следовательно, в силу утверждения $T(\mathfrak{A}) \vdash \psi(X) \rightarrow \varphi(X, \bar{a})$. Вспоминая, что $\psi(X)$ — это $\forall \bar{y} (\varphi(X, \bar{y}) \rightarrow X(\bar{y}))$, получаем, что $T(\mathfrak{A}) \vdash \psi(X) \rightarrow X(\bar{a})$, и, следовательно, $\bar{a} \in T$. Итак, $\varphi(T) \subseteq T$, что и требовалось. $\square$

3.2.4. Теорема. Пусть $\mathfrak{A}$ будет экзистенциально приемлемой алгебраической системой. Тогда следующие условия на предикат R на A эквивалентны:

- (i) $R \in \text{IND}(\exists - \mathfrak{A})$,
- (ii) R является $T(\mathfrak{A})$ -представимым,
- (iii) R является $\Sigma_1^0(\mathfrak{A})$ -определимым.

Замечание. В (iii) $\Sigma_1^0(\mathfrak{A})$ определяется в зависимости от копии $\langle N, < \rangle$ модели $\langle \omega, < \rangle$, где $\mathcal{C} = \langle N, <, \langle \rangle \rangle$ является экзистенциально определимой кодирующей схемой на $\mathfrak{A}$. Из теоремы следует, что по существу $\Sigma_1^0(\mathfrak{A})$ не зависит от используемой кодирующей схемы $\mathcal{C}$.

Доказательство. (i) $\rightarrow$ (ii). Пусть $R = \tau^{-1}\varphi^\infty$, где τ — сечение $\tau(\bar{a}) = (\bar{b}, \bar{a})$ для $\bar{a} \in A^n$ и φ — позитивный экзистенциальный оператор на $\mathfrak{A}$. Тогда по предложению 3.2.3 φ^∞ является

$I(\mathfrak{A})$ -представимым, скажем посредством формулы $\theta(y)$, и мы имеем

$$R(\bar{a}) \Leftrightarrow \tau(\bar{a}) \in \varphi^\infty \Leftrightarrow T(\mathfrak{A}) \vdash \theta(\bar{b}, \bar{a}) \text{ для } \bar{a} \in A^n.$$

Следовательно, R является $T(\mathfrak{A})$ -представимым посредством формулы $\theta(\bar{b}, \bar{x})$.

(ii) $\rightarrow$ (iii). Это просто следствие 2.3.5.

(iii) $\rightarrow$ (i). Это вытекает из предложения 3.2.2. $\square$

Следующее свойство справедливо для р.п. предикатов на ω и является одним из основных структурных свойств, используемых в теории рекурсии и ее обобщениях.

3.2.5. Определение. Класс Γ предикатов на A обладает свойством параметризации, если для каждого $n > 0$ существует предикат $U \subseteq A^{n+1}$ такой, что $U \in \Gamma$ и для каждого $R \subseteq A^n$, лежащего в Γ , существует $a \in A$ такое, что

$$R = U_a = \{\bar{a} \in A^n \mid U(a, \bar{a})\}.$$

3.2.6. Теорема. Если $\mathfrak{A}$ экзистенциально приемлема, то $\text{IND}(\exists - \mathfrak{A})$ обладает свойством параметризации.

Доказательство. По следствию 2.3.5 и теореме 3.2.4 множество $\ulcorner T(\mathfrak{A}) \urcorner$ лежит в $\text{IND}(\exists - \mathfrak{A})$. Нам нужен также следующий факт о кодировании синтаксиса в $\ulcorner T(\mathfrak{A}) \urcorner$.

Предикат Sub является $\Sigma_1^0(\mathfrak{A})$ -предикатом и, следовательно, лежит в $\text{IND}(\exists - \mathfrak{A})$, где для $a, b, c \in A$ $\text{Sub}(a, b, c) \Leftrightarrow$ существует элементарная формула $\theta(\bar{x})$ в $L(\mathfrak{A})$ такая, что $a = \ulcorner \theta(\bar{x}) \urcorner$ и существует $\bar{b}$ такое, что $b = \langle \bar{b} \rangle$ и $c = \ulcorner \theta(\bar{b}) \urcorner$.

Теперь для данного $n > 0$ определим $U \subseteq A^{n+1}$ посредством

$$U(a, \bar{a}) \Leftrightarrow \exists x [\text{Sub}(a, \langle \bar{a} \rangle, x) \wedge x \in \ulcorner T(\mathfrak{A}) \urcorner].$$

Используя свойство замкнутости множества $\text{IND}(\exists - \mathfrak{A})$, видим, что $U \in \text{IND}(\exists - \mathfrak{A})$. Теперь, если $R \subseteq A^n$ лежит в $\text{IND}(\exists - \mathfrak{A})$, то по 3.2.4 он $T(\mathfrak{A})$ -представим, скажем, формулой $\theta(\bar{x})$. Полагаем $a = \ulcorner \theta(\bar{x}) \urcorner$. Тогда для $\bar{a} \in A^n$

$$\begin{aligned} R(\bar{a}) &\Leftrightarrow \ulcorner \theta(\bar{a}) \urcorner \in T(\mathfrak{A}) \\ &\Leftrightarrow U(a, \bar{a}). \end{aligned}$$

Следовательно, $R = U_a$. $\square$

3.3. Позитивная элементарная индукция. В этом пункте мы опишем некоторые свойства позитивной элементарной индукции. Эта теория имеется в книге Московакиса [1], и читатели должны там смотреть детальное изложение предмета.

Если $\mathcal{F}$ — класс элементарных формул языка L^A , то будем писать $\text{IND}(\mathfrak{A})$ вместо $\text{IND}(\text{pos-}\mathcal{F}(\mathfrak{A}))$ и $\kappa(\mathfrak{A})$ вместо $\mid \text{pos-}\mathcal{F}(\mathfrak{A}) \mid$.

3.3.1. Предложение. $\text{IND}(\mathfrak{A})$ позитивно элементарно замкнут над $\mathfrak{A}$ (т. е. если θ допускает кодирование сечениями в классе позитивных элементарных операторов, то $\text{IND}(\mathfrak{A})$ замкнут относительно θ). Следовательно, предикаты $=, R_1, \dots, R_l$ и их дополнения лежат в $\text{IND}(\mathfrak{A})$, и $\text{IND}(\mathfrak{A})$ замкнут относительно $\bigvee^n, \bigwedge^n, \exists^n$ и $\forall^n$ для $n > 0$.

Это является следствием предложения 3.1.4.

3.3.2. Предложение. Пусть Φ будет множеством правил на A , которое регулярно элементарно над $\mathfrak{A}$, и пусть $\varphi: \text{Pow}(A) \rightarrow \text{Pow}(A)$ будет соответствующим монотонным оператором. Тогда φ является позитивным элементарным над $\mathfrak{A}$ и, следовательно, $I(\Phi) = I(\varphi) \in \text{IND}(\mathfrak{A})$.

Доказательство. Пусть Φ будет множеством правил $R_a \rightarrow b$ таких, что $S(a, b)$. Тогда для $X \subseteq A$

$$\varphi(X) = \{b \in A \mid \exists y [S(y, b) \wedge \forall x (R(a, x) \rightarrow X(x))]\}.$$

Если R и S заменить их элементарными определениями, то получим элементарное определение φ . $\square$

3.3.3. Следствие. Если $\mathfrak{A}$ приемлема, то $\ulcorner T_\infty(\mathfrak{A}) \urcorner \in \text{IND}(\mathfrak{A})$, и, следовательно, каждый $T_\infty(\mathfrak{A})$ -представимый предикат лежит в $\text{IND}(\mathfrak{A})$.

Доказательство. Первая часть следует из предложений 3.3.2 и 2.3.10. Последнюю часть доказываем, как последнюю часть следствия 2.3.5, используя некоторые свойства замкнутости множества $\text{IND}(\mathfrak{A})$, данные в 3.3.1. $\square$

3.3.4. Предложение. Если $\varphi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ является позитивным элементарным над $\mathfrak{A}$, то $I(\varphi)$ является $T_\infty(\mathfrak{A})$ -представимым.

Доказательство. Этот результат доказывается, как в доказательстве предложения 3.2.3. Утверждение, использованное там, нужно изменить, заменив $T(\mathfrak{A})$ посредством $T_\infty(\mathfrak{A})$ и разрешив $\theta(X)$ быть элементарной формулой языка $L(\mathfrak{A})$. A -правило теории $T_\infty(\mathfrak{A})$ — это в точности то, что нужно для доказательства в случае, когда в $\theta(X)$ входит квантор всеобщности. $\square$

Как следствие предыдущих двух результатов получается

3.3.5. Теорема. Для приемлемой $\mathfrak{A}$ и предиката R на A $R \in \text{IND}(\mathfrak{A})$ тогда и только тогда, когда R является $T_\infty(\mathfrak{A})$ -представимым.

Как в доказательстве теоремы 3.2.6, имеем

3.3.6. Следствие. Если $\mathfrak{A}$ приемлемая, то $\text{IND}(\mathfrak{A})$ обладает свойством параметризации.

Следующий результат в книге Московакиса [1] называется «обобщенной теоремой Клини». Доказательство, данное там, использует совершенно другой метод, чем используемый нами.

3.3.7. Теорема. Если $\mathfrak{A}$ — счетная приемлемая алгебраическая система и R — предикат на A , то $R \in \text{IND}(\mathfrak{A})$, если и только если R является $\Pi_1^1(\mathfrak{A})$ -предикатом.

Эта теорема непосредственно выводится из следствия 2.3.8 и теоремы 3.3.5.

3.3.8. Определение. Нормой на множестве R называется отображение $\sigma: R \rightarrow \lambda$ множества R на ординал λ . λ называется длиной нормы σ .

Если $R \subseteq A^n$, то с σ связаны $2n$ -местные предикаты $<_\sigma^*$ и $\leq_\sigma^*$, задаваемые так:

$$\bar{a} <_\sigma^* \bar{b} \iff R(\bar{a}) \wedge (R(\bar{b}) \Rightarrow \sigma(\bar{a}) < \sigma(\bar{b})),$$

$$\bar{a} \leq_\sigma^* \bar{b} \iff R(\bar{a}) \wedge (R(\bar{b}) \Rightarrow \sigma(\bar{a}) \leq \sigma(\bar{b})).$$

для $\bar{a}, \bar{b} \in A^n$.

3.3.9. Пример. Если $\varphi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$, то $|\cdot|_\varphi: \varphi^\infty \rightarrow |\varphi|$ является нормой на φ^∞ . Пишем $<_\varphi^*$ и $\leq_\varphi^*$ вместо $<_\sigma^*$ и $\leq_\sigma^*$, когда $\sigma = |\cdot|_\varphi$.

3.3.10. Определение. Пусть Γ будет классом предикатов на A . Если R — предикат на A , то норма σ на R называется Γ -нормой, если $<_\sigma^*$ и $\leq_\sigma^*$ лежат в Γ . Класс Γ нормированный, если каждый предикат из Γ обладает Γ -нормой. Пусть $o(\Gamma)$ обозначает для нормированных Γ точную верхнюю грань длин всех Γ -норм.

3.3.11. Предложение. Класс $\text{IND}(\mathfrak{A})$ нормированный.

Доказательство. Пусть $R = \tau^{-1}\varphi^\infty$, где τ — сечение и φ позитивный элементарный над $\mathfrak{A}$. Положим $\sigma_0(\bar{a}) = |\tau(\bar{a})|_\varphi$ для $\bar{a} \in R$. $\sigma_0: R \rightarrow |\varphi|$ может не быть нормой, так как его область значений может не быть начальным сегментом ординалов. Но существует единственная сохраняющая порядок f , отображающая область значений σ_0 на ординал λ . Тогда, если $\sigma(\bar{a}) = f(\sigma_0(\bar{a}))$ для $\bar{a} \in R$, то $\sigma: R \rightarrow \lambda$ является нормой на R длины $\lambda \leq |\varphi|$.

Заметьте, что для $\bar{a}, \bar{b} \in A^n$ $\bar{a} <_\sigma^* \bar{b}$ тогда и только тогда, когда $\tau(\bar{a}) <_\varphi^* \tau(\bar{b})$ и аналогично для $\leq_\sigma^*$. Следовательно, для доказательства предложения достаточно показать, что $<_\varphi^*$ и $\leq_\varphi^*$ лежат в $\text{IND}(\mathfrak{A})$. Это следует вот из чего:

3.3.12. Первая теорема о пошаговом сравнении. Пусть $\varphi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ будет позитивным элементарным оператором. Тогда существуют позитивные элементарные операторы $\varphi_<, \varphi_\leq: \text{Pow}(A^{2n}) \rightarrow \text{Pow}(A^{2n})$ такие, что

$$<_\varphi^* = I(\varphi_<) \quad \text{и} \quad \leq_\varphi^* = I(\varphi_\leq).$$

Более того, $\varphi_<(X) = \{(\bar{a}, \bar{b}) \in A^{2n} \mid (\bar{b}, \bar{a}) \in \varphi_\leq(X)\}$ для $X \subseteq A^{2n}$.

Доказательство. $\varphi_{\leq}$ и $\varphi_{\leq^*}$ определяются следующим образом. Пусть $\theta(X) = \{(\bar{a}, \bar{b}) \in A^{2n} \mid \bar{a} \in \varphi'(\{\bar{x} \in A^n \mid (\bar{b}, \bar{x}) \in X\})\}$ для $X \subseteq A^{2n}$, где $\varphi'(Y) = \varphi(Y) \cup Y$ для $Y \subseteq A^n$. Затем полагаем $\varphi_{\leq}(X) = \theta(\theta(X))$ для $X \subseteq A^{2n}$ и определяем $\varphi_{\leq}$, как требуется в теореме. Теперь заметим, что θ является позитивным элементарным, и, следовательно, $\varphi_{\leq}$ и $\varphi_{\leq^*}$ такие же. Доказательство того, что эти операторы индуктивно определяют $\leq^*$ и $<^*$, легко вытекает из следующей леммы. $\square$

3.3.13. Лемма. Для всех ординалов λ

$$\bar{a} <^* \bar{b} \wedge \bar{a} \in \varphi^\lambda \Leftrightarrow (\bar{a}, \bar{b}) \in \varphi_{\leq}^\lambda,$$

$$\bar{a} \leq^* \bar{b} \wedge \bar{a} \in \varphi^\lambda \Leftrightarrow (\bar{a}, \bar{b}) \in \varphi_{\leq}^\lambda.$$

Доказательство. Эта лемма доказывается индукцией по λ . $\square$

3.3.14. Определение. Предикат R на A такой, что и R , и $\neg R$ лежат в $\text{IND}(\mathfrak{A})$, называется *гиперэлементарным над $\mathfrak{A}$* . Через $\text{HYP}(\mathfrak{A})$ обозначаем класс таких предикатов.

Этот класс обобщает класс гиперарифметических предикатов на ω .

3.3.15. Следствие. Если $\varphi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ является позитивным элементарным над $\mathfrak{A}$, то $\varphi^\lambda \in \text{HYP}(\mathfrak{A})$ для всех $\lambda < |\varphi|$.

Доказательство. Если $\lambda < |\varphi|$, то $\lambda = |\bar{a}|_\varphi$ для некоторого $\bar{a} \in I(\varphi)$. Тогда

$$\begin{aligned} \varphi^\lambda &= \{\bar{x} \in A^n \mid \bar{x} \leq^* \bar{a}\} = \{\bar{x} \in A^n \mid (\bar{x}, \bar{a}) \in \varphi_{\leq}^\infty\} = \\ &= \{\bar{x} \in A^n \mid (\bar{a}, \bar{x}) \in \varphi_{\leq}^\infty\}, \\ \neg \varphi^\lambda &= \{\bar{x} \in A^n \mid \bar{a} <^* \bar{x}\} = \{\bar{x} \in A^n \mid (\bar{a}, \bar{x}) \in \varphi_{\leq}^\infty\}. \end{aligned}$$

Поэтому, если $\tau(\bar{x}) = (\bar{a}, \bar{x})$ для $\bar{x} \in A^n$, то

$$\varphi^\lambda = \tau^{-1} \varphi_{\leq}^\infty \quad \text{и} \quad \neg \varphi^\lambda = \tau^{-1} \varphi_{\leq}^\infty.$$

Следовательно, $\varphi^\lambda \in \text{HYP}(\mathfrak{A})$. $\square$

Основные свойства класса Π_1^1 -предикатов на ω и, более общо, класса $\text{IND}(\mathfrak{A})$ для приемлемых алгебраических систем $\mathfrak{A}$ содержатся в следующем важном определении, впервые введенном в книге Московакиса [1].

3.3.16. Определение. Класс Γ предикатов на множестве A называется *спекторовским классом над $\mathfrak{A}$* , если:

(i) Γ позитивно элементарно замкнут над $\mathfrak{A}$ (см. предложение 3.3.1);

(ii) Γ содержит кодирующую схему $\mathcal{C}$ на A (т. е. $N, \leq, \text{Seq}$, графики lh, q и s и их дополнения лежат в Γ ; все упомянутые объекты определены в определении 2.3.2);

(iii) Γ обладает свойством параметризации (см. определение 3.2.5);

(iv) Γ нормированный.

3.3.17. Теорема. Если $\mathfrak{A}$ — приемлемая алгебраическая система, то $\text{IND}(\mathfrak{A})$ является наименьшим спекторовским классом над $\mathfrak{A}$.

Этот результат справедлив также при несколько более слабом предположении, что $\mathfrak{A}$ является почти приемлемой, что означает, что $\text{IND}(\mathfrak{A})$ содержит кодирующую схему на A . То, что $\text{IND}(\mathfrak{A})$ является спекторовским классом над $\mathfrak{A}$, получается комбинированием предложений 3.3.1, 3.3.12 и следствия 3.3.6. Чтобы доказать, что он наименьший, требуется следующий результат о спекторовских классах.

3.3.18. Теорема. Пусть Γ будет спекторовским классом над $\mathfrak{A}$, и пусть $\varphi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ будет позитивным элементарным над $\mathfrak{A}$. Тогда $I(\varphi) \in \Gamma$.

Доказательство. Мы укажем схему доказательства. Детали можно найти в 9А книги Московакиса [1]. По свойству параметризации выберем $U \subseteq A^{n+2}$ из Γ для параметризации $(n+1)$ -местных предикатов из Γ . Пусть $\tau: U \rightarrow \kappa$ будет Γ -нормой на U . Положим $Q(t, \bar{a}) \Leftrightarrow \bar{a} \in \varphi(\{\bar{x} \in A^n \mid (t, t, \bar{x}) <^*_{\tau} (t, t, \bar{a})\})$. Тогда, поскольку Γ позитивно элементарно замкнут, $Q \in \Gamma$ и, следовательно, $Q = U_a$ для некоторого $a \in A$.

Положим $P(\bar{a}) \Leftrightarrow Q(a, \bar{a})$ для $\bar{a} \in A^n$. Пусть $\sigma_0: P \rightarrow \kappa$ задается как $\sigma_0(\bar{a}) = \tau(a, a, \bar{a})$ для $a \in P$. σ_0 может быть не сюръективным, но, беря суперпозицию σ_0 с сохраняющим порядок отображением области значений σ_0 на начальный сегмент ординалов, мы получим норму σ на P . Тогда для $\alpha \in A^n$

$$P(\bar{a}) \Leftrightarrow \bar{a} \in \varphi(\{\bar{x} \in A^n \mid \bar{x} <^*_{\sigma} \bar{a}\}).$$

Но легко проверить, что всякий предикат P с нормой, удовлетворяющей этой эквивалентности, должен совпадать с $I(\varphi)$. Следовательно, поскольку $P \in \Gamma$, $I(\varphi) \in \Gamma$. $\square$

Ординал $\kappa(\mathfrak{A})$ может быть охарактеризован через $\text{IND}(\mathfrak{A})$ как точная верхняя грань длин позитивных элементарных индуктивных норм над $\mathfrak{A}$, т. е. имеет место

3.3.19. Теорема. $\kappa(\mathfrak{A}) = o(\text{Ind}(\mathfrak{A}))$.

Следующий результат обобщает теорему Спектора — Ганди для Π_1^1 -предикатов на ω .

3.3.20. Обобщенная теорема Спектора -- Ганди. Пусть $\mathfrak{A}$ будет приемлемой алгебраической системой. Если $R \subseteq A^n$, то $R \in \text{IND}(\mathfrak{A})$, если и только если существует элементарный предикат $\mathcal{R}$ языка второго порядка такой, что для $\bar{a} \in A^n$

$$R(\bar{a}) \Leftrightarrow \exists X \in \text{HYP}(\mathfrak{A}) \mathcal{R}(X, \bar{a}).$$

Этот результат был впервые сформулирован и доказан в книге Московакиса [1]. Упрощение этого доказательства было дано Ацелом [2]. Оно использовало новое доказательство второй теоремы Московакиса о пошаговом сравнении (7С.1 из книги Московакиса [1]). Следующее предложение является главным необходимым нам фактом.

3.3.21. Предложение. Пусть $\varphi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ будет позитивным элементарным над $\mathfrak{A}$. Тогда существует предикат Q второго порядка, элементарный над $\mathfrak{A}$ и такой, что если $\bar{a} \in I(\varphi)$, или $\bar{b} \in I(\varphi)$, то следующие условия эквивалентны:

- (i) $\bar{a} \leq_{\varphi}^* \bar{b}$,
- (ii) $\exists X Q(X, \bar{a}, \bar{b})$,
- (iii) $\exists X \in \text{HYP}(\mathfrak{A}) Q(X, \bar{a}, \bar{b})$.

Доказательство. Пусть $\varphi_{\leq}: \text{Pow}(A^{2n}) \rightarrow \text{Pow}(A^{2n})$ будет оператором, использованным в первой теореме 3.3.12 о пошаговом сравнении. Положим $Q(X, \bar{a}) \Leftrightarrow \bar{a} \in X \wedge X \subseteq \varphi_{\leq}(X)$ для $X \subseteq A^{2n}$ и $\bar{a} \in A^{2n}$. Тогда Q элементарный над $\mathfrak{A}$. (i) и (ii) эквивалентны в силу

$$\begin{aligned} \bar{a} \leq_{\varphi}^* \bar{b} &\Leftrightarrow \neg \bar{b} <_{\varphi}^* \bar{a} \Leftrightarrow (\bar{b}, \bar{a}) \notin \varphi_{\leq}^{\infty} \Leftrightarrow (\bar{a}, \bar{b}) \notin (\varphi_{\leq}^{\infty})^{\infty} \\ &\Leftrightarrow \neg \forall Y [\varphi_{\leq}^{\infty}(Y) \subseteq Y \Rightarrow Y(\bar{a}, \bar{b})] \\ &\Leftrightarrow \exists X [\varphi_{\leq}^{\infty}(\neg X) \subseteq \neg X \wedge X(\bar{a}, \bar{b})] \Leftrightarrow \exists X Q(X, \bar{a}, \bar{b}). \end{aligned}$$

Поскольку (iii) $\Rightarrow$ (ii) тривиально, остается доказать только (i) $\Rightarrow$ (iii). Поэтому пусть $\bar{a} \leq_{\varphi}^* \bar{b}$. Тогда $\bar{a} \in \varphi^{\lambda}$ для некоторого $\lambda < |\varphi|$, и, следовательно, по определению 3.3.13 $(\bar{a}, \bar{b}) \in \varphi_{\leq}^{\lambda}$. Так как $\varphi_{\leq}^{\lambda} \subseteq \varphi(\varphi_{\leq}^{\lambda})$, то $Q(\varphi_{\leq}^{\lambda}, \bar{a}, \bar{b})$. Так как $\lambda < |\varphi| = |\varphi_{\leq}|$, из следствия 3.3.15 получаем, что $|\varphi_{\leq}^{\lambda}| \in \text{HYP}(\mathfrak{A})$. Следовательно, $\exists X \in \text{HYP}(\mathfrak{A}) Q(X, \bar{a}, \bar{b})$. $\square$

Мы закончим наше описание теории позитивной элементарной индукции теоремой Московакиса о нормальной форме для приемлемых алгебраических систем, которую дадим без доказательства. Для этого нам нужно ввести игровой квантор.

В общем случае под квантором на множестве A мы понимаем множество $Q \subseteq \text{Pow}(A)$. Если $R \subseteq A$, то пишем $QzR(z)$ вместо $R \subseteq Q$. Например, кванторы всеобщности и существования на A — это $\exists = \text{Pow}(A) - \{\emptyset\}$ и $\forall = \{A\}$.

Если задана элементарная кодирующая схема для алгебраической системы $\mathfrak{A}$, то игровой квантор G на A — это множество тех $R \subseteq A$, что

$$\{\forall x_1 \exists y_1 \forall x_2 \exists y_2 \dots\} \bigvee_{m \in \omega} R(\langle x_1, y_1, \dots, x_m, y_m \rangle). \quad (*)$$

Уравнение (*) интерпретируется обычным образом через игру $\mathcal{G}(R)$ между двумя игроками $\exists$ и $\forall$, которые по очереди выбирают элементы из A , начиная с $\forall$, чтобы получить последовательность $x_1, y_1, x_2, y_2, \dots$. Если для некоторого m $\langle x_1, y_1, \dots, x_m, y_m \rangle \in R$, то игрок $\exists$ выигрывает. Если этого не происходит, то игрок $\forall$ выигрывает. Теперь (*) интерпретируется как означающее то, что игрок $\exists$ обладает выигрышной стратегией для игры $\mathcal{G}(R)$.

3.3.22. Теорема (5С из книги Московакиса [1]). Пусть $\mathfrak{A}$ будет приемлемой алгебраической системой. Пусть G будет игровым квантором на A относительно некоторой элементарной кодирующей схемы для $\mathfrak{A}$. Тогда для $R \subseteq A^n$ $R \in \text{IND}(\mathfrak{A})$, если и только если существует элементарный предикат $S \subseteq A^{n+1}$ такой, что для $\bar{a} \in A^n$

$$R(\bar{a}) \Leftrightarrow GzS(z, \bar{a}).$$

3.4. Релятивизация относительно нетривиального монотонного квантора. В этом пункте мы укажем, как понятия и результаты предыдущего пункта могут быть обобщены при помощи релятивизации относительно нетривиального монотонного квантора Q на A . $Q \subseteq \text{Pow}(A)$ является нетривиальным, если $Q \neq \emptyset$ и $Q \neq \text{Pow}(A)$. Q является монотонным, если $A \supseteq X \supseteq Y \in Q$ влечет, что $X \in Q$. Квантор $\check{Q}$, дуальный к Q , задается как $\check{Q}zR(z) \Leftrightarrow \neg Qz \neg R(z)$. Язык $L^A(Q)$ определяется, как L^A , и добавляется, что разрешается строить формулы $Qz\varphi(z)$ и $\check{Q}z\varphi(z)$ для всякой формулы $\varphi(z)$.

Стандартная интерпретация L^A расширяется на предложения из $L^A(Q)$ требованием, что

$Qx\varphi(x)$ истинно только и только тогда, когда

$$\{a \in A \mid \varphi(a) \text{ истинно}\} \in Q,$$

и аналогично для $\check{Q}x\varphi(x)$.

Язык $L(\mathfrak{A}, Q)$ — это подязык $L^A(Q)$, соответствующий подязыку $L(\mathfrak{A})$ языка L^A . Позитивные и негативные вхождения предикатов в формулы из $L^A(Q)$ определяем, рассматри-

вая $\mathcal{Q}$ и $\check{\mathcal{Q}}$ таким же образом, что и обычные кванторы. Определим $\mathcal{Q}$ -элементарные формулы языка $L^A(\mathcal{Q})$ аналогично элементарным формулам L^A , за исключением того, что допускается $\mathcal{Q}x$ и $\check{\mathcal{Q}}x$. Теперь определим $\text{IND}(\mathcal{M}, \mathcal{Q})$, как в определении $\text{IND}(\mathcal{M})$, только используем позитивные $\mathcal{Q}$ -элементарные операторы вместо позитивных элементарных.

Теперь результат из 3.3 об $\text{IND}(\mathcal{M})$ переносится на $\text{IND}(\mathcal{M}, \mathcal{Q})$ с подходящими изменениями, а именно «элементарный» должно быть заменено на « $\mathcal{Q}$ -элементарный». Там, где требовалось, чтобы $\mathcal{M}$ была приемлемой, достаточно теперь, чтобы $\mathcal{M}$ была $\mathcal{Q}$ -приемлемой, т. е. существовала $\mathcal{Q}$ -элементарная кодирующая схема. Среди позитивных $\mathcal{Q}$ -элементарных операторов имеются $\mathcal{Q}''$ и $\check{\mathcal{Q}}''$, определяемые аналогично $\mathcal{V}''$ и $\check{\mathcal{E}}''$. Теория $T_\infty(\mathcal{M})$ должна быть заменена на теорию $T_\infty(\mathcal{M}, \mathcal{Q})$. Эта теория получается из $T_\infty(\mathcal{M})$ разрешением использовать $\mathcal{Q}$ -элементарные формулы и добавлением следующих, возможно бесконечных, правил:

$\mathcal{Q}$ -правило: из $\theta(a)$ для $a \in X$ выводится $\mathcal{Q}x\theta(x)$, если $X \in \mathcal{Q}$.

$\check{\mathcal{Q}}$ -правило: из $\theta(a)$ для $a \in X$ выводится $\check{\mathcal{Q}}x\theta(x)$, если $X \in \check{\mathcal{Q}}$. (См. Ацел [1], где рассматриваются такие правила.) Используя $T_\infty(\mathcal{M}, \mathcal{Q})$, результаты 3.3.3 — 3.3.6 переносим на $\text{IND}(\mathcal{M}, \mathcal{Q})$. По-видимому, нет никаких аналогов теоремы 3.3.7. Перенесением теоремы 3.3.17 получаем, что если $\mathcal{M}$ является $\mathcal{Q}$ -приемлемой, то $\text{IND}(\mathcal{M}, \mathcal{Q})$ является наименьшим спекторовским

классом над $\mathcal{M}$, замкнутым относительно всех $\mathcal{Q}''$ и $\check{\mathcal{Q}}''$.

Обобщенная теорема Спектора — Ганди 3.3.20 также переносится на $\text{IND}(\mathcal{M}, \mathcal{Q})$. Конечно, вместо $\text{HYP}(\mathcal{M})$ нужно использовать $\text{HYP}(\mathcal{M}, \mathcal{Q})$.

Теорема о нормальной форме 3.3.22 также переносится, но для нее необходимо обобщить игровые кванторы. Это проделывается в работе Ацела [4], где показывается, как интерпретировать произвольную бесконечную последовательность $\mathcal{Q}_1x_1\mathcal{Q}_2x_2\dots$ негравитальных монотонных кванторов при помощи следующей перемежающейся последовательности обычных кванторов:

$$\exists x_1 \in \mathcal{Q}_1 \forall x_1 \in X_1 \exists x_2 \in \mathcal{Q}_2 \forall x_2 \in X_2 \dots$$

Эта последовательность может быть интерпретирована при помощи игры между двумя игроками, как в определении игрового квантора. Теперь по данной $\mathcal{Q}$ -элементарной кодирующей схеме для алгебраической системы $\mathcal{M}$ мы определяем релятивизацию $\mathcal{Q}^+$ игрового квантора как множество таких $R \subseteq A$, что

$$\{\mathcal{Q}x_1\check{\mathcal{Q}}y_1\mathcal{Q}x_2\check{\mathcal{Q}}y_2\mathcal{Q}x_3\check{\mathcal{Q}}y_3\dots\} \vee R(\langle x_1, y_1, \dots, x_m, y_m \rangle).$$

$m \in \omega$

Заметьте, что $\mathcal{V}^+$ — это в точности игровой квантор $\mathcal{G}$. Теорема 3.3.22 переносится на $\text{IND}(\mathcal{M}, \mathcal{Q})$, если $\mathcal{G}$ заменить на $\mathcal{Q}^+$.

Мы закончим этот пункт формулировкой важного **недавно** полученного результата.

3.4.1. Теорема (Харрингтон [1]). Пусть $\mathcal{M}$ будет приемлемой алгебраической системой. Каждый спекторовский класс над $\mathcal{M}$ имеет вид $\text{IND}(\mathcal{M}, \mathcal{Q})$ для некоторого нетривиального монотонного квантора $\mathcal{Q}$ на A .

3.5. Немонотонная индукция. Первые примеры немонотонных индуктивных определений — это появившиеся при построении различных систем обозначений для все больших сегментов счетных ординалов. Первые такие системы были предложены Чёрчем и Клини для рекурсивных ординалов. Один такой пример — система $\mathcal{O}$ Клини, рассмотренная в 2.2. Первый ординал, не имеющий обозначения в $\mathcal{O}$, есть ординал Чёрча — Клини ω_1 , т. е. рекурсивный аналог первого несчетного ординала. Индуктивное определение $\mathcal{O}$ использует монотонный оператор. Но попытки продолжить $\mathcal{O}$ до систем обозначений для рекурсивных аналогов более высоких числовых классов до сих пор приводили к немонотонным операторам. Например, пусть $\varphi: \text{Pow}(\omega) \rightarrow \text{Pow}(\omega)$ будет монотонным оператором, ассоциированным с регулярно арифметическим множеством правил, порождающим клиниевскую систему $\mathcal{O}$ в 2.2. Мы можем расширить φ , добавляя обозначение 7 (к примеру) для ординала ω_1 и затем продолжая, как и раньше, т. е. мы определяем немонотонный оператор $\varphi_1: \text{Pow}(\omega) \rightarrow \text{Pow}(\omega)$:

$$\varphi_1(X) = \begin{cases} \varphi(X), & \text{если } \varphi(X) \not\subseteq X, \\ \{7\}, & \text{если } \varphi(X) \subseteq X, \end{cases} \text{ для } X \subseteq \omega.$$

Тогда $\varphi_1^\lambda = \varphi^\lambda$ для $\lambda < |\varphi| = \omega_1$, так что $\varphi_1^{\omega_1} = \varphi^{<\omega_1} \cup \{7\} = \mathcal{O} \cup \{7\}$.

Следовательно, $|\varphi_1|_{\omega_1} = \omega_1$. Легко видеть, что $|\varphi_1| = \omega_1 + \omega_1$,

так что φ_1^∞ есть множество обозначений для ординалов $< \omega_1 + \omega_1$. Так можно продолжать достаточно далеко и прийти к системам обозначений для значительно больших ординалов таких, как рекурсивные аналоги конечных и бесконечных спекторовских классов порядковых чисел. (См. Аддисон и Клини [1], Крейдер и Роджерс [1], Патнем [1] и Рихтер [1] — [3].)

Упомянутые работы связаны с деталями конкретных систем обозначений. В работе Патнема [2] предпринят более общий подход, при котором показано, что произвольные Δ_2^1 -индуктивные определения могут дать системы обозначений для начальных сегментов только Δ_2^1 -ординалов (т. е. порядковых типов Δ_2^1 -вполне упорядочений натуральных чисел). В дальней-

ших работах интерес переместился от изучения конкретных индуктивно определяемых систем обозначений к изучению классов $\mathcal{E}$ индуктивных определений на ω и связанных с ними ординалов $|\mathcal{E}|$. Изменение, поддержанное Ганди, привело к работам: Рихтер [4], Ацел и Рихтер [1], Рихтер и Ацел [1], Ондеро [1], Цензер [1] и Рихтер [5]. В этих работах дается характеристика $|\mathcal{E}|$ для различных классов $\mathcal{E}$ через рекурсивные аналоги больших кардиналов. Эти аналоги определяются при помощи теории Крипке о рекурсии на допустимых ординалах. Отправной точкой является рассмотрение допустимых ординалов как рекурсивных аналогов регулярных кардиналов. Оказывается, что первым допустимым и большим ω ординалом является ординал Чёрча — Клини ω_1 , так что эти два подхода к рекурсивным аналогам согласуются. Другими аналогами являются рекурсивно недостижимые (допустимые пределы допустимых ординалов) и рекурсивные ординалы Мало (допустимые α такие, что для всякой α -рекурсивной $f: \alpha \rightarrow \alpha$ существует допустимый $\beta < \alpha$, замкнутый относительно f). Для получения рекурсивных аналогов еще больших кардиналов Рихтер и Ацел [1] ввели принципы рефлексии. Примерами являются Π_{n+2}^0 -рефлексивные ординалы, представляющие рекурсивный аналог Π_n^1 -неописываемых кардиналов для $n > 0$.

Ниже мы сформулируем некоторые полученные результаты. Но сначала нужна конструкция, изобретенная Рихтером [4]. Для данных $\Phi: \text{Pow}(\omega) \rightarrow \text{Pow}(\omega)$ определим $[\Phi, \Psi]: \text{Pow}(\omega) \rightarrow \text{Pow}(\omega)$ так:

$$[\Phi, \Psi](X) = \begin{cases} \Phi(X), & \text{если } \Phi(X) \not\subseteq X, \\ \Psi(X), & \text{если } \Phi(X) \subseteq X, \end{cases} \text{ для } X \subseteq \omega.$$

Заметьте, что введенный выше Φ_1 есть $[\Phi, \Psi]$, где $\Psi(X) = \{7\}$ для всех $X \subseteq \omega$. Если $\mathcal{E}_1, \mathcal{E}_2$ — классы операторов на ω , то положим $[\mathcal{E}_1, \mathcal{E}_2] = \{[\Phi_1, \Phi_2] \mid \Phi_1 \in \mathcal{E}_1 \text{ и } \Phi_2 \in \mathcal{E}_2\}$.

3.5.1. Предложение. (i) $|\Pi_0^0| = \omega$.

(ii) (Ганди, неопубликовано) $|\Pi_1^0| = \omega_1$.

(iii) (Патнем [2]) $|\Delta_2^1| = \delta_2^1$, первому не Δ_2^1 -ординалу.

(iv) (Рихтер [4]) $|\Pi_0^0, \Pi_0^0| = \omega^2$. $|\Pi_1^0, \Pi_0^0|$ равно первому рекурсивно недостижимому ординалу. $|\Pi_1^0, \Pi_1^0|$ равно первому рекурсивному ординалу Мало.

(v) (Ацел и Рихтер [1]) $|\Pi_n^0| = |\Sigma_{n+1}^0|$ равно первому Π_{n+1}^0 -рефлексивному ординалу.

(vi) (Ацел и Рихтер [1]) $|\Pi_1^1|$ равно первому Π_1^1 -рефлексивному ординалу, $|\Sigma_1^1|$ равно первому Σ_1^1 -рефлексивному ординалу.

(vii) (Рихтер [5]) $|\Pi_2^1|$ равно первому Π_2^1 -рефлексивному ординалу.

(viii) (Ондеро [1]) $|\Pi_1^1| < |\Sigma_1^1|$ и $|\Sigma_2^1| < |\Pi_2^1|$.

В вышеупомянутых статьях можно найти значительно большее число результатов. Интересно сравнить эти результаты с соответствующими результатами для классов позитивных и монотонных операторов на ω .

3.5.2. Предложение. (i) $|\text{pos-}\Sigma_1^0| = |\text{mon-}\Sigma_1^0| = \omega$.

(ii) (Спектор [1]) $|\text{pos-}\Pi_1^0| = |\text{mon-}\Pi_1^0| = \omega_1$.

(iii) (Грийо, не опубликовано) $|\text{pos-}\Sigma_1^1| = |\text{mon-}\Sigma_1^1| = |\Sigma_1^1|$.

(iv) (Ганди, не опубликовано) $|\text{pos-}\Sigma_2^1| = |\text{mon-}\Sigma_2^1| = \delta_2^1$.

Московакис недавно поставил проблему характеристики ординала $|\text{pos-}\Pi_2^1| = |\text{mon-}\Pi_2^1|$. До сих пор неизвестно даже, является ли этот ординал допустимым.

Выше мы сформулировали результаты только о $|\mathcal{E}|$. Конечно, класс $\text{IND}(\mathcal{E})$ также представляет интерес. При общих предположениях о $\mathcal{E}$ ординал $|\mathcal{E}|$ допустим и $\text{IND}(\mathcal{E})$ является спекторовским классом таким, что $|\mathcal{E}| = o(\text{IND}(\mathcal{E}))$. Более того, во многих случаях, рассмотренных Рихтером и Ацелом [1], $\text{IND}(\mathcal{E})$ может быть охарактеризован на языке α -рекурсии как класс α -р.п. предикатов на ω , где $\alpha = |\mathcal{E}|$.

Теория немонотонной индукции на ω была наиболее элегантно обобщена на алгебраические системы Московакисом [2]. Центральным в этой работе является понятие *типового немонотонного* класса предикатов второго порядка над абстрактной алгебраической системой $\mathfrak{A}$. Примерами являются классы Σ_k^m -или Π_k^m -определимых предикатов второго порядка над $\mathfrak{A}$ при $k, m \geq 1$ или $m = 0$ и $k \geq 2$. В случае $m = 0$ эти классы определяются в зависимости от гиперэлементарной кодирующей схемы над $\mathfrak{A}$, как в 2.3.

3.5.3. Теорема (Московакис [2]). Пусть $\mathcal{T}$ — *типовой немонотонный класс предикатов второго порядка на $\mathfrak{A}$* . Пусть $\mathcal{E}$ будет *множеством операторов* $\Phi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ таких, что $\{(\bar{x}, X) \in A^n \times \text{Pow}(A^n) \mid \bar{x} \in \Phi(X)\}$ *лежит в $\mathcal{T}$* . Тогда $\text{IND}(\mathcal{E})$ является спекторовским классом над $\mathfrak{A}$ и $|\mathcal{E}| = o(\text{IND}(\mathcal{E}))$.

Московакис собирается охарактеризовать $\text{IND}(\mathcal{E})$ как наименьший спекторовский класс над $\mathfrak{A}$, удовлетворяющий некоторым дополнительным условиям.

Мы закончим этот пункт формулировкой одного частного случая интересного общего результата из статьи Харрингтона и Кекриса [1].

Пусть $\mathfrak{A}$ будет приемлемой алгебраической системой, и пусть $\mathcal{E}(\text{pos-}\mathcal{E}, \text{mon-}\mathcal{E})$ будет классом элементарных (позитивных

элементарных, монотонных элементарных) операторов над $\mathfrak{A}$. Положим $WF = \{S \subseteq A^2 \mid S \text{ фундировано}\}$.

3.5.4. Теорема (Харрингтон и Кекрис [1]). Если WF элементарно над $\mathfrak{A}$, то $IND(\mathcal{E}) = IND(\text{мон-}\mathcal{E})$.

Этот результат контрастирует с ситуацией для счетных $\mathfrak{A}$, где $IND(\text{pos-}\mathcal{E}) = \Pi_1^1(\mathfrak{A}) = IND(\text{мон-}\mathcal{E})$. ($IND(\mathcal{E})$ всегда намного больше, чем $IND(\text{pos-}\mathcal{E})$.)

3.6. Индукция и допустимые множества. В этом пункте мы предполагаем некоторое знакомство с понятием допустимого множества (см. главу 7 «Теории моделей»).

Для данного допустимого множества A пусть $\mathfrak{A} = \langle A, \in \upharpoonright A^2 \rangle$. Класс Σ_1 -формул языка L^A строится из атомарных формул и их отрицаний при помощи $\vee$, $\wedge$, $\exists x$ и ограниченного квантора всеобщности $\forall x \in y$. Как в 2.3, Σ_1 -предикаты над $\mathfrak{A}$ — это те предикаты на A , которые определимы над A посредством Σ_1 -формул из $L(\mathfrak{A})$. (Заметьте, это означает, что разрешаются константы для элементов из A .) Как в 3.1, мы определяем класс операторов $\Phi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$, которые являются позитивными Σ_1 -операторами над $\mathfrak{A}$, ординал $o(A)$ множества A — это наименьший ординал не из A . Наконец, напомним, что предикат $R \subseteq A^n$ является A -конечным, если $R \subseteq A$. (Заметьте, что, поскольку A замкнуто относительно образования пар, $A^n \subseteq A$ для $n > 0$. Поэтому каждый предикат на A является подмножеством A .) Допустимые множества интересны во многом в связи с бесконечными языками L_A , связанными с ними. Напомним, что эти языки являются расширениями языков первого порядка, в которых формулы представлены теоретико-множественно как элементы A , и разрешены бесконечные конъюнкции и дизъюнкции $\bigwedge \Phi$ и $\bigvee \Phi$, если Φ является A -конечным множеством формул. Так же как синтаксис языков первого порядка полон эффективно заданных финитарных индуктивных определений, синтаксис L_A использует следующее. Пусть далее A является фиксированным допустимым множеством.

3.6.1. Определение. (i) Множество правил Φ на A называется A -финитарным, если множество посылок каждого правила из Φ является A -конечным.

(ii) A -финитарное множество правил Φ называется Σ_1 -множеством над $\mathfrak{A}$, если оно таково, как бинарный предикат на A .

Следующий результат существенно обобщает предложение 2.1.2 (на самом деле 2.1.2 является по существу частным случаем, когда A есть множество HF наследственно конечных множеств).

3.6.2. Предложение. Если Φ является A -финитарным множеством правил, которое есть Σ_1 -множество над $\mathfrak{A}$, то $I(\Phi)$ является Σ_1 -множеством над $\mathfrak{A}$.

Доказательство. Пусть $\Phi: \text{Pow}(A) \rightarrow \text{Pow}(A)$ будет монотонным оператором, связанным с Φ . Пусть $\text{Pr}_\Phi(a, b)$, если $a \in A$, является Φ -доказательством для b (см. определение 1.4.1). Из предположений легко следует, что Pr_Φ является Σ_1 -предикатом над $\mathfrak{A}$. Следовательно, было бы достаточно показать, что $I(\Phi) = \{b \in A \mid \exists a \in A \text{Pr}_\Phi(a, b)\}$. Но естественное доказательство этого будет работать, если в $\mathfrak{A}$ выполняется предложение «каждое множество может быть вполне упорядочено».

Следовательно, мы используем модификацию понятия Φ -доказательства. Говорим, что $\{a_\mu\}_{\mu \leq \lambda}$ является Φ -квазидоказательством для b , если

$$(i) a_\lambda = \{b\},$$

$$(ii) a_\nu \in \Phi\left(\bigcup_{\mu < \nu} a_\mu\right) \text{ для всех } \nu \leq \lambda.$$

Как и в доказательстве предложения 1.4.2, можно показать, что для произвольного монотонного оператора Φ

$I(\Phi) = \{a \in A \mid a \text{ обладает } \Phi\text{-квазидоказательством}\}$, (*) а доказательство (*) не требует никакой формы аксиомы выбора, в противоположность доказательству 1.4.2.

