МАТЕМАТИЧЕСКАЯ ЛОГИКА И ОСНОВАНИЯ МАТЕМАТИКИ

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
Москва 1973

ЭЛЕМЕНТЫ МАТЕМАТИЧЕСКОЙ ЛОГИКИ

П. С. НОВИКОВ

ИЗДАНИЕ ВТОРОЕ, ИСПРАВЛЕННОЕ

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1973

517
Н 73
УДК 164

Н $\frac{0223-1842}{042(02)-73}$ 63-73

ОГЛАВЛЕНИЕ

Предисловие ко второму изданию 7

Введение 9

Глава I. **Алгебра высказываний** 36

§ 1. Логические операции (36). § 2. Равносильность формул (41). § 3. Закон двойственности (47). § 4. Проблема разрешения (49). § 5. Представление произвольной двузначной функции посредством формул алгебры высказываний (56). § 6. Совершенные нормальные формы (59).

Глава II. **Исчисление высказываний** 66

§ 1. Понятие формулы (66). § 2. Определение выводимых формул (72). § 3. Теорема дедукции (80). § 4. Некоторые правила исчисления высказываний (83). § 5. Монотонность (87). § 6. Эквивалентные формулы (90). § 7. Некоторые теоремы о выводимости (98). § 8. Связь между формулами алгебры высказываний и исчисления высказываний (104). § 9. Непротиворечивость исчисления высказываний (107). § 10. Полнота исчисления высказываний (109). § 11. Независимость аксиом исчисления высказываний (111).

Глава III. **Логика предикатов** 123

§ 1. Предикаты (123). § 2. Кванторы (128). § 3. Теоретико-множественный смысл предикатов (132). § 4. Аксиомы (136). § 5. Непротиворечивость и независимость аксиом (139). § 6. Взаимно однозначное соответствие областей (142). § 7. Изоморфизм областей и полнота систем аксиом (145). § 8. Аксиомы натурального ряда (149). § 9. Нормальные формулы и нормальные формы (155). § 10. Проблема разрешения (159). § 11. Логика предикатов с одной переменной (160). § 12. Конечные и бесконечные области (168). § 13. Разрешающие функции (функции Сколема) (172). § 14. Теорема Лёвенгейма (178).

Глава IV. **Исчисление предикатов** 183

§ 1. Формулы исчисления предикатов (183). § 2. Замена переменных в формулах (190). § 3. Аксиомы исчисления предикатов (192). § 4. Правила образования выводимых формул (193).

§ 5. Непротиворечивость исчисления предикатов (202). § 6. Полнота в узком смысле (209). § 7. Некоторые теоремы исчисления предикатов (213). § 8. Теорема дедукции (216). § 9. Дальнейшие теоремы исчисления предикатов (221). § 10. Эквивалентные формулы (230). §. 11. Закон двойственности (235). § 12. Нормальные формы (239). § 13. Дедуктивная эквивалентность (243). § 14. Нормальные формулы Сколема (244). § 15. Доказательство теоремы Сколема (251). § 16. Теорема Мальцева (253). § 17. Проблема полноты исчисления предикатов в широком смысле (261). § 18. Замечание о формулах без кванторов (262). § 19. Теорема Гёделя (264). § 20. Система аксиом в исчислении предикатов (273).

Глава V. **Аксиоматическая арифметика** 280

§ 1. Термы. Расширенное исчисление предикатов (280). § 2. Свойства предиката равенства и предметных функций (283). § 3. Отношение эквивалентности (287). § 4. Теорема дедукции (289). § 5. Аксиомы арифметики (290). § 6. Примеры выводимых формул (292). § 7. Рекурсивные термы (296). § 8. Ограниченная арифметика (298). § 9. Рекурсивные функции (303). § 10. Аксиоматическая и содержательная выводимость свойств арифметических функций (305). § 11. Рекурсивные предикаты (310). § 12. Другие способы образования рекурсивных предикатов. Ограниченные кванторы (312). § 13. Приемы образования новых рекурсивных термов (314). § 14. Некоторые теоретико-числовые предикаты и термы (318). § 15. Вычислимые функции (322). § 16. Некоторые теоремы аксиоматической арифметики (327).

Глава VI. **Элементы теории доказательства** 335

§ 1. Постановка вопроса о непротиворечивости и независимости аксиом (335). § 2. Простые множители и простые слагаемые (337). § 3. Примитивно истинные формулы (338). § 4. Операции 1, 2, 3 (342). § 5. Регулярные формулы (345). § 6. Некоторые леммы о регулярных формулах (353). § 7. Операции, двойственные операциям 1, 2, 3 (368). § 8. Свойства операций 1*, 2*, 3* (370). § 9. Регулярность формул, выводимых в арифметике (378). § 10. Непротиворечивость ограниченной арифметики (382). § 11. Независимость аксиомы полной индукции в арифметике (383). § 12. Усиленная теорема о независимости аксиомы полной индукции (385).

Предметный указатель 397

ПРЕДИСЛОВИЕ КО ВТОРОМУ ИЗДАНИЮ

Интенсивное развитие математической логики в последнее время сопровождается увеличением ее роли в математике.

Одной из основных задач математической логики остается анализ оснований математики. Но в настоящее время она уже вышла из рамок этой задачи и оказала существенное влияние на развитие самой математики. Из ее идей возникло точное определение понятия алгоритма, что позволило решить многие вопросы, которые без этого оставались бы в принципе неразрешимыми. Возникший в математической логике аппарат нашел приложение в вопросах конструкций вычислительных машин и автоматических устройств.

Со времени выхода в свет первого издания настоящей книги прошло 14 лет. За это время задача ознакомления широкого круга математиков с основами математической логики стала еще более актуальной. В настоящей книге была сделана попытка дать по возможности доступное изложение основ математической логики. Этой задаче посвящены первые пять глав книги, составляющие ее основное содержание. Последняя, шестая, глава носит более специальный характер и уже не является столь элементарной. В ней рассматриваются методы теории доказательства, посредством которых решаются некоторые вопросы математической логики, возникающие в основном тексте книги.

Настоящее издание по содержанию не отличается от первого издания. В нем исправлены опечатки и заменены устаревшие термины. В частности, удален термин «*истинная* в данном исчислении формула», который в первом издании использовался как синоним термина «*выводимая* в данном исчислении формула». Таким образом, исключена возможность смешения этого понятия с содержательной истинностью формул.

Книга не претендует на полноту освещения всех развивающихся в настоящее время важных направлений в математической логике. Некоторые из этих направлений не затронуты вовсе. С разделами математической логики, которые не отражены в настоящей книге, читатель сможет ознакомиться по книгам:

С. К. Клини, Введение в метаматематику, ИЛ, 1957.

А. И. Мальцев, Алгоритмы и рекурсивные функции, «Наука», 1965.

А. А. Марков, Теория алгорифмов, Труды Матем. ин-та АН СССР им. В. А. Стеклова, Изд-во АН СССР, 1954.

Э. Мендельсон, Введение в математическую логику, «Наука», 1971.

П. С. Новиков

ВВЕДЕНИЕ

В современной математике большое распространение получил так называемый аксиоматический метод. Источником его следует считать открытие Лобачевским неевклидовой геометрии. К настоящему времени аксиоматический метод прошел большую эволюцию, придя в соприкосновение с другими идеями, и породил не только новые методы, но и новые принципы математического мышления. Развитие аксиоматического метода можно разбить на два этапа. Первый продолжается от Лобачевского до работ Гильберта по основаниям математики*), второй — от этих работ Гильберта до наших дней. Этот второй этап представляет собой соединение идей, идущих из геометрии, с развивавшимся параллельно учением, известным под названием «символической» или «математической» логики. В результате возникла новая дисциплина, сохранившая название математической логики.

Прежде чем говорить о самой математической логике, мы рассмотрим вкратце предшествующее ей состояние аксиоматического метода и постараемся уяснить, хотя бы в самых общих чертах, причины возникновения этого метода и стоящие перед ним задачи. Сущность аксиоматического метода состоит в своеобразном способе определить математические объекты и отношения между ними. Предположим, что, изучая систему каких-то объектов, мы употребляем определенные термины, выражающие свойства этих объектов и отношения между ними. При этом мы не определяем ни сами объекты, ни эти свойства и отношения, а высказываем ряд

*) В русском переводе эти работы вышли в 1948 г. (см. Д. Гильберт, Основания геометрии, добавления VI—X).

определенных утверждений, которые должны для них выполняться. Очевидно, эти утверждения выделяют из всевозможных систем объектов, их свойств и отношений между ними такие системы, для которых они выполнены.

Таким образом, сделанные утверждения можно рассматривать как определения системы объектов определенного класса, их свойств и отношений между ними.

Рассмотрим простой пример, с которым нам и в дальнейшем часто придется встречаться. Пусть дана система каких-то объектов, которые мы будем обозначать буквами латинского алфавита, и между ними установлено отношение, выражаемое термином «предшествует». Не определяя ни объектов, ни отношения «предшествует», мы высказываем для них следующие утверждения.

1. *Никакой объект не предшествует сам себе.*

2. *Если x предшествует y, а y предшествует z, то x предшествует z.*

Нетрудно видеть, что существуют системы объектов с таким отношением между ними, что если под термином «*x предшествует y*» понимать данное отношение, то наши утверждения окажутся истинными.

Пусть, например, объектами x, y, ... являются люди, а отношение между x и y представляет собой «x старше y». В таком случае, если «x предшествует y» означает «x старше y», то утверждения 1 и 2 истинны.

Или объектами являются действительные числа, а отношение «x предшествует y» представляет собой «x меньше y». Здесь утверждения 1 и 2, очевидно, также выполнены.

Системы объектов с одним отношением, для которых положения 1 и 2 выполнены, образуют определенный класс, а положения 1 и 2 мы можем рассматривать как определение систем этого класса. Утверждения, посредством которых мы таким образом выделяем совокупность объектов, носят названием аксиом. Если для какой-либо совокупности объектов, их свойств и отношений некоторые аксиомы истинны, то говорят, что данная совокупность объектов удовлетворяет системе этих аксиом, или является интерпретацией данной системы аксиом.

Делая логические выводы из аксиом, мы будем получать утверждения, истинные для любой системы объектов, удовлетворяющей данным аксиомам.

Более значительным примером аксиоматического определения является система аксиом геометрии. Рассматриваемую систему объектов будем разделять на три класса: *«точки»*, *«прямые»* и *«плоскости»* — и будем употреблять для них термины: «точка a принадлежит прямой A», «прямая A принадлежит плоскости $\mathfrak{A}$», «точка a лежит между точками b и c» и другие, выражающие отношения между объектами системы. Вместе с тем, употребляя эти термины, мы не будем вкладывать в них смысла пространственных отношений, а вместо этого выскажем для них некоторую систему аксиом. Это можно сделать по-разному, но существует вполне определенная система аксиом, носящая название «системы аксиом геометрии Евклида». Эта система была предложена Гильбертом. Мы не будем здесь приводить эти аксиомы. Их можно найти в книгах по основаниям геометрии. В этих аксиомах высказаны все те предпосылки, которые явным или неявным образом употреблялись при доказательстве теорем геометрии Евклида. Таким образом, выводимые из этих теорем следствия адекватно выражают свойства евклидова пространства, интуитивное представление о котором было почерпнуто из непосредственного опыта и существует издавна в умах людей.

Ясно, что соответствие между аксиомами и предметами реальности всегда имеет приближенный характер. Если мы, например, поставим вопрос, удовлетворяет ли реальное физическое пространство аксиомам геометрии Евклида, то предварительно мы должны дать физические определения геометрических терминов, содержащихся в аксиомах, как-то: «точка», «прямая», «плоскость» и др. Иными словами, нужно указать те физические реальности, которые этим терминам соответствуют. После этого аксиомы превратятся в физические утверждения, которые можно подвергнуть экспериментальной проверке. После такой проверки мы можем ручаться за истинность наших утверждений с той степенью точности, какую обеспечивают измерительные приборы.

При рассмотрении любой системы аксиом возникает ряд вопросов, которые, в частности, могут решаться и с помощью интерпретаций. Один из этих вопросов — вопрос о непротиворечивости системы аксиом. Мы всегда должны быть уверены, что, делая всевозможные выводы из данной системы аксиом, не придем к противоречию, т. е. не выведем какие-либо несовместимые утверждения. Появление противоречия означало бы, что рассматриваемой системе аксиом не может удовлетворять никакая система объектов и, таким образом, эти аксиомы ничего не описывают. Непротиворечивость системы аксиом может быть доказана построением какой-нибудь точной интерпретации этой системы. Следует заметить, что в догильбертовском аксиоматическом методе это был единственный способ доказательства непротиворечивости.

Аналогично обстоит дело и с вопросом о независимости аксиом. Какая-либо аксиома называется независимой в данной системе аксиом, если она невыводима из остальных аксиом этой системы. Для доказательства независимости какой-либо аксиомы достаточно найти систему объектов, удовлетворяющую всем аксиомам, кроме исследуемой, и не удовлетворяющей этой последней. Иными словами, для доказательства независимости аксиомы требуется найти интерпретацию системы аксиом, полученной из рассматриваемой после замены исследуемой аксиомы ее отрицанием. Поэтому, для того чтобы пользоваться системой аксиом, необходимо иметь заранее такие объекты, свойства и отношения, которые могут служить точной интерпретацией этой системы аксиом.

Интерпретации систем аксиом черпаются из круга математических понятий. *Мощным источником интерпретаций для всевозможных систем аксиом является теория множеств.*

Мы не можем здесь сколько-нибудь подробно вдаваться в изложение теории множеств. Укажем только в самых общих чертах, какими именно объектами она располагает.

Исходными объектами являются натуральные числа. Из совокупности натуральных чисел можно при помощи теоретико-множественных принципов строить новые множества и функции. Укажем некоторые основные принципы построения множеств.

1. Если дано множество объектов, то посредством точно сформулированного признака можно выделить из

него подмножество, т. е. некоторую его часть. Например, из множества всех натуральных чисел можно выделить часть — множество всех простых чисел.

2. Если имеется какая-то совокупность множеств, то можно получить новое множество, объединив все элементы всех этих множеств.

3. Для каждого множества можно образовать множество всех его подмножеств.

4. Допустим, что в силу некоторого признака каждому элементу множества E поставлен в соответствие какой-то элемент множества G. Такое соответствие называется функцией. При этом говорят, что рассматриваемая функция определена на множестве E и принимает значение из множества G. Функции также являются объектами, из которых можно строить множества. В частности, можно образовать множество всех функций, определенных на E и принимающих значения из G.

Перечисленные принципы не исчерпывают всех возможных средств построения теоретико-множественных объектов. Но для дальнейшего изложения мы можем ограничиться описанными здесь средствами. При помощи теоретико-множественных принципов, исходя из совокупности натуральных чисел, рассматриваемой как исходное множество, можно построить все существующие математические понятия. Отсюда же черпаются и интерпретации для систем аксиом.

Возникает вопрос: *является ли теория множеств вполне надежным основанием для аксиоматического метода? В какой мере мы можем быть уверены в непротиворечивости самой теории множеств?*

Эта дисциплина, возникшая в конце прошлого столетия, быстро развиваясь, оказала огромное влияние на математику и имела особенное значение в вопросах оснований математики. Но уже в самом начале возникновения теории множеств было замечено, что использование без всяких ограничений создаваемых ею понятий приводит к противоречию. Это обстоятельство не остановило развития теории множеств, так как в тех пределах, в которых обычно пользуются ее понятиями, противоречий не возникало. Но и дальнейший анализ основ теории множеств не дал никаких удовлетворительных оснований для уверенности, что и в дальнейшем, хотя бы в рамках фактического пользования идеями теории множеств, не может возникнуть противоречие. Таким образом, утверждение об отсутствии противоречий в пределах существующих теоретико-множественных построений является эмпирическим заключением, для которого не имеется достаточно веских оснований. В результате приходится констатировать, что, несмотря на весьма успешное обслуживание теорией множеств аксиоматического метода, основания, на которых она сама строится, неудовлетворительны. Отправляясь от указанных затруднений, дальнейшая критика обратила внимание на одну существенную особенность теории множеств или, лучше сказать, на особенность математического мышления вообще, но проявившуюся наиболее ясно при развитии теории множеств. Речь идет об идее бесконечности, являющейся одним из самых основных элементов математического мышления. В античной математике по отношению к бесконечности была проявлена осторожность. Был произведен в известной мере логический анализ понятий, связанных с бесконечностью. Это выразилось в появлении известных антиномий об «Ахиллесе и черепахе», «летящей стреле», «бесконечной делимости» и др. Осторожность выразилась в требованиях большой строгости, предъявленных к употреблению бесконечности в математических рассуждениях. Современный математический анализ в самом начале своего возникновения под влиянием требований естественных наук и техники стал обращаться с бесконечностью с гораздо большей свободой и меньшей строгостью. Благодаря этому он получил возможность быстро и широко развиваться и сыграть огромную роль в самых разнообразных отраслях науки и в практике. При этом в нем то и дело всплывали трудности, связанные с идеей бесконечности. Эти трудности каждый раз вызывали к жизни критику соответствующих понятий анализа. Наиболее полно это критическое направление выразилось на последнем своем этапе, а именно в трудах Кронекера, Бореля, Лузина и Брауэра. Форма бесконечности, которая лежит в основе теоретико-множественных представлений, получила название «актуальной бесконечности». Прежде чем уточнять это понятие, попытаемся его себе представить при помощи грубого и логически несовершенного описания. Под термином *«актуальная бесконечность»* понимается бесконечная совокупность, построение которой завершено и элементы которой представлены одновременно. Мы будем, например, иметь дело с актуальной бесконечностью, если пересчитаем весь натуральный ряд полностью. Если бы можно было производить любое бесконечное множество строго отделенных друг от друга актов, то не существовало бы никаких математических проблем. Каждая из них была бы решена непосредственной проверкой всех возможных случаев. Идеализированный характер понятия актуальной бесконечности совершенно ясен. Построение бесконечного числа отдельных предметов, выполнение бесконечного числа актов неосуществимо не только в силу недостатка практических средств, но и принципиально не может быть осуществлено никогда и никакими средствами. Вместе с тем математическое мышление широко использует эту идеализацию, например представляя геометрическую фигуру как бесконечную совокупность точек, отрезок времени как бесконечную совокупность моментов, движение как бесконечную совокупность отдельных положений движущегося тела и т. д.

Конкретное проявление идеи актуальной бесконечности состоит в распространении на бесконечность некоторых логических принципов, которые являются совершенно бесспорными в области конечного. Одним из таких принципов является, например, известный закон исключенного третьего, который формулируется следующим образом: *пусть* $\mathfrak{A}$ *— некоторое утверждение, а* $\overline{\mathfrak{A}}$ *— его отрицание*; *тогда справедливо одно из утверждений* $\mathfrak{A}$ *или* $\overline{\mathfrak{A}}$. Предположим, что $\mathfrak{A}$ есть высказывание о предметах бесконечной совокупности, например о всех натуральных числах. Если бы мы могли произвести бесконечное число актов проверки, то легко выяснили бы, что́ именно верно — $\mathfrak{A}$ или $\overline{\mathfrak{A}}$. Предположение о возможности удостовериться, что для любого суждения $\mathfrak{A}$ верно оно или его отрицание, представляет собой частичную замену гипотезы о возможности бесконечного числа актов проверки. Такую же роль играет в теории множеств и абсолютное понимание термина «существование» в применении к бесконечным совокупностям. Для теории множеств характерны теоремы чистого «существования», когда доказывается существование какого-то объекта без того, чтобы этот объект указывался или строился. Такие доказательства часто бывают связаны именно с употреблением закона исключенного третьего.

Рассмотрим пример такого доказательства. Построим бесконечную последовательность целых неотрицательных чисел, связанную с разложением числа $\pi = 3,14\ldots$ в десятичную дробь. Каждый член a_n последовательности определим в зависимости от n-го знака в разложении π. Если n-й знак разложения равен нулю, то соответствующее ему число a_n полагаем также равным нулю. Числа $a_1, a_2, \ldots$ до первого нуля положим равными единице. После того как появился первый нуль (или несколько нулей подряд), следующие числа, отвечающие знакам, не равным нулю, — вплоть до нового нуля — положим равными двум. Затем, после появления нуля (или нескольких нулей подряд), все числа, соответствующие знакам, не равным нулю, — до нового нуля — положим равными трем и т. д. Вообще, если числа последовательности, предшествующие нулю (или группе из нескольких нулей подряд), равны k, то числа последовательности, последующие за этим нулем до следующего нуля, равны $k+1$. Таким образом, мы получим последовательность следующего (примерно) вида:

$$1, \ldots, 1, 0, 2, \ldots, 2, 0, \ldots, k, \ldots, k,$$
$$0, \ldots, 0, k+1, \ldots$$

Докажем, что существует число, которое повторится в этой последовательности бесконечное количество раз. В самом деле, в разложении числа π имеется или конечное число нулей, или бесконечное. В первом случае в последовательности найдется число a_n с наибольшим номером n, равное нулю. После него все числа последовательности равны между собой, и, следовательно, число a_{n+1} повторяется в ней бесконечное число раз. Если в разложении числа π содержится бесконечное количество знаков, равных нулю, то и в нашей последовательности нуль повторится бесконечное количество раз. Таким образом, существование числа, повторяющегося в построенной последовательности бесконечное количество раз, установлено. Однако на вопрос — каково это число — мы ответить не можем, так как неизвестно, содержится ли в разложении π конечное или бесконечное количество нулей. К решению такой задачи не видно никакого подхода. Таким образом, здесь мы имеем пример, когда из доказательства существования некоторого объекта мы никак не можем извлечь указания самого объекта. Это обстоятельство явно связано с актуальной бесконечностью, так как при рассмотрении конечных образований, если существование какого-то объекта доказано, всегда можно отыскать этот объект фактической проверкой всех возможных случаев.

На первый взгляд при рассмотрении таких примеров может показаться, что имеется несоответствие идеи актуальной бесконечности с действительностью. На самом деле это подчеркивает только ограниченный, приближенный характер соответствия рассматриваемых математических представлений и реальной действительности. Поэтому идея актуальной бесконечности в определенных разумных пределах так же может быть использована, как и многие другие идеальные понятия. Приведенное разъяснение, конечно, не исчерпывает всех затруднений, связанных с понятием бесконечности, хотя, по-видимому, можно считать, что сама идея актуальной бесконечности не является причиной возникающих противоречий.

Но если даже принять гипотезу о том, что употребление понятия актуальной бесконечности в обычной теории множеств не приводит к противоречию, то этим трудности теории множеств полностью не устраняются. Появляется другой вопрос: можем ли мы быть уверены в том, что каждая математическая проблема разрешима с помощью принципов теории множеств? Гипотеза о разрешимости любой проблемы средствами теории множеств (в отличие от гипотезы непротиворечивости) представляется нам даже неправдоподобной. Но и для доказательства верности этого предположения необходимо иметь соответствующие средства.

Можно попытаться разрешить указанные вопросы посредством аксиоматического метода. Для этого надо отыскать все предпосылки, из которых делаются выводы в теории множеств, сформулировать их в виде аксиом и попытаться решить для полученной системы аксиом вопрос о *непротиворечивости*. Проблема *разрешимости* в таком случае сводится к проблеме независимости, так как доказать, что данная проблема не разрешима в теории множеств, означает установить, что соответствующее утверждение и его отрицание не выводимы из данных аксиом. Найти систему аксиом, описывающую в известных пределах теорию множеств, возможно, но решение вопросов непротиворечивости и независимости для такой системы аксиом наталкивается на существенные затруднения. Дело в том, что в рассматриваемых вопросах уже мы не можем применить метод интерпретаций. Причиной этого является то обстоятельство, что интерпретации для тех или иных систем аксиом мы обычно находим в пределах теории множеств и в силу этого непротиворечивость самой теории множеств уже должны предполагать.

Для выхода из создавшихся затруднений Гильберт предложил новую точку зрения на рассматриваемые вопросы. Идеи Гильберта явились переломным моментом в вопросах оснований математики и началом нового этапа в развитии аксиоматического метода. Поставим следующий вопрос: в какой мере необходимо для решения вопросов непротиворечивости и независимости пользоваться исключительно методом интерпретаций? Нельзя ли обойтись при решении этих вопросов без интерпретаций?

Допустим, что дана некоторая система аксиом, для которой мы хотим решить вопрос непротиворечивости. Противоречивой системой, как мы уже указывали, называется такая система, в которой выводимо некоторое предложение $\mathfrak{A}$ и вместе с тем его отрицание, которое мы обозначим $\overline{\mathfrak{A}}$. Поэтому для доказательства того, что система аксиом противоречива, достаточно найти какое-либо предложение $\mathfrak{A}$, для которого осуществляется вывод из данной системы аксиом его самого и его отрицания. Чтобы доказать непротиворечивость системы аксиом, достаточно показать, что, какое бы положение ни высказать, не существует вывода из аксиом одновременно его и его отрицания. Если бы мы могли описать всевозможные предложения, которые можно высказать для данной системы аксиом, и вместе с тем описать всевозможные способы дедукции, то, быть может, нам удалось бы из этого описания прямо доказать невозможность существования одновременно выводов какого-либо предложения и его отрицания. Таким же образом можно было бы ставить и вопросы независимости. Доказать, что предложение $\mathfrak{A}$ не зависит от аксиом $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, значило бы тогда извлечь из имеющегося описания выводов доказательство того, что вывода предложения $\mathfrak{A}$ из аксиом $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$ быть не может. С другой стороны, может случиться, что описание всевозможных предложений и выводов не требует привлечения очень сильных средств теории множеств и не включает таких вызывающих сомнения в познавательном отношении идей, как, например, актуальная бесконечность. Описание всевозможных форм дедукции оказалось вполне достижимым и было, в сущности, уже подготовлено предшествующим развитием символической логики. Однако в вопросах непротиворечивости встретились новые трудности. Все же дело было сдвинуто с мертвой точки, и новое направление аксиоматического метода стало развиваться.

Итак, нам прежде всего нужно иметь круг вполне надежных (во всяком случае в отношении непротиворечивости) понятий и принципов мышления, в рамках которого мы будем делать все дальнейшие построения. Чтобы исключить из основного круга понятий все сомнительные элементы теоретико-множественного мышления, естественно пытаться выбрать его возможно более ограниченным. Вместе с тем невозможно полностью исключить из рассмотрения бесконечность; но зато вполне возможно уничтожить ее *«актуальный»* характер. Понятие актуальной бесконечности фигурировало в философии задолго до описываемых здесь работ по основаниям математики, и в качестве противоположного ему понятия рассматривалась идея бесконечности другого рода, которая получила название *«потенциальной бесконечности»*. Смысл этого понятия состоит в том, что рассматривается бесконечное множество осуществимых возможностей. Каждая из них в отдельности осуществима, осуществимо также любое конечное число этих возможностей, но все вместе они неосуществимы. Рассмотрим пример. Будем считать, что построение целого числа осуществлено, если представлено какое-нибудь множество вещей, содержащее данное число элементов. Для каждого данного целого числа принципиально возможно представить себе соответствующее множество. Можно это сделать и для любого конечного количества целых чисел, но осуществить представление всех целых чисел невозможно.

Сомневаться в законности пользования понятием потенциальной бесконечности при настоящем состоянии науки нет никаких разумных оснований. Без такого рода бесконечности не может обойтись не только математика, но и точное естествознание. Во всяком случае по отношению к этому понятию критика основ математики никаких возражений не представляет. Идея потенциальной бесконечности лежит в основе концепции Гильберта.

Остановимся несколько подробнее на основных принципах учения Гильберта. Мы ставим перед собой две задачи.

1. *Найти круг понятий и принципов, которые не содержат сомнительных сторон теоретико-множественного мышления.*

2. *В рамках такого круга понятий поставить вопрос о непротиворечивости и независимости для любой системы аксиом, в частности аксиом теории множеств.*

Если бы удалось на этом пути решать вопросы непротиворечивости и независимости, то мы получили бы возможность обосновать использование идеи актуальной бесконечности и выяснить границы, в которых это возможно. Мы начнем с первой задачи — построения системы понятий и принципов, удовлетворяющих поставленным требованиям.

Будем рассматривать системы, составленные из конечного числа элементов, некоторых отмеченных свойств этих элементов и отношений между ними. Нам безразлично, каковы эти элементы, свойства и отношения. Мы требуем только, чтобы все эти элементы были четко отличимы друг от друга, так же как и их свойства и отношения между ними. Для каждого отмеченного свойства и отношения должно быть точно определено, для каких элементов оно имеет место, для каких нет. Рассмотрим примеры.

1. Дано слово из букв и цифр

$$a2c45e3.$$

Отметим для элементов этого слова два свойства: 1) *быть цифрой*; 2) *быть буквой* — и одно отношение между элементами строчки x и y: *элемент x в слове предшествует y.*

2. Элементами системы шаров пусть будут три белых и четыре черных шара, причем диаметры всех шаров различны, и если расположить эти шары в порядке возрастания диаметров, то цвета их распределятся следующим образом: *белый*, *черный*, *белый*, *черный*, *черный*, *белый*, *черный*. Отмеченными свойствами этой системы будем считать цвета шаров, отмеченным отношением между шарами x и y — отношение: диаметр шара x меньше диаметра y.

3. Система состоит из металлических колец. Отмечено единственное отношение между кольцами, состоящее в том, что одно кольцо надето на другое.

Рассматривая систему, мы будем отвлекаться от качественной природы ее элементов, отмеченных свойств и отношений. Две системы назовем изоморфными, если между их элементами можно установить взаимно однозначное соответствие, при котором отмеченные свойства (отношения) одной системы переходят в отмеченные свойства (отношения) другой системы. Легко заметить, что первые две из приведенных выше систем изоморфны. Изоморфные системы мы не будем различать. Это значит, что мы рассматриваем, по существу, не конкретные системы, а схемы систем. Каждая схема определяет целый класс изоморфных между собой систем, и каждая система этого класса может представлять собой схему, если мы будем делать только такие высказывания, которые применимы к любой системе данного класса.

Для каждой схемы можно найти представителя. Для этого достаточно взять произвольное множество с соответствующим числом элементов:

$$x_1,\ x_2,\ \ldots,\ x_n,$$

выделить из него подмножества:

$$A_1,\ A_2,\ \ldots,\ A_{m_1},$$

соответствующие отмеченным свойствам; затем выделить соответствующие двучленным отношениям множества, элементами которых являются упорядоченные пары (x_i, x_j):

$$B_1,\ B_2,\ \ldots,\ B_{m_2};$$

далее множества, элементами которых являются упорядоченные тройки (x_i, x_j, x_k), и т. д.; наконец, множества, элементами которых являются упорядоченные наборы из s элементов:

$$U_1,\ U_2,\ \ldots,\ U_{m_s}.$$

Последние множества будут соответствовать отношениям между s элементами системы. Представителем схемы может служить группа символов: x_1, x_2, ..., x_n с отмеченными свойствами A_i и отношениями B_1, B_2, ..., U_{m_s} между элементами.

В дальнейшем мы будем рассматривать схемы, содержащие только двучленные отмеченные отношения, т. е. отношения между парами элементов. Во многих случаях будем ограничиваться такими схемами, которые представляются словами, составленными из символов, причем отмеченным отношением является отношение предшествования в слове, а элементами являются сами символы. Например,

$$\alpha\beta\gamma.$$

Здесь отмеченное выражение между элементами выражается следующим образом: α предшествует β, α предшествует γ, β предшествует γ. Для всех остальных пар предшествование не имеет места. Мы будем пользоваться также словами, в которых один и тот же символ может повторяться несколько раз. Например,

$$aabacddc.$$

Это значит, что мы неявно вводим специальные отмеченные свойства: «быть элементом a», «быть элементом b» и т. д. Два элемента, обладающие одним и тем же отмеченным свойством такого типа, называются одинаковыми.

Для краткости в дальнейшем мы будем вместо термина «схема систем» употреблять термин «конфигурация».

Рассмотрим примеры конфигураций.

1. Каждое натуральное число n может рассматриваться как конфигурация, содержащая n элементов; отмеченные свойства и отношения в этой конфигурации вовсе не определены. Все представители такой конфигу-

рации с одинаковым числом элементов изоморфны, поэтому такая конфигурация может служить определением понятия «число элементов».

2. Конфигурация содержит n элементов, и между ними отмечено единственное отношение, выражаемое термином «x предшествует y». Условия, или аксиомы, определяющие это отношение, являются рассмотренными выше аксиомами порядка. При этом к двум аксиомам порядка мы присоединяем еще третью:

если x отлично от y, то или «x предшествует y», или «y предшествует x».

Нетрудно видеть, что представителем такой конфигурации является слово

$$x_1 x_2 \ldots x_n,$$

в котором отношение «x предшествует y» означает: «x расположено левее y в написанном слове».

Далее определяются конструктивные классы конфигураций и конструктивные операции над конфигурациями, причем эти определения должны подчиняться следующим гребованиям. Для каждого элемента конструктивного класса принадлежность его этому классу, исходя из определения, устанавливается посредством принципиально осуществимой совокупности действий. Пусть конструктивная операция $T(\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n)$ ставит произвольно заданной совокупности конфигураций $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$ в сооответствие некоторую конфигурацию $\mathfrak{B}$. При этом определение операции $T(\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n)$ всегда должны давать принципиально осуществимый способ построения конфигурации $\mathfrak{B}$, когда конфигурации $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$ заданы.

Заметим, что в некоторых случаях конструктивная операция $T(\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n)$ может быть определена не для произвольных конфигураций $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$, а для конфигураций, принадлежащих к определенным классам. Для различных переменных $\mathfrak{A}_i$ и $\mathfrak{A}_j$ классы конфигураций, для которых операция T определена, могут оказаться различными.

Простыми примерами конструктивных классов конфигураций являются класс натуральных чисел n, а также класс рассмотренных выше последовательностей или слов.

Для последнего класса определим операцию $S(\mathfrak{A}, \mathfrak{B})$, состоящую в приписывании к слову $\mathfrak{A}$ слова $\mathfrak{B}$. Элементами конфигурации $S(\mathfrak{A}, \mathfrak{B})$ являются все элементы конфигураций $\mathfrak{A}$ и $\mathfrak{B}$. Для любой пары элементов конфигурации $S(\mathfrak{A}, \mathfrak{B})$ определяем отношение порядка. Положим, что каждый элемент, принадлежащий $\mathfrak{A}$, предшествует каждому элементу, входящему в $\mathfrak{B}$. Для пар элементов x и y, входящих в $\mathfrak{A}$ (или в $\mathfrak{B}$), сохраняем те же порядковые отношения «x предшествует y», которые установлены соответственно в конфигурации $\mathfrak{A}$ (или в $\mathfrak{B}$). Легко видеть, что если $\mathfrak{A}$ и $\mathfrak{B}$ предсгавляли соответственно слова

$$x_1x_2 \ldots x_n$$

и

$$y_1y_2 \ldots y_m,$$

то конфигурация $S(\mathfrak{A}, \mathfrak{B})$ может быть представлена в виде слова

$$x_1x_2 \ldots x_ny_1y_2 \ldots y_m.$$

Будем записывать описанную операцию $S(\mathfrak{A}, \mathfrak{B})$ в виде $\mathfrak{A}\mathfrak{B}$. Конструктивный характер ее вполне очевиден. С помощью этой операции можно, исходя из одноэлементных конфигураций, получить класс всевозможных слов.

Другим примером конструктивной операции является операция

$$R(\mathfrak{A}, a, \mathfrak{B}),$$

смысл которой состоит в том, что в слове $\mathfrak{A}$ элемент a всюду, где он входит, заменяется словом $\mathfrak{B}$.

Операция $R(\mathfrak{A}, a, \mathfrak{B})$, носящая название «операции подстановки», часто будет встречаться нам в дальнейшем. Мы воспользуемся ею для определения несколько более сложной операции. Определим операцию

$$T(\mathfrak{A}, a, \mathfrak{B}, n),$$

где a — произвольный элемент, $\mathfrak{A}$ и $\mathfrak{B}$ — произвольные слова, n — натуральное число.

$T(\mathfrak{A}, a, \mathfrak{B}, 1)$ совпадает с $R(\mathfrak{A}, a, \mathfrak{B})$.

$T(\mathfrak{A}, a, \mathfrak{B}, 2)$ есть результат замены в слове $T(\mathfrak{A}, a, \mathfrak{B}, 1)$ элемента a везде, где он входит, словом $\mathfrak{B}$, т. е. это есть

$$R[T(\mathfrak{A}, a, \mathfrak{B}, 1), a, \mathfrak{B}].$$

Аналогичным образом $T(\mathfrak{A}, a, \mathfrak{B}, 3)$ определяется через $T(\mathfrak{A}, a, \mathfrak{B}, 2)$ и т. д. Для определения $T(\mathfrak{A}, a, \mathfrak{B}, n)$ для любого $n > 1$ можно написать следующую рекуррентную формулу:

$$T(\mathfrak{A}, a, \mathfrak{B}, n) = R[T(\mathfrak{A}, a, \mathfrak{B}, n-1), a, \mathfrak{B}].$$

Конструктивный характер этой операции также легко усмотреть из определения.

Конфигурации, конструктивные классы конфигураций и конструктивные операции представляют собой тот круг понятий, который мы принимаем за основу всех дальнейших построений. Более того, мы исключаем пользование понятиями, не сводящимися к ним. Однако для того, чтобы полностью исключить пользование бесконечностью в актуальной форме, мы должны ограничить и средства рассуждений над этими понятиями. Классы конфигураций, которые мы ввели, вообще говоря, уже бесконечны, и употребление для них таких логических принципов, как «закон исключенного третьего», лишает эти бесконечности их потенциального характера. Опишем те логические и математические принципы, пользование которыми допускается. В пределах рассмотрения одной или любого конечного числа конфигураций для всех рассуждений, проводимых в терминах только элементов конфигураций, свойств и отношений между этими элементами, мы допускаем все логические и математические средства без всяких ограничений. Во всех иных рассуждениях ввиду того, что в них уже может войти бесконечность, мы устраняем из общих логических принципов «закон исключенного третьего». Все остальные логические принципы мы сохраняем. В частности, допускается *«закон противоречия»*. Этот закон, как известно, состоит в утверждении невозможности того, что какое-либо высказывание и одновременно его отрицание истинны. В силу этого некоторые формы доказательства от противного находят себе место в допускаемых рассуждениях. Понятие «существования» мы употребляем в смысле «возможности построения». Из математических принципов доказательств мы сохраним один, носящий название *«аксиомы полной индукции»*. Применение этого принципа связано с конструктивными определениями. Допустим, что мы определили некоторую совокупность объектов посредством задания некоторых исходных объектов и операций, применением которых строится любой объект данной совокупности (так определяются, например, конструктивные классы). Тогда принцип полной индукции в применении к данной совокупности формулируется следующим образом.

Если какое-либо утверждение имеет место для исходных объектов данной совокупности и если верность утверждения для результата любой из заданных операций вытекает из верности этого утверждения для объектов, над которыми производится данная операция, то утверждение имеет место для всех объектов данной совокупности.

Этот принцип применим как к описанным выше конструктивным классам, так и к конструктивным операциям. Корректность его относительно идеи потенциальной бесконечности не подлежит никакому сомнению. Описанный круг понятий и средств рассуждения представляет собой определенную систему мышления. Рассуждения и построения, проводимые в рамках этой системы, мы назовем конструктивными или финитными, а всю систему в целом — *финитизмом Гильберта.*

Переходим ко второй задаче — в рамках введенной системы, пользуясь только ее понятиями и принципами, поставить проблемы непротиворечивости и независимости для любых аксиоматических систем. Если бы мы сохранили за аксиомами их прежний смысл, имея в виду находить для них интерпретации в круге понятий финитизма, мы только ограничили бы наши возможности решать вопросы, связанные с аксиомами, так как финитизм оказывается очень слабым средством для того, чтобы доставлять интерпретации для самых простых систем аксиом. Гильберт предложил рассмотреть аксиомы с иной точки зрения. Аксиомы являются определенными высказываниями. Высказывания же, какой бы смысл они не имели, всегда представляют собой сочетание терминов и, может быть, символов, поставленных между собою в какую-то связь. Делая логические выводы, мы переходим от одних сочетаний к другим. Возникает вопрос, нельзя ли дедуктивные операции над высказываниями описать в виде механизма в понятиях финитной системы мышления. Более точно вопрос ставится так:

Нельзя ли все высказывания любого интересующего нас круга вопросов в математике представить в виде конфигураций, а применяемые правила логики — в виде конструктивных операций?

Если это имеет место, то всякая система аксиом может быть представлена как совокупность определенных конфигураций, а выводимые из них следствия образуют конструктивный класс конфигураций. Оказалось, что подобное представление высказываний и логических заключений вполне возможно.

Предположим, что мы определили некоторый класс конфигураций, представляющих собой высказывания, и в нем указаны определенные конфигурации, которые мы называем аксиомами. Пусть вместе с тем указаны и конструктивные операции, представляющие собой логические операции вывода. В таком случае всю полученную систему мы будем называть *формализмом*, формальной логической системой, дедуктивным исчислением или просто *исчислением.* Термины «формализм» и «исчисление» все время будут употребляться у нас как синонимы. Любые высказывания формализма называются формулами. Операции, представляющие собой логические умозаключения, называются *правилами вывода.* Аксиомы и формулы, получаемые из аксиом путем применения правил вывода, называются формулами, выводимыми в данном формализме (в данном исчислении). В формализме могут фигурировать и такие конфигурации, которые не являются формулами, но входят в их состав и участвуют в определении формул. Утверждение, что данная конфигурация выводима, мы будем называть *формальной теоремой*, а фактическое построение выводимой конфигурации путем применения правил вывода — *формальным выводом.*

Вопрос о непротиворечивости ставится в таких исчислениях, для формул которых определено понятие формального отрицания, состоящее в том, что каждой формуле приводится некоторым образом в соответствие другая формула, называемая ее отрицанием. Мы будем называть формализм (исчисление) *противоречивым*, если в нем выводима какая-либо формула, а также и ее отрицание. Проблема независимости аксиом формализма заключается в вопросе: является ли данная аксиома выводимой в формализме, который отличается от рассматриваемого тем, что из списка его аксиом эта аксиома удалена? Или, говоря коротко: выводима ли данная аксиома посредством правил формализма из остальных аксиом?

Круг рассуждений, проводимых о формализмах, ограниченный пределами финитизма, называется *металогикой. Следует строго различать содержательные выводы, которые делаются при доказательстве различных утверждений, касающихся исчисления, и формальные выводы самого исчисления, представленные в виде операций над конфигурациями и рассматриваемые только в качестве таковых.* Символы, не принадлежащие к числу тех элементов, из которых составляются конфигурации, а введенные для обозначения каких-либо понятий, касающихся исчисления, часто называют *металогическими символами.* Аналогичным образом говорят о *металогических рассуждениях.*

Заметим также, что ограничения, о которых мы говорили при описании финитизма Гильберта, ни в коей мере не распространяются на понятия и выводы внутри самих исчислений. Эти ограничения (в частности, ограничение использования закона исключенного третьего) касаются только средств описания формализмов и рассуждений о формализмах.

Рассмотрим пример исчисления.

Предварительно опишем некоторую систему высказываний содержательным (не формальным) образом. В этих высказываниях речь идет о числах (натуральных, действительных, комплексных — не имеет значения). Каждая малая латинская буква изображает произвольное число. Назовем эти буквы переменными, принимающими числовые значения. Будем рассматривать действия сложения и умножения чисел и равенство чисел, обозначая их обычным образом. Выпишем исходные равенства, истинные для всех значений входящих в них переменных.

1. $a+b=b+a$,
2. $(a+b)+c=a+(b+c)$,
3. $ab=ba$,

4. $(ab)\,c = a\,(bc)$,

5. $(a + b)\,c = ac + bc$.

Из этих равенств можно выводить другие, используя два принципа.

1. В истинном равенстве каждую переменную можно заменить всюду, где она входит, любым числовым выражением, составленным из любых переменных.

2. В любом истинном равенстве любое числовое выражение можно заменить выражением, равным ему.

Опишем теперь предложенную систему в виде формализма. Определим сначала конфигурации, соответствующие числовым выражениям и равенствам. Основной запас элементов конфигураций состоит из следующих символов:

1. Малые латинские буквы a, b, ... , x, y, ...
2. Пары скобок ( ).
3. Знаки $=$, $+$.

Конфигурации, отвечающие числовым выражениям, мы назовем термами. Они определяются следующим образом.

Каждая малая латинская буква есть терм.

Если α и β — термы, то $(\alpha + \beta)$ и $(\alpha\beta)$ — также термы.

Этими условиями определяется конструктивный класс слов, которые мы называем термами. В приведенном нами определении термы представляют собой конфигурации, изображаемые числовыми выражениями в таком виде, как они записываются обычно, с той только разницей, что сложные термы заключаются в скобки, например:

$$(a + b), \quad ((a + b)\,c) \quad \text{и т. д.}$$

Мы условимся, ради краткости, внешних скобок не писать.

Равенства определяются как слова вида

$$\alpha = \beta,$$

где α и β — произвольные термы.

Формулами в нашем формализме являются равенства. Терм формулой не является, так как он соответствует не высказыванию, а числу.

В качестве аксиом нашего формализма мы примем выписанные выше формулы 1—5. Приняв аксиомы за исходные выводимые формулы, мы остальные выводимые формулы получим посредством правил вывода нашего формализма, т. е. некоторых конструктивных операций.

Мы введем два правила вывода.