Теперь пусть $\text{qPr}_\Phi(a, b)$, если $a \in A$ является Φ -квазидоказательством для b . Как легко видеть, qPr_Φ является Σ_1 -предикатом над $\mathfrak{A}$, поэтому достаточно доказать

$$\text{Утверждение. } I(\Phi) = \{b \in A \mid \exists a \in A \text{qPr}_\Phi(a, b)\}.$$

Включение $\supseteq$ следует из (*). Для доказательства обратного включения достаточно показать, что правая часть является Φ -замкнутой. Поэтому пусть $\Phi: X \rightarrow b$ будет таким, что каждый элемент из X обладает Φ -квазидоказательством в A , т. е.

$$\forall x \in X \exists a \in A \text{qPr}_\Phi(a, x).$$

Мы должны найти Φ -квазидоказательство для b в A . Поскольку qPr_Φ является Σ_1 -предикатом над $\mathfrak{A}$, можно использовать сильную аксиому Σ_1 -замены для нахождения множества $Y \subseteq A$ такого, что

$$\forall x \in X \exists a \in Y \text{qPr}_\Phi(a, x)$$

и

$$\forall a \in Y \exists x \in X \text{qPr}_\Phi(a, x).$$

Следовательно, каждый $a \in Y$ является последовательностью $\{a_\mu\}_{\mu \leq \lambda_a}$. Пусть λ будет наименьшим ординалом таким, что $\lambda > \lambda_a$ для всех $a \in Y$, $c_\lambda = \{b\}$ и $c_\mu = \bigcup \{a_\mu \mid a \in Y \text{ и } \mu \leq \lambda_a\}$ для $\mu < \lambda$. Тогда, поскольку A является допустимым множеством, $\lambda < o(A)$ и $c \in A$. Далее, по построению c является Φ -квазидоказательством для b . Поэтому $\exists a \in A \text{qPr}_\Phi(a, b)$. $\square$

Заметьте, что из приведенного утверждения следует, что необходимы только Φ -квазидоказательства $\{a_\mu\}_{\mu \in \lambda}$ длины $\lambda < o(A)$. Следовательно, $|\Phi| \leq o(A)$.

З а м е ч а н и е. То же самое доказательство показывает, что если $\mathfrak{A}$ является моделью ZF, то $I(\Phi)$ определимо формулой логики первого порядка над $\mathfrak{A}$, как только Φ является A -финитарным множеством правил, определяемых формулой первого порядка над $\mathfrak{A}$.

Имеется метод доказательства теоремы Барвайса о компактности для L_A , когда A является счетным допустимым множеством, который использует класс позитивных индуктивных определений, являющихся Σ_1 -определениями над $\mathfrak{A}$. Эта идея была впервые предложена Ганди. Вариант этого подхода можно найти у Ацела [1]. Рассмотрим следующий результат:

3.6.3. Теорема (Ганди). Пусть $\varphi: \text{Pow}(A^n) \rightarrow \text{Pow}(A^n)$ будет позитивным Σ_1 -оператором над $\mathfrak{A}$. Тогда:

- (i) если $R \subseteq A^n$ является Σ_1 -множеством над $\mathfrak{A}$, то $\bar{a} \in \varphi(R)$ влечет $\bar{a} \in \varphi(R')$ для некоторого A -конечного $R' \subseteq R$;
- (ii) $I(\varphi)$ является Σ_1 -множеством над $\mathfrak{A}$ и $|\varphi| \leq o(A)$.

Доказательство. (i) Достаточно показать для каждой Σ_1 -формулы $\theta(X)$ из $L(\mathfrak{A})$, содержащей позитивные вхождения n -местной предикатной переменной X и не содержащей никаких других свободных переменных, что если $R \subseteq A^n$ является Σ_1 -множеством над $\mathfrak{A}$, то $\theta(R)$ влечет $\theta(R')$ для некоторого A -конечного $R' \subseteq R$. Это можно доказать непосредственной индукцией по способу построения $\theta(X)$. Главный случай, когда внешним является ограниченный универсальный квантор, требует применения аксиомы Σ_1 -замены.

(ii) Пусть Φ будет множеством правил $X \rightarrow \bar{a}$ таких, что $X \subseteq A^n$ является A -конечным и $\bar{a} \in \varphi(X)$. Ясно, что Φ будет A -финитарным множеством правил, являющимся Σ_1 -множеством над $\mathfrak{A}$. Следовательно, по предложению 3.6.2 $I(\Phi)$ будет Σ_1 -множеством над $\mathfrak{A}$, так что достаточно показать, что $I(\varphi) = I(\Phi)$. Заметим, что φ не обязательно является монотонным оператором, связанным с Φ , но в силу (i) это так для Σ_1 -предикатов над $\mathfrak{A}$, и нам этого будет достаточно. Чтобы показать, что $I(\varphi) \subseteq I(\Phi)$, достаточно показать, что $I(\Phi)$ является Φ -замкнутым, так что пусть $\bar{x} \in \varphi(I(\Phi))$. Так как $I(\Phi)$ является Σ_1 -множеством над $\mathfrak{A}$, то ввиду (i) существует A -конечное $X \subseteq I(\Phi)$ такое, что $\bar{x} \in \varphi(X)$. Следовательно, $\Phi: X \rightarrow \bar{x}$, так что $\bar{x} \in I(\Phi)$. Чтобы показать, что $I(\Phi) \subseteq I(\varphi)$, достаточно показать, что $I(\Phi)$ является Φ -замкнутым. Пусть $\Phi: X \rightarrow \bar{x}$, где $X \subseteq I(\Phi)$. Тогда $\bar{x} \in \varphi(X) \subseteq \varphi(I(\Phi)) = I(\varphi)$, что и требовалось. Наконец, видно, что неравенство $|\varphi| \leq o(A)$ следует из замечания в конце доказательства предложения 3.6.2. $\square$

Мы закончим этот пункт формулировкой главного результата из статьи Барвайса, Ганди и Московакиса [1].

3.6.4. Определение. Пусть A будет допустимым множеством.

- (i) $\pi: D \rightarrow A$ является *проектированием* x на A , если $D \subseteq \{x \in A\}$, и π есть сюръекция на A .

$\mathfrak{A}$ *проектируемо в* x , если существует проектирование x на A , являющееся Δ_1 -оператором над $\mathfrak{A}$ (т. е. график проектирования и его дополнения являются Σ_1 -множествами над $\mathfrak{A}$).

- (ii) $\tau: o(A) \rightarrow A$ называется *разложением* множества A , если $A = \bigcup_{\alpha < o(A)} \tau(\alpha)$.

$\mathfrak{A}$ *разложимо*, если A допускает разложение, которое является Δ_1 -оператором над $\mathfrak{A}$.

3.6.5. Теорема (Барвайс, Ганди и Московакис [1]). Пусть A будет произвольным транзитивным множеством, замкнутым относительно образования пар. Положим

$$A^+ = \bigcap \{B \mid A \subseteq B \text{ и } B \text{ допустимое}\}.$$

Тогда

- (i) A^+ допустимо,
- (ii) $\text{NYP}(\mathfrak{A})$ является множеством A^+ -конечных предикатов на A и $\kappa(\mathfrak{A}) = o(A^+)$ и если $\mathfrak{A}^+ = \langle A^+, \in \upharpoonright A^+ \rangle$, то
- (iii) $\mathfrak{A}^+$ разложимо и проектируемо в A , а $\text{IND}(\mathfrak{A})$ — множество предикатов на A , являющихся Σ_1 -предикатами над $\mathfrak{A}^+$.

З а м е ч а н и я. Этот результат обобщен в двух направлениях. Во-первых, $\text{IND}(\mathfrak{A})$ может быть заменено произвольным спекторовским классом Γ над $\mathfrak{A} = \langle A, \in \upharpoonright A \rangle$ для любого транзитивного множества A . Тогда A^+ должно быть заменено на $M(\Delta)$, где $\Delta = \Gamma \cup \upharpoonright \Gamma$ и $M(\Delta) = \bigcap \{B \mid \Delta \subseteq B \text{ и } B \text{ допустимое}\}$.

В (ii) $\text{NYP}(\mathfrak{A})$ и $\kappa(\mathfrak{A})$ должны быть заменены на Δ и $o(\Gamma)$ соответственно. (iii)' заменяется на (iii)':

- (iii)' Существует предикат R на $M(\Delta)$ такой, что $M(\Delta)$ допустимо относительно R и $\mathcal{M}(\Delta) = \langle M(\Delta), \in \upharpoonright M(\Delta)^2, R \rangle$ разложимо и проектируемо на A . Более того, Γ является множеством предикатов на A , являющихся Σ_1 -предикатами над $\mathcal{M}(\Delta)$.

Хотя R и, следовательно, $\mathcal{M}(\Delta)$ не являются единственными, класс предикатов на $M(\Delta)$, являющихся Σ_1 -предикатами над $\mathcal{M}(\Delta)$, не зависит от выбора R и называется компаньоном Γ . Это первое обобщение дано в 9Е.1 книги Московакиса [1]. Второе обобщение состоит в том, чтобы разрешить $\mathfrak{A}$ быть произвольной абстрактной системой. Для этого требуется поня-

тие допустимой системы с множеством A праэлементов, которое было введено Барвайсом [1], [2]. Детали были разработаны Еннисом [1]. Там Еннис показал, что этот результат все еще выполняется, если в определении спектровского класса условие (ii) ослабить до (ii)'.

(ii)' Γ содержит график функции образования пар на A .

§ 4. Индукция в основаниях математики

В этом последнем параграфе мы кратко рассмотрим роль индуктивных определений в контексте оснований математики. До сих пор мы безоговорочно принимали стандартные рамки современной математики, формализуемой в теории множеств ZF. Но понятие индуктивного определения может быть также рассмотрено в других концептуальных рамках, появившихся в работах по основаниям математики (например, финитистской, предикативной или интуиционистской математике). В рамках неклассической математики возникает вопрос о том, какие индуктивные определения законны.

Будет полезно делать различие между фундаментальными и нефундаментальными индуктивными определениями, следуя терминологии § 53 книги Клини [1]. Это различие касается контекста, в котором задано индуктивное определение. Индуктивное определение области $\mathbb{N}$ натуральных чисел наиболее естественно задается как основное определение объекта нового типа. Но в контексте теории множеств ZF натуральные числа $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots$ являются объектами, которые существуют независимо от индуктивного определения ω . Поэтому последнее не является фундаментальным индуктивным определением. Другим примером является индуктивное определение множества четных чисел как наименьшего множества натуральных чисел, содержащего 0 и $n+2$, как только оно содержит n .

Стандартная модель теории множеств ZF задается фундаментальным индуктивным определением универсума (фундированных) множеств. Оно состоит из набора правил: Если s является множеством объектов универсума, то и само s является объектом универсума.

В то время как фундаментальные индуктивные определения, связанные с концептуальными рамками, обычно будут ясны, для определения того, какие нефундаментальные индуктивные определения законны, может потребоваться дальнейший анализ. Например, для данного набора Φ правил на области $\mathbb{N}$ натуральных чисел мы определили $I(\Phi)$ как $\bigcap \{X \subseteq \mathbb{N} \mid X \text{ является } \Phi\text{-замкнутым}\}$, т. е.

$$n \in I(\Phi) \Leftrightarrow (\forall X \subseteq \mathbb{N}) [X \text{ является } \Phi\text{-замкнутым} \rightarrow n \in X].$$

Но это является непредикативным частным случаем схемы аксиом выделения (подмножество множества $\mathbb{N}$ определяется при помощи квантификации по всем подмножествам $\mathbb{N}$). Если непредикативные определения запрещены, мы должны найти другое возможное определение $I(\Phi)$. Если Φ финитарно, мы можем использовать предложение 1.1.4. В общем случае $I(\Phi)$ можно было бы определить, используя трансфинитные итерации операторов, как в предложении 1.3.1, или трансфинитные доказательства, как в предложении 1.4.2. Но это потребовало бы подходящего понятия ординала, что в свою очередь нуждалось бы в индуктивном определении. Другим подходом является рассмотрение индукции как примитивного метода определения, не требующего оправдания через другие методы.

Примером формальной системы, в которой индукция считается примитивным понятием, является система ID_1 у Фейермана [2] (см. также Фридман [1], Цукер [1] и Мартин-Лёф [1]). Язык системы ID_1 получается из языка формальной арифметики добавлением нового n -арного предикатного символа P_ϕ для каждой арифметической формулы $\phi = \phi(X, \bar{x})$, содержащей только позитивные вхождения n -местной предикатной переменной X и все предметные свободные переменные которой содержатся в $\bar{x} = x_1, \dots, x_n$. Аксиомы системы ID_1 получаются из аксиом формальной арифметики расширением схемы математической индукции на все формулы из ID_1 и добавлением аксиомы и схемы аксиом для каждого P_ϕ :

$$(i) \quad \forall \bar{x} (\phi(P_\phi, \bar{x}) \rightarrow P_\phi(\bar{x})),$$

$$(ii) \quad \forall \bar{x} (\phi(\{\bar{z} \mid \psi(\bar{z})\}, \bar{x}) \rightarrow \psi(\bar{x})) \rightarrow \forall \bar{x} (P_\phi(\bar{x}) \rightarrow \psi(\bar{x}))$$

для всех формул $\psi(\bar{z})$ из ID_1 .

В (ii) $\phi(\{\bar{z} \mid \psi(\bar{z})\}, \bar{x})$ обозначает результат замены каждого вхождения $X(\bar{t})$ в $\phi(X, \bar{x})$ на $\psi(\bar{t})$, где $\bar{t} = t_1, \dots, t_n$ является последовательностью термов, и связанные переменные заменяются в соответствии с обычными соглашениями.

На стандартной модели арифметики эти аксиомы выражают то, что P_ϕ индуктивно определяется позитивным арифметическим оператором, определяемым $\phi(X, \bar{x})$.

Процедура построения ID_1 из формальной арифметики может быть повторена для построения $ID_2, ID_3, \dots$. Но получающиеся системы все же значительно слабее, чем полностью непредикативные системы такие, как арифметика второго порядка. С другой стороны, ID_1 уже сильнее, чем системы предикативной математики из работы Фейермана [1]. Таким образом, индуктивная определимость является понятием, промежуточным по силе между предикативной и полностью непредикативной определимостью.

Было бы интересно сформулировать связную концептуальную доктрину, делающую индукцию главным понятием. В литературе имеются предложения на этот счет, но все же возможность эта не была еще полностью использована.

ЛИТЕРАТУРА

- Аддисон и Клини (Addison J. W., Kleene S. C.)
1. A note on function quantification. — Proc. Amer. Math. Soc., 1957, 8, p. 1002—1006.
- Ацел (Aczel P.)
1. Representability in some systems of second order arithmetic. — Israel J. Math., 1970, 8, p. 309—328.
2. Stage comparison theorem and game playing with inductive definitions. — 1972.
3. Infinitary logic and the Barwise compactness theorem. — In: Proceedings of the Bertrand Russell Logic Conference/Ed. J. Bell, J. Cole, G. Priest and A. Slomson, 1973, p. 234—277.
4. Quantifiers, games and inductive definitions. — In: Third Scandinavian Logic Symposium/Ed. S. Kanger. Amsterdam: North-Holland, 1975, p. 1—14.
- Ацел и Рихтер (Aczel P., Richter W.)
1. Inductive definitions and analogues of large cardinals. — In: Conference in Mathematical Logic — London'70. Berlin: Springer, 1972, p. 1—9.
- Барвайс (Barwise J.)
1. Admissible sets over models of set theory. — In: Generalized Recursion Theory/Ed. J. E. Fenstad and P. G. Hinman. Amsterdam: North-Holland, 1974, p. 97—122.
2. Admissible Sets and Structures. — Berlin: Springer, 1975.
- Барвайс, Ганди и Московакис (Barwise J., Gandy R. O., Moschovakis Y. N.)
1. The next admissible set. — J. Symbolic Logic, 1971, 36, p. 108—120.
- Ганди (Gandy R. O.)
1. Inductive definitions. — In: Generalized Recursion Theory/Ed. J. E. Fenstad and P. G. Hinman. Amsterdam: North-Holland, 1974, p. 265—300.
- Гжегорчик, Мостовский и Рыль-Нардзевский (Grzegorzczuk A., Mostowski A., Ryll-Nardzewski C.)
1. The classical and ω -complete arithmetic. — J. Symbolic Logic, 1958, 23, p. 188—206.
- Грийо (Grilliot T. J.)
1. Model theory for dissecting recursion theory. — In: Generalized Recursion Theory/Ed. J. E. Fenstad and P. G. Hinman. Amsterdam: North-Holland, 1974, p. 421—428.
- Еннис (Ennis G.)
1. An extension of the next admissible set construction. — Mimeographed notes, 1975.
- Клини (Kleene S. C.)
1. Introduction to Metamathematics. — Princeton (N. J.): Van Nostrand, 1952. [Русский перевод: Клини С. К. Введение в метаматематику. — М.: ИЛ, 1957.]
- Крейдер и Роджерс (Kreider D. L., Rogers H., Jr.)
1. Constructive versions of ordinal number classes. — Trans. Amer. Math. Soc., 1961, 100, p. 325—369.
- Мартин-Лёф (Martin-Löf P.)
1. Hauptsatz for the intuitionistic theory of iterated inductive definitions. — In: Proceedings of the Second Scandinavian Logic Symposium/Ed. J. E. Fenstad. Amsterdam: North-Holland, 1971, p. 179—216.

- Московакис (Moschovakis Y. N.)
1. Elementary Induction on Abstract Structures. — Amsterdam: North-Holland, 1974.
2. On non-monotone inductive definability. — Fundam. math., 1974, 82, p. 39—83.
3. On the basic notions in the theory of induction. — Preprint, 1976.
- Онделро (Aanderaa S.)
1. Inductive definitions and their closure ordinals. — In: Generalized Recursion Theory/Ed. J. E. Fenstad and P. G. Hinman. Amsterdam: North-Holland, 1974, p. 207—220.
- Патнем (Putnam H.)
1. Uniqueness ordinals in higher constructive number classes. — In: Essays on the Foundations of Mathematics: Dedicated to A. A. Fraenkel/Ed. Y. Bar-Hillel et al. Jerusalem: Magnes Press, 1961, p. 190—206.
2. On hierarchies and systems of notations. — Proc. Amer. Math. Soc., 1964, 15, p. 44—50.
- Пост (Post E.)
1. Formal reductions of the general combinatorial decision problem. — Amer. J. Math., 1943, 65, p. 197—215.
- Рихтер (Richter W.)
1. Extensions of the constructive ordinals. — J. Symbolic Logic, 1965, 30, p. 193—211.
2. Constructive transfinite number classes. — Bull. Amer. Math. Soc., 1967, 73, p. 261—265.
3. Constructively accessible ordinal numbers. — J. Symbolic Logic, 1968, 33, p. 43—55.
4. Recursively Mahlo ordinals and inductive definitions. — In: Logic Colloquium'69/Ed. R. O. Gandy and C. E. M. Yates. Amsterdam: North-Holland, 1971, p. 273—288.
5. The least Σ_1^1 and Π_1^1 -reflecting ordinals. — 1976.
- Рихтер и Ацел (Richter W., Aczel P.)
1. Inductive definitions and reflecting properties of admissible ordinals. — In: Generalized Recursion Theory/Ed. J. E. Fenstad and P. G. Hinman. Amsterdam: North-Holland, 1974, p. 301—384.
- Смальян (Smullyan R. M.)
1. Theory of Formal Systems. — Princeton (N. J.): Princeton University Press, 1961. [Русский перевод: Смальян Р. М. Теория формальных систем. — М.: Наука, 1981.]
- Спектор (Spector C.)
1. Inductively defined sets of natural numbers. — In: Infinitistic Methods: Proceedings of the Warsaw symposium. Oxford: Pergamon Press, 1961, p. 97—102.
- Фенстади и Хинмен (Fenstad J. E., Hinman P. G., ed.)
1. Generalized Recursion Theory. — Amsterdam: North-Holland, 1974.
- Феферман (Feferman S.)
1. Autonomous transfinite progressions and the extent of predicative mathematics. — In: Logic, Methodology and Philosophy of Science, III/Ed. B. van Rootselaar and J. F. Staal. Amsterdam: North-Holland, 1968, p. 121—135.
2. Formal theories for transfinite iterations of generalized inductive definitions and some subsystems of analysis. — In: Intuitionism and Proof Theory/Ed. A. Kino, J. Myhill and R. E. Vesley. Amsterdam: North-Holland, 1970, p. 303—326.
- Фридман (Friedman H.)
1. Iterated inductive definition and Σ_1^1 — AC. — In: Intuitionism and Proof Theory/Ed. A. Kino, J. Myhill and R. E. Vesley. Amsterdam: North-Holland, 1970, p. 435—442.

- Харрингтон (Harrington L. A.)
 1. Monotone quantifiers and inductive definability. — Mimeographed notes, 1975.
- Харрингтон и Кекрис (Harrington L. A., Kechris A. S.)
 1. On monotone versus non-monotone induction. — Mimeographed notes, 1975.
- Цензер (Cenzer D.)
 1. Ordinal recursion and inductive definitions. — In: Generalized Recursion Theory/Ed. J. E. Fenstad and P. G. Hinman. Amsterdam: North-Holland, 1974, p. 221—264.
- Цукер (Zucker J. I.)
 1. Iterated inductive definitions, trees and ordinals. — In: Metamathematical Investigation of Intuitionistic Arithmetic and Analysis/Ed. A. S. Troelstra. Berlin: Springer, 1973.
- Чэн и Кейслер (Chang C. C., Keisler H. J.)
 1. Model Theory. — Amsterdam: North-Holland, 1973. [Русский перевод: Кейслер Х. Дж., Чэн Ч. Ч. Теория моделей. — М.: Мир, 1977.]

АЛГОРИТМИЧЕСКИЕ ПРОБЛЕМЫ В ТЕОРИИ ПОЛЕЙ (положительные аспекты)

Ю. Л. Ершов

СОДЕРЖАНИЕ

§ 1. Конструктивные поля	270
1. Введение в теорию нумераций (270). 2. Конструктивные поля (273). 3. Конструктивные поля со свойством (F) (281). 4. Конструктивизация универсальной области (288).	
§ 2. Регулярно замкнутые поля	296
1. Алгебраические свойства регулярно замкнутых полей (297). 2. Допустимые классы конечных групп (306). 3. Теоретико-модельные свойства регулярно замкнутых полей (318). 4. Теория стратов Галуа (331).	
Заключение	348
Литература	351

Теория полей всегда являлась ареной, где возникали или апробировались всевозможные алгоритмические проблемы. Начало этому положили многочисленные алгоритмические проблемы теории чисел и алгебраической геометрии. Настоящий обзор будет касаться только новых постановок и только положительных решений алгоритмических проблем: проблем разрешимости элементарных теорий тех или иных классов полей и проблем, связанных с понятием конструктивизации. Хорошо известны результаты об элементарных теориях классических полей:

1. *Элементарная теория поля $\mathbb{Q}$ рациональных чисел неразрешима* (Робинсон [1]).
2. *Элементарные теории каждого из полей $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_k$ (комплексных, вещественных и p -адических чисел соответственно) разрешимы* (Тарский [1], [2], Ершов [1], Акс и Кочен [1]).
3. *Элементарная теория класса всех (простых) конечных полей разрешима* (Акс [2]).

Каждый из положительных результатов относительно элементарных теорий классических полей к настоящему времени получил существенное расширение. Так, теория регулярно замкнутых полей, которая весьма подробно изложена во втором параграфе, является далеко идущим обобщением теории алгебраически замкнутых полей, а источник этого обобщения лежит в исследованиях теории конечных полей. Теория поля $\mathbb{R}$ — теория вещественно замкнутых полей — оказалась первой в классе экзи-

стенциально замкнутых полей с n порядками (или n -упорядоченных полей; см. заключение), имеющих разрешимую теорию (в ан ден Дрис [1]). Разрешимость поля $\mathbb{Q}_p$ привела к проблемам исследования элементарных теорий нормированных полей (Ершов [5]). Оказалось, как и в случае упорядоченных полей, что существует интересная теория кратно нормированных полей (Ершов [7]). Точные формулировки результатов о кратно упорядоченных и кратно нормированных полях будут даны в заключении.

Первый параграф содержит очерковое изложение теории конструктивных полей. Начинается он с краткого изложения некоторых понятий и результатов общей теории нумераций. Существование на русском языке книг Ершова [4], [5] позволило уделять в этом параграфе большее внимание тем вопросам, где встречается специфика теории полей.

Второй параграф содержит подробное алгебраическое, теоретико-модельное изучение класса регулярно замкнутых полей, класса весьма богатого и интересного. В пп. 3 и 4 этого параграфа даются два различных подхода к изучению элементарных теорий регулярно замкнутых полей. Первый подход теоретико-модельный, второй — прямая элиминация кванторов в теории стратов Галуа. Пункт 2 имеет вспомогательный характер, но в этом пункте положительно решается одна алгоритмическая проблема о классах конечных групп, которая существенно используется в следующих пунктах.

Следует отметить, что имеется ряд весьма интересных положительных результатов в изучении алгоритмических проблем над полями, которые не попали в настоящий обзор, ограниченный указанными выше проблемами элементарных теорий и конструктивизаций. В качестве примера укажем на работы Саркисян [1], [2]; Грюнвальд и Сегал [1], [2], в которых положительно решены некоторые алгоритмические вопросы об алгебраических группах над конструктивными полями.

§ 1. Конструктивные поля

1. Введение в теорию нумераций. Пусть S — произвольное непустое не более чем счетное множество. *Нумерацией* множества S называется всякое отображение v множества ω всех натуральных чисел на множество S . Пара $\mathcal{S} = (S, v)$, где v — некоторая нумерация множества S , называется *нумерованным множеством*. Если $\mathcal{S}_0 = (S_0, v_0)$ и $\mathcal{S}_1 = (S_1, v_1)$ — нумерованные множества, то *морфизм* из $\mathcal{S}_0$ в $\mathcal{S}_1$ называется любое отображение $\mu: S_0 \rightarrow S_1$, для которого существует рекурсивная функция f такая, что $\mu v_0 = v_1 f$. Если $S_0 \subseteq S_1$ и μ — отображение вложения, то в случае, когда μ — морфизм из $\mathcal{S}_0$ в $\mathcal{S}_1$, будем гово-

рить, что нумерация v_0 *сводится* к нумерации v_1 , и обозначать это $v_0 \leq v_1$; если еще $S_0 = S_1$ и $v_1 \leq v_0$, то нумерации v_0 и v_1 называются *эквивалентными*, и обозначать это будем так: $v_0 \equiv v_1$. Множество всех морфизмов из $\mathcal{S}_0$ в $\mathcal{S}_1$ обозначается $\text{Mor}(\mathcal{S}_0, \mathcal{S}_1)$. Класс всех нумерованных множеств, расширенный естественным образом «пустым» нумерованным множеством 0 , вместе с определенными выше морфизмами ($|\text{Mor}(0, \mathcal{S})| = 1$, $\text{Mor}(\mathcal{S}, 0) = \emptyset$, если $\mathcal{S} \neq 0$) образует категорию $\mathfrak{N}$ нумерованных множеств.

Рассмотрим несколько примеров.

Пример 1. Пусть $S_2 \equiv \{0, 1\}$; с каждой нумерацией v множества S_2 свяжем множество $M_v \equiv \{x | x \in \omega, vx = 1\}$. Так между нумерациями множества S_2 и собственными подмножествами множества ω устанавливается естественное взаимно однозначное соответствие. Легко видеть из определения, что если v_0 и v_1 — нумерации множества S_2 , то v_0 сводится к v_1 тогда и только тогда, когда множество M_{v_0} m -сводится к множеству M_{v_1} . Таким образом, если через $L(S_2)$ обозначить семейство классов эквивалентных нумераций множества S_2 с частичным порядком, индуцированным отношением сводимости, то $L(S_2)$ естественно изоморфно верхней полурешетке $L_m m$ -степеней всех (собственных) подмножеств множества ω .

Пример 2. Пусть $n \in \omega$, $n \geq 2$, $S_n \equiv \{0, 1, \dots, n-1\}$; тогда, как в примере 1, существует естественная связь нумераций множества S_n и их сводимостей с понятием кратной m -сводимости непересекающихся систем из $n-1$ подмножеств ω . Если $L(S_n)$ — частично упорядоченное множество классов эквивалентных нумераций множества S_n , то оказывается (Ершов [4], приложение II), что $L(S_n)$ обладает довольно удивительными алгебраическими свойствами универсальности, что позволяет установить, в частности, что $L(S_n)$ изоморфно $L(S_2)$.

Пример 3. Пусть $\mathcal{N}$ — семейство всех рекурсивно перечислимых подмножеств ω . Нумерация $v: \omega \rightarrow \mathcal{N}$ называется *вычислимой*, если множество пар $\{\langle x, y \rangle | x \in vy\}$ рекурсивно перечислимо. Если некоторая нумерация эквивалентна вычислимой, то она сама вычислима. Обозначим через $L^0(\mathcal{N})$ частично упорядоченное множество (верхнюю полурешетку) классов эквивалентных вычислимых нумераций. Одним из наиболее замечательных свойств этой полурешетки является существование в $L^0(\mathcal{N})$ наибольшего элемента. Другими словами, существует такая вычислимая нумерация (нумерация Поста) $\pi: \omega \rightarrow \mathcal{N}$, что любая другая вычислимая нумерация к ней сводится. Такие нумерации называются *главными вычислимыми*.

Пример 4. Пусть $R \subseteq \mathcal{N}$ — некоторое семейство рекурсивно перечислимых множеств. Определение вычислимости ну-

мерации $v: \omega \rightarrow R$ то же, что и в примере 3. Пусть $L^0(R)$ — верхняя полурешетка (или пустое множество) классов эквивалентных вычислимых нумераций множества R . Существует большое разнообразие таких полурешеток (см. Ершов [4]).

Одной из главных задач общей теории нумераций является задача: как «правильно» нумеровать те множества, которые естественно возникают при рассмотрении нумерованных множеств. Многие из таких задач сводятся к решению более частной проблемы: как «правильно» занумеровать семейство $\text{Mog}(\mathcal{C}_0, \mathcal{C}_1)$ всех морфизмов из одного нумерованного множества $\mathcal{C}_0$ в другое $\mathcal{C}_1$?

Укажем вкратце схему решения этой проблемы (заметим сразу, что она имеет решение далеко не для всех пар $(\mathcal{C}_0, \mathcal{C}_1)$). Начнем с указания, что категория $\mathfrak{N}$ нумерованных множеств обладает конечными суммами и произведениями. Обозначим через N объект — т. е. нумерованное множество — $(\omega, \text{id}_\omega)$ категории $\mathfrak{N}$.

Пусть $S \in \text{Mog}(\mathcal{C}_0, \mathcal{C}_1)$ — некоторое семейство морфизмов из $\mathcal{C}_0$ в $\mathcal{C}_1$; нумерацию $v: \omega \rightarrow S$ этого семейства назовем *вычислимой*, если связанное с этой нумерацией отображение $\hat{v}: \omega \times S_0 \rightarrow S_1$, определенное так: $\hat{v}(n, s_0) \hat{=} [v(n)](s_0) (\in S_1)$, $n \in \omega$, $s_0 \in S_0$, является морфизмом из прямого произведения $N \times \mathcal{C}_0$ в $\mathcal{C}_1$. Нумерация $v: \omega \rightarrow \text{Mog}(\mathcal{C}_0, \mathcal{C}_1)$ называется *главной вычислимой*, если она вычислима и любая вычислимая нумерация любого семейства $S \in \text{Mog}(\mathcal{C}_0, \mathcal{C}_1)$ к ней сводится. Будем говорить, что для пары нумерованных множеств $(\mathcal{C}_0, \mathcal{C}_1)$ разрешима проблема P (и записывать это просто $P(\mathcal{C}_0, \mathcal{C}_1)$), если семейство $\text{Mog}(\mathcal{C}_0, \mathcal{C}_1)$ обладает главной вычислимой нумерацией. Если для пары $(\mathcal{C}_0, \mathcal{C}_1)$ разрешима проблема P , то главная вычислимая нумерация v^* (определенная однозначно с точностью до эквивалентности) и будет искомой «правильной» нумерацией семейства $\text{Mog}(\mathcal{C}_0, \mathcal{C}_1)$; в этом случае нумерованное множество $(\text{Mog}(\mathcal{C}_0, \mathcal{C}_1), v^*)$ будем обозначать $\mathfrak{Mog}(\mathcal{C}_0, \mathcal{C}_1)$. То, что это решение является «правильным», подтверждает следующая теоретико-категорная теорема, которая сразу устанавливает связь рассматриваемой проблемы с аналогичными проблемами, которые решались, например, в алгебраической геометрии и других разделах математики.

Теорема. Для любой пары $(\mathcal{C}_0, \mathcal{C}_1)$ нумерованных множеств следующие два утверждения эквивалентны;

- 1) для пары $(\mathcal{C}_0, \mathcal{C}_1)$ разрешима проблема P ;
- 2) функтор $\text{Mog}(- \times \mathcal{C}_0, \mathcal{C}_1)$ из категории $\mathfrak{N}$ в категорию множеств представим.

При выполнении этих условий нумерованное множество $\mathfrak{Mog}(\mathcal{C}_0, \mathcal{C}_1)$ и представляет этот функтор, т. е. функторы $\text{Mog}(- \times \mathcal{C}_0, \mathcal{C}_1)$ и $\text{Mog}(-, \mathfrak{Mog}(\mathcal{C}_0, \mathcal{C}_1))$ эквивалентны. $\square$

В книге Ершова [4] указаны некоторые широкие достаточные условия разрешимости проблемы P , которые позволяют, в частности, определить класс (частичных) вычислимых функционалов конечных типов так:

Определим множество T конечных типов следующим рекурсивным определением: $0 \in T$; $\sigma, \tau \in T \Rightarrow (\sigma \times \tau), (\sigma \rightarrow \tau) \in T$.

Пусть $\mathcal{K}_0$ — это множество всех не более чем одноэлементных подмножеств ω , т. е. $\mathcal{K}_0 = \{\emptyset, \{0\}, \{1\}, \dots\}$, а π_0 — главная вычислимая нумерация $\mathcal{K}_0$ (заметим, что $\mathcal{K}_0 \in \mathcal{K}$); полагаем $\mathfrak{P} \hat{=} (\mathcal{K}_0, \pi_0)$.

Если $\mathfrak{P}_\sigma, \mathfrak{P}_\tau$ — нумерованные множества вычислимых функционалов типов σ и τ соответственно, то $\mathfrak{P}_{(\sigma \times \tau)} \hat{=} \mathfrak{P}_\sigma \times \mathfrak{P}_\tau$ и $\mathfrak{P}_{(\sigma \rightarrow \tau)} \hat{=} \text{Mog}(\mathfrak{P}_\sigma, \mathfrak{P}_\tau)$.

2. Конструктивные поля. Начнем с определений, относящихся к произвольной сигнатуре $\sigma_0 = \langle P_0^{n_0}, \dots, P_i^{n_i}, \dots \rangle_{i < k} \cup \langle f_0^{m_0}, \dots, f_j^{m_j}, \dots \rangle_{j < l} \cup \langle c_0, \dots, c_s, \dots \rangle_{s < r}$, $k, l, t \leq \omega$, такой, что функции $i \mapsto n_i, j \mapsto m_j$ рекурсивны. Пусть $\sigma_1 \hat{=} \sigma_0 \cup \langle a_0, a_1, \dots \rangle$ и $g: \omega \rightarrow L_{\sigma_1}$ — гёделева нумерация всех формул сигнатуры σ_1 с равенством, полученная любым естественным образом. Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры σ_0 , а $v: \omega \rightarrow |\mathfrak{A}|$ — нумерация основного множества этой системы, тогда пара $(\mathfrak{A}, v)$ называется *нумерованной системой*. Через $\mathfrak{A}_v$ обозначим обогащение системы $\mathfrak{A}$ до сигнатуры σ_1 , полученное так: $a_n^v \hat{=} vn, n \in \omega$. Обозначим через $\text{Th}_0(\mathfrak{A}, v)$ бескванторную теорию системы $\mathfrak{A}_v$, т. е. совокупность всех бескванторных предложений сигнатуры σ_1 , истинных в $\mathfrak{A}_v$, а через $\text{Th}(\mathfrak{A}, v)$ — элементарную теорию системы $\mathfrak{A}_v$, т. е. совокупность всех предложений сигнатуры σ_1 , истинных в $\mathfrak{A}_v$. Нумерованную систему $(\mathfrak{A}, v)$ назовем *конструктивной*, если разрешима бескванторная теория $\text{Th}_0(\mathfrak{A}, v)$ системы $\mathfrak{A}_v$, т. е. если множество $g^{-1}(\text{Th}_0(\mathfrak{A}, v))$ гёделевых номеров предложений из $\text{Th}_0(\mathfrak{A}, v)$ рекурсивно; $(\mathfrak{A}, v)$ *сильно конструктивна*, если разрешима элементарная теория $\text{Th}(\mathfrak{A}, v)$ системы $\mathfrak{A}_v$. Нумерацию $v: \omega \rightarrow |\mathfrak{A}|$ назовем (*сильной*) *конструктивизацией*, если нумерованная система $(\mathfrak{A}, v)$ (*сильно*) конструктивна. Система $\mathfrak{A}$ называется (*сильно*) *конструктивизируемой*, если у системы $\mathfrak{A}$ имеется по крайней мере одна (*сильная*) конструктивизация.

В качестве примера сильно конструктивизируемых систем можно указать всякую конечную систему конечной сигнатуры. В частности, всякое конечное поле сильно конструктивизируемо.

Поле $\mathbb{Q}$ всех рациональных чисел, очевидно, является конструктивизируемым.

Укажем два очевидных утверждения:

1. Если R — конструктивизируемое кольцо, то и кольцо многочленов $R[x]$ от одной переменной конструктивизируемо. $\square$

2. Если целостное коммутативное кольцо R конструктивизируемо, то конструктивизируемо и его поле частных $F(R)$. $\square$

В качестве следствия этих утверждений получаем

3. Если K — конструктивизируемое поле, то поле $K(x_1, \dots, x_n)$ рациональных функций от n переменных над K также конструктивизируемо. $\square$

З а м е ч а н и е. Классический опыт работы с многочленами позволяет строить по конструктивизации поля K очевидные конструктивизации кольца многочленов от счетного числа переменных $K[x_1, \dots, x_n, \dots]$ и поля частных $K(x_1, \dots, x_n, \dots)$ так, что, в частности, справедливо следующее утверждение.

3'. Если поле K конструктивизируемо, то и чисто трансцендентное расширение $K(x_1, \dots, x_n, \dots)$ степени ω над K также конструктивизируемо. $\square$

4. Если поле K конструктивизируемо, $K(\alpha)$ — простое алгебраическое расширение K , то $K(\alpha)$ конструктивизируемо.

Действительно, если $v: \omega \rightarrow K[x]$ — естественная конструктивизация кольца многочленов от одной переменной, продолжающая некоторую конструктивизацию поля K , а $f \in K[x]$ — минимальный многочлен для α над K , то идеал $(f) \triangleq \{g \mid g \in K[x], f \mid g \text{ (} f \text{ делит } g)\}$ является рекурсивным (т. е. $v^{-1}((f))$ рекурсивно). Отсюда сразу следует, что нумерация $v_\alpha: \omega \rightarrow K(\alpha)$, полученная как композиция нумерации v и естественного эпиморфизма $\varphi: K[x] \rightarrow K(\alpha)$ ($\text{Кер } \varphi = (f)$), является конструктивизацией $K(\alpha)$. $\square$

5. Если K — конструктивизируемое поле, L — конечно порожденное расширение K , то L конструктивизируемо.

Это следствие утверждений 3 и 4. $\square$

Сформулируем теперь один общий результат о существовании конструктивных моделей. Начнем с определений. Пусть Φ — некоторое множество формул сигнатуры σ_0 , содержащих единственную свободную переменную. Φ -алгебраическим элементом алгебраической системы $\mathcal{A}$ сигнатуры σ_0 называется всякий элемент $a \in |\mathcal{A}|$ такой, что $\mathcal{A} \models \varphi(a)$ и множество $\{b \mid b \in |\mathcal{A}|, \mathcal{A} \models \varphi(b)\}$ конечно для некоторой формулы φ из Φ . Через $\mathcal{A}_\Phi$ обозначим подсистему $\mathcal{A}$, порожденную всеми Φ -алгебраическими элементами системы $\mathcal{A}$. Будем говорить, что теория T сигнатуры σ_0 имеет Φ -ядро, если существует такая система $\mathcal{A}^0 \models T$, что для любой системы $\mathcal{A} \models T$ существует изоморфное вложение $\sigma: \mathcal{A}_\Phi^0 \rightarrow \mathcal{A}_\Phi$ такое, что для $a \in |\mathcal{A}_\Phi^0|$ и $\varphi \in \Phi$

$$\mathcal{A}^0 \models \varphi(a) \Leftrightarrow \mathcal{A} \models \varphi(\sigma a).$$

В этом случае алгебраическая система $\mathcal{A}_\Phi^0$ (определенная однозначно с точностью до изоморфизма) и называется Φ -ядром теории T и обозначается $C(T, \Phi)$.

Справедлива (Ершов [5]) следующая

Теорема о ядре. Если T — рекурсивно перечислимая теория сигнатуры σ_0 , Φ — рекурсивно перечислимое множество формул и T имеет Φ -ядро, то оно конструктивизируемо. $\square$

Укажем некоторые применения теоремы о ядре

Пусть (K, v) — конструктивное поле, T_{ac} — теория алгебраически замкнутых полей. Пусть T — теория сигнатуры $\sigma = \sigma_f \cup \langle a_0, a_1, \dots \rangle$, определенная рекурсивной системой аксиом $T_{ac} \cup \text{Th}_0(K, v)$; Φ — совокупность всех бескванторных формул сигнатуры σ , имеющих одну свободную переменную, тогда теория T имеет Φ -ядро и это Φ -ядро естественно изоморфно алгебраическому замыканию поля K . Таким образом получаем

6. Если поле K конструктивизируемо, то конструктивизируемо и его алгебраическое замыкание. $\square$

Из утверждений 6, 3 и 3' следует

7. Любое счетное алгебраически замкнутое поле является конструктивизируемым. $\square$

З а м е ч а н и я 1. Если некоторая теория T допускает эффективную элиминацию кванторов, то всякая конструктивизация системы $\mathcal{A}$ такой, что $\mathcal{A} \models T$, является сильной. Следовательно, любое счетное алгебраически замкнутое поле сильно конструктивизируемо.

2. Имеется другое общее утверждение (Хисамиев [1], Харрингтон [1]), из которого вытекает указанный выше результат: если полная разрешимая теория T категорична в не-счетной мощности, то любая счетная система теории T сильно конструктивизируема.

На самом деле рассуждение, которое проведено перед утверждением 6, дает много больше, но для этого нужно дать еще одно определение. Пусть $\mathcal{A}_0 \leq \mathcal{A}_1$ — две системы сигнатуры σ_0 , $v_0: \omega \rightarrow |\mathcal{A}_0|$ — конструктивизация системы $\mathcal{A}_0$; конструктивизация $v_1: \omega \rightarrow |\mathcal{A}_1|$ системы $\mathcal{A}_1$ продолжает конструктивизацию v_0 , если v_0 сводится к v_1 .

Нетрудно теперь видеть, что справедливо утверждение, более точное, чем утверждение 6:

8. Любая конструктивизация поля K продолжается до некоторой конструктивизации его алгебраического замыкания. $\square$

Впервые это было установлено в работе Рабина [1] совершенно другими методами.

Следующее утверждение дает ответ на более общий вопрос: когда конструктивизация поля K продолжается до некоторой конструктивизации его алгебраического расширения L ?

Предложение 1. Пусть L — алгебраическое расширение поля K ; конструктивизация v поля K продолжается до некоторой конструктивизации поля L тогда и только тогда, когда семейство $S_L \rightleftharpoons \{f \mid f \in K[x], f \text{ имеет корень в } L\}$ — рекурсивно перечислимое подмножество кольца $K[x]$ (снабженного конструктивизацией, продолжающей v).

В основе доказательства лежит алгебраический факт о том, что поле L однозначно определено над K семейством S_L ; это позволяет использовать теорему о ядре для установления достаточности. Необходимость же очевидна. $\square$

Сформулируем теперь одно очень простое общее утверждение.

9. Если $(\mathcal{A}, v)$ — конструктивная модель, $\mathcal{A}_0$ — такая подсистема, что множество $v^{-1}(|\mathcal{A}_0|)$ рекурсивно перечислимо, то $\mathcal{A}_0$ имеет конструктивизацию v_0 и притом такую, что v продолжает конструктивизацию v_0 .

Если f — рекурсивная функция, областью значения которой является $v^{-1}(|\mathcal{A}_0|)$, то $v_0 \rightleftharpoons v \circ f$ — искомая конструктивизация. $\square$

Обратимся к вопросам нумераций подполей конструктивного поля (K, v) . Пусть $S(K)$ — система всех подполей поля K . Нумерацию v^* : $\omega \rightarrow S$ некоторого семейства подполей поля K ($S \subseteq S(K)$) назовем *вычислимой*, если предикат $P(x, y) \rightleftharpoons vx \in v^*y$ рекурсивно перечислим.

Заметим сразу, что если v^* — вычислимая нумерация некоторого семейства подполей конструктивного поля (K, v) , то для любого $x \in \omega$ v^*x — такое подполе поля K , что $v^{-1}(v^*x)$ рекурсивно перечислимо; следовательно, в силу утверждения 9 v^*x имеет такую конструктивизацию v_x , что v продолжает v_x . Такие подполя будем называть *конструктивными подполями*. (Заметим, что с точностью до эквивалентности существует единственная конструктивизация такого подполя такая, что вложение есть морфизм.) Через $S_c(K, v)$ будем обозначать семейство всех конструктивных подполей конструктивного поля (K, v) .

Предложение 2. Существует такая вычислимая нумерация v_c семейства $S_c(K, v)$, что любая вычислимая нумерация v^* : $\omega \rightarrow S \subseteq S_c(K, v)$ семейства конструктивных подполей (K, v) сводится к v_c ; другими словами, v_c — *главная вычислимая нумерация семейства $S_c(K, v)$* .

Пусть $R_0 \rightleftharpoons v^{-1}(P)$, где P — простое подполе поля K ; R_0 рекурсивно перечислимо. Если $R \in \mathcal{P}$, то через $\Phi(R)$ обозначим рекурсивно перечислимое множество, определенное так: $\Phi(R) \rightleftharpoons v^{-1}(P(vR))$, т. е. $\Phi(R)$ — это множество всех v -номеров подполя поля K , порожденного над P множеством vR . По-другому $\Phi(R)$ может быть определено как наименьшее множество, удовлетворяющее условиям:

1) $R \cup R_0 \subseteq \Phi(R)$;

2) если $x_0, x_1, x_2 \in \omega$ таковы, что $x_0, x_1 \in \Phi(R)$ и $vx_0 + vx_1 = vx_2$ или $vx_0 \cdot vx_1 = vx_2$ или $vx_0 + vx_2 = vx_1$ или $vx_0 \neq 0$ и $vx_0 \cdot vx_2 = vx_1$, то $x_2 \in \Phi(R)$.

Отсюда (и из конструктивности поля (K, v)) легко следует, что $\Phi: \mathcal{P} \rightarrow \mathcal{P}$ есть морфизм из $\mathcal{P} (\rightleftharpoons \mathcal{P}, \pi)$ в $\mathcal{P}$, т. е. существует рекурсивная функция g такая, что $\Phi(\pi_x) = \pi_{g(x)}$ для любого $x \in \omega$. Φ является ретрагирующим морфизмом ($\Phi^2 = \Phi$). Определим нумерацию v_c так: $v_c \rightleftharpoons v^{-1}\Phi\pi$. Нетрудная проверка того, что v_c есть искомая нумерация, оставляется читателю. $\square$

Заметим, что вычислимые нумерации семейств подполей (K, v) находятся в естественном взаимно однозначном соответствии с вычислимыми семействами рекурсивно перечислимых множеств из $\Phi(\mathcal{P})$.

Следствие 1. Семейство всех конечно порожденных подполей имеет вычислимую нумерацию.