I. Если $\mathfrak{A}(a)$ — выводимое равенство, содержащее букву a, а β — любой терм, то равенство $\mathfrak{A}(\beta)$, являющееся результатом замены всюду в $\mathfrak{A}$ буквы a термом β, есть также выводимое равенство.

Операция замены представляет собой рассмотренную выше операцию $R(\mathfrak{A}, a, \mathfrak{B})$, которую мы называли операцией подстановки. Это, как мы знаем, конструктивная операция.

II. Если $\mathfrak{A}(\alpha)$ — выводимое равенство, α — содержащийся в нем терм, $\alpha = \beta$ — также выводимое равенство, то равенство $\mathfrak{A}(\beta)$, полученное заменой в $\mathfrak{A}(\alpha)$ терма α термом β, также является выводимым равенством.

Операция замены одного терма другим термом также является конструктивной. Ее смысл и финитно осуществимый характер вполне очевидны.

Введением аксиом и правил вывода мы определили конструктивный класс выводимых равенств.

Формальная трактовка системы числовых аксиом показывает, что можно отвлечься от содержания этих аксиом, рассмотрев их просто как слова, а правила логических заключений — как операции над этими словами. Если мы не будем сопоставлять полученный формализм ни с чем лежащим вне его, то он будет представлять собой внутренним образом определенную систему, состоящую из совокупности слов, называемых равенствами. Из них выделены некоторые слова, которые названы выводимыми равенствами. Это означает только, что они получены из нескольких выбранных слов с помощью определенных правил.

Для приведенного формализма вопрос о непротиворечивости не может быть поставлен ввиду того, что в нем нет отрицания. Но мы можем для него поставить другой вопрос, который имеет известную аналогию с вопросом непротиворечивости. Назовем формализм *«пустым»*, если в нем выводимо всякое равенство. (Аналогия этого понятия с понятием непротиворечивости заключается в том, что, как мы увидим в дальнейшем, во всякой противоречивой системе, содержащей в себе обычные логические принципы, также все формулы выводимы.) Непустота нашей системы доказывается очень просто. Уже формула $a = b$ в ней не может быть выведена. Это легко доказать, пользуясь содержательным смыслом формализма. В самом деле, если бы слово $a = b$ было выводимым, то содержательное числовое равенство $a = b$ должно было бы быть истинным для любых чисел a и b, чего на самом деле нет. Подобное доказательство представляется чужеродным постановке вопроса о непустоте формализма, так как в определение рассматриваемых нами слов и действий над ними понятие числа нигде не входит. Точнее говоря, недостаток этого доказательства заключается в том, что оно опирается на гипотезу о непротиворечивости той числовой системы, которая употребляется для интерпретации. Однако эту интерпретацию можно сделать настолько простой, что вопрос о непротиворечивости для нее отпадет.

Поставим еще один вопрос о нашем формализме: существуют ли такие не выводимые в нем равенства, что если какое-либо из них присоединить к системе аксиом формализма в качестве новой аксиомы, то получится опять непустая система? Или же, наоборот: какое бы невыводимое равенство к системе аксиом ни присоединить, получится пустая система? С аналогичными вопросами мы дальше часто будем встречаться. Если мы присоединим к системе аксиом 1—5 невыводимую формулу $a = b$, то система станет пустой. Действительно, заменяя на основании правила подстановки a и b произвольными термами, мы покажем, что всякое равенство $\alpha = \beta$ выводимо в полученной системе. Однако если мы присоединим к системе аксиом 1—5 невыводимую формулу

$$ab + c = (a + c)(b + c),$$

то получим непустую систему. Невыводимость последней формулы в нашей системе вытекает из того, что она представляет собой неверное числовое равенство, Однако для новой системы аксиом можно найти другую интерпретацию. Будем рассматривать переменные a, b, c, ... как конечные множества (включая и пустое), выражение $(\alpha + \beta)$ как множество, состоящее из всех элементов множества α и всех элементов множества β, или, как говорят, теоретико-множественную сумму, а выражение $(\alpha\beta)$ как множество элементов, принадлежащих и α и β, или теоретико-множественное пересечение. Под равенством термов $\alpha = \beta$ будем понимать совпадение множеств α и β. Тогда все аксиомы, включая и новую, выполняются, а правила вывода по-прежнему приводят только к истинным тождествам. Но тождество $a = b$ не является истинным и в этом формализме, так как a и b могут быть различны. Итак, новая система также непуста.

Вопрос о непустоте нашего формализма (аналогичный вопросу о непротиворечивости) легко решился методом интерпретаций. Однако теперь мы уже не ограничены методом интерпретаций.

Рассмотрим, например, вопрос о независимости первой из аксиом рассматриваемого нами формализма $a = a$. Вопрос этот ставится следующим образом: выводимо ли равенство $a = a$ из других аксиом с помощью правил вывода или нет? Если бы оказалось, что оно выводимо, то в системе аксиом 1—5 оно лишнее в том смысле, что класс выводимых равенств формализма не изменится, если мы его удалим. Доказать независимость этой аксиомы методом интерпретаций еще возможно, но уже гораздо более затруднительно. Значительно проще доказать ее независимость другим путем. Заметим, что во всех остальных аксиомах термы, соединенные знаком равенства, представляют собой конфигурации, никогда не сводящиеся к одному элементу. Иными словами, никакой из этих термов не состоит из одной буквы. Если применить к любому равенству, обладающему этим свойством, наши правила вывода, то получится равенство, также обладающее этим свойством. В самом деле, применяя первое правило, мы заменяем в равенстве буквы термами и, следовательно, можем только усложнить рассматриваемый терм. Применяя второе правило, мы никогда не можем получить равенства, у которого в какой-нибудь части стоит только одна буква, так как терм β, которым заменяется терм α в формуле $\mathfrak{A}(\alpha)$, участвует в уже выведенном по предположению равенстве $\alpha = \beta$ и потому сам содержит больше одной буквы. Отсюда следует, что все формулы, выводимые из системы аксиом 2—5, имеют всегда вид $\alpha = \beta$, где α и β содержат более одной буквы. Поэтому аксиома $a = a$ не может быть выведена из остальных аксиом формализма.

В рассмотренном примере мы имеем дело с очень слабым формализмом. Но аналогичным образом можно строить мощные системы, охватывающие круг дедуктивных средств, которыми пользуется математика во всех своих отраслях: арифметике, анализе, алгебре, теории функций и др.

Первоначальный замысел Гильберта состоял в идее свести все содержательное математическое познание к финитизму и рассмотреть соответствующие математические дисциплины как описанные выше формализмы, считая, что эти формализмы уже ничего не изображают, а являются сами единственным предметом математики. Тогда проблемы оснований математики формулировались бы в понятиях финитизма и можно было бы надеяться решить их средствами финитизма. В этом направлении должен был бы решиться и вопрос о возможности использования теории множеств в широком смысле для вывода суждений финитного характера. Выражая теорию множеств посредством формальных систем и исследуя вопрос о непротиворечивости этих систем, мы выяснили бы границы приложения теоретико-множественной концепции или, по крайней мере, указали бы такие пределы, в которых наверняка противоречий не возникает. Таким образом, мы могли бы вводить употребление актуальной бесконечности и нам было бы известно, когда это возможно. На первый взгляд кажется, что препятствий к выполнению такой программы не возникает. Однако впоследствии выяснилось, что в буквальной своей постановке эта программа невыполнима. Хотя, действительно, все математические высказывания и всякая логическая дедукция могут быть представлены посредством формальных систем Гильберта и в этом смысле формализмы могут неограниченно охватывать все математические знания, но даже для решения вопросов о непротиворечивости основных математических дисциплин финитизма Гильберта недостаточно. Дело в том, что понятия и принципы всей математики не могут быть полностью выражены никакой формальной системой, как бы мощна она ни была. Это обстоятельство, в частности, проявляется в том, что, как показал Гёдель, вопрос о непротиворечивости достаточно богатой формальной системы не может быть решен средствами, которые формализуются в той же системе. Так как средства рассуждений, допускаемые финитизмом, можно выразить в пределах определенного формализма (например, в аксиоматической арифметике, которая описана в главе V), то непротиворечивость такого формализма в рамках финитизма доказать нельзя. Однако нет никаких оснований предполагать, что границы, которые кладет финитизм Гильберта, действительно необходимы для того, чтобы исключить вызывающие сомнения элементы математического мышления. Возможен дальнейший анализ предмета математики и выделения в нем надежных непротиворечивых средств, выходящих за рамки финитизма и все же достаточно сильных для того, чтобы решать интересующие нас вопросы. Но выход за рамки финитизма не уничтожает основной идеи метода, предложенного Гильбертом и состоящего в формализации тех математических систем, которые подлежат обоснованию, средствами некоторого круга понятий, принятых в качестве основы в силу тех или других соображений. На самом деле, если для решения указанных выше вопросов средств финитизма недостаточно, то для постановки этих вопросов этих средств вполне достаточно.

Из сказанного как будто можно заключить, что о непротиворечивости некоторых формализмов мы имеем возможность судить только по тому содержанию, которое они представляют; иными словами, решение проблемы непротиворечивости опять требует метода интерпретаций. Но содержание формализмов, описывающих теоретико-множественные системы, как мы уже неоднократно говорили выше, само нуждается в обосновании. Все же теоретико-множественные интерпретации, за неимением ничего лучшего, применяются и к изучению формализмов. Рассмотрение их с теоретико-множественной точки зрения получило название «содержательного», хотя здесь больше подходит термин «наивно-содержательное» рассмотрение. Удовлетворительного решения вопросов оснований математики такой способ дать не может, и мы находимся здесь перед существенным затруднением. Однако содержание формализмов не обязано быть всегда теоретико-множественным. Критический пересмотр основ теории множеств принес иные, не теоретико-множественные представления, которые способны составить содержание формализмов, свободное от тех элементов теоретико-множественной концепции, которые вызывают сомнение.

Есть основания надеяться, что формализмы, о непротиворечивости которых мы можем судить на основании выражаемого ими содержания, образуют совокупность, хотя и не включающую все непротиворечивые формализмы, но такую, что непротиворечивость любого формализма можно свести к непротиворечивости формализмов данной совокупности уже средствами финитизма Гильберта.

Описанные нами идеи, возникшие из вопросов оснований математики, как это часто бывает, в своем развитии вышли из первоначального круга своих задач. Они внесли принципиально новые понятия и методы, которые стали применяться и в вопросах, не связанных непосредственно с основаниями математики.

Так, из идей математической логики в 30-х годах XX века возникло точное определение понятия алгоритма. Это в свою очередь позволило доказать существование в различных традиционных областях математики неразрешимых алгоритмических проблем. Открытие точного понятия алгоритма породило также некоторые новые подходы к вопросам оснований математики.

Развитие методов математической логики позволило также доказать принципиальную неразрешимость основных проблем теории множеств.

Аппарат математической логики находит применение также в вычислительной математике и в технике в связи с конструкцией сложных автоматических устройств.

АЛГЕБРА ВЫСКАЗЫВАНИЙ

§ 1. Логические операции

Учение о высказываниях, называемое алгеброй высказываний, является первой из формальных логических теорий. Оно не принадлежит к исчислениям того типа, о котором говорится во введении. Но, хотя эти исчисления и являются основным предметом нашей книги, мы начнем изложение основ математической логики с алгебры высказываний. Дело в том, что знакомство с законами алгебры высказываний очень облегчает изучение тех логических исчислений, с которыми мы встретимся в дальнейшем. Кроме того, алгебра высказываний представляет самостоятельный интерес и имеет приложения в других отраслях науки. Она применяется, например, при синтезе релейно-контактных и электронных схем.

Будем рассматривать различные высказывания, предполагая при этом, что они удовлетворяют закону исключенного третьего и закону противоречия, т. е. каждое высказывание или истинно, или ложно и не может быть одновременно и истинно и ложно. (Нет никакой необходимости считать общеобязательными эти законы логики. Но мы ограничиваемся рассмотрением лишь таких вопросов, для которых эти законы имеют место.) Отвлечемся от содержания высказывания и даже от его структуры; в частности, не будем в нем выделять субъект и предикат. Будем ограничиваться только тем его свойством, что оно представляет собой или истину, или ложь. Тогда высказывание можно рассматривать как величину, которая может принимать два значения: «истина» и «ложь».

Пример. Даны суждения: «собака — животное»; «Париж — столица Италии»; «$3<5$»; «в каждом треугольнике биссектриса делит противоположную сторону на равные части».

С нашей точки зрения, первое из этих высказываний может быть заменено символом «истина», второе —

«ложь», третье — «истина» и четвертое — «ложь». Будем обозначать высказывания большими латинскими буквами A, B, ..., а их значения, т. е. истину и ложь, соответственно *И* и *Л*. Во всей этой главе мы рассматриваем высказывания только как величины, принимающие значения *И* и *Л*. В обычной речи употребительны связки между высказываниями: *и*, *или* и др. Эти связки позволяют, соединяя между собой различные высказывания, образовывать новые высказывания. Например, связка «*и*». Пусть даны высказывание «π больше 3» и высказывание «π меньше 4»; мы можем образовать новое высказывание «π больше 3 и π меньше 4». Высказывание «если π иррационально, то π^2 тоже иррационально» получается связыванием двух высказываний связкой *если..., то...* Наконец, мы можем получить из данного высказывания новое, отрицая его. Рассматривая высказывания как величины, принимающие значения *И* и *Л*, мы определим над ними операции, которые позволяют из данных высказываний получать новые. Эти операции, по существу, и выражают упомянутые выше связки, употребительные в обычной речи.

Пусть даны два произвольных высказывания A и B.

1. Первая операция над этими высказываниями представляет собой образование нового высказывания, которое мы будем обозначать $A \& B$ и которое истинно тогда и только тогда, когда A и B истинны. В обычной речи этой операции соответствует соединение высказываний связкой «*и*».

2. Вторая операция над высказываниями A и B, выражаемая в виде $A \vee B$, определяется следующим образом: высказывание $A \vee B$ истинно тогда и только тогда, когда хотя бы одно из первоначальных высказываний истинно.

В обычной речи эта операция соответствует соединению высказываний связкой «*или*». Однако здесь мы имеем не разделительное «*или*», которое понимается в смысле «*либо..., либо...*» и ложно, когда A и B оба истинны. В нашем определении высказывание $A \vee B$ истинно и при истинности обоих высказываний A и B.

3. $A \rightarrow B$; это высказывание ложно тогда и только тогда, когда A истинно, а B ложно. A называется

посылкой, B — *следствием*, а высказывание $A \to B$ — *следованием* или *импликацией*. В обычной речи эта операция соответствует связке *если..., то...*: «если A, то B». Но в нашем определении это высказывание при ложном A всегда истинно независимо от того, истинно или ложно высказывание B. Это обстоятельство можно кратко сформулировать так: «*из ложного следует всё, что угодно*». В обычной речи иногда подразумевается, что, когда A ложно, высказывание «если A, то B» не имеет смысла. Однако такое понимание не может быть здесь принято. Действительно, допустим, например, что доказана какая-то редукция, сводящая некоторое утверждение теории чисел B к гипотезе Римана, которую мы обозначим через A. Неизвестно, справедлива ли гипотеза Римана, однако редукция, т. е. утверждение «из A следует B», справедлива. Таким образом, мы считаем, что утверждение «из A следует B» в данном случае справедливо, хотя A может быть и ложно. С другой стороны, редукция тогда только и представляет интерес, когда неизвестно, истинна ли посылка A. Если бы, в самом деле, мы знали, что посылка истинна, то редукция привела бы к доказательству B.

Кроме того, понятие следования, употребляемое в речи, имеет еще другой оттенок. Высказывание «из того, что у льва есть когти, следует, что снег белый» является истинным в определенном нами смысле. Действительно, высказывание «снег бел», фигурирующее здесь как следствие, истинно, и поэтому всё утверждение также истинно независимо от истинности или ложности посылки. При распространенном же понимании следования из того, что у льва есть когти, никак не следует, что снег белый, так как подразумевается, что следствие должно быть как-то выведено из посылки. А это не может быть сделано, если содержания посылки и следствия совершенно чужеродны. Подобное понимание следования никоим образом не может быть определено в рассматриваемом логическом исчислении, так как оно не может быть сформулировано только в терминах истины и лжи.

4. $\bar{A}$ есть высказывание, которое ложно, когда A истинно, и истинно, когда A ложно. Высказывание $\bar{A}$ называется *отрицанием* A.

5. $A \sim B$ есть высказывание, истинное тогда и только тогда, когда A и B оба истинны или оба ложны. Это высказывание называется *эквивалентностью.*

Пусть X, Y, Z, U, V, $W, \ldots$ — произвольные высказывания, т. е., с нашей точки зрения, величины, принимающие одно из двух значений *И* и *Л*.

При помощи операций &, $\vee$, $\rightarrow$, $\sim$ и $^{-}$ мы можем образовать из них сложные высказывания: 1) $X \& Y$; 2) $X \vee Y$; 3) $X \rightarrow Y$; 4) $\bar{X}$; 5) $X \sim Y$. Из полученного запаса высказываний, применяя те же операции, можно получить новые сложные высказывания, например:

$$X \rightarrow (Y \vee Z),$$

$$\overline{X \sim Y},$$

$$\overline{(X \rightarrow Y)} \rightarrow (X \sim \overline{(U \& V)}),$$

$$X \vee (Y \& Z),$$

$$\overline{\overline{(X \vee Y)} \& (Z \rightarrow (U \rightarrow (V \sim W)))},$$

$$X \& (Y \& (Z \& (U \& (V \& W))))$$

и т. д. Зная значения, которые имеют высказывания X, $Y, \ldots, W$, мы легко можем установить значение составленного из них сложного высказывания. Например:

1. Пусть X есть *И*, Y есть *Л*, Z есть *Л*; тогда сложное высказывание $X \rightarrow (Y \vee Z)$ может быть записано в виде *И* $\rightarrow$ (*Л* $\vee$ *Л*). Значение этого высказывания *Л*. В самом деле, *Л* $\vee$ *Л* есть *Л*; *И* $\rightarrow$ *Л* также есть *Л*.

2. Пусть X есть *Л*, Y есть *Л*, Z есть *И*, U есть *И*, V есть *Л* и W есть *Л*. Рассмотрим сложное высказывание

$$\overline{\overline{(X \vee Y)} \& (Z \rightarrow (U \rightarrow (V \sim W)))}.$$

Его можно написать в виде

$$\overline{\overline{(Л \vee Л)} \& (И \rightarrow (И \rightarrow (Л \sim Л)))}.$$

В таком случае *Л* $\vee$ *Л* есть *Л*, $\overline{Л \vee Л}$ есть *И*. Поэтому сложное высказывание можно переписать так:

$$\overline{И \& (И \rightarrow (И \rightarrow (Л \sim Л)))}.$$

Но *Л* ∼ *Л* есть *И*, *И* → *И* также есть *И*; поэтому высказывание, стоящее под знаком отрицания, имеет значение *И*. Тогда все высказывание примет вид $\overline{И}$, т. е. *Л*.

Всякое сложное высказывание, составленное из некоторых исходных высказываний посредством применения логических операций 1—5, *мы будем называть формулой алгебры высказываний.*

Исходные высказывания при этом могут быть постоянными, т. е. иметь определенное значение *И* или *Л*, или могут не иметь определенного значения. Тогда они обозначаются большими латинскими буквами. В первом случае мы будем называть исходные высказывания постоянными элементарными высказываниями, во втором — переменными элементарными высказываниями. Если мы зададим значения всех переменных элементарных высказываний, то сама формула примет определенное значение. Таким образом, каждая формула определяет некоторую функцию, аргументами которой являются переменные элементарные высказывания.

В дальнейшем мы будем иметь дело преимущественно с такими формулами, которые содержат только переменные элементарные высказывания. Мы будем считать, что если относительно формулы не сделано особых оговорок, то она содержит только переменные элементарные высказывания. Так как аргументы и функции способны принимать только два различных значения, то такая функция может быть полностью описана конечной таблицей. Приведем таблицы для простейших функций:

X	Y	$X \& Y$
И	*И*	*И*
Л	*И*	*Л*
И	*Л*	*Л*
Л	*Л*	*Л*

X	Y	$X \vee Y$
И	*И*	*И*
Л	*И*	*И*
И	*Л*	*И*
Л	*Л*	*Л*

X	Y	$X \to Y$
И	*И*	*И*
Л	*И*	*И*
И	*Л*	*Л*
Л	*Л*	*И*

X	Y	$X \sim Y$
И	*И*	*И*
Л	*И*	*Л*
И	*Л*	*Л*
Л	*Л*	*И*

X	$\overline{X}$
И	*Л*
Л	*И*

§ 2. Равносильность формул

Посредством приведенных операций над высказываниями могут быть образованы другие, сколь угодно сложные высказывания. Например,

$$(A \,\&\, B) \vee C; \quad ((A \to B) \sim C) \,\&\, \overline{((A \vee \overline{B}) \,\&\, \overline{C})}.$$

Каждая формула представляет собой функцию входящих в нее букв A, B, ... *Мы будем называть две формулы* $\mathfrak{A}$ *и* $\mathfrak{B}$ *равносильными, если при любых значениях* $X_1, X_2, \ldots, X_n$, *где* $X_1, X_2, \ldots, X_n$*—совокупность всех переменных, входящих в* $\mathfrak{A}$ *и* $\mathfrak{B}$, *эти формулы принимают одинаковые значения.*

Примеры:

$$\begin{aligned} \overline{\overline{X}} &\quad \text{равносильно} \quad X, \\ X \vee X &\quad \text{равносильно} \quad X, \\ (X \,\&\, \overline{X}) \vee Y &\quad \text{равносильно} \quad Y, \\ X \vee \overline{X} &\quad \text{равносильно} \quad Y \vee \overline{Y}. \end{aligned}$$

Между понятием равносильности и знаком эквивалентности $\sim$ существует следующая связь: *если формулы* $\mathfrak{A}$ *и* $\mathfrak{B}$ *равносильны, то формула* $\mathfrak{A} \sim \mathfrak{B}$ *принимает значение И при всех значениях переменных*, и обратно: *если формула* $\mathfrak{A} \sim \mathfrak{B}$ *принимает значение И при всех значениях переменных, то формулы* $\mathfrak{A}$ *и* $\mathfrak{B}$ *равносильны.*

Справедливость этого утверждения непосредственно вытекает из определения операции $\sim$. Легко видеть, что отношение равносильности двух формул симметрично и транзитивно.

При определении равносильности двух формул не обязательно предполагать, что они содержат одни и те же переменные. Так, в третьем и четвертом примерах мы имеем случай, когда в равносильные формулы входят разные переменные. Вместе с тем очевидно, что если какая-нибудь переменная входит только в одну из двух равносильных формул, то эта формула при всех значениях переменной принимает одно и то же значение, если значения других переменных фиксированы. Иными словами, хотя эта переменная и входит в формулу, но функция, определенная рассматриваемой формулой, от этой переменной не зависит.

Приведем важнейшие примеры равносильных формул:

$$\overline{\overline{X}} \text{ равносильно } X, \tag{1}$$

$$X \& Y \text{ равносильно } Y \& X, \tag{2}$$

$$(X \& Y) \& Z \text{ равносильно } X \& (Y \& Z), \tag{3}$$

$$X \vee Y \text{ равносильно } Y \vee X, \tag{4}$$

$$(X \vee Y) \vee Z \text{ равносильно } X \vee (Y \vee Z), \tag{5}$$

$$X \& (Y \vee Z) \text{ равносильно } (X \& Y) \vee (X \& Z), \tag{6}$$

$$X \vee (Y \& Z) \text{ равносильно } (X \vee Y) \& (X \vee Z), \tag{7}$$

$$X \vee (X \& Y) \text{ равносильно } X, \tag{8}$$

$$X \& (X \vee Y) \text{ равносильно } X, \tag{9}$$

$$\overline{(X \vee Y)} \text{ равносильно } \overline{X} \& \overline{Y}, \tag{10}$$

$$\overline{(X \& Y)} \text{ равносильно } \overline{X} \vee \overline{Y}, \tag{11}$$

$$X \vee X \text{ равносильно } X, \tag{12}$$

$$X \vee \overline{X} \text{ равносильно } И, \tag{13}$$

$$X \& X \text{ равносильно } X, \tag{14}$$

$$X \& \overline{X} \text{ равносильно } Л, \tag{15}$$

$$X \& И \text{ равносильно } X, \tag{16}$$

$$X \vee Л \text{ равносильно } X. \tag{17}$$

Соотношения (1)—(17) легко проверяются на основании определения операций &, $\vee$ и $^{-}$. В тех вопросах, в которых равносильные формулы равноправны, т. е. могут быть заменены одна другой, соотношения равносильности позволяют производить над формулами преобразования, приводящие их к более простому или более удобному виду.

Например, $((X \vee X) \& Y) \vee (X \vee X)$ равносильно $(X \& Y) \vee (X \vee X)$, что в свою очередь равносильно $(X \& Y) \vee X$.

Таким же образом в любой формуле можно заменить любую ее часть равносильной формулой, и при этом получится формула, равносильная данной.

Соотношения (2), (3), (4), (5) указывают, что действия, определенные знаками & и $\vee$, подчинены законам коммутативности и ассоциативности. Поэтому, если формула $\mathfrak{A}$ составлена из формул $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$ только посредством операции &, то, в каком бы порядке мы ни производили эти операции, всегда получим формулу, равносильную формуле $\mathfrak{A}$. Мы будем такую формулу $\mathfrak{A}$ представлять в виде выражения

$$\mathfrak{A}_1 \& \mathfrak{A}_2 \& \ldots \& \mathfrak{A}_n,$$

в котором все скобки, заключающие в себе формулы $\mathfrak{A}_i$, опущены. Точно так же, если формула $\mathfrak{A}$ составлена из формул $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$ только посредством операции $\vee$, мы будем изображать ее в виде

$$\mathfrak{A}_1 \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_n.$$

Соотношение (6) указывает, что операция & дистрибутивна относительно операции $\vee$, подобно тому как обычное арифметическое умножение дистрибутивно относительно сложения. В силу этой аналогии мы будем операцию & называть умножением, а операцию $\vee$ — сложением.

Выражение $\mathfrak{A}_1 \& \mathfrak{A}_2 \& \ldots \& \mathfrak{A}_n$ будем называть логическим произведением, а члены его $\mathfrak{A}_i$ — множителями. Знак & иногда опускают.

Выражение $\mathfrak{A}_1 \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_n$ будем называть логической суммой, а члены его $\mathfrak{A}_i$ — слагаемыми.

Аналогия между законами коммутативности и ассоциативности сложения и умножения и дистрибутивности умножения относительно сложения в алгебре высказываний и такими же законами для сложения и умножения чисел ведет к тому, что над формулами алгебры высказываний можно производить преобразования раскрытия скобок, заключения в скобки, вынесения за скобки общего множителя так же, как и в обычной алгебре.

На основании соотношения (7) операция $\vee$ также дистрибутивна относительно операции &. Поэтому иногда, наоборот, операцию $\vee$ называют умножением, а операцию & — сложением, и при этом указанная аналогия с алгеброй сохраняется.

Преобразования, представляющие собой применение законов дистрибутивности (6) и (7), мы будем называть *дистрибутивными операциями. Соотношение* (6) *будем называть первым дистрибутивным законом, а соотношение* (7) — *вторым дистрибутивным законом.*

Можно еще упростить запись формул, опуская некоторые скобки и считая при этом, что действие умножения предшествует действию сложения, а действия сложения и умножения предшествуют действиям $\rightarrow$ и $\sim$. Или, как говорят еще: умножение *связывает сильнее* сложения, умножение и сложение *связывают сильнее* действий $\rightarrow$ и $\sim$. Кроме того, будем считать, что знак $^{-}$, стоящий над формулой, делает излишними скобки, в которые заключена эта формула. Так, например, формулу

$$XY \vee ZU$$

будем понимать как

$$(X \& Y) \vee (Z \& U);$$

формулу

$$X \vee Y \rightarrow ZU$$

как

$$(X \vee Y) \rightarrow (Z \& U),$$

а формулу

$$\overline{X \vee Y} \& Z$$

как

$$\overline{(X \vee Y)} \& Z.$$

Система элементов, на которой определены действия сложения, умножения и отрицания, удовлетворяющая зависимостям (1)—(17), называется *алгеброй Буля*. Итак, можно сказать, что высказывания и основные логические операции &, $\vee$, $^{-}$ представляют собой алгебру Буля.

Однако существуют и иные системы вещей (не логические системы), также образующие алгебру Буля. Например, система подмножеств некоторого множества R, для которой сложение является теоретико-множественным сложением, умножение — теоретико-множественным пересечением, отрицание — взятием дополнения до R, также является алгеброй Буля (в которой роль *И* играет всё множество R, а роль *Л* — его пустое подмножество).

Укажем еще систему, удовлетворяющую значительной части соотношений (1)—(17). Пусть M — какое-то ограниченное множество действительных чисел, содержащее свою верхнюю грань p и нижнюю грань q. Пусть, кроме того, M симметрично относительно точки $\frac{p+q}{2}$, которую назовем центром множества M. Иначе говоря, если $x \in M$, то точка x', симметрично расположенная относительно центра, также принадлежит M. Действия сложения, умножения и отрицания определены следующим образом. Сохранив за этими действиями логические знаки, мы положим, что

$$x \vee y = \max(x, y), \quad x \& y = \min(x, y),$$

а $\bar{x}$ есть точка, симметричная x. Нетрудно убедиться, что все свойства (1)—(17), за исключением (13) и (15), выполнены для указанных операций (роль *И* здесь играет p, а роль *Л* играет q).

В том случае, когда множество M состоит из двух чисел 0 и 1, эта система представляет собой алгебру высказываний, в которой символы *Л* и *И* заменены соответственно числами 0 и 1.

Логические операции &, $\vee$, $\rightarrow$, $\sim$ и $^{-}$ не являются независимыми друг от друга. Одни из них можно выражать через другие так, что при этом получаются равносильные формулы. Например, знак $\sim$ может быть выражен через знаки $\rightarrow$ и & на основании соотношения

$$X \sim Y \quad \text{равносильно} \quad (X \rightarrow Y) \& (Y \rightarrow X), \qquad (18)$$

которое легко доказывается на основании определения действий $\sim$, $\to$ и &.

Знак $\to$ может быть выражен через знаки $\vee$ и $^{-}$:

$$X \to Y \quad \text{равносильно} \quad \overline{X} \vee Y.$$

Таким образом, знак $\sim$ может быть выражен через знаки &, $\vee$ и $^{-}$:

$$X \sim Y \quad \text{равносильно} \quad (\overline{X} \vee Y) \& (\overline{Y} \vee X). \tag{19}$$

Знак $\sim$ может быть выражен через знаки &, $\vee$ и $^{-}$ еще иначе:

$$X \sim Y \quad \text{равносильно} \quad X \& Y \vee \overline{X} \& \overline{Y}, \tag{20}$$

что также легко доказывается.

Итак, знаки $\to$ и $\sim$ можно выразить через знаки &, $\vee$ и $^{-}$. Можно пойти и дальше и исключить еще один знак, & или $\vee$, по выбору.

Покажем, как выразить & через $\vee$ и $^{-}$.

На основании зависимости (10) мы имеем

$$\overline{\overline{X}} \& \overline{\overline{Y}} \quad \text{равносильно} \quad \overline{\overline{X} \vee \overline{Y}}.$$

На основании (1) $\overline{\overline{X}}$ и $\overline{\overline{Y}}$ можно заменить через X и Y, и, следовательно,

$$X \& Y \quad \text{равносильно} \quad \overline{\overline{X} \vee \overline{Y}}.$$

Знак & выражен, таким образом, через знаки $\vee$ и $^{-}$.

Итак, все операции посредством равносильных выражений можно заменить двумя: $\vee$ и $^{-}$.

Аналогичным образом, используя (11), можно все операции заменить на & и $^{-}$.

З а м е ч а н и е. Если формула $\mathfrak{A}$ содержит только операции &, $\vee$ и $^{-}$, то на основании соотношений (1), (10) и (11) ее можно преобразовать к такому виду, что знаки отрицания будут относиться только к элементарным высказываниям. В самом деле, если знак отрицания стоит над суммой: $\overline{\mathfrak{A} \vee \mathfrak{B}}$, то эту формулу можно заменить на основании (10) произведением $\overline{\mathfrak{A}} \& \overline{\mathfrak{B}}$; если знак $^{-}$ стоит над произведением: $\overline{\mathfrak{A} \& \mathfrak{B}}$, то эту формулу можно заменить суммой $\overline{\mathfrak{A}} \vee \overline{\mathfrak{B}}$; если же знак отрицания стоит над знаком отрицания: $\overline{\overline{\mathfrak{A}}}$, то на основании (1) оба эти знака можно удалить. Делая такие преобразования, мы приведем формулу к такому виду, в котором знак отрицания относится только к элементарным высказываниям.

Примеры.

1. $\overline{\overline{X} \vee \overline{Y}}$.

Преобразовав эту формулу на основании соотношения (10), получим равносильную формулу:

$$\overline{\overline{X}} \& \overline{\overline{Y}}.$$

На основании соотношения (1) двойные знаки отрицания можно удалить, и тогда получим окончательную формулу:

$$X \& Y.$$

2. $\overline{X \& Y \vee \overline{Z}}$.

Преобразовав эту формулу на основании соотношения (10), получим формулу

$$\overline{X \& Y} \& \overline{\overline{Z}}.$$

Преобразовав первый множитель на основании соотношения (11), получим

$$(\overline{X} \vee \overline{Y}) \& \overline{\overline{Z}}.$$

Удалив во втором множителе двойное отрицание, получим окончательно

$$(\overline{X} \vee \overline{Y}) \& Z.$$

§ 3. Закон двойственности

В этом параграфе мы будем рассматривать формулы, содержащие только операции &, $\vee$ и $^{-}$. Как уже установлено выше, всякая формула может быть приведена преобразованиями равносильности к такому виду.

Будем говорить, что *операция & двойственна операции $\vee$ и наоборот*. Введем также понятие двойственных формул. *Формулы $\mathfrak{A}$ и $\mathfrak{A}^*$ называются двойственными, если одна получается из другой заменой каждой операции на двойственную.*

Примеры.

1. $(X \vee \bar{Y}) \& Z$ двойственно $X \& \bar{Y} \vee Z$.

2. $\overline{X \vee Y} \& (X \vee \overline{Y \& Z})$ двойственно $\overline{X \& Y} \vee X \& \overline{Y \vee Z}$.

3. $X \& Y \vee Y \& Z \vee U \& V$ двойственно $(X \vee Y) \& (Y \vee Z) \& \& (U \vee V)$.

4. $X \& (Y \vee Z \& (U \vee V))$ двойственно $X \vee Y \& (Z \vee U \& V)$.

Как для операций, так и для формул отношение двойственности взаимно: если $\mathfrak{A}^*$ двойственно $\mathfrak{A}$, то и, наоборот, $\mathfrak{A}$ двойственно $\mathfrak{A}^*$.

Из равносильностей (10) и (11) легко вывести следующее положение: *если формулы* $\mathfrak{A}(X_1, \ldots, X_n)$ *и* $\mathfrak{A}^*(X_1, \ldots, X_n)$ *двойственны, а* $X_1, \ldots, X_n$ — *все входящие в них элементарные высказывания, то* $\overline{\mathfrak{A}}(X_1, \ldots \ldots, X_n)$ *равносильно* $\mathfrak{A}^*(\bar{X}_1, \bar{X}_2, \ldots, \bar{X}_n)$.

Из этого соотношения в свою очередь вытекает так называемый *закон двойственности*, который формулируется следующим образом.

Если формулы $\mathfrak{A}$ *и* $\mathfrak{B}$ *равносильны, то и двойственные им формулы* $\mathfrak{A}^*$ *и* $\mathfrak{B}^*$ *также равносильны.*

Пусть $\mathfrak{A}(X_1, \ldots, X_n)$ и $\mathfrak{B}(X_1, \ldots, X_n)$ — равносильные формулы, а $X_1, \ldots, X_n$ — входящие в них элементарные высказывания. Тогда

$$\mathfrak{A}^*(X_1, \ldots, X_n) \text{ равносильно } \overline{\mathfrak{A}}(\bar{X}_1, \ldots, \bar{X}_n),$$

а

$$\mathfrak{B}^*(X_1, \ldots, X_n) \text{ равносильно } \overline{\mathfrak{B}}(\bar{X}_1, \ldots, \bar{X}_n).$$

Из равносильности формул $\mathfrak{A}(X_1, \ldots, X_n)$ и $\mathfrak{B}(X_1, \ldots, X_n)$ следует равносильность формул $\mathfrak{A}(\bar{X}_1, \ldots, \bar{X}_n)$ и $\mathfrak{B}(\bar{X}_1, \ldots, \bar{X}_n)$, так как в силу определения равносильности $\mathfrak{A}(X_1, \ldots, X_n)$ и $\mathfrak{B}(X_1, \ldots \ldots, X_n)$ принимают одинаковые значения при любых значениях переменных $X_1, \ldots, X_n$, а следовательно, и при значениях $\bar{X}_1, \ldots, \bar{X}_n$.

В силу сказанного формулы $\mathfrak{A}(\bar{X}_1, \ldots, \bar{X}_n)$ и $\mathfrak{B}(\bar{X}_1, \ldots, \bar{X}_n)$ равносильны, а тогда формулы $\overline{\mathfrak{A}}(\bar{X}_1, \ldots, \bar{X}_n)$ и $\overline{\mathfrak{B}}(\bar{X}_1, \ldots, \bar{X}_n)$ также равносильны. Так как $\mathfrak{A}^*(X_1, \ldots, X_n)$ и $\mathfrak{B}^*(X_1, \ldots, X_n)$ равносильны соответственно формулам $\overline{\mathfrak{A}}(\bar{X}_1, \ldots, \bar{X}_n)$ и $\overline{\mathfrak{B}}(\bar{X}_1, \ldots, \bar{X}_n)$, то они равносильны между собой.

Если, применяя к формуле $\mathfrak{A}$ дистрибутивные преобразования на основании первого дистрибутивного закона, мы получим формулу $\mathfrak{B}$, то переход от двойственной формулы $\mathfrak{A}^*$ к двойственной формуле $\mathfrak{B}^*$ осуществляется дистрибутивными преобразованиями на основании второго дистрибутивного закона. Переход от $\mathfrak{A}^*$ к $\mathfrak{B}^*$ мы будем называть преобразованием, *двойственным* преобразованию, переводящему $\mathfrak{A}$ в $\mathfrak{B}$.

§ 4. Проблема разрешения

Будем называть формулу *тождественно истинной*, если она при всех значениях входящих в нее переменных высказываний принимает значение *И*. Примерами тождественно истинных формул являются формулы:

$$1.\ X \vee \overline{X};\quad 2.\ X \to (Y \to X);\quad 3.\ X \,\&\, (X \to Y) \to Y.$$

Будем называть формулу *выполнимой*, если она принимает значение *И* при некоторых значениях входящих в нее переменных высказываний. Выполнимыми являются формулы:

$$1.\ X;\quad 2.\ X \vee \overline{Y};\quad 3.\ X \to \overline{X}.$$

Будем называть формулу *невыполнимой* или *тождественно ложной*, если она при всех значениях входящих в нее переменных принимает значение *Л*. Отрицание тождественно истинной формулы будет, очевидно, тождественно ложной формулой, и обратно.

Можно поставить следующую задачу: указать единый способ (алгоритм), позволяющий для каждой формулы выяснить, является она тождественно истинной или нет. Имея такой способ, мы одновременно получим также и способ узнавать, будет ли данная формула выполнимой или нет. В самом деле, имея возможность конечным числом действий проверить, является ли произвольная формула тождественно истинной или нет, мы можем для произвольной формулы $\mathfrak{A}$ решить вопрос, является ли $\overline{\mathfrak{A}}$ тождественно истинной формулой или нет. Если $\overline{\mathfrak{A}}$ оказалась тождественно истинной, то это значит, что $\mathfrak{A}$ тождественно ложная и, следовательно, невыполнимая; если $\overline{\mathfrak{A}}$ не является тождественно истинной, то, значит, $\mathfrak{A}$ не является тождественно ложной и, следовательно, будет выполнимой.

Поставленная задача носит название *проблемы разрешения.* Она ставится не только для алгебры высказываний, но и для других логических систем. Для алгебры высказываний эта проблема легко решается.

Пусть $\mathfrak{A}(X_1, \ldots, X_n)$ — формула алгебры высказываний, содержащая элементарные высказывания X_1, $X_2, \ldots, X_n$. Эта формула определяет некоторую функцию переменных $X_1, X_2, \ldots, X_n$, причем как переменные $X_1, X_2, \ldots, X_n$, так и функция $\mathfrak{A}$ могут принимать лишь два значения; число возможных комбинаций значений переменных $X_1, \ldots, X_n$ конечно и равно в точности 2^n. Для каждой такой комбинации мы можем узнать значение формулы $\mathfrak{A}$, подставив вместо $X_1, \ldots, X_n$ их значения и вычислив затем значение формулы $\mathfrak{A}$, что, как мы знаем, достигается конечным числом действий. Узнав значение формулы $\mathfrak{A}$ для каждой комбинации значений переменных $X_1, \ldots, X_n$, мы выясним, является ли она тождественно истинной или нет.

Изложенный способ, конечно, дает принципиальное решение проблемы разрешения, но число испытаний, которые необходимо произвести даже для несложных формул, настолько велико, что часто такая прямая проверка является практически неосуществимой.

Существует другой способ, основанный на приведении формул к так называемой «нормальной форме». Нормальные формы употребляются и в других вопросах математической логики.

Будем называть *элементарным произведением* (соответственно — *элементарной суммой*) произведение (сумму) переменных и их отрицаний. Термин «сумма элементарных произведений» (соответственно — «произведение элементарных сумм») будем понимать расширенно, включая в него и случай, когда сумма сводится к одному слагаемому (соответственно произведение — к одному множителю).

Теорема 1. *Чтобы элементарная сумма была тождественно истинной, необходимо и достаточно, чтобы в ней содержалась хотя бы одна пара слагаемых, из которых одно есть некоторая переменная, а другое — ее отрицание.*

Условие достаточно. В самом деле, если такая пара слагаемых найдется, то сумма имеет вид

$$X \vee \bar{X} \vee Y \vee Z \vee \dots$$

(слагаемых Y, Z, ... может и не быть). Но сумма $X \vee \bar{X}$ тождественно истинна, поэтому и вся рассматриваемая нами сумма тождественна истинна, каковы бы ни были слагаемые Y, Z, ...

Условие необходимо. Допустим, что такой пары слагаемых, из которых одно является отрицанием другого, в сумме нет. В таком случае мы можем каждой переменной, не стоящей под знаком отрицания, дать значение *Л*, а каждой переменной, стоящей под знаком отрицания, значение *И*. Это можно сделать, так как ни одна переменная не входит в сумму одновременно и с отрицанием и без отрицания. После указанной подстановки каждое слагаемое примет значение *Л*. Тогда и вся элементарная сумма примет значение *Л*, и, следовательно, формула не является тождественно истинной, что и требовалось доказать.

Аналогично доказывается

Теорема 2. *Чтобы элементарное произведение было тождественно ложным, необходимо и достаточно, чтобы в нем содержалась хоть одна пара множителей, из которых один является отрицанием другого.*

Формула, равносильная данной формуле и представляющая собой сумму элементарных произведений, называется *дизъюнктивной нормальной формой* данной формулы.

Как мы уже говорили, все логические операции можно свести к трем: $\&$, $\vee$ и $^-$. Предположим, что формулы, для которых мы будем определять нормальные формы, содержат только эти операции. Знак $^-$ можно предполагать отнесенным только к элементарным высказываниям (см. замечание в конце § 2).

Как мы видели выше, с формулой, составленной из переменных и их отрицаний при помощи операций $\&$ и $\vee$, можно производить такие же преобразования, как с алгебраическими выражениями. Можно, следовательно, раскрыть все скобки и представить всякую такую формулу в виде суммы элементарных произведений. Таким образом, доказано, что для любой формулы существует дизъюнктивная нормальная форма.

Пример. Найдем дизъюнктивную нормальную форму формулы

$$X \& \overline{(\overline{Y} \& Z)} \& (U \vee V).$$

Приведем эту формулу сначала к виду, в котором отрицание относится только к элементарным высказываниям:

$$X \& (Y \vee \overline{Z}) \& (U \vee V).$$

Затем, применяя закон дистрибутивности, будем раскрывать скобки, производя действия, аналогичные умножению многочленов. Тогда получим

$$(XY \vee X\overline{Z})(U \vee V)$$

и далее

$$XYU \vee XYV \vee X\overline{Z}U \vee X\overline{Z}V.$$

Полученная формула является дизъюнктивной нормальной формой исходной формулы.

Конъюнктивной нормальной формой данной формулы называется равносильная ей формула, представляющая собой произведение элементарных сумм.

Докажем, что для каждой формулы существует конъюнктивная нормальная форма.

Пусть сначала $\mathfrak{A}$ — произвольная формула, содержащая только операции $\&$, $\vee$ и $^{-}$. Рассмотрим двойственную $\mathfrak{A}$ формулу $\mathfrak{A}^*$. Пусть $\mathfrak{B}^*$ — дизъюнктивная нормальная форма формулы $\mathfrak{A}^*$, а $\mathfrak{B}$ — формула, двойственная $\mathfrak{B}^*$. Так как $\mathfrak{A}^*$ и $\mathfrak{B}^*$ равносильны, то по закону двойственности $\mathfrak{A}$ и $\mathfrak{B}$ также равносильны. Формула $\mathfrak{B}^*$, будучи дизъюнктивной нормальной формой, представляет собой сумму элементарных произведений. Легко видеть, что двойственная $\mathfrak{B}^*$ формула $\mathfrak{B}$ является произведением элементарных сумм. И так как $\mathfrak{B}$ равносильна $\mathfrak{A}$, то, следовательно, она является конъюнктивной нормальной формой формулы $\mathfrak{A}$. Так как для каждой формулы существует равносильная ей формула, содержащая только операции $\&$, $\vee$ и $^{-}$, то, следовательно, для каждой формулы существует конъюнктивная нормальная форма, что и требовалось доказать.