Если h — такая рекурсивная функция, что $\gamma = \pi h$ (γ — стандартная нумерация всех конечных подмножеств ω), то $v_0 \rightleftharpoons v^{-1}\Phi\pi h$ есть вычислимая нумерация всех конечно порожденных подполей. $\square$

Если зафиксировать некоторое конструктивное подполе K_0 , то справедливы утверждения, аналогичные предложению 2 и следствию 1:

Следствие 2. Существует главная вычислимая нумерация семейства $S_c(K_0, K, v) \rightleftharpoons \{L \mid L \in S_c(K, v), K_0 \leq L\}$ всех промежуточных конструктивных подполей. $\square$

Следствие 3. Существует вычислимая нумерация семейства всех подполей K , конечно порожденных над K_0 . $\square$

Как и в случае вычислимых нумераций семейств рекурсивно перечислимых множеств, можно интересоваться, например, однозначными вычислимыми нумерациями подполей. Укажем один из результатов.

Предложение 3. Пусть (K, v) — конструктивное поле, K_0 — конструктивное подполе K такое, что K над K_0 не является конечно порожденным, тогда семейство $S_c(K_0, K, v)$ имеет однозначную вычислимую нумерацию.

Для доказательства предложения нужно воспользоваться теоремой 2 § 6 главы 1 книги Ершова [4] и тем, что семейство $\{v^{-1}L \mid L \in S_c(K_0, K, v)\}$ предельно для вычислимой последовательности

$$\Phi(v^{-1}K_0) \subseteq \dots \subseteq \Phi(v^{-1}K_0 \cup \{0, 1, \dots, n\}) \subseteq \Phi(v^{-1}K_0 \cup \{0, 1, \dots, n, n+1\}) \subseteq \dots \quad \square$$

Введем еще ряд определений. *Гомоморфизмом конструктивной системы $(\mathcal{A}_0, v_0)$ в конструктивную систему $(\mathcal{A}_1, v_1)$ назовем всякое отображение $\mu: |\mathcal{A}_0| \rightarrow |\mathcal{A}_1|$ такое, что μ — гомоморфизм системы $\mathcal{A}_0$ в $\mathcal{A}_1$ и морфизм нумерованного множества*

$(|\mathcal{A}_0|, v_0)$ в нумерованное множество $(|\mathcal{A}_1|, v_1)$. Гомоморфизм конструктивных моделей $\mu: (\mathcal{A}_0, v_0) \rightarrow (\mathcal{A}_1, v_1)$ называется *эквивалентностью*, если μ — изоморфизм $\mathcal{A}_0$ на $\mathcal{A}_1$; системы $(\mathcal{A}_0, v_0)$ и $(\mathcal{A}_1, v_1)$ в этом случае называются *эквивалентными*. Пусть $\mathcal{R}$ — некоторое семейство конструктивных систем; нумерация $\varphi: \omega \rightarrow \mathcal{R}$ этого семейства называется *вычислимой*, если вычислимая индуцированная нумерация семейства рекурсивных множеств $\{g^{-1}(\text{Th}_0(\mathcal{A}, v)) \mid (\mathcal{A}, v) \in \mathcal{R}\}$. Класс конструктивных моделей $\mathcal{R}$ называется *слабо вычислимым*, если существует вычислимая нумерация u такого подкласса $\mathcal{R}_0 \subseteq \mathcal{R}$, что любая конструктивная система из $\mathcal{R}$ эквивалентна подходящей системе из $\mathcal{R}_0$.

Предложение 4. Следующие классы конструктивных полей слабо вычислимы:

- 1) класс конструктивных полей фиксированной характеристики степени трансцендентности $\leq n$ над простым подполем для любого $n \in \omega$;
- 2) класс конструктивных полей фиксированной характеристики конечной степени трансцендентности над простым подполем;
- 3) класс всех конструктивных полей степени трансцендентности $\leq n$ над простым подполем;
- 4) класс всех конструктивных полей конечной степени трансцендентности над простым подполем.

Доказательства этих утверждений вполне аналогичны, поэтому приведем только набросок доказательства утверждения 2).

По утверждению 7 существует некоторая конструктивизация v алгебраически замкнутого поля K счетной степени трансцендентности над простым подполем. Воспользуемся теперь леммой, которая будет доказана позже.

Лемма 1. Если (K_0, v_0) — конструктивное поле конечной степени трансцендентности над простым подполем, а (K, v) — алгебраически замкнутое поле той же характеристики, имеющее степень трансцендентности над простым подполем, не меньшую чем K_0 , то (K_0, v_0) вкладывается в (K, v) как конструктивное подполе. $\square$

В соответствии с леммой достаточно показать, что вычислимо семейство всех конструктивных подполей поля (K, v) , имеющих конечную степень трансцендентности над простым подполем. Поступаем следующим образом. Пусть v_c — главная вычислимая нумерация всех конструктивных подполей поля (K, v) ; для любого $x \in \omega$ пусть K_x — алгебраическое замыкание поля $P(v \upharpoonright^x)$ в поле $v_c \upharpoonright^x(x)$ ($v \upharpoonright^x(x)$). (Здесь l, r — одноместные примитивно рекурсивные функции, осуществляющие вместе с двуместной примитивно рекурсивной функцией s однозначную нумерацию пар натуральных чисел, а γ — стандартная нумерация семейства $P_\omega(\omega)$ всех конечных подмножеств ω .) Ясно,

что отображение $x \mapsto K_x$ есть вычислимая нумерация. Далее, так как K_x есть алгебраическое расширение поля, конечно порожденного над простым подполем P , то K_x имеет конечную степень трансцендентности над P . Наоборот, пусть L — конструктивное подполе поля (K, v) , имеющее конечную степень трансцендентности над P , и пусть u таково, что $L = v_c u$. Далее, пусть $\{a_0, \dots, a_k\}$ — базис трансцендентности L над P и $x_0, \dots, x_k$ — v -номера этих элементов соответственно; если z таково, что $\gamma z = \{x_0, \dots, x_k\}$, а $x \in c(z, u)$, то, очевидно, $K_x = L$. $\square$

Замечание. Класс всех конструктивных полей фиксированной характеристики и класс всех конструктивных расширений фиксированного конструктивного поля не являются слабо вычислимыми. Это вытекает из общих результатов, установленных в работе Добрицы [1]; этот факт установлен также в работе Метакидеса и Нерода [1].

До сих пор обсуждались только вопросы существования конструктивизации или их продолжений. Естественно возникают и вопросы единственности.

Если v_0 и v_1 — две конструктивизации системы $\mathcal{A}$, то они называются *автоэквивалентными*, если конструктивные системы $(\mathcal{A}, v_0)$ и $(\mathcal{A}, v_1)$ эквивалентны; конструктивизации v_0 и v_1 эквивалентны, если они эквивалентны как нумерации множества $|\mathcal{A}|$. Алгебраическая система $\mathcal{A}$ называется *конструктивно устойчивой* (автоустойчивой), если любые ее две конструктивизации эквивалентны (автоэквивалентны).

Простым, но удобным для применений является утверждение

10. Любая конечно порожденная алгебра конечной сигнатуры (т. е. алгебраическая система без предикатных символов в сигнатуре) является конструктивно устойчивой. $\square$

В частности, любое поле, конечно порожденное над своим простым подполем, является конструктивно устойчивым.

Предложение 5. Алгебраически замкнутое поле автоустойчиво тогда и только тогда, когда оно имеет конечную степень трансцендентности над своим простым подполем.

Достаточность будет следовать из рассмотрений следующего пункта. Необходимость вытекает из возможности построения двух конструктивизаций алгебраически замкнутого поля K_ω счетной степени трансцендентности над простым подполем P таких, что при одной конструктивизации свойство алгебраической зависимости над P для конечных подмножеств K_ω разрешимо, а при другой неразрешимо. $\square$

Замечание. Поле K_ω является в терминологии статьи Гончарова [1] моделью с неограниченными ветвлениями, поэтому из общей теоремы этой статьи у поля K_ω существует бесконечно («невчислимо») много неавтоэквивалентных кон-

структуризации. Этот результат о поле K_0 содержится также в работе Метакидеса и Нерода [1].

Рассмотрим более подробно упомянутое в предыдущем предложении свойство алгебраической зависимости. Пусть (K, ν) — конструктивное поле, $K_0 \leq K$ — рекурсивно перечислимое (конструктивное) подполе K . Будем говорить, что понятие алгебраической зависимости в (K, ν) над K_0 эффективно, если существует алгоритм, который по любым двум натуральным числам n и m отвечает на вопрос: будет ли элемент νn алгебраичен над $K_0(\nu m)$. (Здесь νm — конечное множество со стандартным номером m .)

Предложение 6. Алгебраическая зависимость в (K, ν) над K_0 эффективна, если и только если существует рекурсивно перечислимый базис трансцендентности над K_0 .

Необходимость. Рассмотрим только случай, когда степень трансцендентности K над K_0 бесконечна. Строим эффективно последовательность конечных множеств $F_0 \subseteq F_1 \subseteq \dots$ так:

0. Находим наименьшее n_0 такое, что νn_0 не алгебраичен над K_0 ; полагаем $F_0 = \{n_0\}$.

$k+1$. Находим наименьшее n_{k+1} такое, что νn_{k+1} не алгебраичен над $K_0(\nu F_k)$; полагаем $F_{k+1} = F_k \cup \{n_{k+1}\}$.

Если $F_\infty = \bigcup_{n \in \omega} F_n$, то F_∞ рекурсивно перечислимо и νF_∞ — базис трансцендентности K над K_0 .

Достаточность основана на следующих двух фактах:

1) По номеру элемента a поля K и рекурсивно перечисленному заданию базиса K над K_0 можно эффективно найти наименьшее подмножество F базиса такое, что a алгебраичен над $K_0(F)$.

Доказательство основано на лемме 2 § 13 главы 2 книги Зарисского и Самюэля [1]. □

2) По рекурсивно перечисленному заданию базиса K над K_0 и конечному множеству F элементов из K можно эффективно построить новый базис, содержащий некоторое максимальное алгебраически независимое подмножество из F .

Доказательство основано на известной лемме «о замене». □

Предложение доказано. □
Пусть $(\mathcal{A}, \nu)$ — конструктивная система, $\mathcal{A} \leq \mathcal{B}$; конструктивизации ν_0 и ν_1 системы $\mathcal{B}$, продолжающие ν , называются эквивалентными над $(\mathcal{A}, \nu)$, если существует эквивалентность $\mu: (\mathcal{B}, \nu_0) \rightarrow (\mathcal{B}, \nu_1)$ такая, что $\mu \upharpoonright \mathcal{A} = \text{id}_{\mathcal{A}}$.

Аналогом утверждения 10 является

11. Если $\mathcal{B}$ — конечно порожденное расширение алгебры $\mathcal{A}$ конечной сигнатуры, то любые два продолжения на $\mathcal{B}$ любой конструктивизации ν алгебры $\mathcal{A}$ эквивалентны над $(\mathcal{A}, \nu)$. □

Справедливо следующее любопытное

Предложение 7. Любые два продолжения конструктивизации ν поля K на его алгебраическое замыкание K^* эквивалентны над (K, ν) тогда и только тогда, когда для конструктивного поля (K, ν) разрешима проблема разложимости многочленов из $K[x]$.

Достаточность будет установлена в следующем пункте; доказательство необходимости можно найти в работе Метакидеса и Нерода [1]. □

3. Конструктивные поля со свойством (F). Пусть (K, ν) — конструктивное поле. Будем говорить, что оно обладает свойством (F), если множество всех неразложимых многочленов от одной переменной над полем K рекурсивно.

Свойство (F) эквивалентно каждому из следующих:

1) если вложение $(K, \nu) \rightarrow (K^*, \nu^*)$ есть морфизм, где (K^*, ν^*) есть конструктивизация алгебраического замыкания поля K , то $\nu^{*-1}(K)$ — рекурсивное множество;

2) множество всех неразложимых многочленов от одной переменной над K рекурсивно перечислимо.

$(F) \Rightarrow 2)$ очевидно.

$2) \Rightarrow (F)$. Множество всех многочленов от одной переменной состоит из двух непересекающихся взаимно дополнительных подмножеств: разложимых и неразложимых. Если множество неразложимых рекурсивно перечислимо, тогда, взяв всевозможные (нетривиальные) конечные произведения неразложимых, получим, что множество разложимых тоже рекурсивно перечислимо. В силу теоремы Поста эти множества будут рекурсивными.

$(F) \Rightarrow 1)$. Берем элемент a из K^* и находим какой-нибудь многочлен над K , корнем которого он является. Если многочлен разложимый, то, разложив его на множители, найдем неразложимый многочлен, корнем которого является a . Если степень этого многочлена > 1 , то $a \notin K$; в противном случае $a \in K$. Это значит, что K рекурсивно в (K^*, ν^*) ($\nu^{*-1}(K)$ — рекурсивное множество).

$1) \Rightarrow (F)$. Пусть $f \in K[x]$. Над K^* многочлен f разлагается на линейные множители: $f(x) = \prod_{i=0}^k (x - \alpha_i)$. Берем всевозможные произведения $\psi(x) = \prod_{i \in A} (x - \alpha_i)$ и $\varphi(x) = \prod_{i \in A'} (x - \alpha_i)$, где $\emptyset \neq A \subset \{0, \dots, k\}$, $A' = \{0, \dots, k\} - A$. Тогда имеет место представление $f = \psi\varphi$.

Так как K рекурсивно в (K^*, ν^*) , то можно эффективно узнать, лежат коэффициенты многочленов ψ и φ в K или нет. Если найдется множество A такое, чтобы эти ψ и φ были многочленами над K , то многочлен f разложим, а если нет, то неразложим.

3) Существует рекурсивная функция f такая, что $f(n) = [K(v^n): K]$ — степень расширения поля $K(v^n)$ над K .

3) $\Rightarrow$ 1). Пусть f — такая рекурсивная функция, что $f(n) = [K(v^n): K]$. Тогда для любого $n \in \omega$ $v^n \in K \Leftrightarrow f(n) = 1$ и $\text{sg}(f \div 1)$ — характеристическая функция множества $v^{*-1}(K)$; следовательно, $v^{*-1}(K)$ рекурсивно.

($F \Rightarrow$ 3). Пусть вложение $(K, v) \rightarrow (K^*, v^*)$ есть морфизм и (K, v) обладает свойством (F). Для любого $n \in \omega$ эффективно находим минимальный полином, корнем которого является v^n . Степень этого полинома и будет значением функции $f(n) \Leftrightarrow [K(v^n): K]$. Так как эта процедура эффективна, то f будет рекурсивной функцией.

Приведем примеры конструктивных полей, обладающих свойством (F).

Предложение 1. Всякое простое поле (с единственно возможной конструктивизацией) обладает свойством (F).

Это утверждение очевидно для конечных полей и достаточно хорошо известно для поля $\mathbb{Q}$ (см., например, ван дер Варден [1]).

Предложение 2. Если конструктивное поле (K, v) обладает свойством (F), то:

а) поле рациональных функций $K(x)$ от одной переменной над K обладает свойством (F);

б) конечное сепарабельное расширение $K(\alpha)$ обладает свойством (F).

Доказательство утверждения а) использует целозамкнутость кольца $K[x]$ и известный прием Кронекера.

б) Так как свойство (F) эквивалентно 3), то достаточно показать, что функция $f \Leftrightarrow \lambda x [K(\alpha, v^x): K(\alpha)]^*$ рекурсивна.

Возьмем произвольный элемент $\beta \in K^*$, где K^* — алгебраическое замыкание K , и рассмотрим поле $K(\alpha, \beta)$. Так как α — сепарабельный элемент, то в силу теоремы о примитивном элементе (см. ван дер Варден [1], с. 169) существует элемент $\gamma \in K^*$ такой, что $K(\alpha, \beta) = K(\gamma)$. Находим его перебором. Так как (K, v) обладает свойством (F), то эффективно находятся степени $[K(\alpha): K]$ и $[K(\gamma): K]$; из соотношения $[K(\alpha, \beta): K] = [K(\gamma): K] = [K(\alpha, \beta): K(\alpha)] [K(\alpha): K]$ эффективно находим степень $[K(\alpha, \beta): K(\alpha)]$ для каждого $\beta \in K^*$. Таким образом, функция $f \Leftrightarrow \lambda x [K(\alpha, v^x): K(\alpha)]$ рекурсивна, т. е. $K(\alpha)$ удовлетворяет свойству 3), а следовательно, и свойству (F). $\square$

Замечание. Утверждение б), вообще говоря, несправедливо, если отбросить условие сепарабельности (см. Фрелих и Шепердсон [1]).

*) Во избежание путаницы обозначаем λ -оператор и μ -оператор буквами полужирного шрифта. — Прим. ред.

Следствие. Всякое конечно порожденное сепарабельное расширение поля K , обладающее свойством (F), само обладает свойством (F).

Доказываем это, комбинируя 1) и 2). Если степень трансцендентности > 1 , то используем 1) несколько раз. $\square$

Замечание, сделанное в доказательстве предложения по поводу утверждения а), достаточно, чтобы утверждать справедливость следующего предложения.

Предложение 2'. Если конструктивное поле (K, v) обладает свойством (F), то существует конструктивизация v_* чисто трансцендентного расширения $K(x_0, x_1, \dots)$ поля K , продолжающая v , такая, что $(K(x_0, x_1, \dots), v_*)$ обладает свойством (F).

В качестве такой конструктивизации нужно взять конструктивизацию этого поля, «порожденную» естественной конструктивизацией кольца $K[x_0, x_1, \dots]$ многочленов от счетного числа переменных над K . $\square$

Предложение 3. Пусть (K, v) обладает свойством (F), и пусть K' — нормальное расширение K . Тогда существует не более одного продолжения конструктивизации v на K' .

Алгебраическое расширение K' поля K нормально, если любой автоморфизм K^* над K переводит K' на себя. Говоря иначе, K' получается присоединением к K всех корней неразложимых многочленов над K , которые имеют хотя бы один корень в K' .

1. Докажем предложение сначала для сепарабельного случая. Предположим, что существуют два продолжения (K', v'_0) , (K', v_1) . Построим эффективно цепочку полей $K_0 \Leftrightarrow K \leq \leq K_1 \leq \dots$ так, что $\bigcup_{n \in \omega} K_n = K'$, $K_n = K(\alpha_n)$ есть нормальное

расширение K и $\alpha_n = v_1 f(n)$ для подходящей рекурсивной функции f . Рассмотрим $v_1(0)$ и находим для этого элемента неразложимый многочлен над K , корнем которого является $v_1(0)$. Находим все корни $\beta_1, \dots, \beta_k$ этого многочлена; все они принадлежат K' , так как K' нормально. Так как это сепарабельное расширение, то существует $\alpha_0 \in K'$ такой, что $K(\beta_1, \dots, \beta_k) = K(\alpha_0)$; v_1 -номер элемента α_0 можно найти эффективно.

Лемма 1. Пусть конструктивное поле (K, v) обладает свойством (F). Пусть K' — некоторое алгебраическое расширение поля K и v_1 — его конструктивизация, продолжающая v . Тогда $v_1^{-1}(K)$ — рекурсивное множество.

Берем произвольный элемент $v_1 n$ и для него, используя (F), эффективно находим неразложимый полином над K такой, что $v_1 n$ — корень этого полинома. Если степень этого полинома есть 1, то $n \in v_1^{-1}(K)$; если эта степень > 1 , то $n \notin v_1^{-1}(K)$. $\square$

Лемма 2. Пусть конструктивное поле (K, v) обладает свойством (F), K' — некоторое сепарабельное нормальное расширение

поля K и v_1 — конструктивизация K' , продолжающая v . Тогда $v_1^{-1}(K(v_1x_1, \dots, v_1x_k))$ — рекурсивное множество для любых $x_1, \dots, x_k \in \omega$.

Лемма 2 есть простое следствие предложения 1 и леммы 1. $\square$

Продолжим доказательство предложения. По лемме 2 $v_1^{-1}(K(\beta_1, \dots, \beta_k))$ — рекурсивное множество. Для каждого $n \in \omega$ проверяем, справедливо ли равенство $v_1^{-1}(K(v_1n)) = v_1^{-1}(K(\beta_1, \dots, \beta_k))$. Так как расширение сепарабельно, то для некоторого n_0 это будет иметь место, и тогда полагаем $f(0) \doteq n_0$ и $\alpha_0 \doteq v_1 f(0)$.

Далее рассмотрим $v_1(1)$. Используя предложение 1, эффективно находим неразложимый полином над $K(\alpha_0)$, корнем которого является $v_1(1)$; находим все корни $\gamma_1, \dots, \gamma_s$ этого полинома. Рассмотрим поле $K(\alpha_0, \gamma_1, \dots, \gamma_s)$. Ввиду сепарабельности расширения существует $\alpha_1 \in K'$ такой, что $K(\alpha_0, \gamma_1, \dots, \gamma_s) = K(\alpha_1)$. Как и выше, v_1 -номер элемента α_1 находится эффективно, пусть это есть число n_1 , тогда полагаем $f(1) = n_1$ и $\alpha_1 = v_1 f(1)$.

Продолжая это рассуждение, получим цепочку нормальных расширений $K \leq K(\alpha_0) \leq K(\alpha_1) \leq \dots$ поля K и последовательность неразложимых полиномов $f_0, f_1, \dots$ над $K, K(\alpha_0), \dots$ соответственно, корнями которых являются $\alpha_0, \alpha_1, \dots$

Имеем вложения

$$\begin{array}{c} (K, v) \xrightarrow{\mu_2} (K', v_0) \\ \quad \searrow \mu_1 \quad \nearrow \\ (K', v_1) \end{array}$$

Нужно построить эквивалентность μ между нумерованными полями (K', v_0) и (K', v_1) над (K, v) .

Шаг 1. Рассматриваем $v_0(0), v_1(0), \dots$. Находим первое натуральное число k_0 , при котором $f_0(v_0k_0) = 0$, и полагаем $\beta_0 \doteq v_0k_0$ и $\mu(\alpha_0) \doteq \beta_0$ (β_0 есть корень многочлена $f_0(x)$ в K').

Шаг 2. Перебирая $v_0(0), v_0(1), \dots$, эффективно находим первое натуральное число k_1 такое, что $\mu f_1(v_0k_1) = 0$, и полагаем $\beta_1 \doteq v_0k_1$ и $\mu(\alpha_1) \doteq \beta_1$ (β_1 — корень многочлена μf_1 в K').

Взяв в качестве исходного изоморфизма тождественное отображение K на K и продолжая его вышеуказанным способом, получим

$$\begin{array}{ccc} K \leq K(\alpha_0) \leq K(\alpha_1) \leq \dots & & \\ \mu \downarrow \quad \mu \downarrow \quad \mu \downarrow & & \\ K \leq K(\beta_0) \leq K(\beta_1) \leq \dots & & \end{array}$$

Но так как $K(\beta_i)$ — тоже нормальное расширение, то $K(\alpha_i) = K(\beta_i)$, откуда $\bigcup_{i \in \omega} K(\alpha_i) = \bigcup_{i \in \omega} K(\beta_i)$.

Таким образом, эффективно построили изоморфизм «на» между (K', v_1) и (K', v_0) , тождественный на K . Для случая 1 предложение доказано.

2. Рассмотрим теперь чисто несепарабельный случай, т. е. случай, когда K' — чисто несепарабельное расширение поля K , и его характеристика пусть будет p ($p \neq 0$). Для любого $a \in K'$ рассмотрим последовательность $a, a^p, a^{p^2}, \dots$; пусть $v_1 n = a$. Так как K' чисто несепарабельно, то существует $l \in \omega$ такое, что $a^{p^l} \in K$ и v_1 -номер этого элемента эффективно находится; пусть $v_1 k = a^{p^l}$. По v_1 -номеру этого элемента эффективно находится его v -номер, а по v -номеру — его v_0 -номер; пусть v_0 -номер этого элемента будет k' . Решая уравнение $x^{p^l} - v_0 k' = 0$, эффективно найдем v_0 -номер m элемента a . Таким образом, соответствие $v_1 n \rightarrow v_0 m$ будет изоморфизмом (K', v_1) на (K', v_0) , тождественным на K . Для случая 2 предложение доказано.

3. Общий случай. Любое алгебраическое расширение K' поля K может быть получено в два шага: сепарабельное расширение $K \xrightarrow{\mu} K_s$ и затем чисто несепарабельное расширение $K_s \xrightarrow{\mu_s} K'$ (Ленг [1], с. 214). По условию предложения имеем, что (K, v) — конструктивное поле, обладающее свойством (F), и (K', v_0) — конструктивное поле такое, что вложение $(K, v) \xrightarrow{\mu'} (K', v_0)$ есть морфизм, т. е. $\mu' v = v_0 \phi$ для некоторой рекурсивной ϕ .

Для каждого полинома $\xi^n + v x_{n-1} \xi^{n-1} + \dots + v x_0$ над K эффективно можно узнать, сепарабелен он или нет. Берем множество всех сепарабельных многочленов и ищем всевозможные корни в (K', v_0) . Очевидно, что $v_0^{-1}(K_s)$ — рекурсивно перечислимое множество. По утверждению 9 § 1 существует нумерация v_{0s} такая, что (K_s, v_{0s}) — конструктивное поле, и вложение $(K_s, v_{0s}) \xrightarrow{\mu_s} (K', v_0)$ — гомоморфизм, т. е. $\mu_s v_{0s} = v_0 \phi$ для некоторой рекурсивной функции ϕ . Функция $f \doteq \lambda x \mu y (v_0 \phi y = v_0 \phi x)$ показывает, что вложение $\mu: (K, v) \rightarrow (K_s, v_{0s})$ есть гомоморфизм. Таким образом, имеем $(K, v) \xrightarrow{\mu} (K_s, v_{0s}) \xrightarrow{\mu_s} (K', v_0)$. Тогда, если предположить, что существуют две конструктивизации v_0 и v_1 поля K' , то получим

$$\begin{array}{c} (K, v) \xrightarrow{\mu} (K_s, v_{0s}) \xrightarrow{\mu_s} (K', v_0) \\ \quad \searrow \quad \nearrow \\ (K, v) \xrightarrow{\mu} (K_s, v_{1s}) \xrightarrow{\mu_s} (K', v_1) \end{array}$$

Но по первому случаю (K_s, v_{0s}) и (K_s, v_{1s}) эквивалентны и поэтому их можно отождествить, а теперь по второму случаю (K', v_0) и (K', v_1) изоморфны над (K_s, v_{0s}) . $\square$

Замечание. Следствием этого предложения, очевидно, является доказательство достаточности в предложении 6 § 1. В книге Ершова [4] на с. 305, 306 указан явный пример конструктивного поля, являющегося алгебраическим расширением поля $\mathbb{Q}$, для которого проблема продолжения конструктивизации на алгебраическое замыкание имеет не единственное решение. Следовательно, это также пример конструктивного поля, не обладающего свойством (F).

Предложение 4. Пусть (K, v) обладает свойством (F), (K_0, v_0) — конструктивное алгебраическое расширение поля (K, v) , $j_k: K \rightarrow K_0$ — гомоморфизм из (K, v) в (K_0, v_0) ; если $\mu: (K, v) \rightarrow (K_1, v_1)$ — вложение в алгебраически замкнутое поле K_1 , то существует гомоморфизм $\mu_0: (K_0, v_0) \rightarrow (K_1, v_1)$, продолжающий μ , т. е. такой, что диаграмма

$$\begin{array}{ccc} & & (K_0, v_0) \\ & \nearrow j_k & \downarrow \mu_0 \\ (K, v) & & \\ & \searrow \mu & \\ & & (K_1, v_1) \end{array}$$

коммутативна.

Доказательство этого предложения вполне аналогично доказательству предыдущего предложения. Нужно рассмотреть сначала случай сепарабельного расширения, построить такую же возрастающую последовательность конечных расширений поля K и строить последовательно изоморфные вложения этих расширений в K_1 , продолжающие μ и друг друга. Чисто несепарабельный и общий случай рассматриваются вполне аналогично. $\square$

В качестве следствия предложения 4 приведем обещанное доказательство леммы 1 из п. 2. Пусть (K_0, v_0) — конструктивное поле конечной степени трансцендентности над простым подполем P . Пусть $\{a_0, \dots, a_n\}$ — базис трансцендентности K_0 над P . Пусть $K \ni P(a_0, \dots, a_n)$, K — конструктивное подполе поля (K_0, v_0) и, следовательно, существует его конструктивизация v такая, что $j_k: (K, v) \rightarrow (K_0, v_0)$ — вложение конструктивных полей. Предположим, что (K_1, v_1) — конструктивное алгебраически замкнутое поле степени трансцендентности $\geq n+1$ над тем же простым подполем P . Пусть $b_0, \dots, b_n \in K_1$ алгебраически независимы над P , тогда, очевидно, изоморфизм полей $\mu: P(a_0, \dots, a_n) \rightarrow P(b_0, \dots, b_n)$ такой, что $\mu(a_i) = b_i$, $i \leq n$, будет гомоморфизмом из (K, v) в (K_1, v_1) . По предложению 4 суще-

ствует вложение $\mu_0: (K_0, v_0) \rightarrow (K_1, v_1)$ (продолжающее μ), что и требовалось в лемме 1. $\square$

Пусть (K, v) — конструктивное поле, K^* — алгебраическое замыкание K , v^* — конструктивизация K^* , продолжающая v . Рассмотрим всевозможные конечные расширения поля K , лежащие в K^* . Пусть x — стандартный номер конечного множества $\gamma_x = \{n_0, \dots, n_k\}$, тогда определяем $v_\omega(x) \ni K(v^*n_0, \dots, v^*n_k)$. Получим нумерацию всех промежуточных конечно порожденных над K полей, причем предикат $P(x, y) \ni v^*x \in v_\omega y$ рекурсивно перечислим.

Предложение 5. Если конструктивное поле (K, v) обладает свойством (F) и K совершенно, то предикат $P(x, y)$ рекурсивен.

Так как K совершенно, то K^* сепарабельно над K . Чтобы узнать, имеет ли место $v^*x \in v_\omega y$, находим стандартный номер j конечного множества $\gamma_j = \{m_0, \dots, m_s\}$, тогда $v_\omega y = K(v^*m_0, \dots, v^*m_s)$. Так как K^* сепарабельно над K , то по теореме о примитивном элементе существует $v^*k \in K^*$ такой, что $K(v^*k) = K(v^*m_0, \dots, v^*m_s)$. Такой элемент v^*k можно эффективно найти следующим образом. Перечисляем элементы поля K^* : $v^*0, v^*1, \dots$. Для каждого v^*k эффективно проверяем, можно ли v^*k представить в виде полинома от $v^*m_0, \dots, v^*m_s$ и, наоборот, можно ли каждое v^*m_i , $i = 0, \dots, s$, представить в виде полинома от v^*k . Так как полиномы от одной переменной и от $s+1$ переменных над K рекурсивно перечислимы и так как (K^*, v^*) — конструктивное поле, то равенства $v^*k = f(v^*m_0, \dots, v^*m_s)$, $v^*m_0 = f_0(v^*k), \dots, v^*m_s = f_s(v^*k)$ эффективно проверяются, и такие полиномы $f, f_0, \dots, f_s$ обязательно найдутся. Таким образом, для каждого y эффективно находим такое k и полагаем $\varphi y \ni k$; очевидно, φ рекурсивна. Таким образом, имеем $v_\omega y = K(v^*\varphi y)$. Так как (K, v) обладает свойством (F), то степени расширения над K эффективно вычисляются, поэтому из равенства

$$[K(v^*\varphi y, v^*x): K] = [K(v^*\varphi y, v^*x): K(v^*\varphi y)] \cdot [K(v^*\varphi y): K]$$

эффективно вычисляется степень $[K(v^*\varphi y, v^*x): K(v^*\varphi y)]$. Если эта степень равна 1, то $v^*x \in v_\omega y = K(v^*\varphi y)$; если нет, то v^*x не принадлежит $v_\omega y$. Таким образом, $v^{*-1}(v_\omega y)$ — рекурсивное множество, и предикат $P(x, y)$ рекурсивен. $\square$

Пусть $K_\omega \ni \{L \mid K \leq L \leq K^*, L \text{ конечно над } K\}$. Имеем нумерованное множество (K_ω, v_ω) . Рассмотрим отображение $N: K_\omega \rightarrow K_\omega$ такое, что каждому полю $L \in K_\omega$ ставим в соответствие наименьшее нормальное расширение L_0 , содержащее L : $K \leq L_0 \leq K^*$. Так как L — конечное расширение K , то $L = K(a_1, \dots, a_n)$. Рассмотрим для каждого a_i неразложимый много-

член f_i , корнем которого он является. L_0 получается присоединением всех корней многочленов f_i . L_0 — конечное расширение.

Предложение 6. *Отображение N является морфизмом, если конструктивное поле (K, v) обладает свойством (F).*

Для любого x эффективно находим неразложимые полиномы $f_0, \dots, f_k$ над K , корнями которых являются $v^*n_0, \dots, v^*n_k$, где $\{n_0, \dots, n_k\} = \gamma_x$. Число различных корней каждого f_i равно степени этого полинома m_i , деленной на степень несепабельности p^{l_i} , т. е. $m_i p^{-l_i}$; v^* -номера этих корней находятся эффективно; находим стандартный номер y для этого множества v^* -номеров и полагаем $\varphi(x) = y$. Эффективность построения показывает, что φ рекурсивна. Очевидно, что $Nv_\omega x = v_\omega \varphi x$, т. е. N является морфизмом $\square$

Замечание. Любому конечному расширению поставим в соответствие его максимальное сепарабельное подполе. Без свойства (F) можно доказать, что это есть морфизм.

Для любого $L \in K_\omega$ пусть $G(L)$ — группа Галуа поля $N(L) \cap K^*$ — максимального сепарабельного подполя поля $N(L)$ над K , тогда «эффективность» вычисления группы Галуа может быть выражена так:

Предложение 7. *Если (K, v) — конструктивное поле, обладающее свойством (F), то G является морфизмом из (K_ω, v_ω) в естественно нумерованное множество всех конечных групп (нумерация всех таблиц Кэли). $\square$*

4. Конструктивизация универсальной области. Пусть (K, v) — конструктивное поле, $U(K)$ — универсальная область над K , т. е. алгебраически замкнутое K -поле степени трансцендентности ω над K . Из результатов п. 2 легко следует, что конструктивизация v продолжается до некоторой конструктивизации поля $U(K)$; однако ни о какой единственности (над v) такой конструктивизации не может быть и речи. Тем не менее для конструктивных полей, обладающих свойством (F), можно утверждать следующее:

Предложение 1. *Пусть конструктивное поле (K, v) обладает свойством (F), а конструктивизации v_0 и v_1 поля $U(K)$, продолжающие v , таковы, что алгебраическая зависимость над K эффективна при обеих конструктивизациях; тогда v_0 и v_1 эквивалентны над (K, v) .*

По предложению 6 п. 2 в $U(K)$ существуют базисы трансцендентности B_0 и B_1 над K , которые рекурсивно перечислимы в нумерациях v_0 и v_1 соответственно. Тогда поля $K(B_0)$ и $K(B_1)$ являются конструктивными подполями $(U(K), v_0)$ и $(U(K), v_1)$ соответственно. Пусть v'_0 и v'_1 — подходящие конструктивизации этих подполей. Совершенно очевидно, что если $\{b_0, b_1, \dots\}$

— эффективный пересчет B_0 , а $\{c_0, c_1, \dots\}$ — эффективный пересчет B_1 , то K -изоморфизм φ поля $K(B_0)$ на $K(B_1)$ такой, что $\varphi(b_i) = c_i$, $i \in \omega$, будет эквивалентностью $(K(B_0), v'_0)$ и $(K(B_1), v'_1)$ над (K, v) . Теперь необходимо заметить, что конструктивные поля $(K(B_i), v'_i)$, $i = 0, 1$, обладают свойством (F). Это сразу вытекает из наброска доказательства предложения 2' п. 3. Заметим теперь, что конструктивизации v_i поля $U(K)$ являются продолжениями конструктивизаций v'_i полей $K(B_i)$ на их алгебраические замыкания, $i = 0, 1$. Поэтому предложение 3 п. 3 позволяет утверждать, что эквивалентность $\varphi: (K(B_0), v'_0) \rightarrow (K(B_1), v'_1)$ может быть продолжена до некоторой эквивалентности $\psi: (U(K), v_0) \rightarrow (U(K), v_1)$, которая, как и эквивалентность φ , будет эквивалентностью над (K, v) . $\square$

Обозначим через v_u конструктивизацию поля $U(K)$, продолжающую v и такую, что алгебраическая зависимость над K эффективна. Такая нумерация, очевидно, существует для любого конструктивного поля и единственна с точностью до эквивалентности над (K, v) в случае, если (K, v) обладает свойством (F).

Пусть (K, v) — конструктивное поле характеристики 0, обладающее свойством (F). Покажем, что нумерация v_u поля $U(K)$ и индуцированная ей нумерация всех промежуточных конечно порожденных полей удовлетворяет тем же свойствам, которые описаны в предложениях 5, 6 и 7 предыдущего пункта.

Если $x \in \omega$ — стандартный номер конечного множества $S \subseteq \omega$ ($S = \gamma_x$), то через K_x будем обозначать поле $K(v_u(S)) \subseteq U(K)$. Так получаем нумерацию v^* всех конечно порожденных над K подполей поля $U(K)$ ($v^*x \rightleftharpoons K_x$, $x \in \omega$). Пусть f — двуместная функция, определенная так: $f(x, y) \rightleftharpoons [K_x K_y : K_x]$, если эта степень конечна, и $f(x, y) \rightleftharpoons 0$, если $K_x K_y$ — бесконечное расширение K_x , $x, y \in \omega$.

Предложение 2. *Функция f является рекурсивной.*

Для доказательства этого предложения установим предварительно ряд фактов.

1. *Функция $t(x)$, равная степени трансцендентности поля K_x над K , является рекурсивной.*

Действительно, пусть $t_0, t_1, \dots$ — произвольный базис трансцендентности поля $U(K)$ над K ; тогда для любого элемента $\alpha \in U(K)$ найдется такое $n \in \omega$ и такой неприводимый над K многочлен $p_\alpha \in K[x_0, \dots, x_n, y] - K[x_0, \dots, x_n]$, что $p_\alpha(t_0, \dots, t_n, \alpha) = 0$. Этот многочлен однозначно (с точностью до скалярного множителя) определен выбором базиса (точнее, его перечисления). Если базис задан эффективно, то этот многочлен p_α может быть эффективно найден по α . Действительно,

так как поле (K, v) обладает свойством (F) , то семейство всех неприводимых многочленов от любого числа переменных является рекурсивным (прием Кронекера), следовательно, перебирая все такие многочлены в $K[x_0, \dots, x_n, \dots, y]$ и подставляя $t_0, \dots, t_n, \dots, \alpha$, найдем нужный. Пусть $a_0, a_1, \dots$ — эффективный пересчет некоторого фиксированного базиса трансцендентности B_0 поля $U(K)$ над K . Пусть $\gamma_x = \{n_0, \dots, n_s\}$, $n_0 < \dots < n_s$; $\alpha_i \neq v_{\alpha} a_i$, $i \leq s$. Для элемента α_0 эффективно находим неприводимый многочлен $p_0 \in K[x_0, \dots, y] - K[x_0, \dots]$ такой, что $p_0(\bar{\alpha}, \alpha_0) = 0$; если в p_0 ни одна переменная $x_0, \dots$ не входит, то полагаем $S_0 \neq \emptyset$, $D_0 \neq \emptyset$, $B_1 \neq B_0$; если p_0 содержит вхождения переменных x , то пусть i_0 — наименьший индекс такой, что x_{i_0} входит в p_0 ; полагаем тогда $S_0 \neq \{\alpha_0\}$, $D_0 \neq \{i_0\}$, $B_1 \neq (B_0 \cup \{\alpha_0\}) - \{\alpha_{i_0}\}$; $a_1^0, a_1^1, \dots$ — пересчет B_1 такой, что $a_j^1 \neq a_j$, если $j \neq i_0$, и $a_{i_0}^1 \neq \alpha_0$. Предположим, что для $k < s$ множество $S_k \subseteq \{\alpha_0, \dots, \alpha_s\}$, конечное множество $D_k \subseteq \omega$, базис трансцендентности B_{k+1} и его пересчет $a_0^{k+1}, a_1^{k+1}, \dots$ уже определены. Для элемента α_{k+1} находим неприводимый многочлен $p_{k+1} \in K[x_0, \dots, y] - K[x_0, \dots]$ такой, что $p_{k+1}(\bar{\alpha}^{k+1}, \alpha_{k+1}) = 0$. Если многочлен p_{k+1} содержит вхождение переменной x_i такой, что $i \in \omega - D_k$, то пусть i_{k+1} — наименьший такой индекс. Полагаем $S_{k+1} \neq S_k \cup \{\alpha_{k+1}\}$, $D_{k+1} \neq D_k \cup \{i_{k+1}\}$; $B_{k+2} \neq (B_{k+1} \cup \{\alpha_{k+1}\}) - \{\alpha_{i_{k+1}}\}$; $a_i^{k+2} \neq a_i^{k+1}$ для $i \neq i_{k+1}$; $a_{i_{k+1}}^{k+2} \neq \alpha_{k+1}$ для $i = i_{k+1}$. Если же такого i нет, то все остается без изменения. Рассмотрим теперь множество $S_s \subseteq \{\alpha_0, \dots, \alpha_s\}$; из построения видно, что S_s является базисом трансцендентности поля $K_x = K(\alpha_0, \dots, \alpha_s)$ над K ; следовательно, $t(x)$ равно числу элементов множества S_s ; так как построение S_s эффективно, то t — рекурсивная функция. $\square$

2. Существует двуместная рекурсивная функция v такая, что $K_x K_y = K_{v(x, y)}$ для любых $x, y \in \omega$.

В качестве такой функции можно взять функцию, удовлетворяющую условию $\gamma_x \cup \gamma_y = \gamma_{v(x, y)}$. $\square$

Установим теперь рекурсивность функции f . Если $t(v(x, y)) > t(x)$, то $f(x, y) = 0$. Если $t(v(x, y)) = t(x)$, то поле $K_{v(x, y)} = K_x K_y$ является алгебраическим расширением поля K_x . При установлении факта 1 был эффективно найден базис трансцендентности S поля K_x над K . Тогда поля $K_{v(x, y)}$ и K_x являются конечными алгебраическими расширениями поля $K(S)$. Используя теорему о примитивном элементе и эффективный перебор, найдем элементы $\alpha \in K_{v(x, y)}$ и $\beta \in K_x$ такие, что $K_{v(x, y)} = K(S, \alpha)$ и $K_x = K(S, \beta)$. Далее, находя неприводимые над K многочлены p_0 и p_1 из $K[\bar{x}, y]$ такие, что $p_0(S, \alpha) = 0$ и $p_1(S, \beta) = 0$, находим степени $m_0 \neq [K(S, \alpha) : K(S)]$ и $m_1 \neq$

$\neq [K(S, \beta) : K(S)]$, равные y -степеням многочленов p_0 и p_1 соответственно. Тогда $f(x, y) = m_0 m_1^{-1}$. $\square$

Следствие 1. Предикаты $P_0 \neq \{\langle x, y \rangle \mid K_x \leq K_y\}$ и $P_1 \neq \{\langle x, y \rangle \mid K_x = K_y\}$ рекурсивны.

Действительно, имеют место эквивалентности

$$\langle x, y \rangle \in P_0 \Leftrightarrow f(y, x) = 1;$$

$$\langle x, y \rangle \in P_1 \Leftrightarrow \langle x, y \rangle, \langle y, x \rangle \in P_0. \quad \square$$

Следствие 2. Предикат $P \neq \{\langle x, y \rangle \mid v_{\alpha} x \in K_y\}$ рекурсивен.

Действительно, $\langle x, y \rangle \in P \Leftrightarrow f(z, y) = 1$, где z — стандартный номер множества $\gamma_y \cup \{x\}$. $\square$

Предложение 3. Существует двуместная рекурсивная функция g такая, что для любых $x, y \in \omega$, если K_y — алгебраическое расширение K_x , то $K_{g(x, y)}$ — наименьшее расширение Галуа поля K_x , содержащее K_y .

Вычисляем $f(x, y)$; если $f(x, y) = 0$, то полагаем $g(x, y) \neq 0$. Если $f(x, y) > 0$, то в K_y находим такой элемент $\alpha = v_{\alpha} m$, что $f(x, y) = f(x, z)$, где z — стандартный номер множества $\gamma_x \cup \{m\}$; такой элемент найдется по теореме о примитивном элементе. Перебором находим многочлен $p \in K_x[y]$ степени $f(x, y)$, корнем которого является α . Находим теперь в $U(K)$ $f(x, y)$ различных корней этого многочлена $\alpha_1 \neq \alpha, \dots, \alpha_{f(x, y)}$; если $m_1 = m, \dots, m_{f(x, y)}$ — номера этих элементов, а z_0 — стандартный номер множества $\gamma_x \cup \gamma_y \cup \{m_1, \dots, m_{f(x, y)}\}$, то, полагая $g(x, y) \neq z_0$, получим искомую рекурсивную функцию. $\square$

Очевидно, что существует соответствующая эффективизация теории Галуа: существует эффективный способ вычисления по $x, y \in \omega$ таким, что $f(x, y) > 0$, конечной группы Галуа $G_{x, y} \neq \text{Aut}_{K_x} K_{g(x, y)}$. Далее, для любой подгруппы $H \leq G_{x, y}$ можно эффективно вычислить $y_0 \in \omega$ такой, что $K_{y_0} \neq K_{g(x, y)}^H$.

Укажем теперь на некоторые эффективные связи, которые существуют между полиномиальными идеалами над K и точками аффинных пространств над $U(K)$. Пусть $g_1, \dots, g_k \in K[x_1, \dots, x_n]$; через $(g_1, \dots, g_k)$ обозначим идеал этого кольца, порожденный многочленами $g_1, \dots, g_k$. Если I — идеал кольца многочленов $K[x_1, \dots, x_n]$, то через $V(I)$ обозначим множество $\{\bar{x} \mid \bar{x} \in U(K)^n, g(\bar{x}) = 0 \text{ для любого } g \in I\}$. Если $\bar{x} \in U(K)^n$, то через $I(\bar{x})$ обозначим идеал $\{g \mid g \in K[x_1, \dots, x_n], g(\bar{x}) = 0\}$ кольца $K[x_1, \dots, x_n]$.

Ряд важных проблем об идеалах разрешим над произвольными конструктивными полями.