Примеры. Найдем дизъюнктивную и конъюнктивную нормальные формы для некоторых формул.

1. $X(X \to Y)$.

Прежде всего исключим знак $\to$, заменив формулу следующей:

$$X(\overline{X} \vee Y).$$

Эта формула уже представляет собой конъюнктивную нормальную форму. Раскрыв скобки, получим дизъюнктивную нормальную форму:

$$X\overline{X} \vee XY.$$

2. $\overline{X \vee Y} \sim XY$.

Исключим знак $\sim$, пользуясь формулой (20) § 2. Получим формулу

$$\overline{X \vee Y}XY \vee (X \vee Y)\overline{XY}.$$

Преобразуем эту формулу так, чтобы знак отрицания стоял над элементарными высказываниями:

$$\overline{X}\overline{Y}XY \vee (X \vee Y)(\overline{X} \vee \overline{Y}).$$

Раскрывая скобки, получим дизъюнктивную нормальную форму:

$$\overline{X}\overline{Y}XY \vee X\overline{X} \vee X\overline{Y} \vee Y\overline{X} \vee Y\overline{Y}.$$

Чтобы получить конъюнктивную нормальную форму, пользуясь формулой (19) § 2, заменяем исходную формулу произведением двух сумм:

$$((X \vee Y) \vee XY)(\overline{XY} \vee \overline{X \vee Y}).$$

Преобразуем эту формулу к виду, в котором знаки отрицания стоят только над элементарными высказываниями:

$$(X \vee Y \vee XY)(\overline{X} \vee \overline{Y} \vee \overline{X}\overline{Y}).$$

Применяя второй дистрибутивный закон, получим конъюнктивную нормальную форму нашей формулы:

$$(X \vee Y \vee X)(X \vee Y \vee Y)(\overline{X} \vee \overline{Y} \vee \overline{X})(\overline{X} \vee \overline{Y} \vee \overline{Y}).$$

Заметим, что для каждой формулы $\mathfrak{A}$ существует не одна дизъюнктивная и не одна конъюнктивная нормальная форма. Произведя разными способами дистрибутивные операции, мы можем прийти к различным нормальным формам. Рассмотрим, например, формулу

$$X \vee Y \& Z.$$

Эта формула представляет собой дизъюнктивную нормальную форму. Однако ее можно привести дистрибутивными операциями и к другой дизъюнктивной нормальной форме. Применив второй закон дистрибутивности, получим

$$(X \vee Y)(X \vee Z).$$

Применив к этой формуле первый закон дистрибутивности, получим

$$XX \vee XZ \vee YX \vee YZ.$$

Эта формула также является дизъюнктивной нормальной формой формулы $X \vee YZ$. Конечно, различные нормальные формы различны лишь по виду. Все они должны быть равносильны. В дальнейшем (см. § 6) мы выделим среди нормальных форм данной формулы так называемые *совершенные нормальные формы* — дизъюнктивную и конъюнктивную.

Пользуясь нормальными формами, можно указать более простое решение проблемы разрешения, чем метод непосредственной проверки. Допустим, что формула $\mathfrak{A}$ тождественно истинна. Рассмотрим ее конъюнктивную нормальную форму $\mathfrak{A}'$. Она имеет вид произведения $\mathfrak{A}'_1 \ldots \mathfrak{A}'_n$, где каждый множитель является элементарной суммой (в частном случае n может быть равно единице). Так как $\mathfrak{A}'$ тождественно истинна, то каждый множитель должен быть тождественно истинной формулой. Но $\mathfrak{A}'_i$ — элементарная сумма, а по теореме 1 такая сумма может быть тождественно истинной в том и только в том случае, когда она содержит некоторую переменную вместе с ее отрицанием. Поэтому, если формула $\mathfrak{A}$ тождественно истинна, то каждый множитель ее конъюнктивной нормальной формы содержит в качестве слагаемых какую-нибудь переменную и ее отрицание. Мы получили, таким образом, критерий тождественной истинности формулы:

Для того чтобы формула была тождественно истинной, необходимо и достаточно, чтобы каждый множитель ее конъюнктивной нормальной формы имел по крайней *мере два слагаемых, из которых одно является какой-нибудь переменной, а другое — ее отрицанием.*

В силу симметричности операций сложения и умножения в логическом исчислении можно аналогичным образом показать, что:

Для того чтобы формула была тождественно ложной, необходимо и достаточно, чтобы каждое слагаемое ее дизъюнктивной нормальной формы содержало по крайней мере одну пару множителей, из которых один есть какая-нибудь переменная, а другой — ее отрицание.

Полученные критерии дают полное решение проблемы разрешения.

Примеры.

1. Выяснить, будет ли тождественно истинной формула

$$Y \vee X\overline{Y} \vee \overline{X}\overline{Y}.$$

Выносим из двух последних слагаемых $\overline{Y}$ за скобку:

$$Y \vee \overline{Y}(X \vee \overline{X}).$$

Применив второй дистрибутивный закон, получим конъюнктивную нормальную форму нашей формулы:

$$(Y \vee \overline{Y})(Y \vee X \vee \overline{X}).$$

Так как каждый множитель этой формулы содержит какую-нибудь переменную вместе с ее отрицанием, то формула тождественно истинна.

2. Выяснить, будет ли тождественно истинной формула

$$X \& Y \& Z \vee \overline{X} \& \overline{Y} \& Z \vee X \& \overline{Y} \& \overline{Z}.$$

Приведем эту формулу к конъюнктивной нормальной форме. Применив второй дистрибутивный закон, получим ряд формул, соединенных знаком &:

$$(X \vee \overline{X} \vee X)(X \vee \overline{X} \vee \overline{Y}) \ldots$$

Среди множителей этой конъюнктивной нормальной формы найдется формула

$$(X \vee \overline{Y} \vee \overline{Z}).$$

Эта формула не содержит никакой переменной вместе с ее отрицанием и потому не является тождественно истинной. Следовательно, и наша исходная формула не является тождественно истинной. Выясним, будет ли она выполнимой. Для этого заметим, что сама формула представляет собой дизъюнктивную нормальную форму. И так как ни одно из ее слагаемых не содержит переменной вместе с ее отрицанием, то она не является тождественно ложной; следовательно, она выполнима.

§ 5. Представление произвольной двузначной функции посредством формулы алгебры высказываний

Пусть $F(X_1, \ldots, X_n)$ — произвольная функция n переменных $X_1, \ldots, X_n$, причем и переменные и сама функция принимают только два значения *И* и *Л*. Поставим следующий вопрос: *можно ли такую функцию представить какой-либо формулой алгебры высказываний?*

Рассмотрим формулу

$$F(И, \ldots, И)\, X_1 \ldots X_n \vee F(И, \ldots, И, Л)\, X_1 \ldots$$
$$\ldots X_{n-1}\overline{X}_n \vee \ldots \vee F(Л, \ldots, Л)\, \overline{X}_1 \ldots \overline{X}_n, \qquad \text{(a)}$$

которая составлена следующим образом.

Каждое слагаемое этой суммы представляет собой произведение, в котором первый множитель является значением функции F при некоторых определенных значениях переменных $X_1, \ldots, X_n$, остальные же множители представляют собой переменные X_i или отрицания этих переменных. При этом под знаком отрицания находятся те и только те переменные, которые в первом множителе имеют значение *Л*.

Например,

$$F(И, Л, Л, \ldots, И, Л)\, X_1\overline{X}_2\overline{X}_3 \ldots X_{n-1}\overline{X}_n.$$

Вместе с тем рассматриваемая сумма содержит всевозможные слагаемые указанного вида. Нетрудно видеть, что формула (a) определяет именно функцию $F(X_1, \ldots, X_n)$. В самом деле, дадим определенные значения переменным.

Например,

$$X_1 \text{ есть } Л, \quad X_2 \text{ есть } И, \ \ldots, \ X_n \text{ есть } И.$$

Тогда функция примет значение $F(Л, И, \ldots, И)$.

Рассмотрим слагаемое формулы (а)

$$F(Л, И, \ldots, И)\, X_1 X_2 \ldots X_n.$$

Если переменным $X_1, \ldots, X_n$ в этом слагаемом дать те же значения, какие они имеют в первом множителе, т. е. X_1 есть $Л$, X_2 есть $И$, ..., X_n есть $И$, то получится выражение

$$F(Л, И, \ldots, И)\, \overline{Л} И \ldots И.$$

В этом выражении все множители, кроме, быть может, первого, имеют значение $И$, так как знаки отрицания стоят только над символами $Л$, символы же $И$ входят без знака отрицания. В таком случае на основании равносильности (16) из § 2 можно из произведения все эти истинные множители удалить. Следовательно, рассматриваемое слагаемое равносильно первому множителю $F(Л, И, \ldots, И)$. Во всяком другом слагаемом знаки отрицания над переменными распределятся иначе, чем в рассматриваемом, но тогда при замене переменных теми же значениями в произведение либо войдет символ $Л$ без знака отрицания, либо символ $И$ под знаком отрицания. В таком случае один из множителей имеет значение $Л$ и, следовательно, все произведение имеет значение $Л$. Итак, при рассматриваемой подстановке в переменные значений $И$ и $Л$ все слагаемые, кроме одного, имеют значение $Л$, а одно слагаемое имеет значение $F(Л, И, \ldots, И)$, являющееся значением функции F при данных значениях переменных. На основании равносильности (17) из § 2 все слагаемые, кроме $F(Л, И, \ldots, И)$, можно удалить из суммы и сама сумма имеет то же значение, что и слагаемое $F(Л, И, \ldots, И)$. Итак, при произвольной подстановке значений $X_1, \ldots, X_n$ в (а) эта формула имеет то же значение, что и функция F при той же подстановке.

Таким образом, мы показали, что *каждую двузначную функцию* $F(X_1, \ldots, X_n)$ *можно представить в виде формулы алгебры высказываний, именно в виде формулы* (а).

Наше представление пригодно и для функции $\overline{F}(X_1, \ldots, X_n)$. Имеем

$$\overline{F}(X_1, \ldots, X_n) \text{ равносильно } \overline{F}(И, \ldots, И)\, X_1 \ldots X_n \vee \ldots$$
$$\ldots \vee \overline{F}(Л, \ldots, Л)\, \overline{X}_1 \ldots \overline{X}_n.$$

Переходя от этих равносильных формул к их отрицаниям, мы получим

$$\overline{\overline{F}}(X_1, \ldots, X_n) \text{ равносильно }$$
$$\overline{\overline{F}(И, \ldots, И)\, X_1 \ldots X_n \vee \ldots \vee \overline{F}(Л, \ldots, Л)\, \overline{X}_1 \ldots \overline{X}_n}.$$

Проделав преобразования на основании равносильностей (1), (10) и (11) § 2, мы получим

$$F(X_1, \ldots, X_n) \text{ равносильно } (F(И, \ldots, И) \vee \overline{X}_1 \vee \ldots$$
$$\ldots \vee \overline{X}_n) \,\&\, \ldots \,\&\, (F(Л, \ldots, Л) \vee X_1 \vee \ldots \vee X_n).$$

Таким образом, мы нашли для представления рассматриваемой двузначной функции другую форму:

$$(F(Л, \ldots, Л) \vee X_1 \vee \ldots \vee X_n) \,\&\, \ldots$$
$$\ldots \,\&\, (F(И, \ldots, И) \vee \overline{X}_1 \vee \ldots \vee \overline{X}_n). \quad \text{(b)}$$

Нетрудно получить для представления двузначной функции такие формулы, которые содержат только переменные элементарные высказывания.

Допустим, что функция $F(X_1, \ldots, X_n)$ не является тождественно ложной. В таком случае при некоторых значениях переменных она принимает значение *И*. В представлении нашей функции посредством формулы (а) значение *И* могут иметь только те слагаемые, у которых первый множитель имеет значение *И* (так как при ложности одного множителя все произведение ложно). С другой стороны, на основании соотношения (17) § 2 ложные слагаемые можно удалять из суммы. Поэтому в сумме (а) мы можем оставить только те слагаемые, у которых первый множитель имеет значение *И*. Такие слагаемые в рассматриваемом случае должны быть. После удаления ложных слагаемых в каждом из оставшихся слагаемых первый множитель имеет значение *И*. В таком случае на основании (16) § 2 его можно из произведения удалить. *В результате мы получим формулу, равносильную формуле* (а) *и содержащую только переменные элементарные высказывания.* Эта формула является логической суммой различных произведений вида $X_1'X_2' \ldots X_n'$, где X_i' обозначает X_i или $\overline{X}_i$. Как легко видеть из приведенных выше рассуждений, каждой не тождественно ложной функции $F(X_1, X_2, \ldots, X_n)$ отвечает единственное представление такого вида.

Если функция $F(X_1, \ldots, X_n)$ не является тождественно истинной, то ее представление в виде формулы, не содержащей постоянных элементарных высказываний, можно аналогичным образом получить из формулы (b). Это второе представление функции $F(X_1, \ldots, X_n)$, как легко усмотреть, будет двойственным первому.

Примеры.

1. Рассмотрим функцию трех переменных $F(X_1, X_2, X_3)$, которая принимает значение *И*, если все переменные принимают одинаковые значения, и *Л* в остальных случаях. Тогда $F(И, И, И)$ есть *И* и $F(Л, Л, Л)$ есть *И*; при других же значениях переменных $F(X_1, X_2, X_3)$ имеет значение *Л*. Мы можем эту функцию представить следующим образом:

$$X_1X_2X_3 \vee \bar{X}_1\bar{X}_2\bar{X}_3.$$

2. Пусть $F(X_1, X_2, X_3, X_4)$ имеет значение *И* тогда и только тогда, когда хотя бы два каких-нибудь аргумента принимают значение *Л*. В этом случае удобно прибегнуть к второму представлению функции. Это представление будет иметь вид

$$(\bar{X}_1 \vee \bar{X}_2 \vee \bar{X}_3 \vee X_4) \,\&\, (\bar{X}_1 \vee \bar{X}_2 \vee X_3 \vee \bar{X}_4) \,\&\, (\bar{X}_1 \vee X_2 \vee \bar{X}_3 \vee \bar{X}_4) \,\&\, (X_1 \vee \bar{X}_2 \vee \bar{X}_3 \vee \bar{X}_4) \,\&\, (\bar{X}_1 \vee \bar{X}_2 \vee \bar{X}_3 \vee \bar{X}_4)$$

§ 6. Совершенные нормальные формы

В предыдущем параграфе мы для произвольной не тождественно ложной функции $F(X_1, X_2, \ldots X_n)$, зависящей от n переменных, нашли формулу алгебры высказываний, представляющую эту функцию и являющуюся логической суммой различных произведений вида $X'_1X'_2 \ldots \ldots X'_n$, где X'_i обозначает X_i или $\bar{X}_i$. Там же мы отметили, что *каждая не тождественно ложная функция* $F(X_1, X_2, \ldots X_n)$ *имеет единственное представление указанного типа.* Такое представление является дизъюнктивной нормальной формой. Мы знаем, однако, что одна и та же функция может быть представлена различными дизъюнктивными нормальными формами. Таким образом, мы нашли способ выбирать из различных дизъюнктивных нормальных форм, представляющих данную функцию, одну определенную, являющуюся суммой слагаемых вида $X'_1 \ldots X'_n$. Получаемые таким способом дизъюнктивные нормальные формы мы будем называть *совершенными дизъюнктивными нормальными формами.* Можно дать другое определение совершенной дизъюнктивной нормальной формы:

Совершенной дизъюнктивной нормальной формой формулы $\mathfrak{A}(X_1, \ldots X_n)$, *содержащей* n *различных переменных, называется дизъюнктивная нормальная форма, обладающая следующими свойствами:*

a) *в ней нет двух одинаковых слагаемых;*

b) *ни одно слагаемое не содержит двух одинаковых множителей;*

c) *никакое слагаемое не содержит переменной вместе с ее отрицанием;*

d) *в каждом слагаемом содержится в качестве множителя либо переменная* X_i, *либо ее отрицание, где* $i = 1, 2, \ldots, n$.

Нетрудно видеть, что это определение эквивалентно предыдущему. В самом деле, с одной стороны, на основании d) всякое слагаемое дизъюнктивной нормальной формы должно содержать n множителей $X'_1, \ldots, X'_n$. С другой стороны, в силу b) и c) никакого другого множителя это слагаемое содержать не может, так как такой множитель был бы или X_i, или $\bar{X}_i$, а в нашем слагаемом уже есть множитель, представляющий собой или X_i или $\bar{X}_i$. Таким образом, наша форма состоит из слагаемых вида $X'_1 X'_2 \ldots X'_n$. которые в силу условия a) все различны. Поэтому сумма этих слагаемых является тем представлением формулы $\mathfrak{A}(X_1, \ldots, X_n)$, которое мы определили ранее.

Условия a), b), c), d) являются, таким образом, необходимыми и достаточными для того, чтобы дизъюнктивная нормальная форма была совершенной нормальной формой. Вместе с тем эти условия дают возможность высказать правила, позволяющие приводить любую не тождественную ложную формулу к совершенной дизъюнктивной форме. Опишем эти правила. Пусть дана произвольная формула $\mathfrak{A}_1(X_1, \ldots, X_n)$. Приведем ее сначала к какой-нибудь дизъюнктивной нормальной форме. Затем, если какое-нибудь слагаемое $\mathfrak{B}$ не содержит переменной X_i, то заменим его суммой

$$X_i \,\&\, \mathfrak{B} \vee \overline{X}_i \,\&\, \mathfrak{B}.$$

Эта замена представляет собой равносильное преобразование, так как

$$X_i \,\&\, \mathfrak{B} \vee \overline{X}_i \,\&\, \mathfrak{B} \text{ равносильно } (X_i \vee \overline{X}_i) \,\&\, \mathfrak{B}.$$

Но $X_i \vee \overline{X}_i$ тождественно истинно, поэтому

$$(X_i \vee \overline{X}_i) \,\&\, \mathfrak{B} \text{ равносильно } \mathfrak{B}$$

и, следовательно,

$$X_i \,\&\, \mathfrak{B} \vee \overline{X}_i \,\&\, \mathfrak{B} \text{ равносильно } \mathfrak{B}.$$

Таким образом, мы можем изменить нашу нормальную форму так, чтобы условие d) было выполнено.

Если в полученном выражении окажутся одинаковые слагаемые, то, удалив все, кроме одного из них, мы получим опять равносильное выражение. Если после этого в некоторых слагаемых окажется по нескольку одинаковых множителей, то лишние множители можно удалить. Наконец, можно удалить все те слагаемые, которые содержат какую-нибудь переменную вместе с ее отрицанием, так как слагаемые представляют собой тождественно ложные выражения. Если бы все слагаемые оказались таковыми, то, значит, вся сумма тождественно ложна. А тогда и формула $\mathfrak{A}$ тождественно ложна и в силу этого не имеет совершенной дизъюнктивной нормальной формы. Поэтому, если формула $\mathfrak{A}$ не тождественно ложна, то в произвольной ее дизъюнктивной нормальной форме должны присутствовать слагаемые, удовлетворяющие условию c). После удаления всех слагаемых, содержащих какую-нибудь переменную вместе с ее отрицанием, мы получим дизъюнктивную нормальную форму формулы $\mathfrak{A}$, которая удовлетворяет условиям a), b), c), d) и, следовательно, является совершенной нормальной формой. Заметим, что нам нет необходимости знать заранее, является ли $\mathfrak{A}$ тождественно ложной или нет. Проделывая указанные операции, мы это выясним после того, как удалим все слагаемые, содержащие какую-нибудь переменную вместе с ее отрицанием. Если $\mathfrak{A}$ тождественно ложна, то все слагаемые будут удалены и мы не получим совершенной дизъюнктивной нормальной формы.

Аналогичным образом определяется совершенная конъюнктивная нормальная форма. Это определение проводится в терминах, двойственных тем, которые мы употребляли при определении совершенной дизъюнктивной нормальной формы.

Совершенной конъюнктивной нормальной формой формулы $\mathfrak{A}(X_1, \ldots, X_n)$ от n *переменных называется конъюнктивная нормальная форма, представляющая собой произведение различных сумм вида* $X_1' \vee X_2' \vee \ldots \vee X_n'$.

Можно также высказать эквивалентное определение в форме условий.

Совершенной конъюнктивной нормальной формой формулы $\mathfrak{A}(X_1, \ldots, X_n)$ *называется ее конъюнктивная нормальная форма, удовлетворяющая следующим условиям:*

a′) *в ней нет двух одинаковых множителей;*

b′) *ни один множитель не содержит двух одинаковых слагаемых;*

c′) *ни один множитель не содержит какой-нибудь переменной вместе с ее отрицанием;*

d′) *каждый множитель содержит в качестве слагаемого или* X_i, *или* $\bar{X}_i$ *для любого* $i = 1, 2, \ldots, n$.

Можно доказать, что каждая не тождественно истинная формула имеет единственную, с точностью до порядка расположения множителей и слагаемых, совершенную конъюнктивную нормальную форму. Правила приведения произвольной формулы к совершенной конъюнктивной нормальной форме аналогичны тем, которые мы описали для нахождения совершенной дизъюнктивной нормальной формы, и выражаются в двойственных терминах. Доказательства всех утверждений, касающихся совершенной конъюнктивной нормальной формы, можно получить из закона двойственности или же провести их так же, как мы это делали для совершенной дизъюнктивной нормальной формы.

Совершенные нормальные формы позволяют дать критерий равносильности двух произвольных формул $\mathfrak{A}$ и $\mathfrak{B}$.

В самом деле, каковы бы ни были формулы $\mathfrak{A}$ и $\mathfrak{B}$, можно предполагать, что они содержат одни и те же переменные. Если бы это было не так и формула $\mathfrak{A}$, например, не содержала переменной V, входящей в $\mathfrak{B}$, то $\mathfrak{A}$ можно было бы заменить равносильной формулой $\mathfrak{A} \& (V \vee \bar{V})$, которая уже содержит переменную V. Таким образом, любые две формулы можно заменить равносильными им формулами, содержащими одинаковые переменные. После этого эти формулы надо привести к совершенным дизъюнктивным или конъюнктивным нормальным формам. Если $\mathfrak{A}$ и $\mathfrak{B}$ — равносильные формулы, то в силу единственности совершенных нормальных форм как дизъюнктивные, так и конъюнктивные нормальные формы этих формул должны полностью совпадать. Таким образом, сравнение совершенных нормальных форм формул $\mathfrak{A}$ и $\mathfrak{B}$ решает вопрос об их равносильности.