Предложение 4. Для конструктивного поля (K, v) алгоритмически разрешимы следующие проблемы:

а) определить, имеет ли место

$$(g_1, \dots, g_k) \subseteq (h_1, \dots, h_m);$$

Предложение 6. По любой системе многочленов $g_1, \dots, g_k \in K[x_1, \dots, x_n]$ можно эффективно узнать, является ли идеал $(g_1, \dots, g_k)$ собственным; в случае, когда $(g_1, \dots, g_k) \neq K[\bar{x}]$, можно эффективно указать систему $\xi^1, \dots, \xi^s \in U(K)^n$ n -ок из $U(K)$ такую, что

$$V(g_1, \dots, g_k) = \bigcap_{i=1}^s V(I(\xi^i)).$$

Первая проблема эквивалентна разрешимой проблеме определения того, будет ли $1 \in (g_1, \dots, g_k)$. В случае нетривиальности идеала $(g_1, \dots, g_k)$ можно эффективно перечислять все элементы множества $V(g_1, \dots, g_k)$: $\xi^1, \xi^2, \dots$ (Заметим, что $V(g_1, \dots, g_k) \subseteq V(I(\xi))$ для $\xi \in V(g_1, \dots, g_k)$.) Используя предложения 4 и 5, для каждого $s > 0$ проверяем, имеет ли место равенство $V(g_1, \dots, g_k) = \bigcap_{i=1}^s V(I(\xi^i))$. Хорошо известно, что для некоторого s такое равенство должно иметь место (действительно, если $(g_1, \dots, g_k) = \bigcap_{i=1}^t \mathfrak{P}_i$ — представление идеала в виде пересечения примарных, а $\mathfrak{P}_i$ — простой идеал, соответствующий η^i и $\eta^i \in U(K)^n$ — общая точка для идеала $\mathfrak{P}_i$, т. е. $\mathfrak{P}_i = I(\eta^i)$, то

$$V(g_1, \dots, g_k) = \bigcap_{i=1}^t V(\mathfrak{P}_i) = \bigcap_{i=1}^t V(I(\eta^i)).$$

Таким образом, s может быть найдено эффективно. □

§ 2. Регулярно замкнутые поля

Понятие регулярно замкнутого поля является далеким обобщением понятия алгебраически замкнутого поля, однако ряд хороших как алгебраических, так и теоретико-модельных (алгоритмических) свойств последних справедливы и для регулярно замкнутых полей.

Начнем с определений. Напомним (Ленг [1]), что расширение L поля K называется *регулярным*, если L линейно разделено над K с полем K^* — алгебраическим замыканием поля K (эквивалентно: K алгебраически замкнуто в L и L сепарабельно над K).

Поле K называется *регулярно замкнутым*, если для любого регулярного расширения поля L и любого конечного множества $S \subseteq L$ существует K -гомоморфизм кольца $K[S]$ (порожденного над K элементами из S) на K .

Замечание. В п. 1 будут даны эквивалентные определения, более удобные для применений. Укажем еще, что свойство регулярной замкнутости для поля K эквивалентно также сле-

дующему: каждое абсолютно неприводимое многообразие, определенное над K , имеет K -рациональную точку (даже всюду плотное в топологии Зарисского множество K -рациональных точек).

Примерами регулярно замкнутых полей являются алгебраически замкнутые поля, более общо — сепарабельно замкнутые поля. Более нетривиальным примером являются бесконечные поля, удовлетворяющие всем аксиомам теории конечных полей. Регулярная замкнутость последних является следствием глубокого факта — теоремы Вейля о гипотезе Римана для кривых над конечными полями. Это было отмечено еще в 1967 г. независимо Дж. Аксом [1] и Ершовым [2].

Первые два пункта посвящены изложению ряда чисто алгебраических результатов, которые позволят далее в третьем пункте довольно быстро получить основные теоретико-модельные и алгоритмические результаты о регулярно замкнутых полях.

1. **Алгебраические свойства регулярно замкнутых полей.** Все общеалгебраические понятия, которые не определяются в этом параграфе, могут быть найдены в книгах: ван дер Варден [1], Ершов [5], Зарисский и Самюэль [1], Ленг [1].

Предложение 1. Для поля K следующие свойства эквивалентны:

1. K регулярно замкнуто.
2. Для любого его конечно порожденного регулярного расширения $K(S)$ существует K -плейс $p: K(S) \rightarrow K$, который конечен на всех элементах из S .
3. Для любого абсолютно неприводимого многочлена $f \in K[x_1, \dots, x_k, y]$, который как многочлен от y унитарен, сепарабелен и имеет степень больше 1, и для любого $g \in K[x_1, \dots, x_k]$, $g \neq 0$, существуют элементы $\alpha_1, \dots, \alpha_k, \beta$ из K такие, что $f(\alpha_1, \dots, \alpha_k, \beta) = 0$ и $g(\alpha_1, \dots, \alpha_k) \neq 0$.

1 $\Rightarrow$ 2. Докажем чуть более общее утверждение, которое понадобится и в дальнейшем.

Лемма 1. Пусть K — регулярно замкнутое поле, $K \leq K_0 \leq K_1$ — такая башня расширений, что K_1 — конечно порожденное регулярное расширение K и конечное сепарабельное расширение K_0 . Тогда для любого конечного подмножества $S \subseteq K_1$ существуют такие K -плейс $p: K_0 \rightarrow K$ и его продолжение π на K_1 , что π является конечным на S , K -значным (т. е. $\pi(K_1) = K$) и неразветвленным над p .

Выберем в K_0 сепарирующий базис трансцендентности $\bar{t} = t_1, \dots, t_n$; тогда $K \leq K(\bar{t}) \leq K_0 \leq K_1$ и K_1 — конечное сепарабельное расширение $K(\bar{t})$. Из формулировки леммы видно, что ее достаточно доказать для случая $K_0 = K(\bar{t})$. Пусть $\alpha \in K_1$ — такой элемент, что α цел над $K[\bar{t}]$ и $K_1 = K_0(\alpha) =$

$= K(\bar{t}, \alpha)$; через $h(y)$ обозначим минимальный многочлен для α над $K(\bar{t})$, тогда $h(y) \in K[\bar{t}, y]$ ($= K[\bar{t}][y]$). Пусть $d(h)$ — дискриминант многочлена h , тогда $d(h) \in K[\bar{t}]$ и $d(h) \neq 0$, так как α сепарабелен над $K(\bar{t})$. Любой элемент $\beta \in S$ представим в виде

$$\beta = r_0 \alpha^k + r_1 \alpha^{k-1} + \dots + r_k, \text{ где } r_i \in K(\bar{t}), i = 0, \dots, k,$$

$k \in [K_1 : K_0] - 1$. Обозначим через g_β любой ненулевой элемент из $K[\bar{t}]$, который делится на все знаменатели рациональных функций r_i , $i = 0, \dots, k$, тогда $\beta g_\beta \in K[\bar{t}, \alpha]$. Полагаем $g \in \bigcap_{\beta \in S} g_\beta$; тогда $g \neq 0$, $g \in K[\bar{t}]$ и $\beta g \in K[\bar{t}, \alpha]$, $\forall \beta \in K[\bar{t}, g^{-1}, \alpha]$ для любого $\beta \in S$.

Так как K регулярно замкнуто, а $K_1 = K(\bar{t}, g^{-1}, \alpha)$ — регулярное расширение K , то существует K -гомоморфизм φ кольца $K[\bar{t}, g^{-1}, \alpha]$ в K . Заметим, что $\varphi(g) \neq 0$ и $\varphi(d(h)) \neq 0$; следовательно, дискриминант многочлена $(\varphi h)(y)$, равный $\varphi(d(h))$, отличен от нуля. Пусть $\rho: K(\bar{t}) \rightarrow K - K$ -плейс, конечный на $t_1, \dots, t_n$ и такой, что $\rho(t_i) = \varphi(t_i)$, $i = 1, \dots, n$. Существование такого плейса при $n = 1$ очевидно; общий случай устанавливается простой индукцией. Плейс ρ (конечен и) совпадает с φ на кольце $K[\bar{t}]$, следовательно, $\rho(g) = \varphi(g) \neq 0$, ρ определен на g^{-1} и $\rho(g^{-1}) = \varphi(g^{-1})$. Так как дискриминант многочлена $(\rho h)(y) = (\varphi h)(y)$ не равен нулю, то все продолжения плейса ρ на K_1 не разветвлены, а относительная степень такого продолжения определяется степенью образа элемента α над K при этом продолжении. Пусть π — продолжение плейса ρ на K_1 такое, что $\pi(\alpha) = \varphi(\alpha)$; существование такого продолжения следует из того, что $\varphi(\alpha)$ — корень многочлена $\rho h = \varphi h$, так как φ — гомоморфизм из $K[\bar{t}, g^{-1}, \alpha]$ в K . Так как $\varphi(\alpha) \in K$, то π — K -значный плейс, конечный на $\{t_1, \dots, t_n, g^{-1}, \alpha\}$. Но тогда π конечен и на $K[t_1, \dots, t_n, g^{-1}, \alpha]$ и на $S \subseteq K[t_1, \dots, t_n, g^{-1}, \alpha]$. $\square$

$2 \Rightarrow 1$. Очевидно.

$1 \Rightarrow 3$. Пусть K регулярно замкнуто, а f и g такие, как в условии свойства 3. Пусть $K_0 \in K(t_1, \dots, t_k)$ — чисто трансцендентное расширение поля K , а γ — корень многочлена $f(\bar{t}, y) \in K_0[y]$; тогда $K_1 \in K_0(\gamma)$ — регулярное расширение поля K . Следовательно, существует K -гомоморфизм $\varphi: K[t_1, \dots, t_k, g(\bar{t})^{-1}, \gamma] \rightarrow K$; тогда для $\alpha_i \in \varphi(t_i)$, $i = 1, \dots, k$, $\beta \in \varphi(\gamma)$ имеем $f(\alpha_1, \dots, \alpha_k, \beta) = 0$ и $g(\alpha) \neq 0$.

$3 \Rightarrow 1$. Пусть поле K удовлетворяет условию 3. Пусть K_1 — конечно порожденное регулярное расширение K , S — конечное подмножество K_1 . Как в доказательстве леммы 1, находим сепарирующий базис трансцендентности $t_1, \dots, t_n$ и многочлены $f \in K[x_1, \dots, x_n, y]$, $g \in K[x_1, \dots, x_n]$ такие, что $h(y) \in K[\bar{t}, y]$ — минимальный многочлен для элемента $\gamma \in K_1$ та-

кого, что $K_1 = K(\bar{t}, \gamma)$ и γ целый (и сепарабельный) над $K[\bar{t}]$, а $g_* \in g(\bar{t})$ — элемент такой, что $S \subseteq K[\bar{t}, g_*^{-1}, \gamma]$. Заметим, что f — абсолютно неприводимый многочлен над K , так как $K_1 = K(t_1, \dots, t_n, \gamma)$ — регулярное расширение K . По свойству 3 в K существуют элементы $\alpha_1, \dots, \alpha_n, \beta$ такие, что $f(\alpha, \beta) = 0$ и $g(\alpha) \neq 0$. Соответствие $t_i \mapsto \alpha_i$, $\gamma \mapsto \beta$ продолжается до K -гомоморфизма φ_* кольца $K[\bar{t}, \gamma]$ в K ; если $\mathfrak{p}$ — ядро гомоморфизма φ_* , то φ_* однозначно продолжается до K -гомоморфизма ψ из $K[\bar{t}, \gamma]_{\mathfrak{p}}$ — кольца частных относительно простого идеала $\mathfrak{p}$ — в K ; так как $\varphi_*(g_*) = g(\alpha) \neq 0$, то $g_*^{-1} \in K[\bar{t}, \gamma]_{\mathfrak{p}}$, следовательно, $K[S] \subseteq K[\bar{t}, g_*^{-1}, \gamma] \subseteq K[\bar{t}, \gamma]_{\mathfrak{p}}$ и $\varphi \in \psi \upharpoonright K[S]$ задает K -гомоморфизм кольца $K[S]$ в K . $\square$

Следствие. Если K_i , $i \in I$, — направленное по включению семейство регулярно замкнутых полей, то поле $\bigcup_{i \in I} K_i$ также является регулярно замкнутым.

Легко проверить это для свойства 3. $\square$

Установим теперь, что свойство регулярной замкнутости сохраняется при сепарабельных алгебраических расширениях.

Замечание. Это свойство уже отмечалось ранее (Акс [2]) со ссылкой на технику спуска Вейля. Здесь будет приведено независимое доказательство, не использующее алгеброметрической техники.

Предложение 2. Пусть K — регулярно замкнутое поле, K_0 — сепарабельное алгебраическое расширение K . Тогда K_0 также регулярно замкнуто.

Установим сначала утверждение, имеющее и самостоятельный интерес.

Лемма 2. Пусть K_0 — конечно порожденное сепарабельное расширение поля K , L_0 — алгебраическое замыкание K в K_0 , тогда существуют такие расширения $K_0 \subseteq L$, $K \subseteq L_1$, что L_1 — конечно порожденное регулярное расширение K и $L = L_0 L_1$.

Будем предполагать, что K_0 вложено в некоторую универсальную область K_1 над K , т. е. K_1 — алгебраически замкнутое поле, содержащее K и имеющее бесконечную степень трансцендентности над K . Пусть $n \in [L_0 : K]$ и $\varphi_1 = \text{id}_{L_0}$, $\varphi_2, \dots, \varphi_n$ — все различные K -вложения поля L_0 в K_1 (L_0 сепарабельно над K). Продолжим изоморфные вложения $\varphi_1, \varphi_2, \dots, \varphi_n$ до изоморфных вложений $\psi_1 \in \text{id}_{K_0}$, $\psi_2, \dots, \psi_n$ поля K_0 в K_1 так, чтобы было выполнено условие: $\psi_i(K_0)$ и $\psi_j(K_0)$ для $1 \leq i < j \leq n$ алгебраически разделены над K . Пусть L_* — это композит полей $\varphi_1(L_0), \dots, \varphi_n(L_0)$, тогда L_* — наименьшее расширение Галуа поля K , содержащее L_0 . Через G обозначим группу Галуа $\text{Aut}_K L_*$. Пусть $\bar{L}$ — это композит полей $\psi_1(K_0), \dots$

..., $\psi_n(K_0)$; $\bar{L}$ — сепарабельное конечно порожденное расширение K . Если через M_i обозначить композит $\psi_i(K_0)L_*$, $i = 1, \dots, n$, то L_* — алгебраическое замыкание K в M_i и M_i — регулярное расширение L_* для всех $i = 1, \dots, n$. Из построения следует, что M_i и M_j алгебраически разделены над L_* ($i \neq j$), следовательно, они линейно разделены над L_* и $\bar{L} = M_1 \cdot \dots \cdot M_n = M_1 \otimes_{L_*} M_2 \otimes_{L_*} \dots \otimes_{L_*} M_n$. Определим теперь действие группы G на поле $\bar{L}$, согласованное с действием G на L_* . Пусть $\sigma \in G$; зададим действие σ на элементах поля $\psi_i(K_0)$ так: рассмотрим изоморфное вложение $\sigma\psi_i$ поля L_0 в K_1 ; существует такое j , что $\sigma\psi_i = \psi_j$, тогда для элемента $\alpha \in \psi_i(K_0)$ полагаем $\sigma\alpha = \psi_j\psi_i^{-1}(\alpha)$. Рутинная проверка показывает, что так определенное действие σ на компонентах $\psi_i(K_0)$ однозначно продолжается до действия σ на $\bar{L}$, причем это действие σ на L_* совпадает с исходным. Полагаем $L_1 = \bar{L}^G$, тогда L — расширение Галуа поля L_1 с группой Галуа G . K алгебраически замкнуто в L_1 , следовательно, L_1 — регулярное расширение K . Полагаем $L = L_0 L_1 (= L_0 \otimes_K L_1)$ и покажем, что $K_0 \leq L$. Пусть H — такая подгруппа группы G , что $L_0 = L_1^H$ (т. е. $H = \{\sigma \mid \sigma\alpha = \alpha \text{ для любого } \alpha \in L_0\}$); покажем, что $L = L^H$. Действительно, включение $L \leq L^H$ очевидно; так как $\bar{L} = L_* L_1 = L_* \otimes_K L_1$, то $[L : L] = [L_* : L_0] = |H| = [\bar{L} : L^H]$, следовательно, $L = L^H$. Остается показать, что $K_0 \leq L^H$. Пусть $\sigma \in H$, $\alpha \in K_0 = \psi_1(K_0)$; так как $\phi_1 = \text{id}_{L_0}$, то $\sigma\phi_1 = \phi_1$, следовательно, $\sigma\alpha = \psi_1\phi_1^{-1}(\alpha) = \alpha$; итак, $K_0 \leq L^H$. $\square$

Обратимся теперь к доказательству предложения. Если воспользоваться следствием предыдущего предложения, то достаточно доказать утверждение в случае, когда K_0 — конечное расширение K .

Пусть $K_0(t_1, \dots, t_n)$ — конечно порожденное регулярное расширение K_0 . По лемме 2 существует такое конечно порожденное регулярное расширение K_1 поля K , что $K_0(t_1, \dots, t_n) \leq K_0 K_1 = K_0 \otimes_K K_1$. Пусть $\alpha_1 = 1, \alpha_2, \dots, \alpha_k$ — базис K_0 над K , тогда любой элемент γ из $K_0 K_1$ однозначно представим в виде $\gamma = \sum_{i=1}^k \alpha_i \beta_i$, $\beta_i \in K_1$, $i = 1, \dots, k$. Пусть $\beta_{ij} \in K_1$, $i = 1, \dots, k, j = 1, \dots, n$, таковы, что

$$t_j = \sum_{i=1}^k \alpha_i \beta_{ij}, \quad j = 1, \dots, n.$$

Так как $K(\beta_{ij} \mid i = 1, \dots, k; j = 1, \dots, n)$ — регулярное расширение K и K регулярно замкнуто, то существует K -гомоморфизм $\psi: K(\beta_{ij}) \rightarrow K$, который может быть однозначно продолжен до K_0 -гомоморфизма $\psi_*: K_0(\beta_{ij}) \rightarrow K_0$ потому, что $K_0(\beta_{ij}) = K(\beta_{ij}) \otimes_K K_0$;

так как $t_1, \dots, t_n \in K_0(\beta_{ij})$, то $\varphi = \varphi_* \upharpoonright K_0[t_1, \dots, t_n]$ будет искомым K_0 -гомоморфизмом из $K_0[\bar{t}]$ в K_0 . $\square$

Предложение 3. Любое поле K имеет регулярное расширение K_0 , являющееся регулярно замкнутым.

Построение такого расширения является довольно стандартным. Сначала укажем, как построить такое регулярное расширение K' поля K , что для любой пары $\langle f, g \rangle$, $f \in K[x_1, \dots, x_k, y]$, $g \in K[x_1, \dots, x_k]$, f абсолютно неприводим и как многочлен от y унитарен, сепарабелен и имеет степень больше 1, а $g \neq 0$, в K' существуют элементы $\alpha_1, \dots, \alpha_k, \beta$ такие, что $f(\alpha, \beta) = 0$ и $g(\alpha) \neq 0$. Пусть X — множество всех таких пар многочленов и $\leq$ — некоторое вполне упорядочение множества X . Для любого $\xi \in X$ определим регулярное расширение K_ξ поля K по трансфинитной индукции:

Пусть для всех $\eta < \xi$ поля K_η уже построены так, что если $\eta_0 \leq \eta_1 < \xi$, то $K \leq K_{\eta_0} \leq K_{\eta_1}$. Полагаем $K_\xi = K \cup \bigcup_{\eta < \xi} K_\eta$; K_ξ — регулярное расширение поля K . Пусть $\xi = \langle f, g \rangle$; так как f абсолютно неприводим, то поле $K_\xi = K_\xi(t_1, \dots, t_k, \tau)$ — поле частных кольца $\tilde{K}_\xi[x_1, \dots, x_k, y]/(f)$ — регулярное расширение поля $\tilde{K}_\xi$ и, следовательно, регулярное расширение поля K .

Полагая $K' = \bigcup_{\xi \in X} K_\xi$, получим регулярное расширение поля K , удовлетворяющее сформулированным выше условиям. Построим теперь башню расширений

$$K \leq K' \leq \dots \leq K^{(n)} \leq K^{(n+1)} (= K^{(n')}) \leq \dots;$$

тогда $K_0 = \bigcup_{n \in \omega} K^{(n)}$ — регулярное расширение поля K , которое, как видно из построения, удовлетворяет условию свойства 3 предложения 1, т. е. является регулярно замкнутым. $\square$

Для дальнейшего нам понадобится более точный вариант предложения 3, утверждающий, что расширение K_0 можно выбрать с любой (возможной) группой Галуа $G(K_0)$. Под группой Галуа $G(K)$ поля K понимается группа Галуа сепарабельного замыкания K_s поля K над K , т. е. $G(K) = \text{Aut}_K K_s$. Определения и необходимые свойства проконечных групп и (бесконечной) теории Галуа можно найти в книгах Коха [1] и Серра [1]. Все рассматриваемые ниже группы будут проконечными, подгруппы — замкнутыми, а гомоморфизмы — непрерывными.

Напомним, что (проконечная) группа G называется проективной, если для любых гомоморфизма $\varphi: G \rightarrow H_0$ и эпиморфизма $\psi: H_1 \rightarrow H_0$ существует гомоморфизм $\lambda: G \rightarrow H_1$ такой, что $\varphi = \lambda\psi$.

Теорема 1. Пусть K — произвольное поле, H — проективная группа, $\varphi: H \rightarrow G(K)$ — эпиморфизм. Тогда существуют ре-

гулярное регулярно замкнутое расширение L поля K и изоморфизм $\psi: G(L) \rightarrow H$ такие, что композиция $\phi\psi: G(L) \rightarrow G(K)$ совпадает с гомоморфизмом ограничения.

Воспользуемся следующим результатом.

Лемма 3. Для любого поля F и любой проконечной группы H существуют регулярное расширение F_1 поля F и промежуточное поле $F_0 (F \leq F_0 \leq F_1)$ такие, что F_1 — расширение Галуа поля F_0 и $H \cong \text{Aut}_{F_0} F_1$.

Поле F_1 можно выбрать как чисто трансцендентное расширение поля F . Для доказательства см. Уотерхаус [1]. $\square$

Для поля K находим по лемме 3 такие расширения K_0 и K_1 , что $K \leq K_0 \leq K_1$, K_1 — регулярное расширение K , K_1 — расширение Галуа поля K_0 и $\lambda: \text{Aut}_{K_0} K_1 \rightarrow H$ — фиксированный изоморфизм. Рассмотрим расширение $K' \cong K_1 K_s$ поля K_0 , где K_s — сепарабельное замыкание K ; так как K_1 — регулярное расширение K , то $K_s \parallel_{K_0} K_1$ и $K_s \parallel_{K_0} K_1$ (символ $\parallel_K$ означает линейную

разделенность над F). Отсюда сразу следует, что $G' \cong \text{Aut}_{K_0} K' \cong \cong G(K) \text{Aut}_{K_0} K_1$. Рассмотрим в G' замкнутую подгруппу $H' \cong \cong \{(\sigma, \tau) | \phi\lambda(\tau) = \sigma, \sigma \in G(K), \tau \in \text{Aut}_{K_0} K_1\}$; заметим, что H' естественно изоморфна группе H . Полагаем $K_2 \cong K'^{H'}$, тогда, так как H' при ограничении на K_s отображается на всю группу $G(K)$, то K алгебраически замкнуто в K_2 ; но K_2 — подполе K' , которое сепарабельно над K , следовательно, K_2 — регулярное расширение K_0 и существует изоморфизм $\psi': \text{Aut}_{K_0} K' (= H') \rightarrow H$ такой, что $\phi\psi'$ совпадает с гомоморфизмом ограничения $\text{Aut}_{K_0} K' \rightarrow G(K) = \text{Aut}_K K_s$.

Используя предложение 3, найдем регулярное регулярно замкнутое расширение L_0 поля K_2 . Пусть $\mu: G(L_0) \rightarrow G(K_2)$ — эпиморфизм ограничения и $\mu_0: G(L_0) \rightarrow H'$ — композиция отображений μ и естественного эпиморфизма ограничения $G(K_2) \rightarrow H' = \text{Aut}_{K_0} K'$. Так как $H' \cong H$ проективна, то существует подгруппа $H_0 \leq G(L_0)$ такая, что ограничение μ_0 на H_0 есть изоморфизм H_0 и H' . Полагаем $L \cong L_{0s}^{H_0}$; легко проверяется, что L — регулярное расширение поля K , L регулярно замкнуто как сепарабельное расширение регулярно замкнутого поля L_0 (предложение 2) и $G(L) \cong H_0$, причем существует изоморфизм $\psi: G(L) \rightarrow H$, удовлетворяющий сформулированным в теореме условиям. $\square$

Замечание. Условие проективности группы H в теореме является не только достаточным, но и необходимым. Укажем набросок доказательства следующего утверждения:

Если K — регулярно замкнутое поле, то группа $G(K)$ финитно проективна.

Пусть H_0, H_1 — конечные группы, $\phi: G(K) \rightarrow H_0$ — гомоморфизм, $\psi: H_1 \rightarrow H_0$ эпиморфизм. Нужно найти такой гомомор-

физм $\lambda: G(K) \rightarrow H_1$, что $\phi\lambda = \phi$. Пусть H_1 вложена в симметрическую группу S_n степени n ; если $K_1 \cong K(x_1, \dots, x_n)$ — поле рациональных функций от n переменных над K , то S_n действует естественным образом на K_1 . Полагаем $K_0 \cong K_1^{H_1}$; тогда K_1 — расширение Галуа поля K_0 с группой Галуа H_1 . Пусть $L_0 \cong K_s^{\text{Ker } \phi}$, тогда L_0 — конечное расширение Галуа поля K с группой Галуа, изоморфной группе $G_1 \cong \phi(G(K))$; $G_1 \leq H_0$. Рассмотрим K -композит L полей L_0 и K_1 ; поле L является расширением Галуа поля K_0 с группой Галуа G_0 , изоморфной группе $H_1 \times G_1$; рассмотрим в G_0 подгруппу H_2 , соответствующую подгруппе $\{ \langle h, g \rangle | \psi h = g \}$ группы $H_1 \times G_1$. Легко проверить, что поле $L_1 \cong L^{H_2}$ является конечно порожденным регулярным расширением поля K . Пусть $\alpha \in L$ таков, что $L = L_1(\alpha)$; $a_1, \dots, a_k$ — коэффициенты минимального многочлена для α над L_1 , а d — его дискриминант. Для $S = \{a_1, \dots, a_k, d, d^{-1}\}$ найдем (по предположению 1) K -плейс $p: L_1 \rightarrow K$, конечный на S , и пусть $\pi: L \rightarrow K_s$ — какое-нибудь его продолжение до плейса поля L в K_s . Пусть H_3 — группа разложения плейса π над p , $H_3 \leq H_2$; так как p конечен на d и d^{-1} , то π неразветвлен над p и H_3 изоморфна группе Галуа поля $\pi(L)$ над K . Пусть $\lambda_0: G(K) \rightarrow H_3$ — эпиморфизм, индуцированный эпиморфизмом ограничения: пусть $\lambda_1: H_3 \rightarrow H_1$ — гомоморфизм, индуцированный вложением $\langle h, g \rangle \mapsto h$ группы H_2 в H_1 , тогда $\lambda \cong \lambda_1 \lambda_0$ — искомый гомоморфизм из $G(K)$ в H_1 . $\square$

Как отметил Ершов [8], финитная проективность равносильна проективности.

Установим теперь теорему, которая описывает возможные группы разложений для накрытий рациональных точек многообразий над регулярно замкнутыми полями. Такого типа теоремы называются (Фрид и Сакердот [1], Джарден [1]) аналогами теоремы Чеботарева о плотности и играют важную роль в теоремах об элиминации кванторов для «утверждений Галуа». Полученная ниже теорема является наиболее общей и используется в конце этого добавления для элиминации кванторов в теории стратов Галуа.

Пусть K — регулярно замкнутое поле; K_0 — конечно порожденное регулярно расширение K ; K_1 — конечное расширение Галуа поля K_0 ; L_0 — алгебраическое замыкание K в K_1 ; $H \cong \text{Aut}_{K_0} K_1$; $H_0 \cong \text{Aut}_K L_0$; $\psi: H \rightarrow H_0$ — эпиморфизм ограничения. Пусть $\phi: G(K) \rightarrow H_0$ — такой гомоморфизм, что диаграмма

$$\begin{array}{ccc} & G(K) & \\ \swarrow & & \searrow \phi \\ H_0 (= \text{Aut}_K L_0) & \xleftarrow{\psi} & H \end{array}$$

коммутативна. Полагаем $H_1 \triangleq \varphi(G(K))$, $L_1 \triangleq K_s^{\text{Кег } \varphi}$; заметим, что $\text{Aut}_K L_1 = G(K)/\text{Кег } \varphi \simeq H_1$.

Теорема 2 (аналог теоремы Чеботарева о плотности). Для любого конечного подмножества $S \subseteq K_0$ существует K -плейс $p: K_0 \rightarrow K$, конечный на S , и его продолжение $\pi: K_1 \rightarrow L_1$ на K_1 , не разветвленное над p , группой разложения которого над p является H_1 , а изоморфизм $H_1 \simeq \text{Aut}_K L_1 = G(K)/\text{Кег } \varphi$, индуцированный плейсом π , является обратным к изоморфизму $G(F)/\text{Кег } \varphi \simeq H_1$, индуцированному эпиморфизмом φ .

Заметим, что частный случай теоремы, когда $L_0 = K$, т. е. когда K_1 — регулярное расширение K и когда φ — тривиальное отображение ($H_1 = \{e\}$), следует сразу из доказанной ранее леммы 1.

Рассмотрим поле $F \triangleq L_1 K_1$; поле F является расширением Галуа поля K_0 , группа Галуа которого (над K_0) описывается с помощью следующей леммы.

Лемма 4. Пусть M_0 и M_1 — расширения Галуа поля M ,

$$G_0 \triangleq \text{Aut}_M M_0, \quad G_1 \triangleq \text{Aut}_M M_1, \quad H \triangleq \text{Aut}_M (M_0 \cap M_1),$$

тогда композит $M_0 M_1$ есть расширение Галуа поля M и его группа Галуа $H_0 \triangleq \text{Aut}_M M_0 M_1$ изоморфна расслоенному прямому произведению $G_0 \times_H G_1$ групп G_0 и G_1 над H , т. е. подгруппе группы $G_0 \times G_1$, состоящей из всех таких пар $\langle g_0, g_1 \rangle$, что $g_0 \upharpoonright (M_0 \cap M_1) = g_1 \upharpoonright (M_0 \cap M_1)$ (или, что то же, $\pi_0 g_0 = \pi_1 g_1$, где $\pi_i: G_i \rightarrow H$ — отображение ограничения).

Эта лемма есть небольшое уточнение теоремы 5 § 1 главы VIII книги Ленга [1]. $\square$

Так как $F = (L_1 K_0) K_1$ и $L_1 K_0$ — расширение Галуа поля K_0 такое, что $\text{Aut}_K L_1 K_0 \simeq \text{Aut}_K L_1$ и $L_1 K_0 \cap K_1 = L_0 K_0$, то по лемме 4 группа Галуа G поля F над K_0 изоморфна группе $H_1 \times_{H_0} H$;

рассмотрим в G подгруппу H_* , соответствующую подгруппе $\{\langle h, h \rangle | h \in H_1\}$ группы $H_1 \times_{H_0} H$; тогда $H_* \simeq H_1$. Рассмотрим

поле $F_0 \triangleq F^{H_*}$; так как L_1 является алгебраическим замыканием K в F , а группа H_* действует на L_1 так же, как (изоморфная ей группа) $\text{Aut}_K L_1 (= G(K)/\text{Кег } \varphi)$, то K алгебраически замкнуто в F_0 , и так как F , а следовательно, и F_0 сепарабельно над K , то F_0 — регулярное расширение K и $F = F_0 \otimes_K L_1$. Легко

проверяется, что $K_0 \triangleleft F_0$ и F_0 — конечное сепарабельное расширение K_0 . Применяя лемму 1 к $K \triangleleft K_0 \triangleleft F_0$, находим K -плейс $p: K_0 \rightarrow K$, конечный на S , его продолжение π' на F_0 , которое неразветвлено над p и K -значно (т. е. $\pi'(F_0) = K$). Продолжим теперь π' до L_1 -плейса $\pi_0: F = F_0 \otimes_K L_1 \rightarrow L_1$ (такое

продолжение, очевидно, существует и единственно); плейс π_0 неразветвлен над π' и над p . Если через π обозначим ограничение π_0 на K_1 , то π будет искомым продолжением p .

Действительно, так как π_0 не разветвлен над p , то его ограничение π будет не разветвлено; остается заметить, что $\pi(K_1) = L_1$, но это следует из того, что $K \cap F_0 = K_1^{H_*} = K_1^{H_1}$ и $[F: F_0] = [H_*: H_1] = [K_1: K_1 \cap F_0] = [L_1: K]$; $\pi(K_1) = L_1$ и H_1 является группой разложения π над p . $\square$

Важное для дальнейшего следствие теоремы 2 сформулируем в виде отдельного предложения.

Пусть $K \triangleleft K_0 \triangleleft K_1$ — такая башня расширений полей, что K регулярно замкнуто, K_0 — регулярное расширение поля K , K_1 — конечное расширение Галуа поля K_0 . Пусть L_0 — алгебраическое замыкание K в K_1 и L_1 — такое расширение Галуа поля K , что $L_0 \triangleleft L_1$ и существует $\text{Aut}_K L_0$ -изоморфизм групп

$$\varphi: \text{Aut}_{K_0} K_1 \simeq \text{Aut}_K L_1.$$

Предложение 4. В этих условиях для любого конечного подмножества $S \subseteq K_1$ существует K -гомоморфизм ψ кольца $K[S]$ в L_1 такой, что $\psi(S \cap K_0) \subseteq K$ и $\psi(S - K_0) \subseteq L_1 - K$.

Пусть $k \triangleq [K_1: K_0]$, $G \triangleq \text{Aut}_K K_1$, $K_1 = K_0(\gamma)$ и $h = x^k + a_1 x^{k-1} + \dots + a_k \in K_0[x]$ — минимальный многочлен для γ над K_0 . Полагаем $a_i(e) \triangleq a_i$ для $i = 1, \dots, k$; для $e \neq \sigma \in G$ пусть $\sigma \gamma = a_1(\sigma) \gamma^{k-1} + \dots + a_k(\sigma)$, $a_i(\sigma) \in K_0$; для $\tau \in S$ пусть $\tau = a_1(\tau) \gamma^{k-1} + \dots + a_k(\tau)$, $a_i(\tau) \in K_0$.

Если $K'_0 \triangleq K(a_i(\delta) | i = 1, \dots, k, \delta \in G \cup S)$, $K'_1 \triangleq K'_0(\gamma)$, то K'_1 — расширение Галуа поля K'_0 с группой Галуа, естественно изоморфной G ; $K'_1 \cap K_0 = K'_0$ и $S \subseteq K'_1$. Полагаем $S' \triangleq \{\gamma, a_i(\delta), a_i(\delta)^{-1} | a_i(\delta) \neq 0, i = 1, \dots, k, \delta \in S \cup G\}$. Применяя теорему 2 к системе $(K, K'_0, K'_1, S', \varphi)$, найдем K -плейс $p: K'_0 \rightarrow K$ и его L_1 -значное продолжение $\pi: K'_1 \rightarrow L_1$, конечное на S' , группой разложения которого над p будет группа G . Отсюда сразу следует, что π — единственное продолжение p и $L_1 = K(\pi(\gamma))$. Кольцо $K'_0[S']$ содержится в кольце нормирования R_π плейса π ; из определения множества S' видно, что $S \subseteq K'_0[S']$, следовательно, и $K[S] \triangleleft K'_0[S'] \triangleleft R_\pi$. Ограничение π на $K[S]$ задает K -гомоморфизм ψ из $K[S]$ в L_1 . Условие $\psi(S \cap K_0) \subseteq K$ выполнено, так как π есть продолжение K -значного плейса $p: K'_0 \rightarrow K$ и $S \cap K_0 = S \cap K'_0$. Пусть $\tau \in S - K_0$, тогда существует i , $1 \leq i \leq k$, такое, что $a_i(\tau) \neq 0$ (в противном случае $\tau = a_k(\tau) \in K_0$); следовательно, $a_i(\tau)$ и $a_i(\tau)^{-1} \in S'$, поэтому $\psi(a_i(\tau)) \neq 0$.

Но

$$\psi(\tau) = \psi\left(\sum_{i=1}^k a_i(\tau) \gamma^{k-i}\right) = \sum_{i=1}^k \psi(a_i(\tau)) \pi(\gamma)^{k-i}$$

и, следовательно, $\psi(\tau) \notin K$, так как $k = [L_1:K]$ и $L_1 = K(\pi(\gamma))$. $\square$

2. Допустимые классы конечных групп. В этом пункте будут рассматриваться только конечные и проконечные группы. Как и в предыдущем пункте, будем предполагать гомоморфизмы непрерывными, подгруппы замкнутыми и т. д.

Эпиморфизм $\varphi: G \rightarrow H$ проконечных групп называется *накрытием*, если G не имеет собственных (замкнутых!) подгрупп $G_0 < G$ таких, что $\varphi(G_0) = H$. Это свойство эпиморфизма φ эквивалентно следующему: $\text{Ker } \varphi \leq \Phi(G)$, где $\Phi(G)$ — подгруппа Фраттини группы G .

З а м е ч а н и е. Далее будем неоднократно пользоваться (без явного упоминания) следующим очевидным свойством накрытий: если $\varphi: G \rightarrow H$, $\psi: H \rightarrow F$ — эпиморфизмы, то $\psi\varphi$ есть накрытие тогда и только тогда, когда φ и ψ являются накрытиями.

Класс $\mathfrak{G}$ конечных групп назовем *допустимым*, если выполнены следующие три условия:

1. Класс $\mathfrak{G}$ замкнут относительно гомоморфных образов.
2. Класс $\mathfrak{G}$ замкнут относительно накрытий; это означает, что если $\varphi: G \rightarrow H$ — накрытие, $H \in \mathfrak{G}$ и G — конечная группа, то $G \in \mathfrak{G}$.
3. Класс $\mathfrak{G}$ удовлетворяет свойству *коамальгамируемости*: если $G_0, G_1, H_0 \in \mathfrak{G}$, $\varphi_0: G_0 \rightarrow H_0$, $\varphi_1: G_1 \rightarrow H_0$ — эпиморфизмы, то существуют группа $H_1 \in \mathfrak{G}$ и эпиморфизмы $\psi_0: H_1 \rightarrow G_0$ и $\psi_1: H_1 \rightarrow G_1$ такие, что $\varphi_0\psi_0 = \varphi_1\psi_1$.

Примерами допустимых классов групп являются следующие: класс $\mathfrak{G}_\omega$ всех конечных групп; класс $\mathfrak{G}_n$ всех конечных групп, имеющих n порождающих элементов ($n \in \omega$); класс $\mathfrak{G}_\pi$ всех конечных π -групп, где π — произвольное множество простых чисел; класс $\mathfrak{G}_s$ всех конечных разрешимых групп; класс $\mathfrak{G}_N$ всех конечных нильпотентных групп и многие другие (ниже встречаются и другие примеры допустимых классов).

З а м е ч а н и е. В основе доказательства того, что класс $\mathfrak{G}_n$, $n \in \omega$, является допустимым, лежит следующая

Л е м м а Г а ш ю ц а. Если $\varphi: H \rightarrow F$ — эпиморфизм конечных групп, имеющих n порождающих, то для любой системы порождающих $a_1, \dots, a_n$ группы F существует система порождающих $b_1, \dots, b_n$ группы H такая, что $\varphi(b_i) = a_i$, $i = 1, \dots, n$.

Доказательство см. в статье Гашюца [1]. $\square$

Предложение 1. Для любого класса конечных групп $\mathfrak{G}$ существует наименьший допустимый класс $\mathfrak{G}(\mathfrak{G})$, содержащий $\mathfrak{G}$.

В основе доказательства этого предложения лежит лемма 1. формулировке которой предположим определение. Пару эпиморфизмов $\varphi: F \rightarrow G$, $\psi: H \rightarrow G$ назовем *максимальной*, если не существует тройки эпиморфизмов $\lambda: G' \rightarrow G$, $\varphi': F \rightarrow G'$, $\psi': H \rightarrow G'$ такой, что $\text{Ker } \lambda \neq \{e\}$, $\lambda\varphi' = \varphi$, $\lambda\psi' = \psi$.

Л е м м а 1. Если $\varphi: F \rightarrow G$, $\psi: H \rightarrow G$ — максимальная пара эпиморфизмов, G_1 — подгруппа расслоенного произведения $G_0 \rightrightarrows F \times_G H (= \{\langle f, h \rangle \mid \varphi f = \psi h\})$ такая, что $\pi_0(G_1) = F$ и $\pi_1(G_1) = H$ (π_0, π_1 — естественные проекции), то $G_0 = G_1$.

Доказательство будем вести индукцией по числу $|F| + |H|$. Заметим, что группы $\text{Ker } \varphi$ и $\text{Ker } \psi$ можно считать естественно вложенными в G_0 (если $f \in \text{Ker } \varphi$, то $\langle f, e \rangle \in G_0$) так, что имеет место следующая точная последовательность:

$$\{e\} \rightarrow \text{Ker } \varphi \times \text{Ker } \psi \rightarrow G_0 \rightarrow G \rightarrow \{e\}.$$

Предположим, что $F_0 \triangleq G_1 \cap \text{Ker } \varphi \neq \{e\}$. Покажем, что F_0 является нормальной подгруппой в G_0 , а соответствующая ей подгруппа $F_1 \triangleq \{f \mid \langle f, e \rangle \in F_0\}$ — нормальной в группе F . Докажем второе; пусть $f_0 \in F_1$ и $f \in F$; так как G_1 проектируется на F , то $\langle f, h \rangle \in G_1$ для некоторого $h \in H$; следовательно, $\langle f, h \rangle^{-1} \langle f_0, e \rangle \langle f, h \rangle \in G_1$, но $\langle f, h \rangle^{-1} \langle f_0, e \rangle \langle f, h \rangle = \langle f^{-1} f_0 f, e \rangle \in F_0$; $f^{-1} f_0 f \in F_1$ и $F_1 \triangleleft F$. То, что F_0 — нормальная подгруппа группы G_0 , легко вытекает из предыдущего. Рассмотрим группы $F' \triangleq F/F_1$, $G'_0 \triangleq G_0/F_0$, $G'_1 \triangleq G_1/F_0$ и эпиморфизм $\varphi': F' \rightarrow G'$, индуцированный эпиморфизмом φ (напомним, что $F_1 \leq \text{Ker } \varphi$). Из этих определений видно, что φ', ψ — максимальная пара эпиморфизмов, G'_0 естественно изоморфна группе $F' \times_G H$, а G'_1 — под-

группа этой группы, которая проектируется на F' и H соответственно. Но $|F'| + |H| < |F| + |H|$, так как $F_1 \neq \{e\}$, следовательно, по индукционному предположению $G'_0 = G'_1$. Но $F_0 \leq G_1 \leq G_0$ и $G_0/F_0 = G'_0 = G'_1 = G_1/F_0$, поэтому $G_1 = G_0$.

Итак, если $G_1 \cap \text{Ker } \varphi \neq \{e\}$, то $G_1 = G_0$. Аналогично доказывается, что если $G_1 \cap \text{Ker } \psi \neq \{e\}$, то $G_1 = G_0$. Остается рассмотреть случай $G_1 \cap \text{Ker } \varphi = G_1 \cap \text{Ker } \psi = \{e\}$. Пусть $f \in F$; так как G_1 проектируется на F , то существует $h \in H$ такой, что $\langle f, h \rangle \in G_1$; если $h' \in H$ и $\langle f, h' \rangle \in G_1$, то $\langle f, h' \rangle \langle f, h \rangle^{-1} = \langle e, h' h^{-1} \rangle \in G_1 \cap \text{Ker } \psi$. Следовательно, $h' h^{-1} = e$, $h' = h$. Таким образом, для любого $f \in F$ существует единственный $h \in H$ такой, что $\langle f, h \rangle \in G_1$. Этим соответствием задается отображение $\mu: f \mapsto h$, которое, как нетрудно проверить, является изоморфизмом F на H . Кроме того, из $G_1 \leq G_0 = F \times_G H$ следует, что $\psi\mu = \varphi$. Таким образом, F и H изоморфны над G , и тогда из максимальной

пары (φ, ψ) следует, что φ и ψ являются изоморфизмами. Действительно, полагая $G' \cong H$, $\varphi' \cong \mu$, $\psi' \cong \text{id}_H$, $\lambda \cong \psi$, имеем $\lambda\varphi' = \lambda\psi'$, следовательно, из максимальнойности (φ, ψ) имеем $\text{Ker } \lambda = \text{Ker } \psi = \{e\}$, т. е. ψ — изоморфизм, но тогда и $\varphi = \psi\mu$ — изоморфизм. Имеем в этом случае

$$G_0 = \{\langle f, h \rangle \mid \varphi f = \psi h, f \in F, h \in H\} \\ = \{\langle f, h \rangle \mid f = \varphi^{-1}\psi h = \mu h, f \in F, h \in H\} = G_1. \quad \square$$

Следствие. Если $\mathfrak{G}$ — допустимый класс, $F, G, H \in \mathfrak{G}$ и $\varphi: F \rightarrow G$, $\psi: H \rightarrow G$ — максимальная пара эпиморфизмов, то $F \times_G H \in \mathfrak{G}$.

По свойству 3 определения допустимого класса существуют группа $G' \in \mathfrak{G}$ и эпиморфизмы $\varphi': G' \rightarrow F$, $\psi': G' \rightarrow H$ такие, что $\varphi\varphi' = \psi\psi'$. По свойству универсальности расслоенного произведения существует гомоморфизм $\lambda: G' \rightarrow F \times_G H$ такой, что

$$\varphi' = \pi_0 \lambda, \quad \psi' = \pi_1 \lambda, \quad \text{где } \pi_0: F \times_G H \rightarrow F \text{ и } \pi_1: F \times_G H \rightarrow H \text{ — есте-}$$

ственные проекции. Если $G_1 \cong \lambda(G')$, то G_1 — подгруппа $F \times_G H$, проектируемая на F и H соответственно. По лемме 1 $G_1 = F \times_G H$.

Кроме того, G_1 — эпиморфный образ группы $G' \in \mathfrak{G}$, следовательно, $G_1 = F \times_G H \in \mathfrak{G}$ по свойству 1 допустимого класса. $\square$

Обратимся теперь к доказательству предложения 1. Пусть C — класс конечных групп, $\mathfrak{G}(C)$ — наименьший класс конечных групп, содержащий C , замкнутый относительно гомоморфных образов и накрытий и такой, что с каждой максимальной парой $\varphi: F \rightarrow G$, $\psi: H \rightarrow G$ эпиморфизмов такой, что $F, H \in \mathfrak{G}(C)$, группа $F \times_G H \in \mathfrak{G}(C)$. По следствию к лемме 1 класс $\mathfrak{G}(C)$ со-

держится в любом допустимом классе $\mathfrak{G}$ конечных групп, который содержит класс C . Остается заметить, что сам класс $\mathfrak{G}(C)$ допустим. Свойства 1 и 2 выполнены очевидным образом. Проверим свойство 3. Пусть $F, H \in \mathfrak{G}(C)$ и $\varphi: F \rightarrow G$, $\psi: H \rightarrow G$ — эпиморфизмы. Так как группы F, H конечны, то существуют максимальная пара эпиморфизмов $\varphi': F \rightarrow G'$, $\psi': H \rightarrow G'$ и эпиморфизм $\lambda: G' \rightarrow G$ такие, что $\varphi = \lambda\varphi'$, $\psi = \lambda\psi'$. Рассмотрим группу $G_0 \cong F \times_{G'} H$ и эпиморфизмы $\pi_0: G_0 \rightarrow F$, $\pi_1: G_0 \rightarrow H$;

так как $\varphi'\pi_0 = \varphi'\pi_1$, то $\varphi\pi_0 = \lambda\varphi'\pi_0 = \lambda\psi'\pi_1 = \psi\pi_1$; кроме того, $G_0 \in \mathfrak{G}(C)$, так как пара (φ', ψ') максимальна. Свойство 3 для класса $\mathfrak{G}(C)$ проверено. $\square$

Следствие. Если $\mathfrak{G}_0$ и $\mathfrak{G}_1$ — допустимые классы конечных групп, то и $\mathfrak{G}_0 \cap \mathfrak{G}_1$ — допустимый класс. $\square$

Пусть до конца пункта § обозначает произвольный допустимый класс конечных групп. Проконечную группу G будем называть $\mathfrak{G}$ -группой (точнее, *про- $\mathfrak{G}$ -группой*), если семейство $H_1(G)$ всех конечных (непрерывных) гомоморфных образов группы G содержится в $\mathfrak{G}$. Класс всех $\mathfrak{G}$ -групп будем обозначать так: $[\mathfrak{G}]$.