Примеры.

1. *Привести к совершенной дизъюнктивной нормальной форме формулу* $X \vee Y(X \vee \bar{Y})$.

Раскрыв скобки, мы получим дизъюнктивную нормальную форму этой формулы:

$$X \vee YX \vee Y\bar{Y}.$$

Однако полученная формула не является совершенной нормальной формой, так как первое слагаемое не содержит переменной Y, а последнее содержит переменную Y вместе с ее отрицанием. Заменив X на $XY \vee X\bar{Y}$, получим формулу

$$XY \vee X\bar{Y} \vee YX \vee Y\bar{Y}.$$

Удалив два последних слагаемых, получим формулу

$$XY \vee X\bar{Y}.$$

Эта формула удовлетворяет условиям a), b), c), d) и, следовательно, является совершенной дизъюнктивной нормальной формой формулы $X \vee Y(X \vee \bar{Y})$.

Полученная совершенная форма позволяет упростить данную нам формулу. Вынося в совершенной форме X за скобки, получим формулу $X(Y \vee \bar{Y})$, которая равносильна формуле X.

2. *Привести к совершенной конъюнктивной нормальной форме формулу*

$$(X \vee Y)(\overline{Y} \vee Z) \vee (X \vee \overline{Y})(Y \vee Z).$$

Пользуясь вторым дистрибутивным законом, мы приведем эту формулу к конъюнктивной нормальной форме. Получим формулу

$$(X \vee Y \vee X \vee \overline{Y})(X \vee Y \vee Y \vee Z)(\overline{Y} \vee Z \vee X \vee \overline{Y})\,\& \\ \&\,(\overline{Y} \vee Z \vee Y \vee Z).$$

Удалим тождественно истинные множители, а в оставшихся множителях удалим повторяющиеся слагаемые. Получим

$$(X \vee Y \vee Z)(\overline{Y} \vee Z \vee X).$$

Полученная формула удовлетворяет условиям a′), b′), c′), d′) и поэтому является совершенной конъюнктивной нормальной формой данной формулы. Пользуясь вторым дистрибутивным законом, можно дальше упростить эту формулу. Выделяя слагаемое $X \vee Z$, получим

$$X \vee Z \vee Y\overline{Y}.$$

Отбрасывая ложное слагаемое $Y\overline{Y}$, получим окончательно

$$X \vee Z.$$

В заключение этой главы отметим некоторые соотношения равносильности, полезные для упрощения формул (первые два из этих соотношений совпадают с соотношениями (8) и (9)):

$$X \vee XY \text{ равносильно } X; \tag{21}$$

$$X(X \vee Y) \text{ равносильно } X; \tag{22}$$

$$X \vee \overline{X}Y \text{ равносильно } X \vee Y; \tag{23}$$

$$\overline{X} \vee XY \text{ равносильно } \overline{X} \vee Y; \tag{24}$$

$$X(\overline{X} \vee Y) \text{ равносильно } XY; \tag{25}$$

$$\overline{X}(X \vee Y) \text{ равносильно } \overline{X}Y. \tag{26}$$

Эти соотношения можно формулировать в виде правил следующим образом.

Первое. *Если слагаемое некоторой суммы входит множителем в другое слагаемое, то это второе слагаемое можно из суммы удалить.*

Второе. *Если множитель некоторого произведения входит слагаемым в другой множитель, то второй множитель можно удалить.*

Третье и четвертое. *В каждом слагаемом можно удалить множитель, который равносилен отрицанию другого слагаемого.*

Пятое и шестое. *В каждом множителе можно удалить слагаемое, которое равносильно отрицанию другого множителя.*

Примеры.

1. $X \vee XY \vee YZ \vee \bar{X}Z$.

На основании (21) удалим XY. На основании (23) удалим в последнем слагаемом множитель $\bar{X}$. Получим

$$X \vee YZ \vee Z.$$

На основании (21) удалим YZ. Получим

$$X \vee Z.$$

2. $(X \vee Y)(\bar{X}\bar{Y} \vee Z) \vee \bar{Z} \vee (X \vee Y)(U \vee V)$.

Так как $\bar{X}\bar{Y}$ равносильно $\overline{X \vee Y}$, то на основании (25) слагаемое $\bar{X}\bar{Y}$ можно удалить. Получим

$$(X \vee Y) Z \vee \bar{Z} \vee (X \vee Y)(U \vee V).$$

На основании (24) множитель Z можно удалить. Получим

$$(X \vee Y) \vee \bar{Z} \vee (X \vee Y)(U \vee V).$$

Последнее слагаемое содержит множитель $X \vee Y$, совпадающий с первым слагаемым. Поэтому на основании (21) последнее слагаемое можно удалить. Получим окончательно

$$X \vee Y \vee \bar{Z}.$$

ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

§ 1. Понятие формулы

Описание алгебры высказываний, которое мы дали в предыдущей главе, и все рассуждения об этой системе, которые мы там проводили, вполне удовлетворяют требованиям строгости, изложенным во введении, так как они ни в какой мере не используют понятия актуальной бесконечности, т. е. являются конструктивными.

В самом деле, алгебра высказываний рассматривает конечные конфигурации символов и взаимоотношения между ними. Этими конфигурациями символов являются формулы, содержащие буквы и знаки различных операций. Вместо букв можно подставлять символы *И* и *Л* и затем вычислять значение, которое при этом получит формула.

Число букв в формуле конечно, число всевозможных размещений символов *И* и *Л* в этой формуле также конечно. Определения логических операций содержат тоже конечное число условий. С другой стороны, высказывания о формулах мы делали только в терминах указанных символов и отношений между ними, и поэтому подобные высказывания были свободны от употребления актуальной бесконечности.

Несмотря на это, не всегда возможно непосредственно применить алгебру высказываний к высказываниям математики, не привлекая при этом понятия актуальной бесконечности. Чтобы это можно было всегда сделать, мы должны предположить, что каждое высказывание математики либо истинно, либо ложно. Однако подобное допущение уже опирается на понятие актуальной бесконечности. Оно представляет собой закон исключенного третьего, распространенный при этом и на бесконечные совокупности. В таком виде этот принцип не может быть принят в той части математики, которая ставит себе, в частности, задачу обосновать этот закон, показав, что пользование им не приводит к противоречию.

В настоящей главе мы рассмотрим аксиоматическую логическую систему, которая в известном смысле адекватна алгебре высказываний. Систему эту мы будем называть *исчислением высказываний.*

Нам необходимо дать достаточно полное изложение исчисления высказываний ввиду того, что это исчисление входит как составная часть во все другие логические исчисления, которые мы будем в дальнейшем рассматривать.

Описание всякого исчисления, как было сказано во введении, заключает в себе описание символов этого исчисления, формул, являющихся конечными конфигурациями символов, и после этого определение выводимых формул.

Символы исчисления высказываний состоят из знаков трех категорий.

1. Символы первой категории представляют собой большие латинские бувкы A, B, ..., X, Y, Z и те же буквы с индексами A_1, A_2, ... Эти символы мы будем называть *переменными высказываниями.*

2. Вторую категорию составляют символы, которые имеют общее название логических связок. Этих символов имеется четыре:

$$\&, \quad \vee, \quad \rightarrow \quad \text{и} \quad - .$$

Они носят следующие названия: первый — знак *конъюнкции* или логического *умножения*, второй — знак *дизъюнкции* или логического *сложения*, третий — знак *импликации* или логического *следования* и последний — знак *отрицания.*

3. Третью категорию составляет пара символов ( ), называемая *скобками.*

Иных символов, кроме указанных, исчисление высказываний не имеет.

Формулы исчисления высказываний представляют собой конечные последовательности символов описанных категорий. Эти последовательности можно записывать в виде слов в алфавите, составленном из всех указанных символов.

Для обозначения формул мы обычно будем употреблять большие готические буквы $\mathfrak{A}$, $\mathfrak{B}$, ... Буквы эти не являются символами исчисления. Они представляют собой только условные сокращенные обозначения формул.

Не всякое слово, составленное из рассматриваемых символов, является формулой. Полное определение формулы имеет рекурсивный характер: указываются некоторые исходные формулы и затем правила, позволяющие из формул образовывать новые формулы. Смысл этого определения состоит в том, что под формулой мы будем понимать такие и только такие слова, которые могут быть образованы из исходных формул путем последовательного применения правил образования новых формул, указанных в определении.

Определение формулы:

a) Переменное высказывание есть формула.

b) Если $\mathfrak{A}$ и $\mathfrak{B}$ — формулы, то слова

$$(\mathfrak{A} \mathbin{\&} \mathfrak{B}),$$

$$(\mathfrak{A} \vee \mathfrak{B}),$$

$$(\mathfrak{A} \rightarrow \mathfrak{B})$$

и

$$-\mathfrak{A}$$

— также формулы.

В этом определении в a) указываются исходные формулы, которые здесь представляют собой переменные высказывания. Мы будем называть переменные высказывания *элементарными формулами.*

В b) указываются правила, позволяющие из полученных формул образовать новые. Таким образом, понятие формулы полностью определено.

Приведем примеры формул исчисления высказываний. Переменные высказывания A и B являются формулами в силу a). Следовательно, на основании b) слова

$$(A \rightarrow B),$$

$$-A$$

— также формулы. Тогда на том же основании

$$((-A \mathbin{\&} (A \rightarrow B)) \vee (A \mathbin{\&} B))$$

— также формула.

Легко видеть, что слова

$$((A \to -(A \& B)) \to ((C \vee D) \to (A \& B))),$$
$$(((A \& B) \& C) \& D),$$
$$(A \to (B \to (C \to D)))$$

являются формулами.

Наоборот, следующие слова не являются формулами:

$$(A \& B; \quad A - B; \quad \& A;$$
$$A \to B; \quad A \& B; \quad A \vee B.$$

Первое из этих слов содержит незакрытую скобку. При конструкции формул на основании b) никогда не вводится незакрытая скобка. Следовательно, слово $(A \& B$ не может появиться ни при каком акте образования формулы. Легко видеть, что второе и третье слова никак не могут быть построены на основании b). Четвертое слово не является формулой потому, что хотя A и B — формулы, но соединение формул связкой $\to$ всегда сопровождается заключением в скобки; то же самое можно сказать и о двух последних словах.

Из определения формулы видно, что конструкция любой формулы имеет следующий характер.

Берется некоторый запас элементарных формул или, что то же, переменных высказываний:

$$\mathfrak{A}_1^{(0)}, \ \mathfrak{A}_2^{(0)}, \ \ldots, \ \mathfrak{A}_{k_0}^{(0)}.$$

Из них строится несколько формул вида

$$(\mathfrak{A}_i^{(0)} \to \mathfrak{A}_j^{(0)}); \quad (\mathfrak{A}_i^{(0)} \& \mathfrak{A}_j^{(0)}); \quad (\mathfrak{A}_i^{(0)} \vee \mathfrak{A}_j^{(0)}) \quad \text{и} \quad -\mathfrak{A}_i^{(0)}.$$

Полученные формулы обозначим $\mathfrak{A}_1^{(1)}, \ldots, \mathfrak{A}_{k_1}^{(1)}$.

Из формул $\mathfrak{A}_i^{(0)}$ и $\mathfrak{A}_j^{(1)}$ строятся таким же образом новые формулы $\mathfrak{A}_1^{(2)}, \ldots, \mathfrak{A}_{k_2}^{(2)}$ и т. д. В результате мы получаем формулу $\mathfrak{A}_1^{(n)}$, которая и есть формула $\mathfrak{A}$.

Все формулы $\mathfrak{A}_j^{(i)}$, построенные в указанном процессе, называются *частями формулы* $\mathfrak{A}$.

Приведенная схема конструкции формулы такова, что при построении мы осуществляем конструкцию и всех частей формулы. Конечно, можно задать формулу и иначе. Так как каждая формула есть конечная последовательность символов исчисления высказывания, то ее можно построить, просто указав, какой символ будет первым в этой последовательности, какой — вторым и т. д. Рассмотрим, например, слово

$$((A \& B) \rightarrow (C \vee D)).$$

Оно вполне определяется указанием, в какой последовательности взяты символы. Первым идет (, вторым A, третьим & и т. д. Однако не каждое слово является формулой. Мы еще должны доказать, что данное слово есть формула. Для доказательства этого мы должны показать, что написанное нами слово удовлетворяет определению формулы. Но по смыслу определения формулы доказать, что данное слово есть формула, означает построить его, исходя из элементарных формул, посредством конструкций, указанных в b).

Чтобы доказать, что приведенное нами для примера слово есть формула, мы должны рассуждать так. Так как A и B — формулы, то $(A \& B)$ — также формула. Так как C и D — формулы, то $(C \vee D)$ — также формула. Так как $(A \& B)$ и $(C \vee D)$ — формулы, то $((A \& B) \rightarrow \rightarrow (C \vee D))$ — также формула.

Из этого примера видно, что для доказательства того, что данное слово является формулой, требуется произвести его конструкцию по указанной выше схеме, так что при построении формулы мы должны построить и все ее части.

Заметим, однако, что данное нами определение части формулы не является точным. Точное определение части формулы имеет также рекурсивный характер, связанный с операциями, употребляемыми при конструкции формул. Именно, мы сначала высказываем определение частей элементарных формул, а затем, предполагая, что для формул $\mathfrak{A}$ и $\mathfrak{B}$ уже определены части, определяем части формул $(\mathfrak{A} \& \mathfrak{B})$, $(\mathfrak{A} \vee \mathfrak{B})$, $(\mathfrak{A} \rightarrow \mathfrak{B})$ и $\overline{\mathfrak{A}}$. Приведем это определение понятия «части формулы».

1. *Частью каждой элементарной формулы* (т. е. переменного высказывания) *является только она сама.*

2. Допустим, что определены части формул $\mathfrak{A}$ и $\mathfrak{B}$. Частями формулы $(\mathfrak{A} \& \mathfrak{B})$ будут все части формул $\mathfrak{A}$ и $\mathfrak{B}$ и сама формула $(\mathfrak{A} \& \mathfrak{B})$. Так же определяются части формул $(\mathfrak{A} \vee \mathfrak{B})$, $(\mathfrak{A} \rightarrow \mathfrak{B})$ и $\overline{\mathfrak{A}}$.

Части формулы легко усмотреть непосредственно из транскрипции формулы. Для этого и служат скобки, которые указывают последовательность, в которой надо производить операции, чтобы построить формулу.

Введем некоторые изменения в транскрипцию формулы. Заметим, что формула может содержать скобки, заключающие в себе все остальные символы формулы. Например,

$$(\mathfrak{A} \mathbin{\&} \mathfrak{B}).$$

Такие скобки будем называть внешними. Слово $\mathfrak{A} \mathbin{\&} \mathfrak{B}$ без скобок в силу определения формулой не является. Однако для сокращения записи мы будем внешние скобки опускать. При этом мы не меняем определения формулы, а просто не пишем некоторых символов (в данном случае внешних скобок), присутствие которых в последовательности символов, образующих формулу, конечно, подразумевается. Введем еще изменения в транскрипцию формулы в связи со знаком отрицания. Формулу $-\mathfrak{A}$ будем записывать в виде

$$\overline{\mathfrak{A}},$$

причем если $\mathfrak{A}$ имеет внешние скобки, то будем их опускать. После этих изменений транскрипция формул исчисления высказываний будет такая же, как у формул алгебры высказываний. Далее мы воспользуемся теми же правилами опускания скобок, что и в алгебре высказываний. Будем считать, что связка & связывает сильнее, чем все остальные, связка $\vee$ сильнее, чем $\rightarrow$. В силу этого правила формулу

$$(\mathfrak{A} \mathbin{\&} \mathfrak{B}) \vee \mathfrak{C}$$

будем писать в виде

$$\mathfrak{A} \mathbin{\&} \mathfrak{B} \vee \mathfrak{C}.$$

Формулу

$$(\mathfrak{A} \vee \mathfrak{B}) \rightarrow (\mathfrak{C} \mathbin{\&} \mathfrak{D})$$

будем писать в виде

$$\mathfrak{A} \vee \mathfrak{B} \rightarrow \mathfrak{C} \mathbin{\&} \mathfrak{D}$$

и т. д.

Примеры.

1. Формула $-((A \vee B) \to -(C \to D))$ в измененной транскрипции напишется в виде

$$\overline{A \vee B \to \overline{C \to D}}.$$

2. Формула $(-A \vee (B \to (C \& D)))$ напишется в виде

$$\bar{A} \vee (B \to C \& D).$$

Заметим, что можно было бы дать такое определение формулы, что конфигурация ее символов образовала бы сразу ту транскрипцию, которую мы получили после введенных сокращений. Но тогда само определение формулы стало бы более громоздким и формула была бы не простой последовательностью символов, а более сложным образованием. С другой стороны, для записи формулы введенные нами упрощения представляют значительные удобства.

§ 2. Определение выводимых формул

Следующим шагом в описании исчисления высказываний будет выделение некоторого класса формул, которые мы будем называть *выводимыми в исчислении высказываний.* Определение выводимых формул имеет такой же рекурсивный характер, как и определение формулы. Сначала определяются исходные выводимые формулы, а затем определяются правила, позволяющие из имеющихся выводимых формул образовывать новые. Эти правила мы будем называть *правилами вывода*, а исходные выводимые формулы — *аксиомами.* Образование выводимой формулы из исходных выводимых формул, или аксиом, путем применения правил вывода будем называть *выводом* данной формулы из аксиом.

Аксиомы исчисления высказываний

I

1. $A \to (B \to A)$.
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.

II

1. $A \& B \rightarrow A$.
2. $A \& B \rightarrow B$.
3. $(A \rightarrow B) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B \& C))$.

III

1. $A \rightarrow A \vee B$.
2. $B \rightarrow A \vee B$.
3. $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B \rightarrow C))$.

IV

1. $(A \rightarrow B) \rightarrow (\overline{B} \rightarrow \overline{A})$.
2. $A \rightarrow \overline{\overline{A}}$.
3. $\overline{\overline{A}} \rightarrow A$.

Как видно из привиденного списка, аксиомы разбиваются на четыре группы. Все аксиомы группы I из логических связок содержат только импликацию. Эта связка входит и во все остальные группы. Но в группе II к импликации присоединяется конъюнкция, в группе III — дизъюнкция, а в группе IV — отрицание.

Правила вывода.

1. *Правило подстановки.* Пусть $\mathfrak{A}$ — формула, содержащая букву A. Тогда, если $\mathfrak{A}$ — выводимая формула исчисления высказываний, то, заменив в ней букву A всюду, где она входит, произвольной формулой $\mathfrak{B}$, мы также получим выводимую формулу.

2. *Правило заключения.* Если $\mathfrak{A}$ и $\mathfrak{A} \rightarrow \mathfrak{B}$ — выводимые формулы исчисления высказываний, то $\mathfrak{B}$ — также выводимая формула.

Указанием аксиом и правил вывода мы полностью определяем понятие выводимой в исчислении высказываний формулы. Пользуясь правилами вывода, мы можем, исходя из аксиом, конструировать новые выводимые формулы и получить таким образом каждую выводимую формулу. Рассмотрим некоторые примеры.

1. Покажем, что формула

$$(A \rightarrow B) \rightarrow (A \rightarrow A)$$

выводима в исчислении высказываний.

Формула

$$(A \to (B \to A)) \to ((A \to B) \to (A \to A))$$

является результатом подстановки в аксиому I. 2 переменного высказывания A вместо C. Так как посылка полученной импликации есть аксиома I. 1, то, применив правило заключения, получим, что

$$(A \to B) \to (A \to A)$$

— выводимая формула.

2. Покажем, что

$$A \& B \to B \& A$$

— выводимая формула в исчислении высказываний.

Произведем подстановку в аксиому II. 3. Заменив A формулой $A \& B$, получим выводимую формулу

$$(A \& B \to B) \to ((A \& B \to C) \to (A \& B \to B \& C)).$$

Произведем подстановку в эту формулу, заменив C на A. Получим выводимую формулу

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

Мы видим, что посылка этой импликации представляет собой аксиому II. 2. Поэтому, применив правило заключения, мы получим выводимую формулу

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

Посылка в этой формуле является аксиомой II. 1. Применив правило заключения, получим требуемую формулу:

$$A \& B \to B \& A.$$

3. Покажем, что

$$\overline{\overline{\overline{A}}} \to \overline{A}$$

— выводимая формула.

Делаем подстановку в аксиому IV. 1, заменяя B формулой $\overline{\overline{A}}$. Получим выводимую формулу

$$(A \to \overline{\overline{A}}) \to (\overline{\overline{\overline{A}}} \to \overline{A}).$$

Посылка этой формулы есть аксиома IV. 2.

Применив правило заключения, получим требуемую формулу:

$$\overline{\overline{\overline{A}}} \to \overline{A}.$$

Сделаем одно замечание по поводу правила подстановки. Хотя это правило описано совершенно ясно, все же его описание нельзя считать вполне удовлетворительным. Именно, заменяя в формуле букву формулой, мы получаем, конечно, некоторое слово, но еще следует доказать, что это слово является формулой.

Приведем другое определение правила подстановки, эквивалентное старому определению. Оно гораздо более громоздко, но из него будет прямо следовать, что получаемое в результате подстановки слово является формулой. Кроме того, это определение будет полезно в других рассуждениях.

Операция подстановки представляет собой соответствие, в котором каждой формуле $\mathfrak{A}$ при заданной букве A и заданной формуле $\mathfrak{B}$ отвечает вполне определенная формула, которую мы обозначим $S_A^{\mathfrak{B}}(\mathfrak{A})$. Операцию $S_A^{\mathfrak{B}}(\mathfrak{A})$ мы определим следующим образом.

Если $\mathfrak{A}$ есть переменное высказывание A, то $S_A^{\mathfrak{B}}(\mathfrak{A})$ представляет собой формулу $\mathfrak{B}$. Если $\mathfrak{A}$ есть отличное от A переменное высказывание B, то $S_A^{\mathfrak{B}}(\mathfrak{A})$ есть B.

Тем самым мы определили операцию $S_A^{\mathfrak{B}}(\mathfrak{A})$ для всех элементарных формул.

Допустим, что для формул $\mathfrak{A}_1$ и $\mathfrak{A}_2$ определены формулы $S_A^{\mathfrak{B}}(\mathfrak{A}_1)$ и $S_A^{\mathfrak{B}}(\mathfrak{A}_2)$.

Определим операцию подстановки для формул $\mathfrak{A}_1 \mathbin{\&} \mathfrak{A}_2$ $\mathfrak{A}_1 \vee \mathfrak{A}_2$, $\mathfrak{A}_1 \to \mathfrak{A}_2$ и $\overline{\mathfrak{A}_1}$ следующим образом:

$S_A^{\mathfrak{B}}(\mathfrak{A}_1 \mathbin{\&} \mathfrak{A}_2)$	*есть*	*формула*	$S_A^{\mathfrak{B}}(\mathfrak{A}_1) \mathbin{\&} S_A^{\mathfrak{B}}(\mathfrak{A}_2)$,
$S_A^{\mathfrak{B}}(\mathfrak{A}_1 \vee \mathfrak{A}_2)$	»	»	$S_A^{\mathfrak{B}}(\mathfrak{A}_1) \vee S_A^{\mathfrak{B}}(\mathfrak{A}_2)$,
$S_A^{\mathfrak{B}}(\mathfrak{A}_1 \to \mathfrak{A}_2)$	»	»	$S_A^{\mathfrak{B}}(\mathfrak{A}_1) \to S_A^{\mathfrak{B}}(\mathfrak{A}_2)$,
$S_A^{\mathfrak{B}}(\overline{\mathfrak{A}_1})$	»	»	$\overline{S_A^{\mathfrak{B}}(\mathfrak{A}_1)}$.

Мы имеем, таким образом, рекурсивное определение операции $S_A^{\mathfrak{B}}$ для всех формул исчисления высказываний. При этом операция подстановки $S_A^{\mathfrak{B}}$ определена и для формул $\mathfrak{A}$, которые не содержат переменного высказывания A. В этом случае, как легко видеть, $S_A^{\mathfrak{B}}(\mathfrak{A})$ представляет собой $\mathfrak{A}$. Правило подстановки формулируется следующим образом.

Если $\mathfrak{A}$ — выводимая формула, то $S_A^{\mathfrak{B}}(\mathfrak{A})$ — также выводимая формула, каковы бы ни были переменное высказывание A и формула $\mathfrak{B}$.

Из новой формулировки правила подстановки непосредственно вытекает, что результат подстановки в формулу $\mathfrak{A}$ есть также формула.

Рассмотрим операцию $S_A^{\mathfrak{B}}$ на примере.

Найдем

$$S_A^{A \to A \vee C}(A \& B \to (B \vee C) \& \overline{A \to C}). \qquad (1)$$

В силу определения это есть формула

$$S_A^{A \to A \vee C}(A \& B) \to S_A^{A \to A \vee C}((B \vee C) \& \overline{A \to C}).$$

$$S_A^{A \to A \vee C}(A \& B) \quad \text{есть} \quad S_A^{A \to A \vee C}(A) \& S_A^{A \to A \vee C}(B),$$

но

$$S_A^{A \to A \vee C}(A) \quad \text{есть} \quad A \to A \vee C,$$

а

$$S_A^{A \to A \vee C}(B) \quad \text{есть} \quad B.$$

Итак

$$S_A^{A \to A \vee C}(A \& B) \quad \text{есть} \quad (A \to A \vee C) \& B.$$

Далее,

$$S_A^{A \to A \vee C}((B \vee C) \& \overline{A \to C})$$

есть

$$S_A^{A \to A \vee C}(B \vee C) \& S_A^{A \to A \vee C}\overline{(A \to C)};$$

$S_A^{A \to A \vee C}(B \vee C)$ представляет собой $B \vee C$, так как эта формула переменного высказывания A не содержит.

$$S_A^{A \to A \vee C}\overline{(A \to C)} \quad \text{есть} \quad \overline{S_A^{A \to A \vee C}(A \to C)},$$

$$S_A^{A \to A \vee C}(A \to C), \quad \text{очевидно, есть} \quad (A \to A \vee C) \to C.$$

Итак,

$$S_A^{A \to A \vee C}(A \& B \to (B \vee C) \& \overline{A \to C})$$

представляет собой формулу

$$((A \to A \vee C) \& B \to (B \vee C) \& \overline{(A \to A \vee C) \to C}).$$

Мы видим, что в результате рассматриваемой подстановки переменное высказывание A в формуле

$$A \& B \rightarrow (B \vee C) \& \overline{A \rightarrow C}$$

заменилось всюду формулой

$$A \rightarrow A \vee C.$$

Кроме основных правил вывода — правила подстановки и правила заключения — мы будем иметь и другие правила образования выводимых формул, производные от основных правил и являющиеся сокращением многократного применения основных правил. Для всех этих правил мы введем некоторую схему, позволяющую записывать их сокращенно.

Правила выражаются обычно в следующих терминах. «Если формулы $\mathfrak{A}$, $\mathfrak{B}$, ... выводимы, то формулы $\mathfrak{M}$, $\mathfrak{N}$, ... также выводимы». Мы будем записывать такого рода определения в виде схемы

$$\frac{\mathfrak{A}, \mathfrak{B}, \ldots}{\mathfrak{M}, \mathfrak{N}, \ldots}.$$

Основные правила вывода тогда запишутся так.

Правило подстановки

$$\frac{\mathfrak{A}}{S_A^{\mathfrak{B}}(\mathfrak{A})}.$$

Правило заключения

$$\frac{\mathfrak{A}, \mathfrak{A} \rightarrow \mathfrak{B}}{\mathfrak{B}}.$$

Совершим последовательно подстановки в формулу $\mathfrak{A}$ вместо различных переменных высказываний $A_1, \ldots, A_n$. При этом сначала A_1 заменяем формулой $\mathfrak{B}_1$, затем в полученной формуле A_2 заменяем формулой $\mathfrak{B}_2$ и т. д. В результате получим формулу

$$S_{A_n}^{\mathfrak{B}_n}\left(S_{A_{n-1}}^{\mathfrak{B}_{n-1}} \ldots \left(S_{A_1}^{\mathfrak{B}_1}(\mathfrak{A})\right) \ldots\right).$$

Если формулы $\mathfrak{B}_i$ не содержат переменных высказываний $A_1, \ldots, A_n$, то порядок, в каком мы будем делать эти подстановки, безразличен. В противном случае он не безразличен. Введем следующую операцию. Переменные высказывания $A_1, \ldots, A_n$ в формуле $\mathfrak{A}(A_1, \ldots, A_n)$

заменим такими переменными высказываниями, которые не входят ни в какую формулу $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$. Пусть это будут переменные высказывания $X_1, \ldots, X_n$. Тогда мы получим формулу $\mathfrak{A}(X_1, \ldots, X_n)$. После этого совершим последовательные подстановки:

$$S_{X_n}^{\mathfrak{B}_n}\left(\ldots\left(S_{X_1}^{\mathfrak{B}_1}(\mathfrak{A}(X_1, \ldots, X_n))\right)\ldots\right).$$

Получим формулу, относительно которой можно сказать, что она является результатом одновременной замены переменных высказываний $A_1, \ldots, A_n$ соответственно формулами $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$. Полученную операцию обозначим

$$S_{A_1 \ldots A_n}^{\mathfrak{B}_1 \ldots \mathfrak{B}_n}(\mathfrak{A}).$$

Формула $\mathfrak{A}(X_1, \ldots, X_n)$ играет вспомогательную роль в этой операции. Если не производить замены переменных высказываний A_i переменными высказываниями X_i, то при последовательных подстановках замена будет производиться и в переменных высказываниях A_i, входящих в формулы $\mathfrak{B}_j$; тогда результат операции не будет представлять собой одновременной замены переменных высказываний A_i в формуле $\mathfrak{A}$. Формула $\mathfrak{A}(X_1, \ldots, X_n)$ носит название *указующей формулы*. Операцию $S_{A_1 \ldots A_n}^{\mathfrak{B}_1 \ldots \mathfrak{B}_n}(\mathfrak{A})$ мы будем называть *сложной подстановкой в формулу* $\mathfrak{A}$ или просто *подстановкой в формулу* $\mathfrak{A}$. Если $n = 1$, то указующая формула не нужна, так как в этом случае имеем дело с обычным применением правила подстановки. Поэтому, если формула $\mathfrak{A}$ выводима в исчислении высказываний, то формула

$$S_{A_1 \ldots A_n}^{\mathfrak{B}_1 \ldots \mathfrak{B}_n}(\mathfrak{A})$$

также выводима, и мы получаем правило

$$\frac{\mathfrak{A}}{S_{A_1 \ldots A_n}^{\mathfrak{B}_1 \ldots \mathfrak{B}_n}(\mathfrak{A})}.$$

Второе производное правило применяется к формулам вида

$$\mathfrak{A}_1 \to (\mathfrak{A}_2 \to (\ldots (\mathfrak{A}_{n-1} \to \mathfrak{A}_n) \ldots))$$

и выражается так: *если формулы*

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1} \quad и \quad \mathfrak{A}_1 \to (\mathfrak{A}_2 \to (\ldots (\mathfrak{A}_{n-1} \to \mathfrak{A}_n) \ldots))$$

выводимы, то и формула $\mathfrak{A}_n$ *выводима в вычислении высказываний.* Это утверждение легко доказывается последовательным применением правила заключения.

В самом деле, если

$$\mathfrak{A}_1 \quad и \quad \mathfrak{A}_1 \to (\mathfrak{A}_2 \to (\ldots (\mathfrak{A}_{n-1} \to \mathfrak{A}_n) \ldots))$$

— выводимые формулы, то

$$\mathfrak{A}_2 \to (\ldots (\mathfrak{A}_{n-1} \to \mathfrak{A}_n) \ldots)$$

— также выводимая формула.

Так как

$$\mathfrak{A}_2 \quad и \quad \mathfrak{A}_2 \to (\mathfrak{A}_3 \to (\ldots (\mathfrak{A}_{n-1} \to \mathfrak{A}_n) \ldots))$$

— выводимые формулы, то и

$$\mathfrak{A}_3 \to (\ldots (\mathfrak{A}_{n-1} \to \mathfrak{A}_n) \ldots)$$

— также выводимая формула.

Продолжая это рассуждение дальше, мы получим наконец, что $\mathfrak{A}_n$ — выводимая формула в исчислении высказываний.

Таким образом, мы получаем новое правило, которое будем называть *сложным правилом заключения.* Оно записывается в виде схемы

$$\frac{\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_{n-1}, \mathfrak{A}_1 \to (\mathfrak{A}_2 \to (\ldots (\mathfrak{A}_{n-1} \to \mathfrak{A}_n) \ldots))}{\mathfrak{A}_n}.$$

Условимся в дальнейшем использовать букву $\mathfrak{R}$ *для обозначения произвольной формулы, которая выводима в исчислении высказываний, а букву* $\mathfrak{F}$ *— для обозначения такой формулы, для которой формула* $\overline{\mathfrak{F}}$ *выводима в исчислении высказываний.* Иначе говоря, если в дальнейшем встретится символ $\mathfrak{R}$ (или $\mathfrak{F}$), то при этом подразумевается, что $\mathfrak{R}$ (соответственно $\overline{\mathfrak{F}}$) есть произвольная выводимая в исчислении высказываний формула.

Теорема 1. *$B \to \mathfrak{R}$ — выводимая формула.*

Делаем подстановку в аксиому I. 1; заменив A на $\mathfrak{R}$, получим

$$\mathfrak{R} \to (B \to \mathfrak{R}),$$

Так как $\mathfrak{R}$ — выводимая формула, то, применив правило заключения к формулам

$$\mathfrak{R} \quad \text{и} \quad \mathfrak{R} \to (B \to \mathfrak{R}),$$

получим

$$B \to \mathfrak{R}.$$

Теорема 2. *$A \to A$ — выводимая формула.*

В аксиоме I. 2 заменим C на A; получим

$$(A \to (B \to A)) \to ((A \to B) \to (A \to A)).$$

Посылка этой формулы представляет собой аксиому I. 1. Применив правило заключения, будем иметь

$$(A \to B) \to (A \to A).$$

Заменив B на $\mathfrak{R}$, получим

$$(A \to \mathfrak{R}) \to (A \to A).$$

На основании предыдущей теоремы $A \to \mathfrak{R}$ — выводимая формула. Применив правило заключения, получим, что

$$A \to A$$

— выводимая формула.

§ 3. Теорема дедукции

Вместо того, чтобы выводимые в исчислении высказываний формулы выводить из аксиом, применяя непосредственно правила вывода, мы изберем более краткий путь, доказав предварительно так называемую теорему дедукции. Эта теорема позволит нам устанавливать выводимость различных формул гораздо более простым способом, чем непосредственный вывод этих формул.

Мы будем говорить, что *формула $\mathfrak{B}$ выводима из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, если формулу $\mathfrak{B}$ можно вывести только путем правила заключения, приняв за исходные формулы $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ и все истинные в исчислении высказываний формулы.*

Точное определение выводимости формулы $\mathfrak{B}$ из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, называемых исходными, формулируется следующим образом:

а) *каждая формула $\mathfrak{A}_i$ $(1 \leqslant i \leqslant n)$ выводима из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$;*

b) *каждая выводимая в исчислении высказываний формула выводима из* $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$;

c) *если формулы* $\mathfrak{A}$ *и* $\mathfrak{A} \to \mathfrak{B}$ *выводимы из* $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, *то формула* $\mathfrak{B}$ *также выводима из* $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$.

Утверждение, что формула $\mathfrak{B}$ выводима из $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, мы будем обозначать так:

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_n \vdash \mathfrak{B}.$$

Выводимость формулы $\mathfrak{B}$ из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ отличается от выводимости формулы в исчислении высказываний тем, что во втором случае в числе правил вывода имеется правило подстановки, которого нет в первом случае. Можно было бы определить и такую выводимость формулы $\mathfrak{B}$ из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, в которой правило подстановки имело бы место. Если бы мы употребляли понятие выводимости в том и другом смысле, то необходимо было бы различать эти два понятия различными терминами. Однако ввиду того, что мы будем иметь дело с выводимостью $\mathfrak{B}$ из других формул только в одном смысле, соответствующем данному определению, мы не будем для этого понятия вводить нового термина. В случае, когда у нас появится выводимость формулы $\mathfrak{B}$ из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ в другом смысле, мы это обстоятельство оговорим особо. Заметим, что если $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ являются аксиомами или другими выводимыми формулами, то класс выводимых из них формул совпадает с классом всех выводимых в исчислении высказываний формул, так как всякая выводимая формула считается выводимой из любой системы формул.

Мы расширим понимание выражения

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_n \vdash \mathfrak{B} \qquad (1)$$

на случай, когда формул $\mathfrak{A}_i$ вовсе нет ($n = 0$), считая, что тогда $\mathfrak{B}$ является просто выводимой формулой исчисления высказываний. Выражение (1) в этом случае, естественно, превращается в

$$\vdash \mathfrak{B}.$$

Все дальнейшие рассуждения о выводимости формулы $\mathfrak{B}$ из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ будут распространяться и на этот случай.

Теорема дедукции. *Если формула $\mathfrak{B}$ выводима из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, то*

$$\mathfrak{A}_1 \to (\mathfrak{A}_2 \to (\ldots (\mathfrak{A}_n \to \mathfrak{B}) \ldots))$$

— выводимая формула.

Докажем сначала, что если

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n \vdash \mathfrak{B},$$

то

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_{n-1} \vdash \mathfrak{A}_n \to \mathfrak{B}.$$

Доказательство этого утверждения проведем по индукции следующим образом. Сначала докажем, что оно верно, если $\mathfrak{B}$ является либо одной из формул $\mathfrak{A}_i$, либо выводимой формулой исчисления высказываний. Затем покажем, что если наше утверждение верно для формул $\mathfrak{B}'$ и $\mathfrak{B}' \to \mathfrak{B}''$, то оно верно и для $\mathfrak{B}''$.

Если $\mathfrak{B}$ совпадает с формулой $\mathfrak{A}_i$, то либо $i = n$, либо $i < n$. В первом случае $\mathfrak{A}_n \to \mathfrak{A}_n$ — выводимая формула; она получается подстановкой в формулу $A \to A$ (см. теорему 2 § 2). Поэтому

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1} \vdash \mathfrak{A}_n \to \mathfrak{A}_n.$$

Допустим, что $i < n$; тогда подстановками в аксиому I. 1 получаем

$$\vdash \mathfrak{A}_i \to (\mathfrak{A}_n \to \mathfrak{A}_i).$$

Последняя формула, как выводимая, выводима из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1}$. Но формула $\mathfrak{A}_i$ также выводима из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1}$. Поэтому формула $\mathfrak{A}_n \to \mathfrak{A}_i$ выводима из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1}$.

Случай, когда $\mathfrak{B}$ — выводимая формула, очевиден.

Допустим, что формулы $\mathfrak{A}_n \to \mathfrak{B}'$ и $\mathfrak{A}_n \to (\mathfrak{B}' \to \mathfrak{B}''$ выводимы из $\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1}$. Формула

$$(\mathfrak{A}_n \to (\mathfrak{B}' \to \mathfrak{B}'')) \to ((\mathfrak{A}_n \to \mathfrak{B}') \to (\mathfrak{A}_n \to \mathfrak{B}''))$$

является выводимой в исчислении высказываний, так как она получается подстановками в аксиому I. 2. Поэтому эта формула выводима из $\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1}$. Обе посылки этой формулы, по условию, выводимы из $\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1}$. Применив два раза правило заключения, мы получим формулу $\mathfrak{A}_n \to \mathfrak{B}''$, которая, следовательно, также выводима из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1}$.

Таким образом, мы доказали, что если

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_n \vdash \mathfrak{B},$$

то

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1} \vdash \mathfrak{A}_n \to \mathfrak{B}.$$

В случае $n = 1$ доказанное утверждение состоит в следующем:

если $\mathfrak{A}_n \vdash \mathfrak{B}$, то $\vdash \mathfrak{A}_n \to \mathfrak{B}$.

Теперь мы без труда установим справедливость теоремы дедукции. Допустим, что имеет место

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_n \vdash \mathfrak{B}.$$

В таком случае мы будем иметь

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1} \vdash \mathfrak{A}_n \to \mathfrak{B}.$$

Применив то же самое вторично, получим

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-2} \vdash \mathfrak{A}_{n-1} \to (\mathfrak{A}_n \to \mathfrak{B}).$$

Рассуждая так же и далее, мы наконец получим

$$\mathfrak{A}_1 \vdash \mathfrak{A}_2 \to (\mathfrak{A}_3 \to (\ldots \to (\mathfrak{A}_n \to \mathfrak{B}) \ldots)).$$

Применив то же рассуждение еще раз, мы получим

$$\vdash (\mathfrak{A}_1 \to (\mathfrak{A}_2 \to (\mathfrak{A}_3 \to (\ldots \to (\mathfrak{A}_n \to \mathfrak{B}) \ldots)))),$$

чем и доказана теорема дедукции.

§ 4. Некоторые правила исчисления высказываний

Теорема 1.

$$\vdash (A \to B) \to ((B \to C) \to (A \to C)).$$

Рассмотрим формулы $A \to B$, $B \to C$ и A. Из этих формул при помощи только правила заключения можно вывести формулу C. В таком случае на основании теоремы дедукции мы заключаем, что

$$(A \to B) \to ((B \to C) \to (A \to C))$$

— выводимая формула. Теорема доказана.

Сделаем подстановки в эту формулу, заменив A формулой $\mathfrak{A}$, B — формулой $\mathfrak{B}$, а C — формулой $\mathfrak{C}$. Получим выводимую формулу:

$$(\mathfrak{A} \to \mathfrak{B}) \to ((\mathfrak{B} \to \mathfrak{C}) \to (\mathfrak{A} \to \mathfrak{C})).$$

Если формулы $\mathfrak{A} \to \mathfrak{B}$ и $\mathfrak{B} \to \mathfrak{C}$ окажутся выводимыми, то, применив сложное правило заключения к последней формуле, мы найдем, что формула $\mathfrak{A} \to \mathfrak{C}$ также выводима. Таким образом, мы получаем правило, которое записывается так:

$$\frac{\mathfrak{A} \to \mathfrak{B},\ \mathfrak{B} \to \mathfrak{C}}{\mathfrak{A} \to \mathfrak{C}}.$$

Это правило носит название *правила силлогизма.*

Теорема 2.

$$\vdash (A \to (B \to C)) \to (B \to (A \to C)).$$

Рассмотрим формулы $A \to (B \to C)$, B, A. Применив два раза правило заключения, находим

$$A \to (B \to C),\ B,\ A \vdash C.$$

Применив теорему дедукции, получим требуемую формулу. Из выводимости этой формулы так же, как и в предыдущей теореме, извлекаем правило

$$\frac{\mathfrak{A} \to (\mathfrak{B} \to \mathfrak{C})}{\mathfrak{B} \to (\mathfrak{A} \to \mathfrak{C})}.$$

Это правило носит название *правила перестановки посылок.*

Теорема 3.

$$\vdash A \to (B \to A \mathbin{\&} B).$$

Сначала докажем

$$(\mathfrak{R} \to A) \to ((\mathfrak{R} \to B) \to (\mathfrak{R} \to A \mathbin{\&} B)),\ A,\ B \vdash A \mathbin{\&} B$$

($\mathfrak{R}$, как мы условились, обозначает любую выводимую формулу). Обозначим для краткости первую из этих формул через $\mathfrak{A}^0$. Формула $A \to (\mathfrak{R} \to A)$ выводимая. Поэтому формула $\mathfrak{R} \to A$ выводима из формулы A и тем более из формул $\mathfrak{A}^0$, A, B. Мы, таким образом, будем иметь

$$\mathfrak{A}^0,\ A,\ B \vdash \mathfrak{R} \to A.$$

Рассуждая аналогичным образом, получим

$$\mathfrak{A}^0,\ A,\ B \vdash \mathfrak{R} \to B.$$

Из $\mathfrak{A}^0$ путем трехкратного применения правила заключения выводим формулу $A \& B$, откуда следует, что

$$\mathfrak{A}^0,\ A,\ B \vdash A \& B.$$

Применив теорему дедукции, будем иметь

$$\vdash \mathfrak{A}^0 \to (A \to (B \to A \& B)).$$

Но $\mathfrak{A}^0$ — выводимая формула; она может быть получена подстановками в аксиому II. 3 (стр. 73). Отсюда мы получаем

$$\vdash A \to (B \to A \& B),$$

и теорема доказана. Из этой теоремы вытекает правило

$$\frac{\mathfrak{A},\ \mathfrak{B}}{\mathfrak{A} \& \mathfrak{B}}.$$

Обратное правило

$$\frac{\mathfrak{A} \& \mathfrak{B}}{\mathfrak{A},\ \mathfrak{B}}$$

вытекает из аксиом II. 1 и II. 2. Из этих двух правил следует правило $\frac{\mathfrak{A} \& \mathfrak{B}}{\mathfrak{B} \& \mathfrak{A}}$, которое, впрочем, можно извлечь и из формулы

$$\vdash A \& B \to B \& A,$$

выводимость которой была доказана (см. § 2, стр. 74).

Теорема 4.

$$\vdash \mathfrak{F} \to A.$$

Заменив B на $\mathfrak{R}$ в аксиоме IV. 1, получим

$$(A \to \mathfrak{R}) \to (\overline{\mathfrak{R}} \to \overline{A}),$$

но $A \to \mathfrak{R}$ — выводимая формула (см. теорему 1 § 2).