В работе Ершова [8] доказано следующее

Предложение 2. Если $\mathfrak{G}$ — допустимый класс конечных групп, то класс $[\mathfrak{G}]$ всех $\mathfrak{G}$ -групп удовлетворяет следующим условиям:

1. Класс $[\mathfrak{G}]$ замкнут относительно гомоморфных образов.
2. Класс $[\mathfrak{G}]$ замкнут относительно произвольных (в классе проконечных групп) накрытий.

3. Класс $[\mathfrak{G}]$ удовлетворяет свойству коамальгамируемости; если $G_0, G_1 \in [\mathfrak{G}]$, $\varphi_0: G_0 \rightarrow H_0$, $\varphi_1: G_1 \rightarrow H_0$ — эпиморфизмы, то существует группа $H_1 \in [\mathfrak{G}]$ и эпиморфизмы $\psi_0: H_1 \rightarrow G_0$, $\psi_1: H_1 \rightarrow G_1$ такие, что $\varphi_0\psi_0 = \varphi_1\psi_1$. $\square$

$\mathfrak{G}$ -группу G назовем $\mathfrak{G}$ -универсальной, если для любых групп $H_0, H_1 \in \mathfrak{G}$ и эпиморфизмов $\varphi: G \rightarrow H_0$, $\psi: H_1 \rightarrow H_0$ существует эпиморфизм $\varphi': G \rightarrow H_1$ такой, что $\varphi\varphi' = \psi$.

Следующее предложение показывает существование достаточно большого семейства $\mathfrak{G}$ -универсальных групп.

Предложение 3. Любая $\mathfrak{G}$ -группа является гомоморфным образом подходящей $\mathfrak{G}$ -универсальной группы.

Доказательство этого и следующего предложения можно найти в работе Ершова [8]. $\square$

Предложение 4. Любая $\mathfrak{G}$ -универсальная группа является проективной. $\square$

Предложение 3 устанавливает существование $\mathfrak{G}$ -универсальных групп. В некоторых случаях можно установить и единственность.

Предложение 5. Пусть G_0 и G_1 — две $\mathfrak{G}$ -универсальные группы, имеющие конечное или счетное множество порождающих. Если $F \in \mathfrak{G}$, $\varphi: G_0 \rightarrow F$, $\psi: G_1 \rightarrow F$ — эпиморфизмы, то существует изоморфизм $\lambda: G_0 \rightarrow G_1$ этих групп такой, что $\varphi = \psi\lambda$.

Укажем только набросок доказательства, оставляя проверку деталей читателям. Используя условия на мощность порождающих, можно построить две последовательности групп из $\mathfrak{G}$ и эпиморфизмов

$$F = F_0 \leftarrow F_1 \leftarrow \dots,$$

$$F = H_0 \leftarrow H_1 \leftarrow \dots$$

так, что $G_0 \cong \varprojlim F_n$, $G_1 \cong \varprojlim H_n$, а φ и ψ получаются как естественные проекции. Используя $\mathfrak{G}$ -универсальность групп G_0 и G_1 , можно указать две подпоследовательности групп $F_{f(n)}$, $H_{g(n)}$

$F_{f(1)}, \dots; H_{g(0)}, H_{g(1)}, \dots; f(0) < f(1) < \dots, 0 = g(0) < g(1) < \dots$, и построить семейства эпиморфизмов $\varphi_n: F_{f(2n)} \rightarrow H_{g(2n)}$, $\psi_n: H_{g(2n+1)} \rightarrow F_{f(2n+1)}$ такие, что для любого $n \in \omega$ диаграмма

$$\begin{array}{ccccc} F_{f(2n)} & \xleftarrow{\quad} & F_{f(2n+1)} & \xleftarrow{\quad} & F_{f(2n+2)} \\ \varphi_n \downarrow & & \psi_n \uparrow & & \varphi_{n+1} \downarrow \\ H_{g(2n)} & \xleftarrow{\quad} & H_{g(2n+1)} & \xleftarrow{\quad} & H_{g(2n+2)} \end{array}$$

коммутативна.

Семейство эпиморфизмов φ_n , $n \in \omega$, определяет эпиморфизм $\lambda: G_0 \rightarrow G_1$; а семейство эпиморфизмов ψ_n , $n \in \omega$, определяет эпиморфизм $\mu: G_1 \rightarrow G_0$. Коммутативность вышеприведенной диаграммы показывает, что λ и μ — взаимно обратные изоморфизмы. $\square$

Следствие. Если $\mathfrak{G} \subseteq \mathfrak{G}_n$ для некоторого $n \in \omega$, то любые две $\mathfrak{G}$ -универсальные группы изоморфны. $\square$

Замечание. Если не выполнено условие следствия, то существуют сколь угодно мощные $\mathfrak{G}$ -группы, а следовательно, и сколь угодно мощные $\mathfrak{G}$ -универсальные группы.

Пусть G — проконечная группа, $H_f(G)$ — семейство всех конечных гомоморфных образов группы G . Группу G назовем *допустимой*, если для любых $H_0, H_1 \in H_f(G)$ и любых эпиморфизмов $\varphi: G \rightarrow H_0$, $\psi: H_1 \rightarrow H_0$ существует эпиморфизм $\varphi': G \rightarrow H_1$ такой, что $\psi\varphi' = \varphi$.

Предложение 6. Проективная проконечная группа G является допустимой тогда и только тогда, когда $H_f(G)$ — допустимый класс, а G является $H_f(G)$ -универсальной группой.

Пусть G — допустимая группа. Класс $H_f(G)$, очевидно, замкнут относительно гомоморфных образов. Проверим, что $H_f(G)$ удовлетворяет свойству коамальгамируемости. Пусть $G_0, G_1 \in H_f(G)$, $\varphi_0: G_0 \rightarrow H_0$, $\varphi_1: G_1 \rightarrow H_0$ — эпиморфизмы. Так как $H_0 \in H_f(G)$, то существует эпиморфизм $\lambda: G \rightarrow H_0$; по определению допустимости G существуют эпиморфизмы $\varphi'_0: G \rightarrow G_0$ и $\varphi'_1: G \rightarrow G_1$ такие, что $\varphi_0\varphi'_0 = \varphi_1\varphi'_1 = \lambda$. Пусть $N \trianglelefteq \text{Ker } \varphi'_0 \cap \text{Ker } \varphi'_1$, $H_1 \trianglelefteq G/N$, тогда H_1 — конечная группа ($H_1 \cong G_0 \times G_1$), $H_1 \in H_f(G)$ и эпиморфизмы $\varphi'_0: G \rightarrow G_0$ индуцируют эпиморфизмы $\psi_i: H_1 \rightarrow G_i$, причем такие, что $\varphi_0\varphi'_0 = \varphi_1\varphi'_1$. Таким образом, $H_f(G)$ удовлетворяет свойству коамальгамируемости. Пусть $H_0 \in H_f(G)$, $\varphi: H_1 \rightarrow H_0$ — накрытие (H_1 — конечная группа); пусть $\psi: G \rightarrow H_0$ — некоторый эпиморфизм (существование такого эпиморфизма следует из того, что $H_0 \in H_f(G)$). Если G — проективная группа, то существует гомоморфизм $\psi': G \rightarrow H_1$ такой, что $\psi = \varphi\psi'$. Но $\psi'(G)$ — под-

группа H_1 , отображающаяся на H_0 ; так как φ — накрытие, то $\psi'(G) = H_1$ и $H_1 \in H_f(G)$. Таким образом, если G проективна, то класс $H_f(G)$ замкнут и относительно накрытий. Таким образом, установлено, что $H_f(G)$ — допустимый класс; то, что допустимая группа G является $H_f(G)$ -универсальной, очевидно. Необходимость установлена.

Достаточность очевидна, так как из $\mathfrak{G}$ -универсальности группы G следует, что $H_f(G) = \mathfrak{G}$. $\square$

Оставшаяся часть пункта будет посвящена решению следующей алгоритмической проблемы:

По заданному семейству конечных групп $H_0, \dots, H_k$, G узнать, принадлежит ли группа G классу $\mathfrak{G}(H_0, \dots, H_k)$?

Укажем сначала достаточно малый, но просто устроенный допустимый класс $\mathfrak{G}$, который содержит $\mathfrak{G}(H_0, \dots, H_k)$.

Пусть K — класс конечных простых групп такой, что выполнено условие:

(*) если $G \in K$, простое число p делит порядок $|G|$ группы G , то циклическая группа C_p порядка p принадлежит K .

Лемма 2. Если класс K конечных простых групп удовлетворяет условию (*), а $\mathfrak{G}_K$ обозначает класс всех конечных групп, все композиционные факторы которых принадлежат K , то $\mathfrak{G}_K$ — допустимый класс.

Действительно, класс $\mathfrak{G}_K$, очевидно, замкнут относительно гомоморфных образов, прямых произведений и расширений. Следовательно, он замкнут и относительно расслоенных прямых произведений. Таким образом, $\mathfrak{G}_K$ удовлетворяет условиям 1 и 3 определения допустимого класса. Проверим, что $\mathfrak{G}_K$ замкнут относительно накрытий. Пусть $\varphi: F \rightarrow G$ — накрытие и $G \in \mathfrak{G}_K$. Так как $\text{Ker } \varphi \trianglelefteq \Phi(F)$, то композиционные факторы F — это композиционные факторы G вместе с набором групп вида C_p — композиционных факторов нильпотентной группы $\text{Ker } \varphi$. Однако, как известно (Хупперт [1]), если простое число p делит порядок подгруппы Фраттини группы F , то p делит и порядок $|F/\Phi(F)|$, а следовательно, порядок группы G и порядок одного из композиционных факторов группы G . По условию (*) тогда $C_p \in K$ и, следовательно, $F \in \mathfrak{G}_K$. $\square$

Следствие. Класс $\mathfrak{G}_{K,n}$ всех групп из $\mathfrak{G}_K$, имеющих n порождающих, является допустимым.

Действительно, $\mathfrak{G}_{K,n} = \mathfrak{G}_K \cap \mathfrak{G}_n$. $\square$

Опишем один из способов получения универсальной группы для такого класса $\mathfrak{G}_{K,n}$.

Предложение 7. Если F_n — (абстрактная) свободная группа с n порождающими, то семейство $S \triangleq \{N \mid N \text{ — нормальная подгруппа } F_n \text{ и } F_n/N \in \mathfrak{G}_K\}$ направленно (по убыванию),

a (проконечная) группа $G \cong \varprojlim \{F_n/N \mid N \in S\}$ является $\mathbb{G}_{\kappa, n}$ -универсальной.

Установим, что S замкнуто относительно пересечений. Пусть $N_0, N_1 \in S$, рассмотрим два нормальных ряда $N_1 \leq N_0 N_1 \leq F_n$ и $N_0 \cap N_1 \leq N_0 \leq F_n$. Так как $F_n/N_1 \in \mathbb{G}_\kappa$, то $N_0 N_1/N_1 \in \mathbb{G}_\kappa$, но $N_0/N_0 \cap N_1 \cong N_0 N_1/N_1$ и F_n/N_0 принадлежит $\mathbb{G}_\kappa$, следовательно, и $F_n/N_0 \cap N_1 \in \mathbb{G}_\kappa$ и $N_0 \cap N_1 \in S$.

Из определения группы G видно, что $G \in [\mathbb{G}_{\kappa, n}]$. Пусть $a_1, \dots, a_n \in G$ — это образы свободных порождающих группы F_n . Пусть $H_0, H_1 \in \mathbb{G}_{\kappa, n}$, $\varphi: H_1 \rightarrow H_0$ и $\psi: G \rightarrow H_0$ — эпиморфизмы. Система $\psi(a_1), \dots, \psi(a_n)$ порождает H_0 ; по лемме Гашюца в H_1 существует система порождающих $b_1, \dots, b_n$ такая, что $\varphi(b_i) = \psi(a_i)$, $i = 1, \dots, n$. Тогда, очевидно, существует эпиморфизм $\lambda: G \rightarrow H_1$ такой, что $\lambda a_i = b_i$, $i = 1, \dots, n$. Для этого эпиморфизма имеем $\varphi \lambda = \psi$. Таким образом, установлено, что G является $\mathbb{G}_{\kappa, n}$ -универсальной группой. $\square$

По набору конечных групп $H_0, \dots, H_k$ можно эффективно найти наименьший (конечный) класс простых групп K_0 , содержащий все композиционные факторы групп $H_0, \dots, H_k$ и удовлетворяющий условию (*). Если $n_0 \in \omega$ таково, что все группы из $H_0, \dots, H_k$ имеют n_0 порождающих (в качестве такого n_0 можно взять, например, $\max_{i \leq k} |H_i|$), то $\mathbb{G}(H_0, \dots, H_k) \subseteq \mathbb{G}_{\kappa, n_0}$.

Покажем теперь, что принадлежность классу $\mathbb{G}(H_0, \dots, H_k)$ эффективно определяется с помощью некоторой конечной группы F , порядок которой может быть оценен с помощью найденного выше вложения $\mathbb{G}(H_0, \dots, H_k) \subseteq \mathbb{G}_{\kappa, n}$.

Для проконечной группы G через $\psi(G)$ обозначим пересечение всех максимальных открытых нормальных подгрупп группы G ; пусть $\psi_0(G) \cong G$, $\psi_{n+1}(G) \cong \psi(\psi_n(G))$ и $\psi^n(G) \cong G/\psi_n(G)$, $n \in \omega$; ψ^n будет обозначать и естественный эпиморфизм G на $\psi^n(G)$. Последнее определение имеет смысл, так как $\psi_n(G)$ — нормальная (даже характеристическая) подгруппа G для любого $n \in \omega$. Полагаем $l(G) \cong 0$, если $G = \{e\}$, и $l(G) \cong \sup_{n \in \omega} \{n+1 \mid \psi_n(G) \neq \{e\}\}$, если $G \neq \{e\}$.

Лемма 3. Если $\{e\} = G_0 \leq \dots \leq G_n = G$ — субнормальный ряд, факторы которого вполне приводимы (т. е. являются произведениями простых групп), то $l(G) \leq n$.

Эта лемма легко следует из следующих двух легко проверяемых фактов:

1. $\psi(G) \leq G_{n-1}$.
2. Если H — субнормальная подгруппа группы G , то $\psi(H) \leq \psi(G)$. $\square$

Следствие. Для любой группы G $l(G) < \omega$ тогда и только тогда, когда для G существует субнормальный ряд с вполне

приводимыми факторами и $l_0 \cong l(G)$ — минимальная длина такого ряда.

Нужно только заметить, что

$$\{e\} = \psi_{l_0}(G) \leq \psi_{l_0-1}(G) \leq \dots \leq \psi_0(G) = G$$

— нормальный ряд с вполне приводимыми факторами. $\square$

Лемма 4. Если $\varphi: F \rightarrow G$ — эпиморфизм, то $\varphi(\psi_n(F)) \leq \psi_n(G)$ для любого $n \in \omega$; поэтому φ индуцирует эпиморфизмы $\varphi_n: \psi^n(F) \rightarrow \psi^n(G)$ и $l(G) \leq l(F)$.

Достаточно проверить: $\varphi(\psi(F)) \leq \psi(G)$, а это очевидно. $\square$

Вернемся к нашему классу $\mathbb{G}^0 \cong \mathbb{G}(H_0, \dots, H_k)$. Определим сейчас конечную группу F^* , которая в определенном смысле содержит «всю информацию» о классе $\mathbb{G}^0$. Пусть G — $\mathbb{G}^0$ -универсальная группа, $s_0 \cong \max_{i \leq k} l(H_i)$; полагаем $F^* \cong \psi^{s_0}(G)$. Установим основные факты о группе F^* .

1. F^* — конечная группа; ее порядок можно оценить примитивно рекурсивной функцией от s_0, n_0 и $\max_{i \leq k} |H_i|$.

Этот факт вытекает из следующей леммы:

Лемма 5. Если K — конечный класс простых групп, удовлетворяющий свойству (*), $m \cong \max_{P \in K} |P|$, G_0 — $\mathbb{G}_{\kappa, n}$ -универсальная группа, то группа $\psi^*(G_0)$ конечна и ее порядок можно оценить сверху примитивно рекурсивной функцией $g(n, m, k)$.

Воспользуемся предложением 7: $G_0 \cong \varprojlim \{F_n/N \mid N \triangleleft F_n, F_n/N \in \mathbb{G}_\kappa\}$. Это представление позволяет вычислить $\psi^*(G_0)$ следующим образом:

Пусть $N_0 \cong F_n$; $N_{k+1} \cong \bigcap \{N \mid N \triangleleft N_k, N_k/N \in K\}$, $k \in \omega$; тогда $\psi^*(G_0) \cong F_n/N_k$.

Используя формулы из книги Холла [1], установим оценки порядков групп F_n/N_k :

а) число $M_{n, k}$ подгрупп индекса $\leq k$ в свободной группе F_n оценивается сверху числом $k(k!)^{n-1}$;

б) индекс пересечения всех подгрупп индекса $\leq k$ в F_n оценивается сверху числом $k^{k(k!)^{n-1}}$.

Подгруппа N_1 имеет в F_n индекс $\leq l_0 \cong m^{m(m!)^{n-1}}$; тогда N_1 — свободная группа с числом порождающих $\leq 1 + l_0(n-1)$.

Полагая $n_0 \cong n$, $l_{k+1} \cong m^{m(m!)^{n_k-1}}$, $n_{k+1} \cong 1 + l_k(n_k - 1)$, индукцией получаем, что N_{k+1} имеет индекс $\leq l_k$ в N_k и N — свободная группа с числом порождающих $\leq n_k$.

Оценивая $|\psi^*(G_0)|$, имеем

$$|\psi^*(G_0)| = |F_n/N_k| = |F_n/N_1| \cdot |N_1/N_2| \cdot \dots \cdot |N_{k-1}/N_k|$$

$$\leq l_0 \cdot l_1 \cdot \dots \cdot l_{k-1} = \prod_{i \leq k} l_i.$$

Ясно, что $\prod_{i \leq k} l_i$ — примитивно рекурсивная функция от n, m и k . $\square$

Так как $\mathbb{G}^0 \in \mathbb{G}_{K_0, n_0}$, то по предложению 3 и следствию предложения 5 существует эпиморфизм $\mathbb{G}_{K_0, n_0}$ -универсальной группы G_0 на $\mathbb{G}^0$ -универсальную группу G , который индуцирует эпиморфизм группы $\psi^{s_0}(G_0)$ на F^* . Оценка порядка $|\psi^{s_0}(G_0)|$, полученная в лемме, дает и оценку порядка $|F^*|$. $\square$

2. $H_i \in H_i(F^*)$, $i \leq k$.

Действительно, для любого $i \leq k$ существует эпиморфизм $\varphi_i: G \rightarrow H_i$, который индуцирует эпиморфизм $\varphi'_i: F^*(=\psi^{s_0}(G)) \rightarrow H_i = \psi^{s_0}(H_i)$, так как $l(H_i) \leq s_0$. $\square$

3. $l(H) > s_0$ для любого собственного накрытия $\varphi: H \rightarrow F^*$; $l(F^*) = s_0$.

Предположим противное, и пусть $\varphi: H \rightarrow F^*$ — собственное накрытие такое, что $l(H) = s_0$. Так как $H \in \mathbb{G}^0$, то существует эпиморфизм $\psi: G \rightarrow H$, который индуцирует эпиморфизм $\psi': F^* \rightarrow H (= \psi^{s_0}(H))$, но тогда $|H| \leq |F^*|$ и H не может быть собственным накрытием конечной группы F^* . То, что $l(F^*) = s_0$, следует из определения $F^* \Rightarrow \psi^{s_0}(G)$. $\square$

Будем говорить, что группа F однородна, если для любых двух эпиморфизмов $\varphi_i: F \rightarrow H$, $i = 0, 1$, на конечную группу существует автоморфизм $\lambda: F \rightarrow F$ такой, что $\varphi_0 = \varphi_1 \lambda$.

Замечание. Более точным, но более громоздким названием этого свойства было бы *конечная кооднородность*.

4. Группа F^* однородна.

Из предложения 5 следует, что группа G — допустимая конечно порожденная группа — является однородной, а однородность F^* вытекает из однородности G , так как $F^* = G/\psi_{s_0}(G)$, а $\psi_{s_0}(G)$ — характеристическая подгруппа G . $\square$

Покажем, что факты 1, 3, 4 уже влекут важную информацию. Пусть F — конечная однородная группа, а $s \in \omega$ таково, что $l(F) = s$ и $l(H) > s$ для любого собственного накрытия H группы F . Пусть $\mathbb{G}_F$ — класс всех конечных групп, которые являются гомоморфными образами всевозможных конечных накрытий группы F .

Предложение 8. Класс $\mathbb{G}_F$ является допустимым; конечная группа H принадлежит $\mathbb{G}_F$ тогда и только тогда, когда $\psi^s(H) \in H_i(F)$ и группа $H_F \Rightarrow H \times_{\psi^s(H)} F$ (не зависящая от выбора эпиморфизма $F \rightarrow \psi^s(H)$), является накрытием группы F .

Проверим, что $\mathbb{G}_F$ — допустимый класс. Из определения видно, что $\mathbb{G}_F$ замкнут относительно гомоморфных образов. Для

проверки замкнутости $\mathbb{G}_F$ относительно накрытий установим следующую лемму.

Лемма 6. Если $\varphi_i: H_i \rightarrow H$, $i = 0, 1$, — максимальная пара эпиморфизмов и φ_0 — накрытие, то $\pi_1: H_0 \times_H H_1 \rightarrow H_1$ — накрытие.

Пусть $H^* \leq H_0 \times_H H_1$ и $\pi_1(H^*) = H_1$; тогда $\varphi_1 \pi_1(H^*) = H$; но $\varphi_1 \pi_1 = \varphi_0 \pi_0$, и тогда $\pi_0(H^*)$ — такая подгруппа H_0 , что $\varphi_0 \pi_0(H^*) = H$. Так как φ_0 — накрытие, то $\pi_0(H^*) = H_0$; тогда по лемме 1 $H^* = H_0 \times_H H_1$ и, следовательно, π_1 — накрытие. $\square$

Пусть $\varphi'_0: H_0 \rightarrow H'$ — накрытие и $H' \in \mathbb{G}_F$; так как $H' \in \mathbb{G}_F$, то существует группа H_1 и эпиморфизмы $\varphi'_1: H_1 \rightarrow H'$ и $\psi: H_1 \rightarrow F$ причем ψ — накрытие. Найдем группу H , эпиморфизм $\lambda: H \rightarrow H'$ и максимальную пару эпиморфизмов $\varphi_i: H_i \rightarrow H$ такую, что $\lambda \varphi_i = \varphi'_i$, $i = 0, 1$. Отметим, что φ_0 является накрытием, так как φ'_0 — накрытие. По лемме 6 проекция $\pi_1: H_0 \times_H H_1 \rightarrow H_1$ является

накрытием, но тогда $\psi \pi_1$ есть накрытие группы F , следовательно, H_0 , как гомоморфный образ накрытия $H_0 \times_H H_1$ группы F ,

лежит в $\mathbb{G}_F$.

Прежде чем доказывать для $\mathbb{G}_F$ свойство коамальгамируемости, установим заключительное утверждение предложения. Для группы H такой, что $\psi^s(H) \in H_i(F)$, пусть $\varphi_i: F \rightarrow \psi^s(H)$, $i = 0, 1$, — два эпиморфизма, тогда из однородности группы F следует существование автоморфизма $\lambda: F \rightarrow F$ такого, что $\varphi_0 = \varphi_1 \lambda$; тогда пара изоморфизмов (id_H, λ) определяет изоморфизм группы

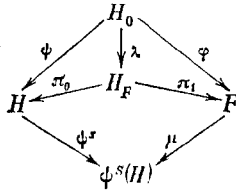
$$H_F^0 \Rightarrow \{ \langle h, f \rangle \mid \psi^s h = \varphi_0 f, h \in H, f \in F \}$$

на группу

$$H_F^1 \Rightarrow \{ \langle h, f \rangle \mid \psi^s h = \varphi_1 f, h \in H, f \in F \}.$$

Таким образом, группы H_F^0 и H_F^1 изоморфны над H и, следовательно, однозначно определены над H ; любую из таких групп будем обозначать H_F ; ее проекция на F определена с точностью до автоморфизма группы F . Итак, если $\psi^s(H) \in H_i(F)$ и H_F — накрытие F , то H как гомоморфный образ H_F принадлежит $\mathbb{G}_F$. Наоборот, пусть $\varphi: H_0 \rightarrow F$ — накрытие, $\psi: H_0 \rightarrow H$ — эпиморфизм. Тогда φ и ψ индуцируют эпиморфизмы $\varphi_s: \psi^s(H_0) \rightarrow F (= \psi^s(F))$, $\psi_s: \psi^s(H_0) \rightarrow \psi^s(H)$. Так как $\varphi = \varphi_s \psi^s$ и φ — накрытие, то φ_s — накрытие; но $l(\psi^s(H_0)) = s$, следовательно, $\psi^s(H_0)$ не может быть собственным накрытием. Отсюда φ_s

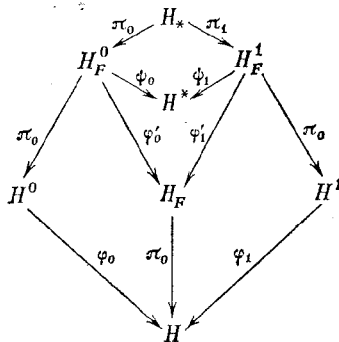
изоморфизм и $\psi^s(H)$ — гомоморфный образ $\psi^s(H_0) \simeq F$, т. е. $\psi^s(H) \in H_f(F)$. Рассмотрим коммутативную диаграмму



где $\mu \Leftarrow \psi^s \phi_s^{-1}$, а λ — гомоморфизм, определенный по свойству универсальности расслоенного произведения $H_F = H \times_{\psi^s(H)} F$. За-

метим теперь, что из $l(F) = s$ следует, что пара эпиморфизмов (ψ^s, μ) является максимальной, следовательно, из леммы 1 сразу вытекает, что λ — эпиморфизм. Так как $\phi = \pi_1 \lambda$ — накрытие, то и π_1 — накрытие.

Установим теперь свойство коамальгируемости для класса $\mathfrak{G}_F$. Пусть $\phi_0: H^0 \rightarrow H$, $\phi_1: H^1 \rightarrow H$ — пара эпиморфизмов и $H^0, H^1, H \in \mathfrak{G}_F$; тогда ϕ_i индуцируют эпиморфизмы $\phi'_i: H_F^i \rightarrow H_F$, $i=0, 1$. Заметим, что ϕ'_i является накрытием; действительно, композиция эпиморфизмов ϕ'_i и $\pi_1: H_F \rightarrow F$ является накрытием (это есть $\pi_1: H_F^i \rightarrow F$), следовательно, и ϕ'_i — накрытие, $i=0, 1$. Найдем для этой пары (ϕ'_0, ϕ'_1) эпиморфизмов группу H^* , эпиморфизм $\lambda: H^* \rightarrow H_F$ и максимальную пару эпиморфизмов $\psi_0: H_F^0 \rightarrow H^*$, $\psi_1: H_F^1 \rightarrow H^*$ такие, что $\phi'_i = \lambda \psi_i$, $i=0, 1$. Заметим, что из равенства $\phi'_0 = \lambda \psi_0$ и того, что ϕ'_0 — накрытие, следует, что ψ_0 — накрытие. По лемме 6 проекция $\pi_1: H_* (\Leftarrow H_F^0 \times_{H^*} H_F^1) \rightarrow H_F^1$ является накрытием; но H_F^1 — накрытие F ; следовательно, H_* — накрытие F и $H_* \in \mathfrak{G}_F$. Рассмотрим коммутативную диаграмму



показывает, что $\mathfrak{G}_F$ удовлетворяет и условию коамальгируемости. $\square$

Следствие 1. $\mathfrak{G}_F = \mathfrak{G}(F)$.

Очевидно. $\square$

Следствие 2. $\mathfrak{G}_{F^*} = \mathfrak{G}^0$.

Действительно, из факта 2 следует, что $\mathfrak{G}^0 = \mathfrak{G}(H_0, \dots, H_k) \subseteq \mathfrak{G}_{F^*}$. По определению $F^* \in \mathfrak{G}^0$; следовательно, $\mathfrak{G}_{F^*} = \mathfrak{G}(F^*) \subseteq \mathfrak{G}^0$. $\square$

Укажем теперь, как решать упомянутую выше алгоритмическую проблему о принадлежности конечной группы G допустимому классу $\mathfrak{G}(H_0, \dots, H_k)$.

1. По набору групп $H_0, \dots, H_k$ строим конечный класс K_0 простых групп, состоящий из всех композиционных факторов группы $H_0 \times \dots \times H_k$ и циклических групп C_p для всех простых p , которые делят порядок $|H_0 \times \dots \times H_k|$.

2. Пусть $s_0 \Leftarrow \max_{i \leq k} l(H_i)$, $n_0 \Leftarrow \max_{i \leq k} |H_i|$, $R_0 \Leftarrow g(n_0, n_0, s_0)$, где g — примитивно рекурсивная функция, определенная в доказательстве леммы 5.

3. Перебирая все конечные группы порядка $\leq R_0$, выберем из них все такие F из $\mathfrak{G}_{K_0, n_0}$, которые удовлетворяют условиям: 1) $H_i \in H_f(F)$, $i \leq k$; 2) F — однородная группа; 3) $l(F) = s_0$ и $l(H) > s_0$ для любого собственного накрытия H группы F .

Алгоритмическая проверка свойств 1) и 2) и свойства $l(F) = s_0$ очевидна. Укажем, как проверять свойство $l(H) > s_0$ для любого собственного накрытия H группы F . Для этого достаточно ограничиться рассмотрением минимальных собственных накрытий:

Пусть $\phi: H \rightarrow F$ — накрытие и N — максимальный нормальный делитель H , лежащий в $\text{Ker } \phi$ и отличный от $\text{Ker } \phi$; тогда ϕ индуцирует накрытие $\phi': H' \rightarrow F$, $H' \Leftarrow H/N$ и $\text{Ker } \phi' = \text{элементарная абелева } p\text{-группа для некоторого простого } p \text{ такого, что } p \mid |F|$. Заметим, что если $l(H') > s_0$, то и $l(H) > s_0$, поэтому достаточно ограничиться рассмотрением собственного накрытия $\phi: H \rightarrow F$, ядро которого не содержит собственных нормальных делителей и, следовательно, является элементарной абелевой p -группой. Оценим порядок этого ядра. Пусть F_{n_0} — (абстрактная) свободная группа с n_0 порождающими и $\psi: F_{n_0} \rightarrow F$ — некоторый эпиморфизм; его можно продолжить до некоторого гомоморфизма $\psi': F_{n_0} \rightarrow H$ в H . Но так как ϕ — накрытие, то ψ' — эпиморфизм; ψ' индуцирует эпиморфизм $\psi^*: \text{Ker } \psi \rightarrow \text{Ker } \phi$, а $\text{Ker } \psi$ — подгруппа F_{n_0} индекса $|F|$, следовательно, $\text{Ker } \psi$ — свободная группа с $n_1 \Leftarrow (1 + |F| \cdot (n_0 - 1))$ порождающими. Поэтому $\text{Ker } \phi$ не может иметь более чем n_1 порождающих и

$|\text{Ker } \varphi| \leq p^n \leq |F|^{|\varphi|^2} \leq R_0^{R_0^2}$. Отсюда следует, что достаточно рассматривать накрытия $\varphi: H \rightarrow F$, порядок которых $\leq R_0^{R_0^2+1}$.

Таким образом, путем конечного перебора найдем все (с точностью до изоморфизма) группы $F_1, \dots, F_t$, удовлетворяющие сформулированным выше условиям 1)–3). Предложение 1 позволяет эффективно перечислять класс $\mathfrak{G}(H_0, \dots, H_k)$; продолжая перечисление этого класса до тех пор, пока не найдем такого i_0 , $1 \leq i_0 \leq t$, что $F_{i_0} \in \mathfrak{G}(H_0, \dots, H_k)$. Заметим, что такое i_0 обязательно найдется, так как среди групп $F_1, \dots, F_t$ находится группа F^* (см. выше факты 1–4 о группе F^*). Покажем, что $F_{i_0} \simeq F^*$. Как при доказательстве следствия 2 предложения 8, имеем $\mathfrak{G}(H_0, \dots, H_k) = \mathfrak{G}_{F_{i_0}}$. В частности, $F^* \in \mathfrak{G}_{F_{i_0}}$ и, следовательно, существует конечная группа F_0 , накрытие $\psi: F_0 \rightarrow F_{i_0}$ и эпиморфизм $\varphi: F_0 \rightarrow F^*$. Эти эпиморфизмы индуцируют эпиморфизмы $\psi_s: \psi^s(F_0) \rightarrow F_{i_0}$, $\varphi_s: \psi^s(F_0) \rightarrow F^*$, но ψ_s как накрытие должен быть изоморфизмом, следовательно, $\varphi_s \psi_s^{-1}: F_{i_0} \rightarrow F^*$ — эпиморфизм и $|F^*| \leq |F_{i_0}|$. Аналогично, из того, что $F_{i_0} \in \mathfrak{G}(H_0, \dots, H_k) = \mathfrak{G}_{F^*}$, получаем $|F_{i_0}| \leq |F^*|$, следовательно, $F^* \simeq F_{i_0}$.

Итак, группа F^* найдена. Теперь для любой конечной группы G имеем: $G \in \mathfrak{G}(H_0, \dots, H_k) \Leftrightarrow G \in \mathfrak{G}_{F^*} \Leftrightarrow \psi^s(G) \in H_1(F^*)$ и $\pi_1: G_F \rightarrow F$ — накрытие. Последнее свойство проверяется эффективно.

3. Теоретико-модельные свойства регулярно замкнутых полей. В начале пункта будем рассматривать только случай полей характеристики 0. Пусть σ_f — это обычная сигнатура теории полей $\langle +, \cdot, -, ^{-1}, 0, 1 \rangle$. Начнем с вопросов выразимости некоторых свойств полей на элементарном языке.

Пусть $\mathfrak{G}$ — произвольный допустимый класс конечных групп, $\mathfrak{F}_{\mathfrak{G}}$ — класс всех полей (характеристики 0), группа Галуа которых является $\mathfrak{G}$ -группой, и $\mathfrak{F}_{\mathfrak{G}}^*$ — класс всех регулярно замкнутых полей из $\mathfrak{F}_{\mathfrak{G}}$, группа Галуа которых является $\mathfrak{G}$ -универсальной.

Предложение 1. *Классы полей $\mathfrak{F}_{\mathfrak{G}}$ и $\mathfrak{F}_{\mathfrak{G}}^*$ являются аксиоматизируемыми. Если $\mathfrak{G}$ — рекурсивный класс конечных групп, то эти классы рекурсивно аксиоматизируемы.*

Для любого поля K и любого фиксированного $n \in \omega$, $n > 0$ любая n -мерная K -алгебра A с фиксированным базисом $e_1, \dots, e_n$ однозначно определяется своими структурными константами $c_{ij}^k: e_i e_j = \sum_{k=1}^n c_{ij}^k e_k$, $1 \leq i, j \leq n$. Это позволяет на элементарном языке записывать высказывание о существовании n -мер-

ных K -алгебр с теми или иными элементарными свойствами, утверждение о том, что для всех n -мерных K -алгебр выполняются определенные элементарные свойства и многое другое. Однако приведение явной формулы, выражающей это свойство, как правило, трудно из-за громоздкости записи. Приведем один пример: укажем, как записать формулу E_n , утверждающую, что у поля K существует по крайней мере одно расширение степени n .

Пусть y_{ij}^k , $1 \leq i, j, k \leq n$, — различные переменные, подразумеваемые значения которых — структурные константы соответствующей K -алгебры.

Формула $A(\bar{y}) \Leftrightarrow \bigwedge_{k=1}^n \bigwedge_{i,j=1}^n y_{ij}^k = y_{ji}^k$ «выражает» коммутативность алгебры.

Формула $B(\bar{y}) \Leftrightarrow \bigwedge_{i=1}^n (y_{ii}^1 = 1 \wedge \bigwedge_{j \neq i} y_{ij}^1 = 0)$ выражает существование единицы (точнее, что e_1 — единица).

Формула $C(\bar{y}) \Leftrightarrow \bigwedge_{1 \leq i, j, k \leq n} \left(\bigwedge_{s=1}^n \left(\sum_{k=1}^n y_{ji}^s y_{ik}^s = \sum_{k=1}^n y_{ij}^s y_{kl}^s \right) \right)$ выражает ассоциативность.

Формула

$$D(\bar{y}) \Leftrightarrow \forall \bar{x} \forall \bar{z} \left[\left(\bigvee_{i=1}^n x_i \neq 0 \right) \wedge \left(\bigvee_{i=1}^n z_i \neq 0 \right) \rightarrow \bigvee_{k=1}^n \left(\sum_{i,j=1}^n y_{ij}^k x_i z_j \neq 0 \right) \right]$$

выражает условие отсутствия делителей нуля.

Полагая $E_n \Leftrightarrow \exists \bar{y} (A(\bar{y}) \wedge B(\bar{y}) \wedge C(\bar{y}) \wedge D(\bar{y}))$, получим нужную формулу.

Аналогично (но более громоздко) можно написать предложение Q_H , выражающее существование расширения Галуа L поля K , группа Галуа которого изоморфна группе H . Используя предложения Q_H , можно написать систему аксиом для класса $\mathfrak{F}_{\mathfrak{G}}$. Таковой будет $T_{\mathfrak{G}} \Leftrightarrow T_{\mathfrak{F}}^0 \cup \{ \neg Q_H \mid H \text{ — конечная группа, } H \notin \mathfrak{G} \}$, где $T_{\mathfrak{F}}^0$ — система аксиом для теории полей характеристики 0. Для аксиоматизации класса $\mathfrak{F}_{\mathfrak{G}}^*$ понадобятся более сложные предложения. Пусть $\varphi: H \rightarrow F$ — эпиморфизм конечных групп, тогда по φ можно эффективно построить предложение Q_{φ} , удовлетворяющее следующему семантическому условию для любого поля K :

$K \models Q_{\varphi} \Leftrightarrow$ для любых расширения Галуа L поля K и изоморфизма $\lambda: F \rightarrow \text{Aut}_K L$ существуют расширения Галуа $M \geq L$ поля K и изоморфизм $\mu: H \rightarrow \text{Aut}_K M$ такие, что $\lambda \varphi = \mu \lambda$, где $\lambda: \text{Aut}_K M \rightarrow \text{Aut}_K L$ — проекция ограничения.

Тогда системой аксиом для теории класса $\mathfrak{F}_0$ будет $T_0 \cup T_R \cup U \{Q_\Phi | \Phi: H \rightarrow F - \text{эпиморфизм, } H \in \mathfrak{G}\}$, где T_R — система аксиом для класса регулярно замкнутых полей, которая будет сейчас указана.

Для написания системы аксиом T_R воспользуемся свойством 3 предложения 1 п. 1 и для любого $n \in \omega, n > 0$ напишем предложение P_n , выражающее следующее свойство поля K : для любого абсолютно неприводимого многочлена $f \in K[x_1, \dots, x_k, y]$, $k \leq n$, $\deg f \leq n$, который как многочлен от y унитарен и сепарабелен, любого многочлена $g \in K[x_1, \dots, x_k]$, $g \neq 0$, $\deg g \leq n$, существуют $\alpha_1, \dots, \alpha_k, \beta$ в K такие, что $f(\bar{\alpha}, \beta) = 0$, $g(\bar{\alpha}) = 0$. Единственное, что нужно понять для записи такого предложения, — это то, что свойство абсолютной неприводимости f может быть записано элементарно. Однако хорошо известный прием Кронекера (см., например, Джарден и Кинне [1]) показывает, что достаточно проверить просто неприводимость f над расширениями L поля K , степень которых над K не превосходит n^n . Тогда $T_R \equiv \{P_n | n \in \omega, n > 0\}$. $\square$

Для теоретико-модельного изучения регулярно замкнутых полей и даже просто регулярных расширений удобно формульно расширить сигнатуру теории полей так, чтобы расширениями в этой сигнатуре были в точности регулярные расширения. Пусть $\sigma_R \equiv \sigma_f \cup \{W^n | n \in \omega, n > 1\}$ — формульное расширение σ_f , где W^n определяется (в классе полей) формулой

$$W^n(x_1, \dots, x_n) \equiv \exists y (y^n + x_1 y^{n-1} + \dots + x_{n-1} y + x_n = 0).$$

Каждое поле K имеет естественное обогащение K_R до сигнатуры σ_R , причем, если $K \leq L$, то $K_R \leq L_R$ тогда и только тогда, когда K алгебраически замкнуто в L . В частности, когда K — поле характеристики 0, это равносильно регулярности расширения L .

В дальнейшем поля из классов $\mathfrak{F}_0$ и $\mathfrak{F}_0$ будем рассматривать (не оговаривая впредь) как модели сигнатуры σ_R , опуская символ R в обозначении K_R для обогащения K до сигнатуры σ_R .

Предложение 2. Если $K, L, M \in \mathfrak{F}_0$, $K \leq L$, $K \leq M$, то существуют $K_0 \in \mathfrak{F}_0$, $K \leq K_0$ и K -изоморфизмы $\varphi: L \rightarrow K_0$, $\psi: M \rightarrow K_0$ в K_0 из L и M соответственно.

Регулярные вложения $K \leq L$ и $K \leq M$ индуцируют эпиморфизмы групп Галуа $\varphi: G(L) \rightarrow G(K)$ и $\psi: G(M) \rightarrow G(K)$. Группы $G(K)$, $G(L)$ и $G(M)$ принадлежат классу $\mathfrak{G}$; по предложению 2 п. 2 существует $\mathfrak{G}$ -группа F и эпиморфизмы $\varphi_0: F \rightarrow G(L)$, $\psi_0: F \rightarrow G(M)$ такие, что $\varphi\varphi_0 = \psi\psi_0$; по предложению 3 этого же п. 2 можно считать, что F $\mathfrak{G}$ -универсальна, а следовательно (предложение 4 п. 2), и проективна. Используя теорему 1 п. 1, найдем $L_0 \geq L$ и $M_0 \geq M$ и изоморфизмы $\lambda: F \rightarrow G(L_0)$, $\mu: F \rightarrow G(M_0)$

такие, что композиции $\lambda\lambda, \mu\mu'$ ($\lambda: G(L_0) \rightarrow G(L)$, $\mu': G(M_0) \rightarrow G(M)$ — проекции ограничения) совпадают с φ_0 и ψ_0 соответственно. Рассмотрим поле K_1 — поле частных тензорного произведения $L_0 \otimes_K M_0$ и его расширение Галуа K_2 — поле частных тензорного произведения $L_0^s \otimes_{K_1} M_0^s$, где K_1^s, L_0^s, M_0^s — алгебраические замыкания полей K, L_0, M_0 соответственно. Группа Галуа $\text{Aut}_{K_1} K_2$ по лемме 4 п. 1 изоморфна группе $G(L_0) \times_{G(K)} G(M_0)$; выберем в этой группе подгруппу F' , соответствующую подгруппе $\{(h_0, h_1) | h_0 \in G(L_0), h_1 \in G(M_0), \text{ существует } f \in F \text{ такой, что } h_0 = \lambda f, h_1 = \mu f\}$ группы $G(L_0) \times_{G(K)} G(M_0)$. Эта

подгруппа естественно изоморфна группе F . Пусть $K_3 \equiv K_2^{F'}$; так как F' действует на L_0^s и M_0^s как $G(L_0)$ и $G(M_0)$ соответственно, то L_0 и M_0 алгебраически замкнуты в K_3 . Пусть K_3^s — алгебраическое замыкание поля K_3 , башня расширений $K_3 \leq \dots \leq K_2 \leq K_3^s$ определяет эпиморфизм $\pi: G(K_3) \rightarrow \text{Aut}_{K_3} K_3^s = F'$; так как F' проективна, то в $G(K_3)$ имеется подгруппа F'' , изоморфно проектируемая на F' . Пусть $K_4 \equiv K_3^{F''}$, тогда K_4 — также регулярное расширение L_0 и M_0 и $G(K_4) = F''$. По теореме 1 п. 1 для K_4 существует регулярное регулярно замкнутое расширение K_0 такое, что $G(K_0) \cong F''$ (заметьте, что $F'' \cong F' \cong F$ $\mathfrak{G}$ -универсальна и проективна). Итак, $K_0 \in \mathfrak{F}_0$, а L и M_0 , а следовательно, L и M имеют регулярные K -вложения в K_0 . $\square$

Теорема 1. Класс $\mathfrak{F}_0$ является модельным пополнением для класса $\mathfrak{F}_0$ (в сигнатуре σ_R).

Предложение 2 показывает, что достаточно установить модельную полноту (аксиоматизируемого) класса $\mathfrak{F}_0$. Для этого достаточно воспользоваться критерием модельной полноты Робинсона и следующим утверждением.

Лемма 1. Пусть $K \in \mathfrak{F}_0$, $L \in \mathfrak{F}_0$ и $K \leq L$, тогда $K \leq_1 L$; это означает, что для любой $\exists$ -формулы $\Phi(\bar{x})$ (сигнатуры σ_R) и любого набора элементов $\bar{a} \in K$ $L \models \forall(\bar{a})$ влечет $K \models \Phi(\bar{a})$.

Элементарные рассуждения показывают, что достаточно рассматривать случай, когда $\Phi(\bar{x})$ имеет вид $\exists y \Psi(\bar{x}, y)$, матрица (бескванторная) Ψ формулы Φ есть конъюнкция формул вида

$$t_i(\bar{x}, \bar{y}) = 0, i = 1, \dots, k, \neg W_{n_i}(q_i^1(\bar{x}, \bar{y}), \dots, q_i^{n_i}(\bar{x}, \bar{y})), i = 1, \dots,$$

s , где термы t_i, q_i^j — это многочлены из $\mathbb{Q}[\bar{x}, \bar{y}]$. Для этого достаточно элиминировать каждое позитивное вхождение предиката W_n , заменив его на определение; подформулы вида $t(\bar{x}, \bar{y}) \neq 0$ заменяются на $\exists v (vt - 1 = 0)$. Пусть $\bar{a} \in K$ — такой набор, что $L \models \Phi(\bar{a})$, тогда существует набор $\bar{b} \in L$

такой что $L \models \Psi(\bar{a}, \bar{b})$. Для истинности формулы $\Phi(\bar{a})$ в K нужно найти в K такие значения $\bar{y}$, которые являются корнями системы полиномов $t_i(\bar{a}, \bar{y}) = 0, i = 1, \dots, k$, а ни один из полиномов $p_j \equiv z^{n_j} + q_j^1(\bar{a}, \bar{y})z^{n_j-1} + \dots + q_j^{n_j}(\bar{a}, \bar{y}), j = 1, \dots, s$, не

имеет ни одного решения в K . Перемножая полиномы p_j , получим полином $q(\bar{y}, z) \in K[\bar{y}, z]$, унитарный в z , такой, что истинность $\Phi(\bar{a})$ в K равносильна существованию такого решения $\bar{\alpha}$ системы $t_i(\bar{a}, \bar{y}) = 0, i = 1, \dots, k$, что многочлен $q(\bar{\alpha}, z)$ не имеет ни одного корня в K . Рассмотрим регулярное расширение $L_0 \models K(\bar{b})$ поля K и его расширение Галуа L_1 , полученное присоединением к L_0 всех корней $\gamma_1, \dots, \gamma_t$ многочлена $q(\bar{b}, z)$. Пусть $L_2 \models L \cap L_1$, и пусть $G \models \text{Aut}_L L_1$; K_0 — алгебраическое замыкание K в L_1 ; $H \models \text{Aut}_K K_0$ и $\pi: G \rightarrow H$ — эпиморфизм ограничения. Так как $L \in \mathfrak{F}_0$ и $\text{Aut}_L L_1 \simeq G$, то $G \in \mathfrak{G}$; поле K принадлежит $\mathfrak{F}_0$, следовательно, группа $G(K)$ является $\mathfrak{G}$ -универсальной, и поэтому эпиморфизм $\pi_0: G(K) \rightarrow H$ может быть поднят до эпиморфизма $\pi_1: G(K) \rightarrow G$ такого, что $\pi \pi_1 = \pi_0$. Пусть $S \models \{\bar{b}, \gamma_1, \dots, \gamma_t\}$; воспользуемся предложением 4 п. 1 для нахождения K -гомоморфизма ψ кольца $K[S]$ в поле $L_* \models K^{s \text{ Ker } \pi_0}$ такого, что $\psi(S \cap L_2) \subseteq K$, $\psi(S - L_2) \subseteq L_* - K$. Тогда $\psi(\bar{b}) \in K$, $\psi(\gamma_i) \notin K$, так как $\gamma_i \in L, i = 1, \dots, t$. Так как ψ — K -гомоморфизм, то $\psi(\bar{b})$ дает решение системы уравнений $t_i(\bar{a}, \bar{y}) = 0, i = 1, \dots, k$, а $\psi(\gamma_1), \dots, \psi(\gamma_t)$ — это все корни многочлена $q(\psi(\bar{b}), z) = \psi(q(\bar{b}, z))$. Как было уже отмечено выше, все элементы $\psi(\gamma_1), \dots, \psi(\gamma_t)$ не лежат в K , следовательно, $q(\psi(\bar{b}), z)$ не имеет корней в K и $K \models \Psi(\bar{a}, \psi(\bar{b})), K \models \Phi(\bar{a})$. $\square$

Установим еще более сильное утверждение:

Теорема 1'. Класс $\mathfrak{F}_0^*$ является подмодельно полным.

Определение подмодельной полноты см. в книге Сакса [1].

Пусть $K_0, K_1 \in \mathfrak{F}_0^*$ и L — подмодель $K_i, i = 0, 1$; это означает, что L — поле сигнатуры σ_R , на котором предикаты W^n индуцированы этими предикатами в K_0 (или, что то же, в K_1), но, вообще говоря, L не есть σ_R -обогащение какого-нибудь поля. Пусть L_0 и L_1 — алгебраические замыкания поля L в K_0 и K_1 соответственно. Так как многочлен $f = x^k + a_1 x^{k-1} + \dots + a_k \in L[x]$ имеет корень в L_i тогда и только тогда, когда $L \models \models W^k(a_1, \dots, a_k)$, то по теореме 3 § 3 главы 6 книги Ершова [5] существует L -изоморфизм L_0 на L_1 , который, очевидно, будет σ_R -изоморфизмом. K_0 и K_1 являются регулярными расширениями L_0 и L_1 соответственно. По предложению 2 найдется поле $K \in \mathfrak{F}_0^*$, являющееся регулярным расширением K_0 и L -изоморфизм φ поля K_1 в K . Но из модельной полноты класса $\mathfrak{F}_0^*$ следует, что $K_0 \leq K, \varphi K_1 \leq K$; здесь $\leq$ обозначает элементарную вложимость. Отсюда следует элементарная эквивалентность

моделей $\langle K_0, a \rangle_{a \in L}$ и $\langle K_1, a \rangle_{a \in L}$, т. е. класс $\mathfrak{F}_0^*$ подмодельно полон. $\square$

Следствие 1. Теория $\text{Th}(\mathfrak{F}_0^*)$ допускает элиминацию кванторов.

См. книгу Сакса [1], § 13. $\square$

Следствие 2. Два поля $K_0, K_1 \in \mathfrak{F}_0^*$ элементарно эквивалентны тогда и только тогда, когда поля $\text{Abs } K_0$ и $\text{Abs } K_1$ изоморфны; здесь $\text{Abs } K_i$ — это алгебраическое замыкание поля рациональных чисел $\mathbb{Q}$ в $K_i, i = 0, 1$. $\square$

Теорема 2. Класс $\mathfrak{F}_0^*$ имеет разрешимую элементарную теорию тогда и только тогда, когда $\mathfrak{G}$ — рекурсивный класс групп.

Необходимость очевидна, так как $H \in \mathfrak{G} \Leftrightarrow \neg Q_H \notin \text{Th}(\mathfrak{F}_0^*)$

Установим достаточность. Пусть $\mathfrak{G}$ рекурсивен, тогда по предположению 1 теория $\text{Th}(\mathfrak{F}_0^*)$ рекурсивно аксиоматизируема. По следствию 1 теоремы 1' теория $\text{Th}(\mathfrak{F}_0^*)$ допускает элиминацию кванторов, поэтому для любого предложения Φ сигнатуры σ_R существует бескванторное предложение Φ^* , эквивалентное предложению Φ относительно $\text{Th}(\mathfrak{F}_0^*)$ (т. е. $\Phi \rightarrow \Phi^*, \Phi^* \rightarrow \Phi \in \text{Th}(\mathfrak{F}_0^*)$). Рекурсивная аксиоматизируемость теории $\text{Th}(\mathfrak{F}_0^*)$ показывает, что Φ^* может быть найдено по Φ эффективно. Для доказательства разрешимости $\text{Th}(\mathfrak{F}_0^*)$ достаточно теперь эффективно проверить выполнимость бескванторных предложений. Ясно, что достаточно ограничиться предложениями Φ^* вида

$$\bigwedge_{i=0}^k W^{n_i}(q_1^i, \dots, q_{n_i}^i) \wedge \bigwedge_{j=k+1}^s \neg W^{n_j}(q_1^j, \dots, q_{n_j}^j),$$

где $q_i^j \in \mathbb{Q}, i = 1, \dots, s, j = 1, \dots, n_i$.

Пусть $f_i(x) \equiv x^{n_i} + q_1^i x^{n_i-1} + \dots + q_{n_i}^i, i \leq s$. Построим эффективно поле разложения K всех многочленов $f_i, i \leq s$, над $\mathbb{Q}$. Пусть $G \models \text{Aut}_{\mathbb{Q}} K$; теперь проверяем, существует ли такая подгруппа $H \leq G$, что выполнены условия: 1) $H \in \mathfrak{G}$; 2) поле K^H содержит хотя бы один корень каждого из многочленов $f_i, i \leq k$; 3) K^H не содержит ни одного из корней многочлена

$$\prod_{i=k+1}^s f_i.$$

Если такой подгруппы H не существует, то Φ^* невыполнима, т. е. $\neg \Phi^* \in \text{Th}(\mathfrak{F}_0^*)$, если же такая H существует, то Φ^* выполнима. Действительно, в этом случае поле K^H можно вложить в такое алгебраическое расширение L поля $\mathbb{Q}$, что $G(L) \in \mathfrak{G}$ и $K \cap L = K^H$. Поле L имеет теперь регулярное расширение L_0 на $\mathfrak{F}_0^*$; тогда $L_0 \models \Phi^*$.

Остается заметить, что проверка существования группы H , удовлетворяющей перечисленным выше свойствам 1)–3), может быть осуществлена эффективно (см. § 1). $\square$

Как было отмечено в статье Ершова [6], класс всех регулярно замкнутых полей имеет неразрешимую теорию. Основной причиной неразрешимости является то, что группой Галуа регулярно замкнутого поля может быть любая проективная группа (см. теорему 1 п. 1). Однако если ограничиться достаточно хорошими группами — допустимыми, то, как будет видно из дальнейшего, ситуация остается хорошей.

Пусть R_0^* — класс всех регулярно замкнутых полей K (характеристики 0), у которых группа Галуа $G(K)$ допустима. Заметим, что из предложения 6 п. 2 следует равенство $R_0^* = \bigcup \{ \mathfrak{F}_0^* \mid \mathfrak{F}_0^* \text{ — допустимый класс конечных групп} \}$.

Теорема 3. Элементарная теория класса R_0^* разрешима.

Укажем сначала рекурсивную систему аксиом для теории $\text{Th}(R_0^*)$. Такой системой аксиом, как нетрудно проверить, будет $T_R^0 \cup T_R \cup \{ Q_H \rightarrow Q_F \mid \varphi: H \rightarrow F \text{ — эпиморфизм конечных групп} \}$. Отсюда следует, что теория $\text{Th}(R_0^*)$ рекурсивно перечислима. Остается установить, что множество $C(R_0^*)$ предложений, совместных с $\text{Th}(R_0^*)$, также рекурсивно перечислимо, так как для любого предложения Φ

$$\Phi \notin \text{Th}(R_0^*) \Leftrightarrow \neg \Phi \in C(R_0^*).$$

Для поля $K \in R_0^*$ через $D_s(K)$ обозначим множество $\{ W^n(q_1, \dots, q_n) \mid n > 1, q_1, \dots, q_n \in Q \leq K, K \models W^n(q_1, \dots, q_n) \} \cup \{ \neg W^n(q_1, \dots, q_n) \mid n > 1, q_1, \dots, q_n \in Q \leq K, K \models \neg W^n(q_1, \dots, q_n) \} \cup \{ Q_H \mid H \text{ — конечная группа, } K \models Q_H \} \cup \{ \neg Q_H \mid H \text{ — конечная группа, } K \models \neg Q_H \}$.

Лемма 2. Для любого поля $K \in R_0^*$ теория, определенная системой аксиом $\text{Th}(R_0^*) \cup D_s(K)$, является полной.

Пусть L — любое поле, удовлетворяющее системе аксиом $\text{Th}(R_0^*) \cup D_s(K)$; так как $L \models \text{Th}(R_0^*)$, то группа Галуа $G(L)$ поля L является допустимой; так как из $L \models D_s(K)$ следует, что $L \models Q_H \Leftrightarrow K \models Q_H$ для любой конечной группы H , то $H_f(G(L)) = H_f(G(K))$, т. е. $G(L)$ является $H_f(G(K))$ -универсальной группой и $K, L \in \mathfrak{F}_{H_f(G(K))}^*$. Далее $L \models W^n(q_1, \dots, q_n) \Leftrightarrow K \models W^n(q_1, \dots, q_n)$ для любых $n > 1, q_1, \dots, q_n \in Q$; отсюда по теореме 3 § 3 главы 6 книги Ершова [5] поля $\text{Abs } L$ — алгебраическое замыкание Q в L — и $\text{Abs } K$ — алгебраическое замыкание Q в K — изоморфны. Тогда по следствию 2 теоремы 1' поля L и K элементарно эквивалентны. Так как L было произвольным полем, удовлетворяющим системе аксиом $\text{Th}(R_0^*) \cup D_s(K)$, то это множество является системой аксиом полной теории (поля K). $\square$

Если предложение Φ совместно с теорией $\text{Th}(R_0^*)$, то существует поле $K \in R_0^*$ такое, что $K \models \Phi$. По лемме 2 и теореме полноты тогда имеем $\text{Th}(R_0^*) \cup D_s(K) \vdash \Phi$ и $\text{Th}(R_0^*) \cup D_0 \vdash \Phi$, где $D_0 \subseteq D_s(K)$ конечно. Таким образом, если $D_0, D_1, \dots$ — последовательность всех конечных множеств предложений вида $W^n(q_1, \dots, q_n), \neg W^n(q_1, \dots, q_n), Q_H, \neg Q_H$, совместных с $\text{Th}(R_0^*)$, то $C(R_0^*) = \{ \Phi \mid \text{существует } n \in \omega \text{ такое, что } \text{Th}(R_0^*) \cup D_n \vdash \Phi \}$. Если последовательность $D_0, D_1, \dots$ можно выбрать эффективно, то тогда ясно, что $C(R_0^*)$ рекурсивно перечислимо, а теория $\text{Th}(R_0^*)$ разрешима (рекурсивна). Для эффективного нахождения такой последовательности достаточно уметь для любого конечного множества D предложений указанного выше вида эффективно узнавать совместность системы аксиом $\text{Th}(R_0^*) \cup D$.

Укажем, как это можно сделать. Пусть $D = \{ W^{n_i}(q_1^i, \dots, q_{n_i}^i) \mid i = 0, \dots, k \} \cup \{ \neg W^{n_i}(q_1^i, \dots, q_{n_i}^i) \mid i = k+1, \dots, s \} \cup \{ Q_{H_i} \mid i = 0, \dots, t \} \cup \{ \neg Q_{H_i} \mid i = t+1, \dots, l \}$. Полагаем $f_i \doteq x^{n_i} + q_1^i x^{n_i-1} + \dots + q_{n_i}^i \in Q[x], i \leq s, p \doteq \prod_{i \leq s} f_i$. Пусть K — поле

разложения многочлена p над Q , тогда K — конечное расширение Галуа с группой Галуа $G \doteq \text{Aut}_Q K$. Пусть $G_1, \dots, G_m$ — все подгруппы группы G такие, что для $1 \leq j \leq m$ поле $K_j \doteq K^{G_j}$ содержит хотя бы один корень для каждого многочлена $f_i, i \leq k$, и не содержит ни одного корня многочлена $f_i, k < i \leq s$. Может оказаться, что таких подгрупп группа G не содержит ($m = 0$); в этом случае, очевидно, D не совместно с $\text{Th}(R_0^*)$. Если $m > 0$, то проверяем, существует ли такое $j, 1 \leq j \leq m$, что для любого $i, t < i \leq l$, группа H_i не принадлежит допустимому классу $\mathfrak{G}(H_0, \dots, H_t, G_j)$. В предыдущем пункте было установлено, что такую проверку можно проделать эффективно. Если такого индекса j не найдется, то D , очевидно, не совместно с $\text{Th}(R_0^*)$. Предположим, что $j, 1 \leq j \leq m$, таково, что $H_i \notin \mathfrak{G}(H_0, \dots, H_t, G_j)$ для всех $i, t < i \leq l$. Пусть $\varphi: G(K_j) \rightarrow G_j$ — эпиморфизм ограничения (заметим, что $G_j = \text{Aut}_{K_j} K$); пусть H — минимальная подгруппа группы $G(K_j)$, которая отображается на G_j (существование такой (замкнутой) подгруппы установлено, например, в работе Ершова [8]); тогда H — накрытие группы G_j и, следовательно, $H \in [\mathfrak{G}(H_0, \dots, H_t, G_j)]$. Пусть $L \doteq K_j^{H^H}$, тогда $G(L) = H$ и $K \cap L = K_j$; поле L принадлежит классу $\mathfrak{F}_0^*(H_0, \dots, H_t, G_j)$, следовательно, по предложению 2 L может быть вложено в поле $L_0 \in \mathfrak{F}_0^*(H_0, \dots, H_t, G_j) \subseteq R_0^*$. Но из того, что $K \cap L_0 = K \cap L = K_j$ и $H_0, \dots, H_t \in H_f(G(L_0)), H_{t+1}, \dots$

..., $H_1 \neq H_f(G(L_0))$, следует, что $L_0 = D$. Таким образом, можно эффективно проверить совместность любого конечного множества D предложений указанного выше вида с теорией $\text{Th}(R_0^*)$; отсюда, как было отмечено выше, уже и вытекает разрешимость этой теории. $\square$

Замечание. Теория $\text{Th}(R_0^*)$, как легко видеть, не допускает элиминации кванторов. Однако в следующем пункте будет рассмотрена другая сигнатура такая, что полученная теория $TS_G(R_0^*)$ этого класса полей R_0^* — теория стратов Галуа — допускает элиминацию кванторов, а $\text{Th}(R_0^*)$ эффективно сводится к $TS_G(R_0^*)$.

Укажем теперь еще один возможный подход к изучению элементарных теорий регулярно замкнутых полей, принадлежащий Уилеру [1]. Пусть K — произвольное поле (ограничимся случаем характеристики 0), σ_K — расширение сигнатуры σ , константами для элементов из K . Пусть F_K — класс всех K -полей, в которых K алгебраически замкнуто; этот класс аксиоматизируем в сигнатуре σ_K .

Следующая теорема (Уилер [1]) дает ответ на вопрос, для каких полей K (характеристики 0) класс F_K имеет модельный компаньон в сигнатуре σ_K .

Теорема 4. а) *Экзистенциально замкнутыми системами для F_K являются регулярно замкнутые поля из F_K , не имеющие собственных алгебраических расширений, в которых K алгебраически замкнуто.*

б) *Класс F_K имеет модельный компаньон тогда и только тогда, когда K имеет ограниченный коранг, т. е. для любого натурального $n > 1$ поля K имеет только конечное число расширений степени n .*

Утверждение а) достаточно просто следует из уже известных свойств регулярно замкнутых полей.

В утверждении б) установим только положительную часть: существование модельного компаньона, или, что то же, аксиоматизируемость класса полей из утверждения а) теоремы в случае, когда поле K имеет ограниченный коранг. Выберем для любого $n > 1$ конечное семейство S_n неприводимых унитарных многочленов над K таких, что если L — расширение степени n поля K , то существует $f \in S_n$ такой, что $L = K(\alpha)$, где α — корень f . Далее записываем для каждого $m > 1$ аксиому $\mathcal{A}_m$, утверждающую для произвольного K -поля L , что в любом расширении L_0 степени m поля L существует корень хотя бы

одного многочлена из множества $\bigcup_{n=2}^m S_n$. Тогда система аксиом $\{\mathcal{A}_m | m > 1\}$ выделяет среди K -полей те поля, которые не имеют собственных алгебраических расширений, в которых K алгеб-

раически замкнуто. Отсюда сразу следует аксиоматизируемость класса F_K всех экзистенциально замкнутых систем в F_K . $\square$

Замечание. Из предыдущих рассмотрений и утверждения а) теоремы легко вытекает, что в случае ограниченности коранга поля K теория $\text{Th}(F_K^*)$ класса F_K^* всех экзистенциально замкнутых систем из F_K является полной. В случае ненулевой характеристики, который также рассматривался в работе Уилера [1], это не так.

Укажем теперь соответствующий результат об элементарных теориях.

Теорема 5. *Если K — поле характеристики 0, ограниченного коранга, имеющее такую конструктивизацию v , что для конструктивного поля (K, v) разрешима проблема разложимости и существует сильно вычислимая последовательность S_n , $n > 1$, многочленов над K , удовлетворяющая сформулированным в доказательстве теоремы 4 свойствам, то элементарная теория $\text{Th}(F_K^*)$ разрешима.*

Действительно, из условий теоремы следует рекурсивная аксиоматизируемость теории $\text{Th}(F_K^*)$, а по замечанию эта теория полна; отсюда и следует разрешимость. $\square$

В заключение пункта вкратце (без полных деталей) рассмотрим случай ненулевой (фиксированной для дальнейшего) характеристики p . Начнем с напоминания некоторых алгебраических определений и фактов.

Пусть K — поле (характеристики $p \neq 0$); через K^p обозначается подполе всех p -х степеней элементов K ; семейство элементов $\alpha_1, \dots, \alpha_n$, $n \geq 1$, поля K назовем p -зависимым, если существует набор элементов $y_\sigma \in K$, $\sigma \in \{0, 1, \dots, p-1\}^n$, из которых не все равны нулю, такой, что $\sum_{\sigma} y_\sigma^\sigma \alpha_1^{(\sigma,1)}, \dots, \alpha_n^{(\sigma,n)} = 0$,

где для $\sigma \in \{0, 1, \dots, p-1\}^n$ (σ, i) — это i -я компонента вектора σ , т. е. $\sigma = \langle (\sigma, 1), \dots, (\sigma, n) \rangle$. Семейство $S \subseteq K$ называется p -зависимым, если существует конечное подсемейство $S_0 \subseteq S$, которое является p -зависимым. В противном случае семейство S называется p -независимым.

1. Семейство $\alpha_1, \dots, \alpha_n$ является p -независимым тогда и только тогда, когда $[K^p(\alpha_1, \dots, \alpha_n) : K^p] = p^n$. $\square$

Отношение p -независимости удовлетворяет свойствам аксиоматического понятия зависимости, предложенного в книге Зарисского и Самюэля [1]. А именно, если для любого $S \subseteq K$ положить $\varphi(S) = K^p(S)$, то выполнены следующие свойства:

2. Если $S_0 \subseteq S_1$, то $\varphi(S_0) \subseteq \varphi(S_1)$. $\square$

3. Если $\alpha \in K$, $S \subseteq K$ и $\alpha \in \varphi(S)$, то существует конечное подмножество $S_0 \subseteq S$ такое, что $\alpha \in \varphi(S_0)$. $\square$

4. $S \subseteq \varphi(S)$, $\varphi(\varphi(S)) = \varphi(S)$ для любого $S \subseteq K$. $\square$

5. (Свойство замены). Если $S \subseteq K$, $\alpha, \beta \in K$, то из $\beta \in \varphi(S \cup \{\alpha\})$ и $\beta \notin \varphi(S)$ следует, что $\alpha \in \varphi(S \cup \{\beta\})$. $\square$

Поэтому можно определить понятие p -базиса и доказать все естественные свойства, связанные с p -независимыми множествами, p -базисами и т. п. Так, p -базисом K назовем такое p -независимое множество $B \subseteq K$, что $K = K^p(B)$.

Для $S \subseteq K$ через $S^{p^{-n}}$ обозначим множество $\{\alpha^{p^{-n}} | \alpha \in S\}$, тогда $K(S^{p^{-n}})$ — расширение $K(\{\alpha^{p^{-n}} | \alpha \in S\})$ поля K , $n \in \omega$; через $K(S^{p^{-\omega}})$ обозначим расширение $\bigcup_{n \in \omega} K(S^{p^{-n}})$. Справедливы следующие факты:

6. Если $T \cup S$ — p -независимое семейство в K , то $T \cup S^{p^{-n}}$ — p -независимое семейство в $K(S^{p^{-n}})$, а T — p -независимое семейство в $K(S^{p^{-\omega}})$; если еще $T \cup S$ — p -базис, то $T \cup S^{p^{-n}}$ — p -базис в $K(S^{p^{-n}})$, а T — p -базис в $K(S^{p^{-\omega}})$. $\square$

Заметим, что если $S \cup \{\alpha, \beta\}$ — p -независимое семейство, то $S \cup \{\alpha, \alpha\beta\}$ и $S \cup \{\beta, \alpha\beta\}$ — также p -независимые семейства. Отсюда следует

7. Если $S \cup \{\alpha, \beta\}$ — p -независимое семейство в K , то $S \cup \{\alpha\}$ и $S \cup \{\beta\}$ — p -независимые семейства в $K((\alpha\beta)^{p^{-\omega}})$. $\square$

Обобщая этот факт, имеем:

8. Если $S \cup S_0 \cup S_1$ — p -независимое семейство, $\varphi: S_0 \rightarrow S_1$ — одно-однозначное отображение, $T = \{\alpha\varphi(\sigma) | \alpha \in S_0\}$, то $S \cup S_0$ и $S \cup S_1$ — p -независимые семейства в поле $K(T^{p^{-\omega}})$. $\square$

Укажем связь p -независимости с регулярностью расширений.

9. Пусть K алгебраически замкнуто в L , тогда следующие условия эквивалентны:

- 1) L — регулярное расширение K ;
- 2) любое p -независимое семейство S в K остается p -независимым в L ;
- 3) любое конечное p -независимое семейство S в K остается p -независимым в L ;
- 4) существует p -базис B поля K , который является p -независимым в L ;
- 5) существует p -базис B поля L такой, что $B \cap K$ — p -базис поля K ;
- 6) для любого p -базиса B_0 поля K существует p -базис B поля L такой, что $B \cap K = B_0$. $\square$

Последний факт подсказывает, как формульно расширить сигнатуру σ_K , чтобы для полей характеристики p вложимость обогащений означала в точности регулярность расширения. Для

каждого $n \geq 1$ определим n -местный предикат V^n $\exists$ -формулой, выражающей p -зависимость элементов, т. е. так, чтобы в любом естественно обогащенном поле K выполнялось следующее: для $\alpha_1, \dots, \alpha_n \in K$

$$K \models V^n(\alpha_1, \dots, \alpha_n) \Leftrightarrow \alpha_1, \dots, \alpha_n \text{ } p\text{-зависимы в } K.$$

Полагая $\sigma_R^p \Leftarrow \sigma_R \cup \{V^n | n \geq 1\}$ и рассматривая поля характеристики p как алгебраические системы сигнатуры σ_R^p , имеем:

$$K \leq L \Leftrightarrow L \text{ — регулярное расширение поля } K.$$

Полагаем для поля K $\tau(K) = \omega$, если в K существует бесконечное p -независимое подмножество, и $\tau(K) = n < \omega$, если K имеет p -базис из n элементов. Заметим, что $\tau(K) = 0$ означает, что K совершенно. Если $\tau(K) < \omega$, то $[K: K^p] = p^{\tau(K)}$. Для любого допустимого класса конечных групп $\mathfrak{G}$, любого $\alpha \leq \omega$ обозначим через $\mathfrak{F}_{\mathfrak{G}, \alpha}$ класс всех полей K характеристики p таких, что $G(K) \in [\mathfrak{G}]$ и $\tau(K) \leq \alpha$. Справедлив следующий аналог теоремы 1.

Теорема 6. Класс полей $\mathfrak{F}_{\mathfrak{G}, \alpha}$ (в сигнатуре σ_R^p) имеет модельное пополнение $\mathfrak{F}_{\mathfrak{G}, \alpha}^*$, состоящее в точности из регулярно замкнутых полей K таких, что $G(K) = \mathfrak{G}$ -универсальная группа и $\tau(K) = \alpha$.

Для доказательства теоремы нужны аналоги предложения 2 и леммы 1.

Аналог предложения 2 доказывается так же, как предложение 2; единственная дополнительная трудность возникает из-за того, что при $K, L, M \in \mathfrak{F}_{\mathfrak{G}, \alpha}$, $K \leq L$, $K \leq M$ для поля $L \otimes_K M$ может оказаться $\tau(L \otimes_K M) > \alpha$ (это возможно только в случае конечного α). Пользуясь фактом 8, для поля $L \otimes_K M$ можно найти чисто несепарабельное расширение L_0 такое, что $\tau(L_0) \leq \alpha$ и L_0 — регулярное расширение как L , так и M .

На аналоге леммы 1 остановимся более подробно.

Лемма 3. Пусть $K \in \mathfrak{F}_{\mathfrak{G}, \alpha}$, $L \in \mathfrak{F}_{\mathfrak{G}, \alpha}$ и $K \leq L$, тогда $K \leq_1 L$.

Используя то, что предикаты V^n определяются $\exists$ -формулами, легко заметить, как в доказательстве леммы 1, что для доказательства леммы достаточно установить следующее утверждение:

Пусть $p_1, \dots, p_k \in K[y_1, \dots, y_n] = K[\bar{y}]$, $q \in K[\bar{y}, z]$ — унитарный многочлен относительно z , $I_0, \dots, I_s \subseteq \{1, \dots, n\}$ таковы, что существуют $\alpha_1, \dots, \alpha_n \in L$ такие, что $p_i(\bar{\alpha}) = 0$, $i = 1, \dots, k$; многочлен $q(\bar{\alpha}, z)$ не имеет ни одного корня в L , и для любого j , $j \leq s$, семейство $\{\alpha_i | i \in I_j\}$ p -независимо; тогда в K существуют такие элементы $\beta_1, \dots, \beta_n$, что $p_i(\bar{\beta}) = 0$, $i = 1, \dots, k$; многочлен $q(\bar{\beta}, z)$ не имеет ни одного корня в K , семейства $\{\beta_i | i \in I_j\}$ p -независимы для любого $j \leq s$.

Докажем это утверждение сначала для случая, когда L является относительно совершенным расширением K , т. е. если p -базис поля K является и p -базисом поля L . Зафиксируем некоторый p -базис B поля K , который по предположению будет p -базисом и поля L . Тогда по «свойству замены» для любого $j \leq s$ существует семейство $B_j = \{\gamma_{j,1}, \dots, \gamma_{j,n_j}\} \subseteq B$, где $n_j \equiv |I_j|$, такое, что $B' \equiv (B - B_j) \cup \{\alpha_i | i \in I_j\}$ есть p -базис поля L . Любой элемент из B_j p -зависит от B' ; для каждого элемента $\gamma_{j,t} \in B_j$ зафиксируем некоторую p -зависимость элемента $\gamma_{j,t}$ от B' , т. е. выражение

$$\pi_{j,t} \equiv \sum_{\sigma \in S_{j,t}} y(j, t, \sigma)^p q_\sigma = 0,$$

где $S_{j,t}$ конечно, $q_\sigma, \sigma \in S_{j,t}$, — различные одночлены от $B' \cup \{\gamma_{j,t}\}$ и $y(j, t, \sigma) \neq 0$ для всех $\sigma \in S_{j,t}$, $t = 1, \dots, n_j$. Полагаем $S \equiv \{\alpha_1, \dots, \alpha_n\} \cup \{\delta | \delta \text{ — корень многочлена } q(\bar{\alpha}, z) \text{ в поле } L_1 \text{ — поле разложения многочлена } q(\bar{\alpha}, z) \text{ над полем } L_0 \equiv K(\bar{\alpha}, y(j, t, \sigma)) \cup \{y(j, t, \sigma), y(j, t, \sigma)^{-1} | j \leq s, \sigma \in S_{j,t}, t = 1, \dots, n_j\}$. Далее, поступая, как в доказательстве леммы 1, находим K -гомоморфизм φ кольца $K[S]$ в некоторое конечное расширение Галуа K_1 поля K такое, что $\varphi(S \cap L_0) \subseteq K$, $\varphi(S - L_0) \subseteq K_1 - K$. Тогда элементы $\beta_i \equiv \varphi(\alpha_i)$, $i = 1, \dots, n$, удовлетворяют заключению утверждения. То, что $p_i(\beta) = 0$, $i = 1, \dots, k$, и что $q(\beta, z)$ не имеет корней в K , очевидно. Заметим только, что для любого $j \leq s$ семейство $\{\beta_i | i \in I_j\}$ p -независимо. Действительно, рассмотрим соотношение

$$0 = \varphi(\pi_{j,t}) = \sum_{\sigma \in S_{j,t}} \varphi(y(j, t, \sigma))^p \varphi(q_\sigma);$$

по выбору S имеем, что $\varphi(y(j, t, \sigma)) \neq 0$, следовательно, эти выражения дают p -зависимость элементов из B_j от семейства $(B - B_j) \cup \{\beta_i | i \in I_j\}$, но так как $|B_j| = |I_j|$, то отсюда следует, что $(B - B_j) \cup \{\beta_i | i \in I_j\}$ является p -базисом K , а следовательно, семейство $\{\beta_i | i \in I_j\}$ p -независимо.

Избавимся теперь от ограничения относительной совершенности L над K . Пусть L не является относительно совершенным над K ; заметим, что это возможно только в случае $\alpha = \omega$. Пусть B — p -базис поля K , $S_0 \subseteq L$ таково, что $B \cup S_0$ — p -базис поля L . Так как $\tau(K) = \omega$, то существуют элементарное расширение K' поля K и множество $S_1 \subseteq K'$ такое, что $B \cup S_1$ — p -базис поля K' и $|S_0| \leq |S_1|$. Зафиксируем одно-однозначное отображение $\varphi: S_0 \rightarrow S_1$ и рассмотрим в поле $L' \equiv K' \otimes_K L$ множество $T \equiv \{\alpha\varphi(\alpha) | \alpha \in S_0\}$; пусть $L'' \equiv L' (T^{p^{-\omega}})$, тогда по факту 8 L'' будет регулярным расширением поля K' и поля L . Используя то, что $K', L \in \mathfrak{F}_{\omega, \omega}$, вложим L'' в его сепарабельное алгебраическое расширение L''' такое, что $L''' \in \mathfrak{F}_{\omega, \omega}$, а K' и L алгебраически замкнуты в L''' . Итак, имеем $K \leq K' \leq L'''$, $L \leq L'''$, $L \cap K' = K$ и (по построению L''') L''' — относительно совершенное расширение K' . Используя $\bar{\alpha} \in L^n$ и уже рассмотренный случай, находим в K' набор элементов $\bar{\beta}$, удовлетворяющий в K' сформулированным условиям. Но так как K' — элементарное расширение K , то и в K найдутся элементы $\bar{\beta}'$, удовлетворяющие этим условиям. □

Используя лемму 3 и аналог предложения 2, уже нетрудно установить и теорему 6. □

Теорема 7. 1) Классы полей $\mathfrak{F}_{\omega, \alpha}$ с рекурсивным $\mathfrak{G}$ и любым $\alpha \leq \omega$ имеют разрешимую теорию.

2) Класс R_p^* всех регулярно замкнутых полей характеристики p , имеющих допустимую группу Галуа, имеет разрешимую теорию.

Доказывается так же, как теоремы 2 и 3. □

4. Теория стратов Галуа. Как отмечалось в предыдущем пункте, теория класса полей R_0^* в сигнатуре σ_R не допускает элиминации кванторов. В работе Фрида и Сакердота [1] при изучении элементарной теории класса всех конечных полей был предложен новый язык, в котором рассматриваемая теория допускает элиминацию кванторов; в дальнейшей работе Фрида [1] этот подход был расширен на большее число классов полей. В настоящем пункте предлагается модифицированное изложение этого подхода и указывается процедура элиминации кванторов для класса полей R_0^* в этом новом языке.

В основе этого подхода лежит понятие страта Галуа, с определения которого и начнем изложение. Зафиксируем для дальнейшего некоторое поле K характеристики 0 и его универсальную область $U(K)$, т. е. алгебраически замкнутое расширение K , имеющее бесконечную степень трансцендентности над K . Для $\bar{\xi} = \xi_1, \dots, \xi_n \in U(K)$ через $K[\bar{\xi}]$ обозначается кольцо, порожденное над K элементами $\xi_1, \dots, \xi_n$, а через $K(\bar{\xi})$ — поле частных этого кольца. Элемент $\eta \in K[\bar{\xi}]$ назовем *сглаживающим* для этого кольца, если $\eta \neq 0$, а кольцо $K[\bar{\xi}, \eta^{-1}]$ является целозамкнутым.

Предложение 1. Для любого $\bar{\xi} \in U(K)^n$ существует сглаживающий элемент для кольца $K[\bar{\xi}]$.

Используя нормализационную лемму (Зарисский и Самюэль [1], с. 305, теорема 8), найдем такие k линейных комбинаций $\eta_1, \dots, \eta_k$ элементов $\xi_1, \dots, \xi_n$, что кольцо $K[\bar{\xi}]$ цело над $K[\eta_1, \dots, \eta_k]$ и k — степень трансцендентности $K(\bar{\xi})$ над K . Далее в поле $K(\bar{\xi})$ выбираем элемент ζ такой, что $K(\bar{\xi}) =$

$= K(\eta_1, \dots, \eta_k, \xi)$. Умножая ξ на подходящий элемент из $K[\eta_1, \dots, \eta_k]$, можно считать, что ξ цел над кольцом $K[\eta_1, \dots, \eta_k]$. Пусть $p \in K(\eta_1, \dots, \eta_k)[x]$ — минимальный (унитарный) многочлен для ξ над $K(\eta_1, \dots, \eta_k)$; так как ξ цел над кольцом $K[\eta_1, \dots, \eta_k]$ и это кольцо целозамкнуто ($K[\eta_1, \dots, \eta_k]$ изоморфно кольцу многочленов над K от k переменных, так как $\eta_1, \dots, \eta_k$ алгебраически независимы над K), то $p \in K[\eta_1, \dots, \eta_k, x]$. Пусть $\eta_0 \neq d(p) (= \pm R(p, p'), R(f, g)$ — результат многочленов f и g) — дискриминант многочлена p , тогда $\eta_0 \neq 0$, так как ξ сепарабелен над $K(\eta_1, \dots, \eta_k)$ и $\eta_0 \in K[\eta_1, \dots, \eta_k]$. Из доказательства теоремы 7 на с. 303 в книге Зарисского и Самюэля [1] видно, что кольцо $K[\eta_1, \dots, \eta_k, \eta_0^{-1}]$ целозамкнуто; так как $K[\xi]$ цело над $K[\eta_1, \dots, \eta_k]$, то $K[\xi] \subseteq K[\eta_1, \dots, \eta_k, \eta_0^{-1}]$ и $K[\eta_1, \dots, \eta_k, \eta_0^{-1}] = K[\xi, \eta_0^{-1}]$. Следовательно, η_0 — сглаживающий элемент для кольца $K[\xi]$. $\square$

Замечание. Если η — сглаживающий элемент для $K[\xi]$, $\delta \in K[\xi]$ и $\delta \neq 0$, то $\eta\delta$ — также сглаживающий элемент для $K[\xi]$.

Стратом (или *n-стратом*, $n \in \omega$) Галуа над полем K назовем всякую систему

$$\mathcal{S} = \langle \xi_1, \dots, \xi_n; \eta; \alpha; H \rangle$$

такую, что выполнены следующие четыре условия:

- 1) $\xi_1, \dots, \xi_n, \eta, \alpha \in U(K)$;
- 2) η — сглаживающий элемент для $K[\xi]$;
- 3) $K(\xi, \alpha)$ — расширение Галуа поля $K(\xi)$ и H — подгруппа группы Галуа $\text{Aut}_{K(\xi)} K(\xi, \alpha)$ этого расширения;

- 4) элемент α цел над $K[\xi, \eta^{-1}]$, а его дискриминант над $K(\xi)$ обратим в кольце $K[\xi, \eta^{-1}]$.

Замечание. Из условий 1) и 4) вытекает, что кольцо $K[\xi, \eta^{-1}, \alpha]$ также является целозамкнутым.

Если $\mathcal{S}$ — страт Галуа, то через $K(\mathcal{S})$ будем обозначать поле $K(\xi)$, а через $\dim \mathcal{S}$ — степень трансцендентности поля $K(\mathcal{S})$ над K .

Замечание. Если $n = 0$, то сглаживающий элемент η для K — это произвольный ненулевой элемент из K , не играющий никакой роли; поэтому можно определить 0-страт Галуа как пару $\langle \alpha; H \rangle$, где $\alpha \in U(K)$, $K(\alpha)$ — расширение Галуа поля K и $H \leq \text{Aut}_K K(\alpha)$.

Для того чтобы иметь определенные интуитивные основания для использования стратов Галуа, укажем, какие условия мож-

но накладывать на точки произвольного K -поля, используя n -страт $\mathcal{S}$.

Пусть $\mathcal{S} = \langle \xi; \eta; \alpha; H \rangle$ — n -страт Галуа, L — произвольное K -поле. Предположим, что задан K -гомоморфизм $\varphi: K[\xi, \eta^{-1}] \rightarrow L$; свяжем с этим гомоморфизмом некоторую подгруппу G_φ группы Галуа $G \cong \text{Aut}_{K(\xi)} K(\xi, \alpha)$, которая определена однозначно с точностью до сопряженности в группе G . Эту группу G_φ (точнее — класс сопряженных подгрупп) назовем L -группой разложения гомоморфизма φ . Пусть p_α — минимальный многочлен для α над $K(\xi)$; из условий, наложенных в определении страта, следует, что $p_\alpha \in K[\xi, \eta^{-1}, x]$; пусть $q_\alpha \neq \varphi p_\alpha$, $q_\alpha \in L[x]$; заметим, что из обратимости дискриминанта элемента α (многочлена p_α) в $K[\xi, \eta^{-1}]$ следует, что дискриминант многочлена q_α отличен от нуля. Пусть α' — произвольный корень многочлена q_α в алгебраическом замыкании L^* поля L ; гомоморфизм φ однозначно продолжается до гомоморфизма $\varphi_\alpha: K[\xi, \eta^{-1}, \alpha] \rightarrow L(\alpha')$ с условием $\varphi_\alpha(\alpha) = \alpha'$. Пусть $\mathfrak{P}_\alpha \neq \text{Ker } \varphi_\alpha$, $R_\alpha \neq \varphi_\alpha^{-1}(L)$; $K[\xi, \eta^{-1}] \leq R_\alpha \leq K[\xi, \eta^{-1}, \alpha]$; полагаем $G_\alpha \neq \{\sigma \mid \sigma \in G, \mathfrak{P}_\alpha^\sigma = \mathfrak{P}_\alpha, \forall \rho \in R_\alpha (\rho - \rho^\sigma \in \mathfrak{P}_\alpha)\}$. Эту группу и назовем L -группой разложения гомоморфизма φ_α . Нетрудно проверить, что G_α естественно изоморфна группе Галуа $\text{Aut}_L L(\alpha')$. Если $\tau \in G$ и $\alpha'' \neq \varphi_\alpha(\alpha^{\tau^{-1}})$, то α'' — также корень многочлена q_α (когда σ пробегает G , тогда $\varphi_\alpha(\alpha^\sigma)$ пробегает все (различные) корни многочлена q_α : если $p_\alpha = (x - \alpha) \cdot \dots \cdot (x - \alpha^\sigma)$, то $q_\alpha = \varphi p_\alpha = \varphi_\alpha p_\alpha = (x - \alpha') \cdot \dots \cdot (x - \varphi_\alpha(\alpha^\sigma))$). Техническая проверка показывает, что $G_\alpha = G_\alpha^\tau$; таким образом, когда α' пробегает все корни многочлена q_α , тогда G_α пробегает класс сопряженных подгрупп $\{G_\alpha, \dots\}$. Любую группу из этого класса назовем L -группой разложения гомоморфизма φ .

Проведенные выше рассуждения оправдывают в какой-то мере введение следующих n -местных предикатов $P_\mathcal{S}$ на любом K -поле L для любого n -страта Галуа $\mathcal{S} = \langle \xi; \eta; \alpha; H \rangle$.

Пусть L — K -поле, $\xi'_1, \dots, \xi'_n \in L$, тогда полагаем $L \models \models P_\mathcal{S}(\xi')$, только если выполнено следующее условие: ξ' является специализацией ξ , гомоморфизм специализации $\psi: K[\xi] \rightarrow K[\xi'] \leq L$ таков, что $\psi(\eta) \neq 0$, H является L -группой разложения гомоморфизма $\varphi: K[\xi, \eta^{-1}] \rightarrow L$, определенного однозначно по ψ .

Если $\mathfrak{K}$ — некоторый класс K -полей, то через $TS_K(\mathfrak{K})$ обозначим элементарную теорию класса $\mathfrak{K}$ в сигнатуре $\sigma_\mathcal{S}$.

$\Rightarrow \langle P_{\mathcal{G}} | \mathcal{G} \rangle$ — страт Галуа над K (без равенства); назовем ее теорией стратов Галуа класса $\mathfrak{R}$.

Заметим, что элементарная теория $\text{Th}(\mathfrak{R})$ легко сводится к $\text{TS}_K(\mathfrak{R})$. А именно, пусть $u, v, w \in U(K)$ — алгебраически независимые элементы над K , полагаем

$$\mathcal{G}_0 \Rightarrow \langle u, u; 1; 1; e \rangle (e — единичная группа);$$

$$\mathcal{G}_1 \Rightarrow \langle u, v, u+v; 1; 1; e \rangle;$$

$$\mathcal{G}_2 \Rightarrow \langle u, v, uv; 1; 1; e \rangle.$$

Тогда легко понять, что для любого K -поля L предикаты $P_{\mathcal{G}_0}(x, y)$, $P_{\mathcal{G}_1}(x, y, z)$, $P_{\mathcal{G}_2}(x, y, z)$ в точности совпадают с предикатом равенства ($x = y$), предикатом ($x + y = z$) и предикатом ($xy = z$) соответственно.

Полагаем далее

$$\mathcal{G}'_0 \Rightarrow \langle u, v, u-v; 1; e \rangle;$$

$$\mathcal{G}'_1 \Rightarrow \langle u, v, w; w-(u+v); 1; e \rangle;$$

$$\mathcal{G}'_2 \Rightarrow \langle u, v, w; w-uv; 1; e \rangle.$$

Тогда предикаты $P_{\mathcal{G}'_0}(x, y)$, $P_{\mathcal{G}'_1}(x, y, z)$, $P_{\mathcal{G}'_2}(x, y, z)$ совпадают соответственно с предикатами ($x \neq y$), ($x + y \neq z$), ($xy \neq z$).

Отсюда уже очевидно, как переделать любую формулу $\Phi(\bar{x})$ языка L_{σ_K} в формулу $\Phi^*(\bar{x})$ языка L_{σ_G} так, что для любого K -поля L и любых $\bar{\xi} \in L^n$

$$L \models \Phi(\bar{\xi}) \Leftrightarrow L \models \Phi^*(\bar{\xi}).$$

Замечание. Нетрудно видеть, что справедливо и обратное: теория стратов Галуа сводится к элементарной теории соответствующего класса полей, точнее: для любого n -страта Галуа $\mathcal{G}$ существует формула $\mathfrak{A}(\mathcal{G})$ сигнатуры σ_K с n свободными переменными такая, что для любого K -поля L и любых $\bar{\eta} \in L^n$ $L \models P_{\mathcal{G}}(\bar{\eta}) \Leftrightarrow L \models \mathfrak{A}(\mathcal{G})(\bar{\eta})$. Однако эффективно по $\mathcal{G}$ найти такую формулу можно, только если сделать некоторые предположения о поле K . Например, для построения формулы $\mathfrak{A}(\mathcal{G})$ нужно найти базис идеала $I(\bar{\xi})$ и т. п.

Ближайшая задача состоит в том, чтобы показать, что отрицание предиката вида $P_{\mathcal{G}}$ и конъюнкция предикатов $P_{\mathcal{G}_0}$ и $P_{\mathcal{G}_1}$ могут быть (эквивалентно) представлены в виде дизъюнкции подходящих предикатов вида $P_{\mathcal{G}}$.

Начнем с одной общей конструкции — стратификации $\text{St}(\mathcal{G}, I)$ n -страта $\mathcal{G}$ относительно идеала $I \leq K[x_1, \dots, x_n]$. Сразу нужно сделать замечание, что $\text{St}(\mathcal{G}, I)$ — это некоторое

(быть может, пустое) множество n -стратов Галуа, которое, вообще говоря, определено не однозначно по $\mathcal{G}$ и I .

Пусть $I \leq K[x_1, \dots, x_n]$ — идеал в кольце многочленов от n переменных над K ; набор $\bar{\eta} \in U(K)^n$ называется *корнем идеала I* , если $g(\bar{\eta}) = 0$ для любого $g \in I$. Система $\bar{\eta}^1, \dots, \bar{\eta}^s \in U(K)^n$ называется *полным набором корней идеала I* , если все $\bar{\eta}^i$, $i = 1, \dots, s$, являются корнями идеала I и для любого корня $\bar{\eta}$ идеала I существует такое j , $1 \leq j \leq s$, что $\bar{\eta}$ есть специализация $\bar{\eta}^j$. Заметим, что любой идеал $I \neq K[\bar{x}]$ имеет конечный полный набор корней. Это соответствует представлению алгебраического множества $V_K(I) \Rightarrow \{\bar{\eta}^i | \bar{\eta}^i \in U(K)^n, \bar{\eta}^i \text{ — корень идеала } I\}$ в виде объединения $\bigcup_{i=1}^s V_K(\bar{\eta}^i)$ K -многообразий, т. е. неприводимых над K алгебраических множеств.

Итак, пусть $\mathcal{G} = \langle \bar{\xi}; \eta; \alpha; H \rangle$ — n -страт Галуа, I — идеал кольца $K[\bar{x}] = K[x_1, \dots, x_n]$. Полагаем $I_1 \Rightarrow (I(\bar{\xi}) \cup I)$ — идеал, порожденный объединением идеалов $I(\bar{\xi})$ и I ; пусть $\bar{\xi}^1, \dots, \bar{\xi}^s$ — полный набор корней идеала I_1 . Если $I_1 = K[\bar{x}]$, то $s = 0$ и $\text{St}(\mathcal{G}, I) \Rightarrow \emptyset$. Так как $I(\bar{\xi}) \leq I_1$, то все $\bar{\xi}^j$ являются специализациями точки $\bar{\xi}$; пусть $\varphi_j: K[\bar{\xi}] \rightarrow K[\bar{\xi}^j]$ — соответствующий гомоморфизм, $j = 1, \dots, s$. Выбираем теперь те индексы j , для которых $\eta_j \Rightarrow \varphi_j(\eta) \neq 0$. Предположим, что $t \leq s$ таково, что $\eta_j \neq 0 \Leftrightarrow 1 \leq j \leq t$. Для любого j , $1 \leq j \leq t$, пусть $\alpha_{j1}, \dots, \alpha_{js_j}$ — это все корни многочлена $\varphi_j(p_\alpha) \in K[\bar{\xi}^j][x]$ (p_α — минимальный многочлен для α над $K(\bar{\xi})$; $p_\alpha \in K[\bar{\xi}, \eta^{-1}, x]$, φ_j естественно продолжен на $K[\bar{\xi}, \eta^{-1}]$) такие, что $K(\bar{\xi}^j)$ -группы разложения гомоморфизмов $\psi_j^i: K[\bar{\xi}, \eta^{-1}, \alpha] \rightarrow K(\bar{\xi}^j, \alpha_{ji})$, $\psi_j^i \supseteq \varphi_j$, $\psi_j^i(\alpha) = \alpha_{ji}$, $i = 1, \dots, s_j$, содержат группу H . Группу H отождествим с подгруппой группы Галуа $\text{Aut}_{K(\bar{\xi}^j)} K(\bar{\xi}^j, \alpha_{ji})$, естественно изоморфной $K(\bar{\xi}^j)$ -группе разложения гомоморфизма ψ_j^i . Выбираем далее такой многочлен $g_j \in K[\bar{x}]$, что $\delta_j \Rightarrow g_j(\bar{\xi}^j) \neq 0$ и $\eta^j \Rightarrow \eta_j \delta_j$ — сглаживающий элемент для кольца $K[\bar{\xi}^j]$. Полагаем

$$\begin{aligned} \text{St}^t(\mathcal{G}, I) \Rightarrow \{ \langle \bar{\xi}^j; \eta^j; \alpha_{ji}; H \rangle | i = 1, \dots, s_j \} \\ \cup \text{St}(\mathcal{G}, (I \cup \{g_j\})), \quad j = 1, \dots, t; \\ \text{St}(\mathcal{G}, I) \Rightarrow \bigcup_{j=1}^t \text{St}^t(\mathcal{G}, I). \end{aligned}$$

Заметим, что для любого j , $1 \leq j \leq t$, идеал $I_1 = (I(\bar{\xi}) \cup I)$ собственно содержится в идеале $(I(\bar{\xi}) \cup I \cup \{g_j\})$.

Нётеровость кольца $K[\bar{x}]$ гарантирует корректность этого определения. Заметим еще, что если $I \not\subseteq I(\bar{\xi})$, то для любого $\mathcal{G}' \in \text{St}(\mathcal{G}, I)$ имеем $\dim \mathcal{G}' < \dim \mathcal{G}$.

Основное свойство этой конструкции выражает следующее

Предложение 2. Для любого K -поля L и любого $\bar{\xi}' \in L^*$ имеет место эквивалентность

$$L \models \bigvee_{\mathcal{G}' \in \text{St}(\mathcal{G}, I)} P_{\mathcal{G}'}(\bar{\xi}') \Leftrightarrow L \models P_{\mathcal{G}}(\bar{\xi}') \text{ и } \bar{\xi}' - \text{корень} \\ \text{идеала } I \text{ (т. е. } \bar{\xi}' \in V_k(I)).$$

Замечание. Если $\text{St}(\mathcal{G}, I) = \emptyset$, то $\bigvee_{\mathcal{G}' \in \text{St}(\mathcal{G}, I)} P_{\mathcal{G}'}(\bar{\xi}')$ означает тождественно ложную формулу 0.

Итак, пусть $\mathcal{G}' \in \text{St}(\mathcal{G}, I)$ и $L \models P_{\mathcal{G}'}(\bar{\xi}')$; предположим сначала, что $\mathcal{G}'$ имеет вид $\langle \bar{\xi}'; \eta'; \alpha_{\mu}; H \rangle$, $1 \leq j \leq t$, $1 \leq i \leq s_j$. Тогда $\bar{\xi}'$ является K -специализацией точки $\bar{\xi}'$, следовательно, $\bar{\xi}' \in V_k(I)$. Если φ — гомоморфизм специализации из $K[\bar{\xi}']$ в L ($\varphi(\bar{\xi}'_i) = \bar{\xi}'_i$, $i = 1, \dots, n$), то $\eta' \neq \varphi(\eta') \neq 0$ и существует элемент $\alpha' \in L^*$ такой, что φ продолжается до гомоморфизма $\psi: K[\bar{\xi}', \eta'^{-1}, \alpha_{\mu}] \rightarrow L(\alpha')$, $\psi(\alpha_{\mu}) = \alpha'$, такого, что H — L -группа разложения этого гомоморфизма. Пусть $\psi'_j: K[\bar{\xi}, \eta^{-1}, \alpha] \rightarrow K(\bar{\xi}', \alpha_{\mu})$ — гомоморфизм, определенный при построении множества $\text{St}'(\mathcal{G}, I)$, тогда если $\bar{\psi} \Rightarrow \psi\psi'_j: K[\bar{\xi}, \eta^{-1}, \alpha] \rightarrow L(\alpha')$, то легко видеть, что L -группой разложения гомоморфизма $\bar{\psi}$ будет H , следовательно, $L \models P_{\mathcal{G}}(\bar{\xi}')$. Если же $\mathcal{G}' \in \text{St}(\mathcal{G}, (I \cup \{g_j\}))$, то нужно воспользоваться подходящим индуктивным предположением, чтобы получить $L \models P_{\mathcal{G}'}(\bar{\xi}') \Rightarrow L \models P_{\mathcal{G}}(\bar{\xi}')$ и $\bar{\xi}' \in V_k(I \cup \{g_j\}) \Rightarrow L \models P_{\mathcal{G}}(\bar{\xi}')$ и $\bar{\xi}' \in V_k(I)$. Таким образом, импликация $\Rightarrow$ установлена.

Пусть $\bar{\xi}' \in L^n$, $L \models P_{\mathcal{G}}(\bar{\xi}')$ и $\bar{\xi} \in V_k(I)$. Тогда из $P_{\mathcal{G}}(\bar{\xi}')$ следует, что $\bar{\xi}' \in V_k(\bar{\xi})$, $\bar{\xi}' \in V_k(\bar{\xi}) \cap V_k(I) = V_k(I(\bar{\xi}) \cup I)$. Следовательно, для некоторого j , $1 \leq j \leq s$, $\bar{\xi}'$ является специализацией точки $\bar{\xi}'$. Гомоморфизм специализации $\varphi: K[\bar{\xi}] \rightarrow K[\bar{\xi}']$ может быть пропущен через гомоморфизм $\varphi_j: K[\bar{\xi}] \rightarrow K[\bar{\xi}']$ ($\varphi = \varphi'_j \varphi_j$, где $\varphi'_j: K[\bar{\xi}'] \rightarrow K[\bar{\xi}']$ — также гомоморфизм специализации). Так как $\eta' \neq \varphi(\eta) \neq 0$, то и $\eta_j \neq \varphi_j(\eta) \neq 0$, следовательно, $j \leq t$.

Пусть элемент $\alpha' \in L^*$ таков, что продолжение $\psi: K[\bar{\xi}, \eta^{-1}, \alpha] \rightarrow L(\alpha')$ гомоморфизма φ , удовлетворяющее условию $\psi(\alpha) = \alpha'$, имеет L -группой разложения группу H . Тогда существует i ,

$1 \leq i \leq s_j$, такое, что ψ можно представить в виде композиции гомоморфизмов

$$\psi_i: K[\bar{\xi}, \eta^{-1}, \alpha] \rightarrow K[\bar{\xi}', \eta_j^{-1}, \alpha_{\mu}], \psi_{\mu}(\alpha) = \alpha_{\mu}$$

и

$$\psi'' : K[\bar{\xi}', \eta_j^{-1}, \alpha_{\mu}] \rightarrow L(\alpha'), \psi''(\alpha_{\mu}) = \alpha'.$$

Но тогда L -группой разложения гомоморфизма ψ'' будет H . Если $\varphi'(\eta') \neq 0$, то отсюда следует, что $L \models P_{\langle \bar{\xi}'; \eta'; \alpha_{\mu}; H \rangle}(\bar{\xi}')$.

Если же $\varphi'(\eta') = \varphi'(\eta_j) \varphi'(\delta_j) = 0$, то $\varphi'(\delta_j) = 0$ и $g_j(\bar{\xi}') = 0$, а поэтому $\bar{\xi}' \in V_k(I \cup \{g_j\})$. Используя подходящее индукционное предположение, получаем в этом случае $L \models P_{\mathcal{G}'}(\bar{\xi}')$ для некоторого $\mathcal{G}' \in \text{St}(\mathcal{G}, (I \cup \{g_j\}))$. Таким образом, установлена и обратная импликация. $\square$

Для n -страта Галуа $\mathcal{G} = \langle \bar{\xi}; \eta; \alpha; H \rangle$ определим конечное (быть может, пустое) множество n -стратов $N(\mathcal{G})$ следующим образом: пусть $p_1, \dots, p_s, g \in K[\bar{x}] - \{0\}$ таковы, что $p_1, \dots, p_s$ — базис идеала $I(\bar{\xi})$ (если $I(\bar{\xi}) = \{0\}$, то $s = 0$) и $\eta = g(\bar{\xi})$; пусть $\bar{\xi}_1^*, \dots, \bar{\xi}_n^* \in U(K)$ алгебраически независимы над K , тогда полагаем

$$N_0(\mathcal{G}) \Rightarrow \{ \langle \bar{\xi}^*; p_i(\bar{\xi}^*); 1; e \rangle \mid i = 1, \dots, s \};$$

$$N_1(\mathcal{G}) \Rightarrow \text{St}(\langle \bar{\xi}^*; 1; 1; e \rangle, (g)).$$

Пусть, далее, $G \Rightarrow \text{Aut}_{K(\bar{\xi})} K(\bar{\xi}, \alpha)$ и $H, H_1, \dots, H_k$ — максимальное семейство попарно не сопряженных подгрупп группы G , т. е. эти подгруппы попарно не сопряжены в G , но любая подгруппа $G_0 \leq G$ сопряжена в G с одной из групп $H, H_1, \dots, H_k$.

Пологаем $N_2(\mathcal{G}) \Rightarrow \{ \langle \bar{\xi}; \eta; \alpha; H_i \rangle \mid i = 1, \dots, k \}$ и

$$N(\mathcal{G}) \Rightarrow N_0(\mathcal{G}) \cup N_1(\mathcal{G}) \cup N_2(\mathcal{G}).$$

Предложение 3. Для любого K -поля L , любого набора $\bar{\xi}' \in L^n$ имеет место эквивалентность

$$L \models \bigwedge_{\mathcal{G}' \in N(\mathcal{G})} P_{\mathcal{G}'}(\bar{\xi}') \Leftrightarrow L \models \bigvee_{\mathcal{G}' \in N(\mathcal{G})} P_{\mathcal{G}'}(\bar{\xi}').$$

Пусть $L \models \bigwedge_{\mathcal{G}' \in N(\mathcal{G})} P_{\mathcal{G}'}(\bar{\xi}')$. Если $\bar{\xi}'$ не является специализацией точки $\bar{\xi}$, то для некоторого i , $1 \leq i \leq s$, должно быть $p_i(\bar{\xi}') \neq 0$; но тогда, очевидно, $L \models P_{\langle \bar{\xi}^*; p_i(\bar{\xi}^*); 1; e \rangle}(\bar{\xi}')$.

Пусть ξ' — специализация ξ и $\varphi: K[\xi] \rightarrow K[\xi']$ — гомоморфизм специализации. Если $\varphi(\eta) = \varphi(g(\xi)) = g(\xi') = 0$, то $\xi' \in V_K(g)$ и, следовательно, по предложению 2 $L \models \bigvee_{\xi' \in N_1(\xi)} P_{\xi'}(\xi')$. Пусть, наконец, $\varphi(\eta) \neq 0$; пусть α' — корень многочлена $\varphi\alpha$ и $\psi: K[\xi, \eta^{-1}, \alpha] \rightarrow L(\alpha')$ — продолжение гомоморфизма φ такое, что $\psi(\alpha) = \alpha'$. Пусть G_0 — L -группа разложения этого гомоморфизма. Если бы G_0 была сопряжена в G с H , то $L \models P_{\xi}(\xi)$; следовательно, G_0 не сопряжена с H и сопряжена с H_i для некоторого i , $1 \leq i \leq k$; поэтому $L \models P_{\langle \xi; \eta; \alpha, H_i \rangle}(\xi')$. Импликация $\Rightarrow$ доказана.

Если $L \models \bigvee_{\xi' \in N_n(\xi)} P_{\xi'}(\xi')$, то ξ' не является специализацией ξ и, следовательно, $L \models \neg P_{\xi}(\xi')$. Если $L \models \bigvee_{\xi' \in N_1(\xi)} P_{\xi'}(\xi')$, то $L \models P_{\xi'}(\xi')$ для $\xi' \in \text{St}(\langle \xi^*; 1; 1; e \rangle, (g))$, и тогда либо ξ' не является специализацией ξ , либо гомоморфизм специализации $\varphi: K[\xi] \rightarrow K[\xi']$ переводит η в 0 ($\eta = g(\xi)$); в любом случае имеем $L \models \neg P_{\xi}(\xi')$. Пусть, наконец, $L \models P_{\xi'}(\xi')$, $\xi' = \langle \xi; \eta; \alpha; H_i \rangle \in N_2(\xi)$, $1 \leq i \leq k$; тогда существует α' и гомоморфизм $\psi: K[\xi, \eta^{-1}, \alpha] \rightarrow L(\alpha')$, продолжающий гомоморфизм специализации и такой, что $\psi(\alpha) = \alpha'$ и L -группой разложения гомоморфизма ψ является группа H_i ; так как H не сопряжена с H_i , то получаем $L \models \neg P_{\xi}(\xi')$. Импликация $\Leftarrow$ и предложение доказаны. $\square$

Пусть $\xi = \langle \xi; \eta; \alpha; H \rangle$ и $\xi' = \langle \xi; \eta'; \alpha'; H' \rangle$ — n -страты Галуа. Определим конечное множество $C(\xi, \xi')$ n -стратов Галуа (индукцией по $\dim \xi'$). Пусть $\xi_1, \dots, \xi_k$ — это все элементы множества $\text{St}(\xi, I(\xi'))$. Для i , $1 \leq i \leq k$, пусть $\xi_i = \langle \xi^i; \eta_i; \alpha_i; H_i \rangle$ и $\varphi_i: K[\xi; \eta^{-1}, \alpha] \rightarrow K(\xi^i, \alpha_i)$ — гомоморфизм (такой, что $\varphi_i(\alpha) = \alpha_i$), определенный по построению n -стратов из $\text{St}(\xi, I(\xi'))$, и пусть G_i — $K(\xi^i)$ -группа разложения (подгруппа группы $G \triangleq \text{Aut}_{K(\xi)} K(\xi, \alpha)$) этого гомоморфизма. Так как $\xi' \rightarrow \xi^i$ — специализация, то существует гомоморфизм специализации $\psi_i: K[\xi'] \rightarrow K[\xi^i]$. Если $\psi_i(\eta') = 0$, то полагаем $C_i(\xi, \xi') \triangleq \emptyset$. Пусть $\delta_i \triangleq \psi_i(\eta') \neq 0$ и ψ_i продолжено естественным образом до гомоморфизма $\psi_i: K[\xi', \eta'^{-1}] \rightarrow K[\xi^i, \delta_i^{-1}]$. Пусть $\rho_{\alpha'}$ — минимальный многочлен для α' над $K(\xi')$, тогда $\rho_{\alpha'} \in K[\xi', \eta'^{-1}, x]$. Пусть β_i — один из корней многочлена $\psi_i \rho_{\alpha'}$ в $U(K)$. Свяжем с ним гомоморфизм $\psi_i: K[\xi', \eta'^{-1}, \alpha] \rightarrow$

$\rightarrow K(\xi^i, \beta_i)$, продолжающий ψ_i и такой, что $\psi_i(\alpha') = \beta_i$; пусть H^i — $K(\xi^i)$ -группа разложения гомоморфизма $\psi_i (H^i \leq G' \triangleq \text{Aut}_{K(\xi')} K(\xi', \alpha'))$. Рассмотрим расширение $K(\xi^i, \alpha_i, \beta_i)$ поля $K(\xi^i)$; это расширение является расширением Галуа поля $K(\xi^i)$; пусть $G_0 \triangleq \text{Aut}_{K(\xi^i)} K(\xi^i, \alpha_i, \beta_i)$; заметим, что группу H^i можно естественно отождествить с группой $\text{Aut}_{K(\xi^i)} K(\xi^i, \beta_i)$; пусть $\lambda: G_0 \rightarrow H^i$, $\lambda': G_0 \rightarrow G_i \triangleq \text{Aut}_{K(\xi^i)} K(\xi^i, \alpha_i)$ — эпиморфизмы ограничения. Выбираем теперь все подгруппы $F \leq G_0$ такие, что $\lambda'(F) = H$, а $\lambda(F)$ — подгруппа H^i , сопряженная в G' с H' . Пусть $F_1, \dots, F_{k_i}$ — все такие подгруппы. Выбираем далее $\gamma_i \in K[\xi^i, \alpha_i, \beta_i]$ таким, что $K(\xi^i, \alpha_i, \beta_i) = K(\xi^i, \gamma_i)$, и такой сглаживающий элемент η_i' для $K[\xi^i]$, что дискриминант элемента γ_i обратим в $K[\xi^i, \eta_i'^{-1}]$. Пусть $g_i \in K[\xi]$ таков, что $\eta_i' = g_i(\xi^i)$; полагаем теперь $C_i(\xi, \xi') \triangleq \{ \langle \xi^i; \delta_i \eta_i \eta_i'; \gamma_i; F_i \rangle \mid 1 \leq i \leq k_i \} \cup \{ C(\xi, \xi') \mid \xi' \in \text{St}(\xi', (g_i)) \}$ и, наконец,

$$C(\xi, \xi') \triangleq \bigcup_{i=1}^k C_i(\xi, \xi').$$

Предложение 4. Для любого K -поля L и любого набора $\bar{\eta} \in L^n$ имеет место эквивалентность

$$L \models P_{\xi}(\bar{\eta}) \wedge P_{\xi'}(\bar{\eta}) \Leftrightarrow L \models \bigvee_{\xi'' \in C(\xi, \xi')} P_{\xi''}(\bar{\eta}).$$

1 Пусть $\bar{\eta} \in L^n$ и $L \models P_{\xi}(\bar{\eta}) \wedge P_{\xi'}(\bar{\eta})$; пусть $\varphi: K[\xi] \rightarrow K[\bar{\eta}]$, $\varphi': K[\xi'] \rightarrow K[\bar{\eta}]$ — гомоморфизмы специализации; тогда $\varphi(\eta) \neq 0$, $\varphi'(\eta') \neq 0$ и существуют $\beta, \beta' \in L^*$ такие, что φ и φ' продолжаются до гомоморфизмов $\psi: K[\xi, \eta^{-1}, \alpha] \rightarrow L(\beta)$, $\psi': K[\xi', \eta'^{-1}, \alpha'] \rightarrow L(\beta')$ таких, что $\psi(\alpha) = \beta$, $\psi'(\alpha') = \beta'$ и L -группами разложений ψ и ψ' являются соответственно H и H' . Так как $L \models P_{\xi}(\bar{\eta})$ и $\bar{\eta} \in V_K(\xi')$, то по предложению 2 существует индекс i , $1 \leq i \leq k$, такой, что $L \models P_{\xi_i}(\bar{\eta})$. Можно даже предполагать, что гомоморфизм $\psi: K[\xi, \eta^{-1}, \alpha] \rightarrow L(\beta)$ можно разложить в композицию гомоморфизмов $\varphi_i: K[\xi, \eta^{-1}, \alpha] \rightarrow K[\xi^i, \eta_i^{-1}, \alpha_i]$, $\varphi_i(\alpha) = \alpha_i$, и $\varphi_i': K[\xi^i, \eta_i^{-1}, \alpha_i] \rightarrow L(\beta)$, $\varphi_i'(\alpha_i) = \beta$. Пусть $\psi_i': K[\xi^i] \rightarrow K[\bar{\eta}]$ — гомоморфизм специализации; так как $\varphi' = \psi_i' \psi_i$ и $\varphi'(\eta') \neq 0$, то $\delta_i = \psi_i(\eta') \neq 0$; пусть ψ_i обозначает также естественное расширение ψ_i до гомоморфизма из $K[\xi', \eta'^{-1}]$ в $K[\xi^i, \delta_i^{-1}]$. Пусть $\rho_{\alpha'}$ — минимальный многочлен для α' над $K(\xi')$ ($\rho_{\alpha'} \in K[\xi', \eta'^{-1}, x]$) и β_0 — один из корней многочлена

$\psi_i p_{\alpha'}$. Пусть, как в определении множества $C'(\mathcal{S}, \mathcal{S}')$, элемент $\gamma_i \in K[\xi^i, \alpha_i, \beta_0]$ таков, что $K(\xi^i, \gamma_i) = K(\xi^i, \alpha_i, \beta_0)$, а элемент $\eta_i = g_i(\xi^i) \in K[\xi^i]$ таков, что дискриминант элемента γ_i обратим в кольце $K[\xi^i, \eta_i^{-1}]$; пусть $\rho_i = \delta_i \eta_i \eta_i'$. Предположим, что $g_i(\eta) \neq 0$; в этом случае существует гомоморфизм $v: K[\xi^i, \rho_i^{-1}] \rightarrow L$, продолжающий специализацию $\xi^i \rightarrow \bar{\eta}$. Этот гомоморфизм может быть продолжен до гомоморфизма $v': K[\xi^i, \rho_i^{-1}, \alpha_i] \rightarrow L(\beta)$ так, что $v'(\alpha_i) = \beta$; далее, v' может быть продолжен до гомоморфизма $v'': K[\xi^i, \rho_i^{-1}, \alpha_i, \beta_0] \rightarrow L(\beta, \beta')$. Пусть $F \leq G_0 (= \text{Aut}_{K(\xi^i)} K(\xi^i, \gamma_i))$ — L -группа разложения гомоморфизма $v'': K[\xi^i, \rho_i^{-1}, \gamma_i] (= K[\xi^i, \rho_i^{-1}, \alpha_i, \beta_0]) \rightarrow L(\beta, \beta')$. Ограничение v'' на $K[\xi^i, \eta_i^{-1}, \alpha_i]$ дает в точности гомоморфизм φ' , следовательно, ограничение L -группы разложения F на $K(\xi^i, \alpha_i)$ дает L -группу разложения этого гомоморфизма, а эта группа есть в точности группа H , т. е. $\lambda'(F) = H$. Ограничение v'' на $K[\xi^i, \delta_i^{-1}, \beta_0]$ в композиции с гомоморфизмом специализации $\psi_i: K[\xi^i, \eta_i'^{-1}, \alpha'] \rightarrow K[\xi^i, \delta_i^{-1}, \beta_0]$, $\psi_i(\alpha') = \beta_0$ задает гомоморфизм из $K[\xi^i, \eta_i'^{-1}, \alpha']$ в $L(\beta, \beta')$, продолжающий гомоморфизм специализации $\xi^i \mapsto \bar{\eta}$; пусть H'' — L -группа разложения этого гомоморфизма; эта группа сопряжена с группой H' в G' , так как известно, что существует гомоморфизм $\psi': K[\xi^i, \eta_i'^{-1}, \alpha'] \rightarrow L(\beta')$, продолжающий гомоморфизм специализации $\xi^i \mapsto \bar{\eta}$ и такой, что его L -группой разложения будет H' . Группа H'' является L -группой разложения и гомоморфизма $K[\xi^i, \delta_i^{-1}, \beta_0] \rightarrow L(\beta, \beta')$, следовательно, $\lambda(F) = H''$, H'' сопряжена с H' в G' , следовательно, F совпадает с одной из групп $F_1, \dots, F_{k_i}$ и $L \models P_{\langle \xi^i, \rho_i; \gamma_i, F_j \rangle}(\bar{\eta})$, для некоторого j , $1 \leq j \leq k_i$; но $\langle \xi^i, \rho_i; \gamma_i, F_j \rangle \in C^i(\mathcal{S}, \mathcal{S}') \subseteq C(\mathcal{S}, \mathcal{S}')$. В случае $g_i(\eta) = 0$ из $L \models P_{\mathcal{S}'}(\bar{\eta})$ имеем $L \models P_{\mathcal{S}''}(\bar{\eta})$ для некоторого $\mathcal{S}'' \in \text{St}(\mathcal{S}', (g_i))$, и подходящее индукционное предположение дает $L \models P_{\mathcal{S}^*}(\bar{\eta})$ для некоторого $\mathcal{S}^* \in C(\mathcal{S}, \mathcal{S}'')$; но $C(\mathcal{S}, \mathcal{S}'') \subseteq C(\mathcal{S}, \mathcal{S}')$ и импликация $\Rightarrow$ доказана.

Пусть теперь $L \models P_{\mathcal{S}''}(\bar{\eta})$ для некоторого n -страта $\mathcal{S}''$ из $C(\mathcal{S}, \mathcal{S}')$. Рассмотрим случай, когда $\mathcal{S}''$ имеет вид $\langle \xi^i; \eta^i (= \delta_i \eta_i \eta_i'); \gamma_i; F_j \rangle$, $1 \leq i \leq k$, $1 \leq j \leq k_i$. Пусть $\gamma \in L^*$ и гомоморфизм $\varphi: K[\xi^i, (\eta^i)^{-1}, \gamma_i] \rightarrow L(\gamma)$, продолжающий гомоморфизм специализации $\xi^i \mapsto \bar{\eta}$, таков, что L -группой разложения φ является F_j . Заметим, что так как кольцо $K[\xi^i, (\eta^i)^{-1}]$

γ_i целозамкнуто, α_i цел над $K[\xi^i]$ и $\alpha_i \in K(\xi^i, \gamma_i)$, то $\alpha_i \in K[\xi^i, (\eta^i)^{-1}, \gamma_i]$; так как $\eta^i = \delta_i \eta_i \eta_i'$, то $\eta_i^{-1} \in K[\xi^i, (\eta^i)^{-1}, \gamma_i]$; следовательно, $K[\xi^i, \eta_i^{-1}, \alpha_i] \leq K[\xi^i, (\eta^i)^{-1}, \gamma_i]$. Пусть φ' — ограничение φ на $K[\xi^i, \eta_i^{-1}, \alpha_i]$. L -группой разложения гомоморфизма φ' будет ограничение группы F_j на $K(\xi^i, \alpha_i)$, т. е. группа $\lambda'(F_j)$; но по выбору групп $F_1, \dots, F_{k_i}$ имеем $\lambda'(F_j) = H$, т. е. L -группой разложения гомоморфизма φ' будет H . Если ψ — композиция гомоморфизмов $\varphi_i: K[\xi^i, \eta_i^{-1}, \alpha] \rightarrow K[\xi^i, \eta_i^{-1}, \alpha_i]$ и φ' , то L -группой разложения ψ также будет H и, следовательно, $L \models P_{\mathcal{S}}(\bar{\eta})$. Рассмотрим теперь гомоморфизм $\psi_i': K[\xi^i, \eta_i'^{-1}, \alpha'] \rightarrow K[\xi^i, \delta_i^{-1}, \beta]$ и ограничение ψ' гомоморфизма φ на кольцо $K[\xi^i, \delta_i^{-1}, \beta]$. L -группой разложения гомоморфизма ψ' будет ограничение F_j на поле $K(\xi^i, \beta)$, т. е. группа $H'' \cong \lambda(F_j)$. Но по выбору групп $F_1, \dots, F_{k_i}$ группа H'' должна быть сопряжена с H' в G' . Композиция гомоморфизмов ψ' и ψ_i' дает гомоморфизм из $K[\xi^i, \eta_i'^{-1}, \alpha']$ в $L(\beta, \beta')$, продолжающий специализацию $\xi^i \mapsto \bar{\eta}$, L -группой разложения которого является группа H'' , сопряженная с H' в G' . Но тогда существует и гомоморфизм $\psi^*: K[\xi^i, \eta_i'^{-1}, \alpha'] \rightarrow L(\beta, \beta')$, продолжающий гомоморфизм специализации $\xi^i \mapsto \bar{\eta}$, L -группой разложения которого будет H' . Следовательно, $L \models P_{\mathcal{S}'}(\bar{\eta})$ и $L \models P_{\mathcal{S}}(\bar{\eta}) \wedge P_{\mathcal{S}'}(\bar{\eta})$. В случае, когда $\mathcal{S}'' \in C(\mathcal{S}, \mathcal{S}')$, $\mathcal{S}^* \in \text{St}(\mathcal{S}', (g_i))$, можно воспользоваться индуктивным предположением, чтобы утверждать, что $L \models P_{\mathcal{S}}(\bar{\eta}) \wedge P_{\mathcal{S}^*}(\bar{\eta})$, но из $\mathcal{S}^* \in \text{St}(\mathcal{S}', (g_i))$ и $L \models P_{\mathcal{S}^*}(\bar{\eta})$ следует, что $L \models P_{\mathcal{S}'}(\bar{\eta})$. $\square$

Замечание. Пусть $m < n$ и $\mathcal{S} = \langle \xi_1, \dots, \xi_m; \eta; \alpha; H \rangle$ — m -страт Галуа; пусть $\xi_{m+1}, \dots, \xi_n$ — элементы из $U(K)$, которые алгебраически независимы над $K(\xi_m)$, тогда $\mathcal{S}_0 = \langle \xi_1, \dots, \xi_m, \xi_{m+1}, \dots, \xi_n; \eta; \alpha; H \rangle$ является n -стратом Галуа и для любого K -поля L и любого набора $\xi' \in L^n$

$$L \models P_{\mathcal{S}}(\xi'_1, \dots, \xi'_m) \iff L \models P_{\mathcal{S}_0}(\xi').$$

Это замечание позволяет применять предложение 4 к конъюнкции произвольных стратов.

Следствие. Любая бескванторная формула Φ языка TS_K теории стратов эквивалентна дизъюнкции элементарных формул.

Это следствие двух предыдущих предложений и замечания. $\square$

Обратимся теперь к вопросу об элиминации квантора существования, навешенного на элементарную формулу.

Пусть $n > 0$ и $\mathfrak{S} = \langle \bar{\xi}; \eta; \alpha; H \rangle$ — n -страт Галуа. Определим теперь конечное семейство $\text{pr } \mathfrak{S}$ ($n-1$ -стратов Галуа. Определение разбивается на два существенно различных случая.

Случай 1. Элемент ξ_n алгебраичен над $K(\bar{\xi}_{n-1}) \cong K(\xi_1, \dots, \xi_{n-1})$. Выбираем $\beta \in U(K)$ так, что β цел над $K[\bar{\xi}_{n-1}]$ и $K(\bar{\xi}_{n-1}, \beta)$ — минимальное расширение Галуа поля $K(\bar{\xi}_{n-1})$, содержащее элементы ξ_n и α . Выбираем в $K[\bar{\xi}_{n-1}]$ ненулевой элемент η_0 такой, что выполнены условия: η_0 — сглаживающий элемент для $K[\bar{\xi}_{n-1}]$; дискриминант элемента β над $K(\bar{\xi}_{n-1})$ обратим в кольце $K[\bar{\xi}_{n-1}, \eta_0^{-1}]$; элементы η и ξ_n целы над $K[\bar{\xi}_{n-1}, \eta_0^{-1}]$; элемент $N_{K(\bar{\xi}_{n-1}, \beta)/K(\bar{\xi}_{n-1})}(\eta)$ обратим в $K[\bar{\xi}_{n-1}, \eta_0^{-1}]$. Пусть $g \in K[\bar{x}_{n-1}] \cong K[x_1, \dots, x_{n-1}]$ таков, что $\eta_0 = g(\bar{\xi}_{n-1})$. Пусть $G \cong \text{Aut}_{K(\bar{\xi})} K(\bar{\xi}, \alpha)$; $G_1 \cong \text{Aut}_{K(\bar{\xi}_{n-1})} K(\bar{\xi}_{n-1}, \beta)$; $G_2 \cong \{\sigma \mid \sigma \in G_1, \sigma(\xi_n) = \xi_n\}$; $\varphi: G_2 \rightarrow G$ — естественный эпиморфизм ограничения; пусть $H_1, \dots, H_k$ — все подгруппы группы G_2 такие, что $\varphi(H_i) = H$.

Полагаем

$$\text{pr } \mathfrak{S} \cong \{ \langle \bar{\xi}_{n-1}; \eta_0; \beta; H_i \rangle \mid i = 1, \dots, k \} \cup \{ \text{pr } \mathfrak{S}' \mid \mathfrak{S}' \in \text{St}(\mathfrak{S}, (g)) \}.$$

Предложение 5. При сформулированных выше условиях для любого K -поля L и любых $\eta_1, \dots, \eta_{n-1} \in L$ имеет место эквивалентность

$$L \models (\exists x_n P_{\mathfrak{S}})[\bar{\eta}_{n-1}] \Leftrightarrow L \models \bigvee_{\mathfrak{S}' \in \text{pr } \mathfrak{S}} P_{\mathfrak{S}'}(\bar{\eta}_{n-1}).$$

Пусть $\eta_n \in L$ таков, что $L \models P_{\mathfrak{S}}(\bar{\eta})$. Пусть $\varphi: K[\bar{\xi}] \rightarrow L$ — гомоморфизм специализации $\bar{\xi} \rightarrow \bar{\eta}$; пусть α' — такой элемент L^* , что φ продолжается до гомоморфизма $\psi: K[\bar{\xi}, \eta^{-1}, \alpha] \rightarrow L(\alpha')$, $\psi(\alpha) = \alpha'$, L -группой разложения которого будет H . Если $g(\bar{\eta}_{n-1}) \neq 0$, то ψ можно продолжить до гомоморфизма $\psi': K[\bar{\xi}_{n-1}, \eta_0^{-1}, \beta] \rightarrow L(\gamma)$ для подходящего $\gamma \in L^*$. Заметим, что $K[\bar{\xi}, \eta^{-1}, \alpha] \leq K[\bar{\xi}_{n-1}, \eta_0^{-1}, \beta]$, так как $K[\bar{\xi}_{n-1}, \eta_0^{-1}, \beta]$ цело замкнуто, ξ_n, η и α целы над $K[\bar{\xi}_{n-1}, \eta_0^{-1}]$ и η обратим в $K[\bar{\xi}_{n-1}, \eta_0^{-1}, \beta]$, так как обратима его норма. Пусть $G' \subset L$ -группа разложения гомоморфизма ψ' ; $G' \leq G_2$, так как $\psi'(\xi_n) = \psi(\xi_n) \in L$ и ограничение G' на $K(\bar{\xi}, \alpha)$ — это в точности группа H . Следовательно, G' совпадает с одной из групп $H_1, \dots, H_k$ и

$$L \models \bigvee_{i=1}^k P_{\langle \bar{\xi}_{n-1}; \eta_0; \beta; H_i \rangle}(\bar{\eta}_{n-1}). \text{ Если же } g(\bar{\eta}_{n-1}) = 0, \text{ то } \bar{\eta} \in V_K(g)$$

и, следовательно, по предложению 2 $L \models P_{\mathfrak{S}'}(\bar{\eta})$ для некоторого n -страта $\mathfrak{S}' \in \text{St}(\mathfrak{S}, (g))$. Используя индуктивное предположение, отсюда получаем, что $L \models \bigvee_{\mathfrak{S}' \in \text{pr } \mathfrak{S}} P_{\mathfrak{S}'}(\bar{\eta}_{n-1})$; но $\text{pr } \mathfrak{S} \subseteq \text{pr } \mathfrak{S}$ и, следовательно, импликация $\Rightarrow$ установлена.

Наоборот, предположим, что $L \models P_{\mathfrak{S}_i}(\bar{\eta}_{n-1})$, где $\mathfrak{S}_i = \langle \bar{\xi}_{n-1}; \eta_0; \beta; H_i \rangle$, $1 \leq i \leq k$. Тогда существуют $\gamma \in L^*$ и гомоморфизм $\varphi: K[\bar{\xi}_{n-1}, \eta_0^{-1}, \beta] \rightarrow L(\gamma)$, продолжающий гомоморфизм специализации $\bar{\xi}_{n-1} \rightarrow \bar{\eta}_{n-1}$ и имеющий H_i своей L -группой разложения. Как было отмечено выше, кольцо $K[\bar{\xi}, \eta^{-1}, \alpha]$ содержится в кольце $K[\bar{\xi}_{n-1}, \eta_0^{-1}, \beta]$. Полагаем $\eta_n = \varphi(\xi_n)$; так как L -группа разложения H_i содержится в G_2 , то $\eta_n = \varphi(\xi_n) \in L$. Если φ' — ограничение φ на $K[\bar{\xi}, \eta^{-1}, \alpha]$, то φ' есть продолжение гомоморфизма специализации $\bar{\xi} \rightarrow \bar{\eta}$ и его L -группой разложения будет ограничение H_i на $K(\bar{\xi}, \alpha)$, но по выбору $H_1, \dots, H_k$ это будет группа H . Итак, $L \models P_{\mathfrak{S}}(\bar{\eta})$ и $L \models (\exists x_n P_{\mathfrak{S}})[\bar{\eta}_{n-1}]$. Если $L \models P_{\mathfrak{S}'}(\bar{\eta}_{n-1})$ для $\mathfrak{S}' \in \text{pr } \mathfrak{S}$, $\mathfrak{S}' \in \text{St}(\mathfrak{S}, (g))$, то можно воспользоваться индуктивным предположением. Импликация $\Leftarrow$, а вместе с ней и предположение установлены. $\square$

Рассмотрим теперь оставшийся случай.

Случай 2. Элемент ξ_n трансцендентен над $K(\bar{\xi}_{n-1})$. Пусть $\beta \in K(\bar{\xi}, \alpha)$ таков, что β цел над $K[\bar{\xi}_{n-1}]$ и $K(\bar{\xi}_{n-1}, \beta)$ — алгебраическое замыкание поля $K(\bar{\xi}_{n-1})$ в $K(\bar{\xi}, \alpha)$. Пусть $g \in K(\bar{\xi}_{n-1}, \beta)[x, y]$ — минимальный многочлен такой, что $g(\xi_n, \alpha) = 0$ (так как α цел над $K[\bar{\xi}]$, то g унитарен в y); тогда g — абсолютно неприводимый многочлен. Установим теперь необходимый для дальнейшего построения алгебраический факт.

Лемма. Пусть $L_0 = L(\alpha_1, \dots, \alpha_k)$ — конечно порожденное расширение поля L , $g \in L[\alpha_1, \dots, \alpha_k, x_1, \dots, x_n]$ — абсолютно неприводимый многочлен (как многочлен от $\bar{x}$), тогда существует элемент $\delta \in L[\bar{\alpha}]$, $\delta \neq 0$ такой, что для любого L -гомоморфизма $\varphi: L[\bar{\alpha}] \rightarrow L_1$ в L -поле L_1 такого, что $\varphi(\delta) \neq 0$, многочлен $\varphi g \in L_1[\bar{x}]$ остается абсолютно неприводимым.

Для доказательства этой леммы воспользуемся тем, что любая формула $\Phi(\bar{z})$ языка теории полей эквивалентна относительно теории алгебраически замкнутых полей бескванторной формуле $\Phi'(\bar{z})$, а любая бескванторная формула эквивалентна дизъюнкции формул вида $\bigwedge_{i=1}^s f_i(\bar{z}) = 0 \wedge h(\bar{z}) \neq 0$, где f_i, h —

многочлены от $\bar{z}$ с рациональными коэффициентами. Заменим теперь все коэффициенты многочлена g неопределенными коэффициентами $\bar{z}$ и запишем формулу $\Phi(\bar{z})$, выражающую непри-

водимость полученного многочлена (неприводимость над алгебраически замкнутым полем эквивалентна абсолютной неприводимости). Так как набор коэффициентов $\bar{b}$ многочлена g удовлетворяет формуле Φ , то для некоторого дизъюнктивного члена формулы Φ' должно быть $f_i(\bar{b})=0$, $i=1, \dots, s$, и $h(\bar{b}) \neq 0$.

Так как свойство $\bigwedge_{i=1}^s f_i(\bar{b})=0$ сохраняется при любом гомоморфизме, то, полагая $\delta \Leftarrow h(\bar{b})$, получаем нужный элемент. $\square$

Выбираем в $K[\bar{\xi}_{n-1}]$ такой сглаживающий элемент η_0 , что выполнены следующие условия: дискриминант элемента β над $K[\bar{\xi}_{n-1}]$ обратим в $K[\bar{\xi}_{n-1}, \eta_0^{-1}]$; коэффициенты многочлена g целы над $K[\bar{\xi}_{n-1}, \eta_0^{-1}]$; если $\delta \in K[\bar{\xi}_{n-1}, \eta_0^{-1}, \beta]$ — элемент, существование которого утверждается в лемме, то $\delta_0 \Leftarrow N_{K(\bar{\xi}_{n-1}, \beta)/K(\bar{\xi}_{n-1})}(\delta)$ обратим в $K[\bar{\xi}_{n-1}, \eta_0^{-1}]$. Пусть $h \in K[\bar{x}_{n-1}]$ таков, что $\eta_0 = h(\bar{\xi}_{n-1})$. Если $G \Leftarrow \text{Aut}_{K(\bar{\xi})} K(\bar{\xi}, \alpha)$, $G_0 \Leftarrow \text{Aut}_{K(\bar{\xi}_{n-1})} K(\bar{\xi}_{n-1}, \beta)$ и $\lambda: G \rightarrow G_0$ — эпиморфизм ограничения, то полагаем $H_0 \Leftarrow \lambda(H)$ и

$$\text{pr } \mathfrak{S} \Leftarrow \{ \langle \bar{\xi}_{n-1}; \eta_0; \beta; H_0 \rangle \} \cup \{ \text{pr } \mathfrak{S}' \mid \mathfrak{S}' \in \text{St}(\mathfrak{S}, (h)) \}.$$

Напомним, что в предыдущем пункте через Q_H обозначалось предложение в языке сигнатуры σ_f , утверждающее, что у поля существует расширение Галуа с группой Галуа, изоморфной H ; через Q_H будем обозначать «перевод» этого предложения в язык сигнатуры TS_K .

Предложение 6. Для любого регулярно замкнутого K -поля L с допустимой группой Галуа и любых $\eta_1, \dots, \eta_{n-1} \in L$ имеет место эквивалентность

$$L \models (\exists x_n P_{\mathfrak{S}})[\bar{\eta}_{n-1}] \Leftrightarrow L \models \left(\bigvee_{\mathfrak{S}' \in \text{pr } \mathfrak{S}} P_{\mathfrak{S}'}(\bar{\eta}_{n-1}) \right) \wedge Q_H^*.$$

Пусть $\eta_n \in L$ — такой элемент, что $L \models P_{\mathfrak{S}}(\bar{\eta})$; пусть $\gamma \in L^*$ и гомоморфизм $\varphi: K[\bar{\xi}, \eta^{-1}, \alpha] \rightarrow L(\gamma)$ таков, что φ продолжает гомоморфизм специализации $\bar{\xi} \mapsto \bar{\eta}$ и имеет H своей L -группой разложения. Предположим, что $\varphi(\eta_0) \neq 0$, тогда φ однозначно продолжается до гомоморфизма $\varphi': K[\bar{\xi}, \eta_0^{-1}, \eta^{-1}, \alpha] \rightarrow L(\gamma)$. Пусть ψ — ограничение гомоморфизма φ' на $K[\bar{\xi}_{n-1}, \eta_0^{-1}, \beta]$, тогда L -группой разложения ψ будет ограничение H на поле $K(\bar{\xi}_{n-1}, \beta)$, т.е. группа $\lambda(H) = H_0$. Следовательно, $L \models$

$\models P_{\langle \bar{\xi}_{n-1}; \eta_0; \beta; H_0 \rangle}(\bar{\eta}_{n-1})$. Если же $\varphi(\eta_0) = 0$, т.е. $h(\bar{\eta}_{n-1}) = 0$, то $\bar{\eta} \in V_K((h))$ и, следовательно, по предложению 2 существует $\mathfrak{S}' \in \text{St}(\mathfrak{S}, (h))$ такой, что $L \models P_{\mathfrak{S}'}(\bar{\eta})$. Используя индуктивное предположение, можно заключить, что $L \models \bigvee_{\mathfrak{S}' \in \text{pr } \mathfrak{S}} P_{\mathfrak{S}'}(\bar{\eta})$; но

$\text{pr } \mathfrak{S}' \subseteq \text{pr } \mathfrak{S}$, следовательно, импликация $\Rightarrow$ установлена (справедливость Q_H^* для L очевидна, так как H — L -группа разложения гомоморфизма φ).

Пусть теперь $L \models P_{\mathfrak{S}'}(\bar{\eta}_{n-1})$, где $\mathfrak{S}' = \langle \bar{\xi}_{n-1}; \eta_0; \beta; H_0 \rangle$ и φ — гомоморфизм из $K[\bar{\xi}_{n-1}, \eta_0^{-1}, \beta]$ в $L(\beta')$, $\varphi(\beta) = \beta'$, продолжающий гомоморфизм специализации $\bar{\xi}_{n-1} \mapsto \bar{\eta}_{n-1}$ и имеющий H_0 своей L -группой разложения. Заметим, что из выбора η_0 следует, что многочлен $g \in K[\bar{\xi}_{n-1}, \eta_0^{-1}, \beta, x, y]$ и $\varphi(\delta) \neq 0$, следовательно, многочлен $g' \Leftarrow \varphi g \in L(\beta')[x, y]$ абсолютно неприводим. Пусть γ — трансцендентный элемент над $L(\beta')$ и ε — корень неприводимого многочлена $g'(\gamma, y) \in L(\beta', \gamma)[y]$ и $L_0 \Leftarrow L(\beta', \gamma, \varepsilon)$. Гомоморфизм φ можно продолжить до гомоморфизма $\psi: K[\bar{\xi}, \eta_0^{-1}, \beta, \eta^{-1}, \alpha] \rightarrow L_0$ так, что $\psi(\xi_n) = \gamma$, $\psi(\alpha) = \varepsilon$. Пусть $G' = L(\gamma)$ -группа разложения гомоморфизма ψ , ограниченного на $K[\bar{\xi}, \eta^{-1}, \alpha]$. $G' \leq G$ и ограничение G' на $K(\bar{\xi}_{n-1}, \beta)$ есть L -группа разложения гомоморфизма φ , т.е. H_0 . Пусть $\lambda': G' \rightarrow H_0$ — эпиморфизм ограничения. Рассмотрим $\text{Ker } \lambda'$; это группа всех автоморфизмов поля L_0 над $L(\beta', \gamma)$. Так как расширение L_0 получено присоединением корня ε неприводимого многочлена $g'(\gamma, y)$, полученного специализацией многочлена $g(\xi_n, y)$, то эта группа изоморфна группе всех автоморфизмов поля $K(\bar{\xi}, \alpha)$ над $K(\bar{\xi}_{n-1}, \beta)$, т.е. ядру гомоморфизма $\lambda: G \rightarrow G_0$. Но отсюда сразу следует, что $G' = \lambda^{-1}(H_0)$; в частности, $H \leq G'$. Итак, имеем: L — регулярно замкнутое поле с допустимой группой Галуа $G(L)$; $L(\gamma)$ — регулярное расширение L ; $L(\gamma, \beta', \varepsilon)$ — расширение Галуа поля $L(\gamma)$ с группой Галуа G' ; $L(\beta')$ — алгебраическое замыкание L в $L(\gamma, \beta', \varepsilon)$ (так как $g'(x, y)$ — абсолютно неприводимый многочлен) с группой Галуа H_0 . Предположим теперь, что поле L имеет некоторое расширение Галуа с группой Галуа, изоморфной H , т.е. $L \models Q_H$; это равносильно тому, что $H \in H_f(G(L))$; тогда из допустимости группы $G(L)$ следует, что существует гомоморфизм $\mu: G(L) \rightarrow G'$ такой, что $\mu(G(L)) = H$ и диаграмма

$$\begin{array}{ccc} & G(L) & \\ \pi \swarrow & & \searrow \mu \\ H_0 & \xleftarrow{\lambda'} & G' \end{array}$$

коммутативна, где π — эпиморфизм ограничения $G(L)$ на $L(\beta')$. Воспользуемся теперь теоремой 2 п. 1 (аналог теоремы Чеботарева о плотности) и найдем $\beta'' \in L^*$ и плейсы $p: L(\gamma) \rightarrow L$ и $\pi: L(\gamma, \beta', \epsilon) \rightarrow L(\beta', \beta'')$ такие, что p конечен на $\gamma, \psi(\eta), \psi(\eta^{-1}), \psi(\alpha)$, группой разложения π над p будет H и изоморфизм H на $\text{Aut}_L L(\beta', \beta'')$ является обратным к изоморфизму $G(L)/\text{Ker } \mu \rightarrow H$, индуцированному эпиморфизмом μ . Нетрудно проверить, что плейс π конечен на β' и ϵ , а определенный этим плейсом гомоморфизм $L[\gamma, \beta', \epsilon, \psi^{-1}(\eta^{-1}), \psi(\alpha), \beta] \rightarrow L(\beta', \beta'')$ в композиции с гомоморфизмом ψ задает гомоморфизм $\psi^*: K[\xi, \eta^{-1}, \alpha] \rightarrow L(\beta', \beta'')$, L -группой разложения которого будет группа H . Следовательно, $L \models (\exists x_n P_{\mathcal{G}})[\bar{\eta}_{n-1}]$. Если же $L \models P_{\mathcal{G}}(\bar{\eta}_{n-1})$ для $\mathcal{G} \in \text{pr } \mathcal{G}^*$, $\mathcal{G}^* \in \text{St}(\mathcal{G}, (h))$, то можно воспользоваться индуктивным предположением, чтобы утверждать, что из $L \models Q_H$ следует $L \models (\exists x_n P_{\mathcal{G}})[\bar{\eta}_{n-1}]$. $\square$

Замечание. Как видно из всего предыдущего, условие регулярной замкнутости и допустимости группы Галуа поля использовались только при установлении импликации $\Leftarrow$ предложения 6.

Теорема 1. Пусть $R^*(K)$ — класс регулярно замкнутых K -полей с допустимой группой Галуа, тогда произвольная формула теории стратов Галуа эквивалентна относительно $R^*(K)$ дизъюнкции формул вида

$$P_{\mathcal{G}} \wedge Q_{H_1}^* \wedge \dots \wedge Q_{H_k}^* \wedge \neg Q_{G_1}^* \wedge \dots \wedge \neg Q_{G_m}^*.$$

Это простое следствие предложений 3—6. $\square$

Для того чтобы элиминация кванторов была эффективной, нужно сделать некоторые предположения о поле K . Предположим, что поле K обладает такой конструктивизацией v , что для конструктивного поля (K, v) разрешима проблема разложимости. Тогда существует продолжение v до конструктивизации v_u универсальной области $U(K)$ такой, что в конструктивном поле $(U(K), v_u)$ разрешима проблема алгебраической зависимости над K . Используя эту нумерацию v_u , можно занумеровать все n -страты Галуа $\mathcal{G}$, $n \in \omega$, так, что конструкции множеств $\text{St}(\mathcal{G}, I)$, $N(\mathcal{G})$, $C(\mathcal{G}, \mathcal{G}')$, $\text{pr}(\mathcal{G})$ могут быть проделаны эффективно. Примером поля K , для которого все это может быть проделано, является поле $\mathbb{Q}$ рациональных чисел. Тогда класс $R^*(\mathbb{Q})$ — это просто класс R_0^* — класс регулярно замкнутых полей характеристики 0 с допустимой группой Галуа.

Теорема 2. Любая формула теории стратов Галуа эффективно эквивалентна относительно класса R_0^* дизъюнкции формул

вида

$$P_{\mathcal{G}} \wedge Q_{H_1}^* \wedge \dots \wedge Q_{H_k}^* \wedge \neg Q_{G_1}^* \wedge \dots \wedge \neg Q_{G_m}^*.$$

Из теоремы 2 можно получить разрешимость теории стратов Галуа класса R_0^* . Для этого достаточно показать, что для любого предложения $\mathcal{G}$ языка $TS_{\mathcal{G}}$ можно проверить, совместно ли это предложение с теорией $TS_{\mathcal{G}}(R_0^*)$. Для этого по теореме 2 достаточно уметь проверять совместность предложения вида, указанного явно в теореме 2, для 0-стратов Галуа $\mathcal{G}$. Каждый 0-страт Галуа имеет вид $\langle \alpha, H \rangle$, где $Q(\alpha)$ — расширение Галуа поля $\mathbb{Q}$ и H — подгруппа группы Галуа $\text{Aut}_{\mathbb{Q}} \mathbb{Q}(\alpha)$.

Лемма. Предложение $P_{\langle \alpha, H \rangle} \wedge Q_{H_1}^* \wedge \dots \wedge Q_{H_k}^* \wedge \neg Q_{G_1}^* \wedge \dots \wedge \neg Q_{G_m}^*$ совместно с теорией $TS_{\mathcal{G}}(R_0^*)$ тогда и только тогда, когда все группы $G_1, \dots, G_m$ не принадлежат допустимому классу групп $\mathcal{G}(H, H_1, \dots, H_k)$.

Необходимость очевидна. Установим достаточность. Пусть $\varphi: G(\mathbb{Q}) \rightarrow \text{Aut}_{\mathbb{Q}} \mathbb{Q}(\alpha)$ — эпиморфизм ограничения и G_0 — минимальная подгруппа $G(\mathbb{Q})$, которая отображается на H . Тогда G_0 — накрытие H и, следовательно, является $\mathcal{G}(H)$ -группой. Тогда существует универсальная $\mathcal{G}(H, H_1, \dots, H_k)$ -группа G_0^* и эпиморфизм $\lambda: G_0^* \rightarrow G_0$. По теореме 1 п. 1 существует регулярно замкнутое поле L , являющееся регулярным расширением поля $\mathbb{Q}^{G_0^*}$, группой Галуа которого будет G_0^* . Тогда $L \in R_0^*$ и, как легко видеть, в поле L будет истинно указанное предложение при условии, что $G_i \notin \mathcal{G}(H, H_1, \dots, H_k)$, $i = 1, \dots, m$. $\square$

Следствие. Теория $TS_{\mathcal{G}}(R_0^*)$ разрешима.

Это следует из разрешимости проблемы: имеет ли место $G \in \mathcal{G}(H_0, \dots, H_k)$ (см. п. 2). $\square$

Из отмеченной выше эффективности сводимости элементарной теории к теории стратов Галуа получаем другое доказательство теоремы 3 п. 3.

Если ограничиться рассмотрением регулярно замкнутых классов K -полей, у которых группы Галуа являются $\mathcal{G}$ -универсальными для фиксированного допустимого класса групп $\mathcal{G}$ (обозначим этот класс полей $R(K, \mathcal{G})$), то можно получить теорему об «абсолютной» элиминации кванторов:

Теорема 3. Любая формула теории стратов Галуа эквивалентна относительно класса $R(K, \mathcal{G})$ дизъюнкции элементарных формул. $\square$

Если $\mathcal{G}$ — рекурсивный класс групп, поле K обладает нужной конструктивизацией, то элиминация кванторов для теории $R(K, \mathcal{G})$, имеющая место по теореме 3, может быть проделана эффективно.

Заключение

Укажем точные формулировки упомянутых вначале результатов о кратно упорядоченных и кратно нормированных полях.

Пусть $n > 0$, $K = \langle K, P_1, \dots, P_n \rangle$ — n -упорядоченное поле, здесь P_i — конус неотрицательных элементов i -го порядка; $x \leq_i y$ означает $y - x \in P_i$, $x <_i y$ означает $x \leq_i y$ и $x \neq y$; $|x|_i$ — элемент из $\{x, -x\} \cap P_i$, $i = 1, \dots, n$.

Обозначим через D_n класс всех n -упорядоченных полей K таких, что выполнены следующие два условия:

1. Для любых $a_1, \dots, a_n, e_1, \dots, e_n \in K$, $0 <_i e_i$, $i = 1, \dots, n$, существует $b \in K$ такой, что $|b - a_i| <_i e_i$.
2. Для любых $a \in K$ и неприводимого многочлена $f \in K[x, y]$, если $f(a, y)$ меняет знак при любом порядке $\leq_i$, $i = 1, \dots, n$, то существуют c и d в K такие, что $f(c, d) = 0$.

Следующая теорема из работы ван ден Дриса [1] обобщает хорошо известный результат о вещественно замкнутых полях на любое $n > 0$.

Теорема 1. *Класс D_n является модельным компаньоном для класса всех n -упорядоченных полей и имеет разрешимую теорию.* $\square$

Обратимся теперь к нормированным полям. Начнем с напоминания некоторых определений и введения соответствующих обозначений.

Пусть K — поле, R — кольцо нормирования поля K , т.е. такое подкольцо поля K , что для любого $x \in K^\times$ ($K^\times$ — мультипликативная группа ненулевых элементов поля K) $x \in R$ или $x^{-1} \in R$; R является локальным кольцом, максимальный идеал которого обозначим $\mathfrak{m}(R)$; фактор-поле $R/\mathfrak{m}(R)$ — поле вычетов кольца R — будем обозначать K_R . Естественный гомоморфизм $R \rightarrow K_R$ будем обозначать чертой (если $a \in R$, то $\bar{a} \in K_R$ — образ элемента a при этом гомоморфизме). Кольцо R определяет на K линейный предпорядок $\leq_R$: $a \leq_R b \Leftrightarrow b - a \in R$; $a, b \in K$. Полагаем $a \equiv_R b$, если $a \leq_R b$ и $b \leq_R a$; $a <_R b$, если $a \leq_R b$ и $\neg(a \equiv_R b)$. Предпорядок $\leq_R$ индуцирует линейный порядок $\leq_R$ на фактор-группе $K^\times/R^\times$, где $R^\times \equiv R - \mathfrak{m}(R) = \{a | a \in K, a \equiv_R 1\}$ — мультипликативная группа обратимых элементов кольца R . Линейно упорядоченную группу $\langle K^\times/R^\times, \leq_R \rangle$ будем называть группой нормирования и обозначать Γ_R ; гомоморфизм из $K^\times$ в Γ_R называется нормированием; будем обозначать его v_R .

Кольцо R и нормированное поле $\langle K, R \rangle$ называется *гензелевым*, если для любого унитарного многочлена $f \in R[x]$ и элемента $\alpha \in R$ такого, что $f'(\alpha)^2 <_R f(\alpha)$, существует $\alpha_0 \in R$ такой,

что $f(\alpha_0) = 0$ и $\alpha - \alpha_0 \equiv_R f'(\alpha) f'(\alpha)^{-1}$ (здесь штрих означает формальную производную).

Если K' — расширение поля K , R' — кольцо нормирования поля K' такое, что $R' \cap K = R$, то обозначать это будем так: $\langle K, R \rangle \leq \langle K', R' \rangle$; заметим, что в этом случае существуют естественные вложения $K_R \rightarrow K'_R$ и $\Gamma_R \rightarrow \Gamma_{R'}$; осуществляя естественное отождествление, будем считать, что $K_R \leq K'_R$ и $\Gamma_R \leq \Gamma_{R'}$.

Для любого нормированного поля $\langle K, R \rangle$ существует «наименьшее» расширение $\langle K', R' \rangle$ такое, что $\langle K, R \rangle \leq \langle K', R' \rangle$ и R' гензелево; это расширение называется *гензелелизацией* и обозначается $\langle K, R \rangle^h = \langle K^h, R^h \rangle$; для гензелелизации имеет место $K_R = K_R^h$, $\Gamma_R = \Gamma_{R^h}$.

Пусть $\mathfrak{F}$ — класс полей характеристики 0, $\mathfrak{G}$ — класс линейно упорядоченных групп. Обозначим через $\langle \mathfrak{F}, \mathfrak{G} \rangle$ класс всех гензелевых нормированных полей $K = \langle K, R \rangle$ таких, что $K_R \in \mathfrak{F}$, $\Gamma_R \in \mathfrak{G}$.

Основная теорема (см. Ершов [5]) об алгоритмических свойствах гензелевых полей утверждает следующее:

Если классы $\mathfrak{F}$ и $\mathfrak{G}$ имеют разрешимую теорию, то и класс $\langle \mathfrak{F}, \mathfrak{G} \rangle$ нормированных полей имеет разрешимую теорию.

Перейдем теперь к кратно нормированным полям. Пусть $n > 1$ — натуральное число; K — поле, $R_1, \dots, R_n$ — собственные кольца нормирований поля K . Алгебраическую систему $K = \langle K, R_1, \dots, R_n \rangle$ будем называть *n -кратно нормированным полем*. Если $K' = \langle K', R'_1, \dots, R'_n \rangle$ — другое n -кратно нормированное поле, то запись $K \leq K'$ будет обозначать, что $K \leq K'$ и $R'_i \cap K = R_i$, $i = 1, \dots, n$; используем обозначения $K_i \equiv K_{R_i}$, $\Gamma_i \equiv \Gamma_{R_i}$, $K'_i \equiv K'_{R'_i}$, $\Gamma'_i \equiv \Gamma_{R'_i}$, $i = 1, \dots, n$; тогда из $K \leq K'$ следует, что $K_i \leq K'_i$, $\Gamma_i \leq \Gamma'_i$, $i = 1, \dots, n$.

Сформулируем теперь «аналог» гензелевости для кратно нормированных полей. n -кратно нормированное поле K называется *когерентно полным*, если выполнены следующие два условия:

1. Для любых $a_1, \dots, a_n \in K$, $\gamma_1, \dots, \gamma_n \in K^\times$ существует $b \in K$ такой, что $\gamma_i <_{R_i} b - a_i$, $i = 1, \dots, n$.

2. Для $R \equiv \bigcap_{i=1}^n R_i$, любого многочлена $f \in R[x_1, \dots, x_k, y]$,

унитарного в y и неприводимого над K , для любых $a_1, \dots, a_k$, $\beta \in R$ таких, что $f'_y(\bar{\alpha}, \beta)^2 <_{R_i} f(\bar{\alpha}, \beta)$, $i = 1, \dots, n$, и для

любого $\gamma \in K^\times$ существуют $\alpha'_1, \dots, \alpha'_k, \beta' \in R$ такие, что $f(\bar{\alpha}', \beta') = 0$, $\gamma <_{R_i} \alpha'_s - \alpha_s$, $s = 1, \dots, k$, $i = 1, \dots, n$, и

$$\beta - \beta' =_{R_i} f(\bar{\alpha}, \beta) f'_{\gamma}(\bar{\alpha}, \beta)^{-1}, \quad i = 1, \dots, n.$$

Следующее утверждение указывает на существование достаточного количества когерентно полных полей.

Предложение. Пусть K — n -кратно нормированное поле, тогда существует такое когерентно полное n -кратно нормированное поле K' , что

$$K \leq K', \quad K_i = K'_i \text{ и } \Gamma_i \leq \Gamma'_i, \quad i = 1, \dots, n. \quad \square$$

Здесь символ $\leq$ означает элементарную вложимость.

Пусть $\mathfrak{F}_1, \dots, \mathfrak{F}_n$ — классы полей характеристики 0, $\mathfrak{G}_1, \dots, \mathfrak{G}_n$ — классы нетривиальных линейно упорядоченных групп; обозначим через $\langle \mathfrak{F}_1, \dots, \mathfrak{F}_n; \mathfrak{G}_1, \dots, \mathfrak{G}_n \rangle$ класс всех n -кратно нормированных полей K таких, что K когерентно полно, $K_i \in \mathfrak{F}_i$, $\Gamma_i \in \mathfrak{G}_i$, $i = 1, \dots, n$.

Теорема 2 (Ершов [7]) Если классы $\mathfrak{F}_1, \dots, \mathfrak{F}_n, \mathfrak{G}_1, \dots, \mathfrak{G}_n$ имеют разрешимую теорию, то и класс $\langle \mathfrak{F}_1, \dots, \mathfrak{F}_n; \mathfrak{G}_1, \dots, \mathfrak{G}_n \rangle$ имеет разрешимую теорию. $\square$

Замечание. Из сформулированного выше предложения вытекает, что теория класса $\langle \mathfrak{F}_1, \dots, \mathfrak{F}_n; \mathfrak{G}_1, \dots, \mathfrak{G}_n \rangle$ существенно зависит от теорий всех классов $\mathfrak{F}_1, \dots, \mathfrak{F}_n, \mathfrak{G}_1, \dots, \mathfrak{G}_n$. А именно, справедливо следующее:

$$\begin{aligned} \text{Если } \text{Th}(\langle \mathfrak{F}_1, \dots, \mathfrak{F}_n; \mathfrak{G}_1, \dots, \mathfrak{G}_n \rangle) = \\ = \text{Th}(\langle \mathfrak{F}'_1, \dots, \mathfrak{F}'_n; \mathfrak{G}'_1, \dots, \mathfrak{G}'_n \rangle), \\ \text{то } \text{Th}(\mathfrak{F}_i) = \text{Th}(\mathfrak{F}'_i), \dots, \text{Th}(\mathfrak{F}_n) = \text{Th}(\mathfrak{F}'_n), \\ \text{Th}(\mathfrak{G}_1) = \text{Th}(\mathfrak{G}'_1), \dots, \text{Th}(\mathfrak{G}_n) = \text{Th}(\mathfrak{G}'_n). \end{aligned}$$

В основе доказательства теоремы 2 лежит теоретико-модельное изучение когерентно полных полей, а именно доказательство того, что такие поля являются экзистенциально замкнутыми полями в классе n -кратно нормированных полей в подходящем формульном расширении сигнатуры.

Справедливо расширение этой теоремы и на случай p -адических нормирований. Возможно и естественное соединение теорем 1 и 2, если рассматривать n -кратно упорядоченные и одновременно m -кратно нормированные поля.

В работах ван ден Дриса [2] и Ершова [7] на основе соответственно теорем 1 и 2 указаны примеры алгебраических расширений поля $\mathbb{Q}$, имеющих разрешимые элементарные теории и отличные от ранее известных.

Интересным расширением упомянутых выше результатов об n -кратно упорядоченных полях является работа Джекоба

[1], в которой изучаются не независимые упорядочения, а поля с некоторой фиксированной «зависимостью» между конечным числом порядков, точное выражение которой может быть дано в терминах пространства порядков (см. Маршалл [1]). Оказалось, что класс таких полей имеет модельный компаньон с разрешимой теорией. А описание экзистенциально замкнутых полей в этом классе дается индуктивно в соответствии с индуктивным описанием конечных пространств порядков, данным в работе Маршалла [1]. Любопытным обстоятельством является то, что в таких полях возникают формульно определяемые кольца нормирований так, что если пространство порядков связно, то имеется гензелево кольцо нормирования, а если не связно, то система колец нормирований, соответствующих связным компонентам, является когерентно полной. Таким образом, разрешимость теории этого модельного компаньона может быть доказана индукцией с использованием сформулированных выше теорем 1 и 2.

ЛИТЕРАТУРА

- Адлер и Кифе (Adler A., Kiefe C.)
1. Pseudofinite fields, procyclic fields and model-completions. — Pacific J. Math., 1976, 62, p. 305—309.
- Акс (Ax J.)
1. Solving diophantine problems modulo every prime. — Ann. Math., 1967, 85, p. 161—183.
2. The elementary theory of finite fields. — Ann. Math., 1968, 88, p. 239—271.
- Акс и Кочен (Ax J., Kochen S.)
1. Diophantine problems over local fields, III: Decidable fields. — Ann. Math., 1966, 83, p. 437—456.
- ван дер Варден (van der Waerden B. L.)
1. Алгебра — 2 изд. — М.: Наука, 1979.
- Гашюи (Gaschütz W.)
1. Zu einem von B. H. and H. Neumann gestellten Problem. — Math. Nachr., 1956, 14, S. 249—252.
- Гончаров С. С.
1. Автоустойчивость моделей и абелевых групп. — Алгебра и логика, 1980, 19, № 1, с. 23—44.
- Грюнберг (Grunberg K. W.)
1. Projective profinite groups. — J. London Math. Soc., 1967, 42, № 1, p. 155—165.
- Грюнвальд и Сегал (Grunewald F. J., Segal D.)
1. The solubility of certain decision problems in algebra and arithmetic. — Bull. Amer. Math. Soc., 1979, 1, № 6, p. 915—918.
2. Some general algorithms, I: Arithmetic groups. — Ann. Math., 1982.
- Джарден (Jarden M.)
1. The elementary theory of ω -free Ax fields. — Invent. Math., 1976, 38, p. 187—206.
2. An analogue of Cebotarev density theorem for fields of finite corank. — J. Math. Kyoto Univ., 1980, 20, № 1, p. 141—147.

- Джарден и Кинне (Jarden M., Kiehne U.)
1. The elementary theory of algebraic fields of finite corank. — *Invent. Math.*, 1975, 30, p. 275—294.
- Джекоб (Jacob B.)
1. The model theory of «*R*-formal» fields. — *Ann. Math. Logic*, 1980, 19, № 3, p. 263—282.
- Добрица В. П.
1. О рекурсивно-номерованных классах конструктивных расширений и автоустойчивости алгебр. — *Сиб. матем. ж.*, 1975, 16, № 6, с. 1148—1154.
- ван ден Дрис (van den Dries L. P. D.)
1. Model theory for fields. — *Utrecht*, 1978.
2. New decidable fields of algebraic numbers. — *Proc. Amer. Math. Soc.*, 1979, 77, № 2, p. 251—253.
- Ершов Ю. Л.
1. Об элементарных теориях локальных полей. — *Алгебра и логика*, 1965, 4, № 2, с. 5—30.
2. Поля с разрешимой теорией. — *ДАН СССР*, 1967, 174, № 1, с. 19—20.
3. Теория нумераций, 3 (Конструктивные модели). — Новосибирск: изд. Новосибирск. гос. ун-та, 1974.
4. Теория нумераций. — М.: Наука, 1977.
5. Проблемы разрешимости и конструктивные модели. — М.: Наука, 1980.
6. Регулярно замкнутые поля. — *ДАН СССР*, 1980, 251, № 4, с. 783—785.
7. Кратно нормированные поля. — *ДАН СССР*, 1980, 253, № 2, с. 274—277.
8. О проконечных группах. — *Алгебра и логика*, 1980, 19, № 5, с. 552—565.
9. Об элементарных теориях регулярно замкнутых полей. — *ДАН СССР*, 1981, 257, № 2, с. 271—274.
10. Элиминированность кванторов в регулярно замкнутых полях. — *ДАН СССР*, 1981, 258, № 1, с. 16—20.
11. Алгебраические свойства регулярно замкнутых полей. — *Тр. матем. ин-та АН СССР им. В. А. Стеклова*, 158. М.: Наука, 1981, с. 80—86.
12. Неразрешимость регулярно замкнутых полей. — *Алгебра и логика*, 1981, 20, № 4, с. 389—394.
13. Кратно нормированные поля. — *УМН*, 1982, 37, № 3, с. 55—93.
14. Вполне вещественные расширения полей. — *ДАН СССР*, 1982, 263, № 5, с. 1047—1049.
- Зарисский и Самюэль (Zarissky O., Samuel P.)
1. Коммутативная алгебра, т. I. — М.: ИЛ, 1963.
- Кох (Koch H.)
1. Теория Галуа *p*-расширений. — М.: Мир, 1973.
- Ленг (Lang S.)
1. Алгебра. — М.: Мир, 1968.
- Маршалл (Marshall M.)
1. Classification of finite spaces of orderings. — *Canad. J. Math.*, 1979, 31, № 2, p. 320—330.
- Метакидес и Нерод (Metakides G., Nerode A.)
1. Effective content of field theory. — *Ann. Math. Logic*, 1979, 17, № 3, p. 289—320.
- Престел (Prestel A.)
1. Decidable theories of preordered fields. — *Math. Ann.*, 1982, 258, № 4, p. 481—492.
- Рабин (Rabin M. O.)
1. Computable algebra, general theory and theory of computable fields. — *Trans. Amer. Math. Soc.*, 1960, 95, № 2, p. 341—360.

- Робинсон (Robinson J.)
1. The undecidability of algebraic rings and fields. — *Proc. Amer. Math. Soc.* 1959, 10, p. 950—957.
- Сакс (Sacks G.)
1. Теория насыщенных моделей. — М.: Мир, 1976.
- Саркисян Р. А.
1. Проблема сопряженности для наборов целочисленных матриц. — *Матем. заметки*, 1979, 25, № 6, с. 811—824.
2. Алгоритмические вопросы для линейных алгебраических групп, I, II. — *Матем. сб.*, 1980, 113, № 2, 3.
- Сейденберг (Seldenberg A.)
1. Constructions in algebra. — *Trans. Amer. Math. Soc.*, 1974, 197, p. 273—313.
- Серр (Serre J. P.)
1. Когомологии Галуа. — М.: Мир, 1968.
- Тарский (Tarski A.)
1. Arithmetical classes and types of algebraically closed and real closed fields. — *Bull. Amer. Math. Soc.*, 1949, 55, p. 64.
2. A Decision Method for Elementary Algebra and Geometry. — 2nd revised ed. — Berkeley; Los Angeles, 1951.
- Уилер (Wheeler W. H.)
1. Model-complete theories of pseudo-algebraically closed fields. — *Ann. Math. Logic*, 1979, 17, № 3, p. 205—226.
- Уотерхаус (Waterhouse W. C.)
1. Profinite groups are Galois groups. — *Proc. Amer. Math. Soc.*, 1974, 42, № 2, p. 639—640.
- Фрёллих и Шепердсон (Fröhlich A., Shepherdson J. C.)
1. Effective procedures in field theory. — *Phil. Trans. Roy. Soc., London*, 1956, A248, p. 407—432.
- Фрид (Fried M.)
1. Toward a general theory of diophantine problems with application to *p*-adic fields and fields of finite corank. — *Irvine (U. S. A.)*, 1978, preprint.
- Фрид и Сакердот (Fried M., Sacerdote G.)
1. Solving diophantine problems over all residue class fields of a number field and all finite fields. — *Ann. Math.*, 1976, 104, p. 203—233.
- Харрингтон (Harrington L.)
1. Recursively presentable prime models. — *J. Symbolic Logic*, 1974, 39, № 2, p. 305—309.
- Хисамиев К. Г.
1. О сильно конструктивных моделях разрешимой теории. — *ИАН КазССР, сер. физ.-матем.*, 1974, № 1, с. 83—84.
- Холл (Hall M.)
1. Теория групп. — М.: ИЛ, 1962.
- Хупперт (Huppert B.)
1. Endliche Gruppen I. — Berlin; Heidelberg; N. Y.: Springer, 1967.
- Черлин, ван ден Дрис, Макинтайр (Cherlin G., van den Dries L., Macintyre A.)
1. Decidability and undecidability theorem for PAC-fields. — *Bull. Amer. Math. Soc.*, 1981, 4, № 1, p. 101—104.
2. The elementary theory of regular closed fields. — *New Haven (U. S. A.)*, 1982, preprint.

Алгоритм 10
— разрешающий 77
Алфавит 55
Аналог машины Тьюринга 136
— теоремы Чеботарева о плотности 303, 304
Арифметика второго порядка 121
— Пресбургера 85, 88

Вычисление детерминированное 107
— значения объекта 195
— недетерминированное 107
Вычислимость относительная 22

Гензелизация 349
Гипотеза Роджерса 119
Гомеоморфизм множеств рекурсив-
ный 129
Гомоморфизм 277
Грамматика двусмысленная 66
— контекстно свободная 66
— фразовая структурная 65
Группа Галуа поля 301
— допустимая 310
— конечно представляемая 61
— нормирования 348
— проконечная проективная 301
— финитно проективная 301
— рекурсивно представляемая 61

Дерево 98
— фундированное 232
Длина дерева 232
— нормы 251
— слова 104
Доказательство 29
— приоритетное 142, 152
Дополнение степени относительное 128

Зависимость эффективная алгебраи-
ческая 280
Заключение 65, 226

Игра 233
— Гейла-Стьюарта 123
Игрок 233
Идеал 116
Иерархия аналитическая 42
— арифметическая 40
Индекс функции 20, 187
Индукция немонотонная 257
— позитивная элементарная 249
Инструкция 10, 12
Итерация операции скачка 124

Категория нумерованных множеств 271
Квантор всеобщности 180
— дуальный 180, 255
— игровой 255
— монотонный 255
— на множестве 179, 255
— нетривиальный 255
— ограниченный 240
— Суслина 180
— существования 180
Класс групп инвариантный 62
— — наследственный 62
— — нетривиальный 62
— замкнутый 186, 215
— клиниевский 194
— конечных групп допустимый 306
— конструктивных моделей слабо
вычислимым 278
— нормированный 215, 251
— предикатов спекторовский 253
— тиговой немонотонный 259
— функционалов вычислимым 273
— — допускающих кодирование 188
— — конечно порожденный 189
— — нормальный 199
— — подходящий 169
— ω -параметризованный 215
Код функции 187
Кодирование кортежей 187
Кольцо гензелево 348
Компаньон 263
Композиция 170
Конструктивизация автоэквивалент-
ные 279
— эквивалентные 279

Конфигурация 18, 53
— остановки 18
Координатность конечная 314
Коранг 326
Корень дерева 232
— идеала 334

Лемма Гашюца 306
— о совместной индукции 172
— — числовом селекторе 192
Лента 12

Машина Тьюринга 12
— — универсальная 18
Местность 202
Метод интерпретаций 94
— переноса индексов 209, 211
— приоритета 37, 126
— — «с бесконечными нарушения-
ми» 120
— элиминации кванторов 85
Минимизация 171
Много-однозначность 27
Множество аналитическое 39, 43
— арифметическое 39
— диофантово 68
— индуктивно определенное 226,
229, 230
— корекурсивно перечислимое 128
— — — относительно степени 129
— креативное 36
— линейно упорядоченное 85
— максимальное 127
— морфизмов 271
— натуральных чисел 10, 114, 136
— независимое 116
— нетривиальное 69
— нормированное 186
— нумерованное 270
— определенное 38
— полуразрешимое 23
— полурекурсивное 24
— посылок 226
— правил детерминированное 228
— — регулярное арифметическое 237
— — — элементарное 243
— — рекурсивно перечислимое 236
— — рекурсивное 236
— — A -финитарное 260
— — Φ -замкнутое 226
— — Φ -плотное 234
— простое 36
— рекурсивно перечислимое (р.п.)
25, 126
— — — относительно степени 115
— — слов рекурсивно перечислимое 61

Множество степеней 115
— — определенное 123
— — слабо определенное 124
— — точечное типа k 214
— эффективно перечислимое 24
— α -конечное 138, 139
— α -рекурсивно перечислимое 137,
139
— α -рекурсивное 137, 139
Модель простая 92
— с неограниченными ветвлениями
279
Морфизм 270
Мощность модели 90

Набор корней идеала полный 335
Накрытие 306
Номер гёделев 29
Норма 251
— на предикате 185
Нормирование 348
Нумерация вычисляемая 271, 272, 276,
278
— — главная 271, 272
— Клини 202
— множества 270
— Поста 271

Область поля универсальная 331
Обозначение ординала 46
Образующие представления 59
Объект высшего типа 193
—, рекурсивный по Клини относи-
тельно объекта 213
— типа 2 177
— Туге 177
Одно-однозначность 27
Оператор, допускающий кодирова-
ние сечениями 244
— дуальный 234
— монотонный 167, 216, 229
— рекурсивный 48
— x -базируемый 231
Операция скачка 114
— сцепления 55
Описание мгновенное 18
Определение индуктивное 224
— — немонотонное 257
— — финитарное 227
— — функционала 169
— — частичной функции 169
— — разбором случаев 170
Определимость неявная инвариантная
141
Оракул 22

- Ординал допустимый 137
 — рекурсивный Мало 258
 — — недостижимый 258
 — — счетный 43
 — ω_1 46
 — фундированной части 228
 — Чёрча — Клини 238
 Отображение $\mathcal{X}$ -рекурсивное 196
 Пара точная 118
 — эпиморфизмов максимальная 307
 — α -р.п. степеней минимальная 143
 Переменная 65
 Подполе конструктивное 276
 Подстановка проектирований 170
 — сцеплений 195
 — точечных проектирований 195
 — функциональная 171
 Подфункционал 205
 Поле Гензельево 348
 — действительных чисел 91
 — когерентно полное 349
 — нормированное 348
 — регулярное замкнутое 296
 — упорядоченное вещественно замкнутое 91
 — n -кратно нормированное 349
 Полурекурсивность относительная 32
 Полушка вычислимых нумераций 271
 — классов эквивалентных вычислимых нумераций 272
 — степеней верхняя 114, 115
 — m -степеней верхняя 271
 — α -степеней верхняя 142
 Последовательность функционалов нормальная 184, 200
 Правило 226
 Предикат алгебраический 88
 — гиперэлементарный 252
 — диофантов 68
 — полиномиальный 88
 — полурекурсивный относительно Φ 178
 — разрешимый 17
 — рекурсивно перечислимый (р.п.) 53
 — рекурсивный 13, 23
 — универсальный 25
 — фундированный 227
 — A -конечный 260
 — $\mathcal{E}$ -индуктивный 244
 — $\mathcal{F}$ -определенный 240
 — $\mathcal{F}$ -полурекурсивный 178, 185
 — $\mathcal{F}$ -рекурсивный 185
 Предложение маркированное 243
 Представление 59
 — групповое 61
 Принцип Ф-индукции 227
 Проблема выполнимости 108
 — Гильберта десятая 51, 67, 69
 — неразрешимая 51
 — обобщенной конечности 138, 139
 — основная для корекурсивно перечислимых множеств 128
 — остановки 20, 52
 — Поста 34, 37, 126, 142
 — разрешимости 51, 70, 71, 77, 78
 — — элементарных теорий 269
 — Сакса 116
 — слов 55, 61
 — соответствия 63
 — спектра 82
 — P 272
 — $P = NP$ 82, 109
 Программа 10
 — Гильберта 80
 — недетерминированная 107
 Продолжение конструктивизации 275
 Продукция 55
 — обратная 58
 — полутуэвская 55
 Проектирование 170, 263
 — точечное 195
 Проекция 40
 — ординала 148, 149, 151
 Пространство точек объектов вышших типов 194
 Протокол вычисления 18
 Процедура разрешающая 78
 — эффективная 10
 Процесс полутуэвский 55
 — туэвский 59
 Про- $\mathcal{G}$ -группа 309
 Пятёрка 14, 53
 Разложение 263
 Ранг 89
 Расширение поля регулярное 296
 Рекурсивность в 33
 — относительная 32, 114
 — по Клини 196
 — — относительная 196
 — — Клини, 205
 Рекурсия примитивная 172
 — сводная 201
 Релятивизация 95, 169
 — игрового квантора 256
 — к степени 118
 — I 118
 Решетка α -р.п. множеств 143
 Сверхскачок 220
 Сводимость 27, 271
 — нумераций 271

- Сводимость по Тьюрингу 33, 114
 — точечных множеств 216
 Свойство замены 328
 — коамальгамируемости 306
 — минимальности 169
 — параметризации 249
 — перечисления 187, 215
 — предполнеупорядоченности 186, 215
 — (F) 281
 Семейство p -зависимое 327
 — p -независимое 327
 Сечение 244
 Сигнатура функционала 168
 Символ 12, 55
 — начальный 65
 Система автоустойчивая 279
 — индуцированная 95
 — конструктивизируемая 273
 — конструктивно устойчивая 279
 — нумерованная 273
 — — конструктивная 273
 — — сильно конструктивная 273
 — обозначений Клини для рекурсивных ординалов 238
 — ординальных обозначений 46
 — почти приемлемая 253
 — приемлемая 253
 — проектируемая 263
 — разложимая 263
 — сильно конструктивизируемая 273
 — соответствия Поста 63
 — степеней полная 125
 — универсальная 190
 — — хорошая 191, 201
 — F -приемлемая 241
 — Q -приемлемая 256
 Скачок 34
 Слово 55, 98
 — Поста 56
 Сложность внутренняя 104
 Соотношение 59
 «Соревнование по трудолюбию» Радо 14
 Состояние 12
 — начальное 18
 Степень 112
 — высокая 127
 — клиниевская 213
 — конструктивная 122
 — минимальная 117
 — множества 114
 — неконструктивности 122
 — неразрешимости 33, 112
 — низкая 127
 — почти рекурсивная 130
 — расщепляемая 119
 Степень рекурсивно перечислимая (р.п.) 34, 126
 — — относительно степени 115
 — рекурсивных функций 114
 — тьюрингова 112
 — функции 114
 — чащеобразная 119
 — n -точная над I 125
 Страт Галуа 331, 332
 Стратегия выигрышная 123, 233
 Стратификация 334
 Сужение функционала 176
 Схема кодирующая 241
 — $\mathcal{F}$ -определяемая 241
 Сцепление 193
 Таг-проблема 67
 Таг-система 67
 Тезис Чёрча 15
 Теорема 29
 — Гёделя о неполноте 81
 — Клини обобщенная 251
 — Матиясевича 68
 — о дереве 98
 — — нормальной форме 19
 — — для приемлемой системы 254, 255
 — — параметризации 26
 — — перечисления 189, 200
 — — плотности р.п. степеней 126
 — — α -р.п. степеней 143
 — — пошаговом сравнении 182
 — — — вторая 254
 — — — первая 251
 — — предполнеупорядоченности 186
 — — разложения 142, 144
 — — рекурсии 28
 — — — вторая 191, 201
 — — — первая 174
 — — транзитивности 43
 — — функциональной подстановке 173
 — — частичных подстановках 208
 — — ядре 275
 — об иерархии 41
 — — индукционной полноте 175
 — — обращении 120
 — — ограниченном кванторе 72
 — — операции скачка 152
 — — униформизации 151
 — — ускорении 21
 — Спектора — Ганди обобщенная 254
 Теория аксисматизированная 89
 — алгебраически замкнутых полей 90, 275
 — булевых алгебр 101

- Теория вещественно замкнутых полей 91, 92
 — вполне упорядоченных множеств 100
 — второго порядка вполне упорядоченных множеств 100
 — — — линейно упорядоченных множеств 99
 — — — монадическая 97
 — — — слабая 97
 — действительных чисел 88, 269
 — дискретного порядка 85
 — заданная аксиоматически 82
 — — семантически 82, 84
 — категоричная в мощности 89
 — коммутативных групп 94
 — комплексных чисел 269
 — конечных полей 94, 269
 — линейно упорядоченных множеств 85, 94, 99
 — модельно полная 92
 — мультипликативной полугруппы целых чисел 94
 — неразрешимая 79
 — полная 30, 83
 — поля p -адических чисел 93, 269
 — разрешимая 78
 — рациональных чисел 90, 269
 — регулярно замкнутого поля 324
 — рекурсивно аксиоматизируемая 30
 — р.п. степеней 127
 — системы 84
 — сложения натуральных чисел 85
 — степеней 122
 — — глобальная 125
 — — локальная 125
 — стратов Галуа 333
 — умножения натуральных чисел 107
 Техника блочная 162
 Тип точки 193
 Точка 193
 — неподвижная 168, 169
 — $\mathcal{F}$ -неподвижная 169
- Формула ограниченная элементарная 240
 —, определяющая оператор 246
 — универсально истинная 242
 — экзистенциальная 240
 — элементарная 240
 — Q -элементарная 256
 —, T -представляющая предикат 239
 — Π^1_n -пренексная 240
 — Σ^1_n -пренексная 240
- Функционал 168
 — вычисления значения функции 170
 — добавления переменных 170
- Функционал нормальный 182
 — оперативный 169
 — рекурсивный 22
 — $\mathcal{F}$ -рекурсивный 169
- Функция алгебраическая 88
 — всюду определенная 10
 — декодирующая 18
 — длины 195
 — кодирующая 18, 236
 — нигде не определенная 167
 — общерекурсивная 16
 — перехода 12
 — повышения типа 194
 — понижения типа 194
 — пошагового сравнения 182
 — предельно рекурсивная относительно функции 115
 — предшествования 172
 — примитивно рекурсивная 16
 — продуктивная 36
 — производящая 23
 — распознавания типа 195
 — рекурсивная 10, 13, 22
 — следования 98, 170
 — тождественная 170
 — универсальная 187
 — характеристическая множества 170
 — — равенства 170
 — частичная 10, 167
 — эффективно вычислимая 10
 — $\mathcal{H}$ -рекурсивная 195
 — α -рекурсивная 137
 — λ -определимая 16
- Характер точки 204
- Цепочка 55
 — пустая 55
- Часть предиката фундирования 227
- Числа действительные рекурсивные 47
 — натуральные 136
- Эквивалентность конструктивных моделей 278
 — нумераций 271
 — нумерованных систем 278
 — по Тьюрингу 33
- Элемент сглаживающий 331
 — Φ -алгебраический 274

- Ядро 233, 234
 Язык второго порядка монадический 97
 — — — — слабый 97
 — первого порядка полный 240
 —, порожденный полутуэвским процессом 65
 Ячейка памяти 12
- A -множество 43
 A -правило 242
 k -класс точечный 214
 k -оболочка 214
 k -сечение 214
 L -группа разложений гомоморфизма 333
 m -сводимость кратная 272
 n -страт Галуа 332
 p -базис 328
 Q -правило 256
 s - m -теорема 26, 191, 200
 s - m - n -функция 191
 Θ -группа 309
 α -вычислимость 141
 α -конечность 139
 α^* -конечность 144
 α -рекурсивность относительная 141
 — слабая 142
- α -р.п. степень 149
 α -сводимость 140
 α -степень 142
 Γ -норма 186, 251
 Δ_n -класс 41
 Δ^1_n -класс 42
 Δ^1_2 -ординал 257
 Π_n -класс 40
 Π^1_n -формула 240
 Π^1_1 -класс 42
 Σ_n -класс 40
 Σ^1_n -класс 42
 Σ^1_n -формула 240
 Σ_1 -множество правил 260
 Σ_1 -формула 260
 $\Sigma_1(\mathcal{U})$ -множество правил 242
 Σ_2 -кофинальность 147
 σ -кольцо эффективное 238
 Φ -доказательство 227, 232
 Φ -индукция 227
 Φ -ядро 274, 275
 ϕ -доказательство 231
 ϕ -квазидоказательство 261
 ω -правило 237

ОГЛАВЛЕНИЕ

Предисловие редактора русского перевода	5
Введение	7
Глава 1. ЭЛЕМЕНТЫ ТЕОРИИ РЕКУРСИИ. <i>Герберт Б. Эндертон</i>	9
Глава 2. НЕРАЗРЕШИМЫЕ ПРОБЛЕМЫ. <i>Мартин Девис</i>	51
Глава 3. РАЗРЕШИМЫЕ ТЕОРИИ. <i>Михаэль О. Рабин</i>	77
Глава 4. СТЕПЕНИ НЕРАЗРЕШИМОСТИ. ОБЗОР РЕЗУЛЬТАТОВ <i>Стивен Г. Симпсон</i>	112
Глава 5. ТЕОРИЯ α -РЕКУРСИИ. <i>Ричард А. Шор</i>	134
Глава 6. РЕКУРСИЯ В ВЫСШИХ ТИПАХ. <i>Александр С. Кекрис, Янис Н. Московакис</i>	166
Глава 7. ВВЕДЕНИЕ В ТЕОРИЮ ИНДУКТИВНЫХ ОПРЕДЕЛЕНИЙ. <i>Петер Ацел</i>	224
Дополнение. АЛГОРИТМИЧЕСКИЕ ПРОБЛЕМЫ В ТЕОРИИ ПОЛЕЙ (положительные аспекты). <i>Ю. Л. Ершов</i>	269
Предметный указатель	354

СПРАВОЧНАЯ КНИГА ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ

Часть III

ТЕОРИЯ РЕКУРСИИ

Редактор В. В. Донченко

Технический редактор С. Я. Шкляр. Корректор Т. С. Вайсберг

ИБ № 11561

Сдано в набор 09.03.82. Подписано к печати 21.10.82. Формат 60×90¹/₁₆. Бумага тип. № 1. Литературная гарнитура. Высокая печать. Условн. печ. л. 22,5. Уч.-изд. л. 24,15. Тираж 20000 экз. Заказ № 2312 Цена 2 р.

Издательство «Наука»

Главная редакция физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15.

Отпечатано с матриц Ленинградской типографии № 2 головного предприятия в Ленинградской типографии № 4 ордена Трудового Красного Знамени Ленинградского объединения «Техническая книга» им. Евгения Соколовой Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 191208, Ленинград, Социалистическая ул., 14.