Применив правило заключения, получим формулу

$$\vdash \overline{\overline{\mathfrak{F}}} \to \overline{A},$$

где, пользуясь определением формулы $\mathfrak{F}$, мы заменили $\mathfrak{R}$ на $\overline{\mathfrak{F}}$. Подставив $\overline{A}$ вместо A, получим

$$\vdash \overline{\overline{\mathfrak{F}}} \to \overline{\overline{A}}.$$

Из последней формулы и аксиом IV. 2 и IV. 3 путем правила силлогизма получим

$$\vdash \mathfrak{F} \to A.$$

Теорема 5.

$$\vdash (A \to (B \to C)) \to (A \& B \to C), \tag{a}$$

$$\vdash (A \& B \to C) \to (A \to (B \to C)). \tag{b}$$

Докажем первое утверждение. Имеем

$$A \to (B \to C),\ A \& B \vdash C.$$

В самом деле, формулы

$$A \& B \to A \text{ и } A \& B \to B$$

суть аксиомы и потому выводимы в исчислении высказываний. Поэтому формулы A и B выводимы из формул $A \to (B \to C)$ и $A \& B$.

Применив правило заключения сначала к формулам

$$A \text{ и } A \to (B \to C)$$

и затем еще раз к формулам

$$B \text{ и } B \to C,$$

заключаем, что C выводима из формул $A \to (B \to C)$, $A \& B$. Отсюда на основании теоремы дедукции следует справедливость утверждения (a).

Докажем утверждение (b).

Рассмотрим систему формул

$$A \& B \to C,\ A,\ B.$$

Покажем, что из этой системы выводима формула C. На основании теоремы 3 имеем

$$\vdash A \to (B \to A \& B).$$

Отсюда следует, что формула $A \& B$ выводима из формул

$$A \& B \to C,\ A,\ B.$$

В таком случае и C выводима из этих же формул. Применив теорему дедукции, получаем утверждение (b) теоремы.

Из доказанной теоремы вытекают два правила:

$$\frac{\mathfrak{A} \to (\mathfrak{B} \to \mathfrak{C})}{\mathfrak{A} \& \mathfrak{B} \to \mathfrak{C}} \text{ и } \frac{\mathfrak{A} \& \mathfrak{B} \to \mathfrak{C}}{\mathfrak{A} \to (\mathfrak{B} \to \mathfrak{C})}.$$

Первое из этих правил назовем *правилом соединения посылок*, а второе — *правилом разъединения посылок*.

Теорема 6.

$$\vdash \mathfrak{A} \& \overline{\mathfrak{A}} \to \mathfrak{F}.$$

Из аксиомы I. 1 подстановкой получим

$$\vdash A \to (\mathfrak{R} \to A).$$

Кроме того, из аксиомы IV. 1 получим, имея в виду, что $\overline{\mathfrak{R}}$ есть $\mathfrak{F}$:

$$\vdash (\mathfrak{R} \to A) \to (\overline{A} \to \mathfrak{F}).$$

Применяем к этим двум формулам правило силлогизма:

$$\vdash A \to (\overline{A} \to \mathfrak{F}),$$

откуда по правилу соединения посылок следует

$$\vdash A \& \overline{A} \to \mathfrak{F}.$$

Наконец, подстановка дает искомую формулу

$$\vdash \mathfrak{A} \& \overline{\mathfrak{A}} \to \mathfrak{F}.$$

§ 5. Монотонность

Будем говорить, что формула $\mathfrak{A}$ сильнее (хотя, может быть, точнее было бы говорить «не слабее») формулы $\mathfrak{B}$, если $\vdash \mathfrak{A} \to \mathfrak{B}$.

Определение. *Формула $\mathfrak{A}(A)$, содержащая переменное высказывание A, называется монотонно возрастающей (соответственно монотонно убывающей) по A, если из $\mathfrak{B}_1 \to \mathfrak{B}_2$ следует $\mathfrak{A}(\mathfrak{B}_1) \to \mathfrak{A}(\mathfrak{B}_2)$ (соответственно: из $\mathfrak{B}_1 \to \mathfrak{B}_2$ следует $\mathfrak{A}(\mathfrak{B}_2) \to \mathfrak{A}(\mathfrak{B}_1)$).* Здесь, как и всегда в дальнейшем, $\mathfrak{A}(\mathfrak{B}_1)$ и $\mathfrak{A}(\mathfrak{B}_2)$ обозначают формулы, получаемые из $\mathfrak{A}(A)$ заменой переменного высказывания A соответственно формулами $\mathfrak{B}_1$ и $\mathfrak{B}_2$.

Значение понятия монотонности видно из следующей теоремы.

Теорема. *Все основные логические операции монотонны по всем участвующим в них переменным высказываниям: формулы $A \& B$ и $A \vee B$ монотонно возрастают по A и B, $\bar{A}$ убывает по A, $A \to B$ убывает по A и возрастает по B.*

Доказательство. 1. Формула $A \& B$ монотонно возрастает по A и по B. Действительно, пусть

$$\vdash \mathfrak{B}_1 \to \mathfrak{B}_2. \tag{a}$$

Подстановкой в аксиому II. 1 получаем

$$\vdash \mathfrak{B}_1 \& B \to \mathfrak{B}_1. \tag{b}$$

Из этих формул по правилу силлогизма следует

$$\vdash \mathfrak{B}_1 \& B \to \mathfrak{B}_2. \tag{c}$$

Подстановками в аксиому II. 3 ($\mathfrak{B}_1 \& B$ на место A, $\mathfrak{B}_2$ на место B и B на место C) получим

$$\vdash (\mathfrak{B}_1 \& B \to \mathfrak{B}_2) \to [(\mathfrak{B}_1 \& B \to B) \to (\mathfrak{B}_1 \& B \to \mathfrak{B}_2 \& B)]. \tag{d}$$

Формулы $\mathfrak{B}_1 \& B \to B$ и $\mathfrak{B}_1 \& B \to \mathfrak{B}_2$ выводимые. Поэтому, применив к (d) дважды правило заключения, получим

$$\vdash \mathfrak{B}_1 \& B \to \mathfrak{B}_2 \& B.$$

Этим доказано, что формула $A \& B$ монотонно возрастает по A. Монотонное возрастание по B доказывается аналогично.

2. Формула $A \vee B$ монотонно возрастает по A и по B. Докажем, например, что $A \vee B$ монотонно возрастает по B.

Пусть

$$\vdash \mathfrak{B}_1 \to \mathfrak{B}_2. \tag{a}$$

Из аксиомы III. 2 получаем подстановкой

$$\vdash \mathfrak{B}_2 \to A \vee \mathfrak{B}_2. \tag{b'}$$

Правило силлогизма дает теперь

$$\vdash \mathfrak{B}_1 \to A \vee \mathfrak{B}_2. \tag{c'}$$

Кроме того, подстановка в III. 1 дает

$$\vdash A \to A \vee \mathfrak{B}_2. \tag{c''}$$

Теперь делаем подстановку в аксиому III. 3 $\mathfrak{B}_1$ вместо B и $A \vee \mathfrak{B}_2$ вместо C. Получаем

$$\vdash (A \to A \vee \mathfrak{B}_2) \to [(\mathfrak{B}_1 \to A \vee \mathfrak{B}_2) \to (A \vee \mathfrak{B}_1 \to A \vee \mathfrak{B}_2)]. \tag{d'}$$

Применим к (d′) дважды правило заключения, используя (c′) и (c″). Получаем

$$\vdash A \vee \mathfrak{B}_1 \to A \vee \mathfrak{B}_2.$$

3. Формула $\bar{A}$ монотонно убывает по A. Это следует непосредственно из аксиомы IV. 1.

4. Формула $A \to B$ монотонно возрастает по B и монотонно убывает по A.

Докажем, что формула $A \to B$ монотонно убывает по A. Пусть

$$\vdash \mathfrak{B}_1 \to \mathfrak{B}_2. \qquad \text{(a)}$$

В силу доказанной монотонности формулы $A \& B$ имеем

$$\vdash (\mathfrak{B}_2 \to B) \& \mathfrak{B}_1 \to (\mathfrak{B}_2 \to B) \& \mathfrak{B}_2. \qquad \text{(e)}$$

Далее, из выводимой формулы $A \to A$ (см. стр. 80) подстановкой получаем

$$\vdash (\mathfrak{B}_2 \to B) \to (\mathfrak{B}_2 \to B)$$

и, применив правило соединения посылок, находим

$$\vdash (\mathfrak{B}_2 \to B) \& \mathfrak{B}_2 \to B. \qquad \text{(f)}$$

С помощью правила силлогизма получаем из (e) и (f)

$$\vdash (\mathfrak{B}_2 \to B) \& \mathfrak{B}_1 \to B.$$

Применив к полученной формуле правило разъединения посылок, получаем требуемое:

$$\vdash (\mathfrak{B}_2 \to B) \to (\mathfrak{B}_1 \to B).$$

Докажем теперь, что формула $A \to B$ монотонно возрастает по B.

Пусть $\vdash \mathfrak{B}_1 \to \mathfrak{B}_2$. Аналогично формуле (f) получаем

$$\vdash (A \to \mathfrak{B}_1) \& A \to \mathfrak{B}_1. \qquad \text{(f′)}$$

Из (a) и (f′) по правилу силлогизма имеем

$$\vdash (A \to \mathfrak{B}_1) \& A \to \mathfrak{B}_2,$$

откуда, применив правило, обратное правилу соединения посылок, получим

$$\vdash (A \to \mathfrak{B}_1) \to (A \to \mathfrak{B}_2),$$

что и требовалось доказать.

Из определения монотонности следует, что если формула $\mathfrak{A}(\mathfrak{B})$ монотонно возрастает по своей части $\mathfrak{B}$ и если

$$\vdash \mathfrak{A}(\mathfrak{B}_1),$$

то, заменив $\mathfrak{B}_1$ более слабой формулой $\mathfrak{B}_2$, получим также выводимую формулу; если же $\mathfrak{A}(\mathfrak{B})$ убывает по $\mathfrak{B}$, то $\mathfrak{A}(\mathfrak{B}_1)$ остается выводимой при замене $\mathfrak{B}_1$ более сильной формулой.

Эти соображения часто позволяют упрощать доказательства, в которых производится замена части какой-нибудь формулы более слабой или более сильной формулой. В таких сучаях обычно достаточно проверить, имеется ли нужная монотонность.

§ 6. Эквивалентные формулы

Формулу, имеющую вид

$$(\mathfrak{A} \to \mathfrak{B}) \,\&\, (\mathfrak{B} \to \mathfrak{A}),$$

мы будем сокращенно записывать в виде

$$\mathfrak{A} \sim \mathfrak{B}.$$

Знак $\sim$ не является символом исчисления высказываний, а употребляется только для сокращения указанного выше выражения. Вместе с тем пользование им представляет большие удобства. (Можно было бы ввести в исчисление высказываний символ $\sim$ в качестве его символа таким образом, чтобы полученная при этом система была в известном смысле вполне адекватна рассматриваемой нами системе, но тогда пришлось бы ввести еще новые аксиомы и исчисление усложнилось бы. С другой стороны, никаких преимуществ при этом мы бы не получили.)

Знак $\sim$ мы будем называть *знаком эквивалентности*, формулу $\mathfrak{A} \sim \mathfrak{B}$ — *эквивалентностью.*

Рассмотрим в качестве примера выражение

$$A \sim \bar{\bar{A}}.$$

Аксиомы IV.2 и IV.3 имеют вид

$$A \to \bar{\bar{A}} \text{ и } \bar{\bar{A}} \to A.$$

Применив к ним правило $\dfrac{\mathfrak{A},\ \mathfrak{B}}{\mathfrak{A}\ \&\ \mathfrak{B}}$, получим

$$\vdash (A \to \overline{\overline{A}})\ \&\ (\overline{\overline{A}} \to A)$$

или, если записать это выражение в принятой нами форме,

$$\vdash A \sim \overline{\overline{A}}.$$

Мы будем говорить, что *формулы* $\mathfrak{A}$ *и* $\mathfrak{B}$ *эквивалентны, если имеет место*

$$\vdash \mathfrak{A} \sim \mathfrak{B}.$$

Заметим сразу же, что всякие две выводимые формулы исчисления высказываний эквивалентны.

Соотношение эквивалентности формул симметрично, т. е. если $\mathfrak{A}$ эквивалентно $\mathfrak{B}$, то и $\mathfrak{B}$ эквивалентно $\mathfrak{A}$. В самом деле, если имеет место

$$\vdash \mathfrak{A} \sim \mathfrak{B}$$

или, иначе,

$$\vdash (\mathfrak{A} \to \mathfrak{B})\ \&\ (\mathfrak{B} \to \mathfrak{A}),$$

то в силу правила $\dfrac{\mathfrak{A}\ \&\ \mathfrak{B}}{\mathfrak{A},\ \mathfrak{B}}$ мы имеем

$$\vdash \mathfrak{A} \to \mathfrak{B} \text{ и } \vdash \mathfrak{B} \to \mathfrak{A}.$$

Применив обратное правило $\dfrac{\mathfrak{A},\ \mathfrak{B}}{\mathfrak{A}\ \&\ \mathfrak{B}}$, получим

$$\vdash (\mathfrak{B} \to \mathfrak{A})\ \&\ (\mathfrak{A} \to \mathfrak{B}),$$

или

$$\vdash \mathfrak{B} \sim \mathfrak{A}.$$

Соотношение эквивалентности транзитивно, т. е. *если* $\mathfrak{A}$ *эквивалентно* $\mathfrak{B}$ *и* $\mathfrak{B}$ *эквивалентно* $\mathfrak{C}$, *то* $\mathfrak{A}$ *эквивалентно* $\mathfrak{C}$.

Действительно, из $\vdash \mathfrak{A} \sim \mathfrak{B}$ и $\vdash \mathfrak{B} \sim \mathfrak{C}$ следует $\left(\text{на основании } \dfrac{\mathfrak{A}\ \&\ \mathfrak{B}}{\mathfrak{A}\ \ \mathfrak{B}}\right)$, что

$$\vdash \mathfrak{A} \to \mathfrak{B};\quad \vdash \mathfrak{B} \to \mathfrak{C}.$$

Применив к этим формулам правило силлогизма, получим

$$\vdash \mathfrak{A} \to \mathfrak{C}.$$

В силу симметрии эквивалентности будем иметь

$$\vdash \mathfrak{C} \to \mathfrak{A}.$$

И, наконец, применив правило $\frac{\mathfrak{A},\ \mathfrak{B}}{\mathfrak{A} \,\&\, \mathfrak{B}}$, получим

$$\vdash \mathfrak{A} \sim \mathfrak{C}.$$

Чтобы доказать выводимость эквивалентности

$$\mathfrak{A} \sim \mathfrak{B},$$

достаточно доказать выводимость двух импликаций

$$\mathfrak{A} \to \mathfrak{B} \text{ и } \mathfrak{B} \to \mathfrak{A},$$

и, обратно, эти импликации выводимы, если выводима эквивалентность $\mathfrak{A} \sim \mathfrak{B}$.

Справедливость этого легко усмотреть из сказанного выше. То же положение можно записать в виде двух правил:

$$\frac{\mathfrak{A} \to \mathfrak{B},\ \mathfrak{B} \to \mathfrak{A}}{\mathfrak{A} \sim \mathfrak{B}}, \quad \frac{\mathfrak{A} \sim \mathfrak{B}}{\mathfrak{A} \to \mathfrak{B},\ \mathfrak{B} \to \mathfrak{A}}.$$

Пользуясь введенным ранее понятием, сформулируем это утверждение так:

Чтобы формулы $\mathfrak{A}$ и $\mathfrak{B}$ были эквивалентны, необходимо и достаточно, чтобы $\mathfrak{A}$ была сильнее $\mathfrak{B}$ и $\mathfrak{B}$ сильнее $\mathfrak{A}$.

Пример. Из доказанной эквивалентности

$$A \sim \overline{\overline{A}}$$

посредством подстановки получаем, что формулы $\mathfrak{A}$ и $\overline{\overline{\mathfrak{A}}}$ эквивалентны.

Теорема эквивалентности. *Пусть формула $\mathfrak{A}(A)$ содержит или не содержит переменное высказывание A, и пусть формулы $\mathfrak{B}_1$ и $\mathfrak{B}_2$ эквивалентны. Тогда формулы $\mathfrak{A}(\mathfrak{B}_1)$ и $\mathfrak{A}(\mathfrak{B}_2)$, получаемые из $\mathfrak{A}(A)$ заменой A соответственно на $\mathfrak{B}_1$ и $\mathfrak{B}_2$, также эквивалентны.*

Иначе:

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to [\mathfrak{A}(\mathfrak{B}_1) \sim \mathfrak{A}(\mathfrak{B}_2)]. \tag{I}$$

Доказательство будем проводить индукцией по числу логических операций, с помощью которых составлена формула $\mathfrak{A}(A)$.

Если число этих операций равно нулю, то формула $\mathfrak{A}(A)$ есть либо A, либо переменное высказывание B, отличное от A. В первом случае формула (I) имеет вид

$$(\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow (\mathfrak{B}_1 \sim \mathfrak{B}_2),$$

а во втором —

$$(\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow (\mathfrak{A} \sim \mathfrak{A}).$$

Первая из этих формул получается подстановкой в выведенную ранее формулу $A \rightarrow A$, а вторая выводима в силу теорем 1 и 2 § 2.

Пусть теперь утверждение (I) выполнено для всех формул, которые получены не более чем n операциями, и пусть $\mathfrak{A}(A)$ составлена $n+1$ операциями. Последняя операция, участвующая в составлении $\mathfrak{A}(A)$, — это одна из четырех возможных операций &, $\vee$, $\rightarrow$ или —. Поэтому формула $\mathfrak{A}(A)$ имеет одну из следующих форм:

$$\mathfrak{A}_1(A) \,\&\, \mathfrak{A}_2(A), \quad \mathfrak{A}_1(A) \vee \mathfrak{A}_2(A), \quad \mathfrak{A}_1(A) \rightarrow \mathfrak{A}_2(A), \quad \overline{\mathfrak{A}_1(A)},$$

где формулы $\mathfrak{A}_1(A)$ и $\mathfrak{A}_2(A)$ образованы уже не более чем n операциями.

Отсюда следует, что теорема будет доказана, если в предположении, что выполнены

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1(\mathfrak{B}_1) \sim \mathfrak{A}_1(\mathfrak{B}_2)] \tag{a}$$

и

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_2(\mathfrak{B}_1) \sim \mathfrak{A}_2(\mathfrak{B}_2)], \tag{b}$$

будут доказаны утверждения

1. $\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \sim \mathfrak{A}_1(\mathfrak{B}_2) \,\&\, \mathfrak{A}_2(\mathfrak{B}_2)]$,
2. $\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1(\mathfrak{B}_1) \vee \mathfrak{A}_2(\mathfrak{B}_1) \sim \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)]$,
3. $\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow \{[\mathfrak{A}_1(\mathfrak{B}_1) \rightarrow \mathfrak{A}_2(\mathfrak{B}_1)] \sim [\mathfrak{A}_1(\mathfrak{B}_2) \rightarrow \mathfrak{A}_2(\mathfrak{B}_2)]\}$,
4. $\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\overline{\mathfrak{A}_1(\mathfrak{B}_1)} \sim \overline{\mathfrak{A}_1(\mathfrak{B}_2)}]$

[для случая 4 нужно предположить только (a)].

Итак, докажем 1—4.

1. Подстановками в аксиому II. 1 получим

$$\vdash \mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \rightarrow \mathfrak{A}_1(\mathfrak{B}_1). \tag{1}$$

С другой стороны, из данного (a), которое можно записать в виде

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow \{[\mathfrak{A}_1(\mathfrak{B}_1) \rightarrow \mathfrak{A}_1(\mathfrak{B}_2)] \,\&\, [\mathfrak{A}_1(\mathfrak{B}_2) \rightarrow \mathfrak{A}_1(\mathfrak{B}_1)]\},$$

применением аксиомы II. 1 и правила силлогизма получим

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1(\mathfrak{B}_1) \rightarrow \mathfrak{A}_1(\mathfrak{B}_2)],$$

откуда по правилу перестановки посылок следует

$$\vdash \mathfrak{A}_1(\mathfrak{B}_1) \rightarrow [(\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow \mathfrak{A}_1(\mathfrak{B}_2)]. \qquad (2)$$

Из (1) и (2) получаем по правилу силлогизма

$$\vdash \mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \rightarrow [(\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow \mathfrak{A}_1(\mathfrak{B}_2)],$$

откуда, если переставить посылки, получим

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \rightarrow \mathfrak{A}_1(\mathfrak{B}_2)]. \qquad (3)$$

Совершенно аналогично можно получить

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \rightarrow \mathfrak{A}_2(\mathfrak{B}_2)]. \qquad (4)$$

Сделав подстановки в аксиому II. 3 и дважды применив правило заключения [на основании (3) и (4)], получим

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \rightarrow \mathfrak{A}_1(\mathfrak{B}_2)] \,\&$$
$$\& \,[\mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \rightarrow \mathfrak{A}_2(\mathfrak{B}_2)]. \qquad (5)$$

С другой стороны, применив к аксиоме II. 3 правило соединения посылок и сделав подстановки, получим

$$\vdash [\mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \rightarrow \mathfrak{A}_1(\mathfrak{B}_2)] \,\&\, [\mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \rightarrow$$
$$\rightarrow \mathfrak{A}_2(\mathfrak{B}_2)] \rightarrow [(\mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \rightarrow \mathfrak{A}_1(\mathfrak{B}_2) \,\&\, \mathfrak{A}_2(\mathfrak{B}_2)]. \qquad (6)$$

Применение правила силлогизма к (5) и (6) дает

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \rightarrow \mathfrak{A}_1(\mathfrak{B}_2) \,\&\, \mathfrak{A}_2(\mathfrak{B}_2)]. \qquad (7)$$

Из (7) и из утверждения

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1(\mathfrak{B}_2) \,\&\, \mathfrak{A}_2(\mathfrak{B}_2) \rightarrow \mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1)], \qquad (8)$$

доказываемого аналогично, получаем применением аксиомы II. 3

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1(\mathfrak{B}_1) \,\&\, \mathfrak{A}_2(\mathfrak{B}_1) \sim \mathfrak{A}_1(\mathfrak{B}_2) \,\&\, \mathfrak{A}_2(\mathfrak{B}_2)].$$

2. Из определения эквивалентности и аксиомы II. 1 следует

$$\vdash (A \sim B) \rightarrow (A \rightarrow B). \qquad (9)$$

Кроме того, имеет место (аксиома III. 1)

$$\vdash B \to B \vee C. \tag{10}$$

Далее, из теоремы 1 § 4 подстановкой получаем

$$\vdash (A \to B) \to [(B \to B \vee C) \to (A \to B \vee C)],$$

откуда, переставив посылки и применив правило заключения [на основании (10)] получим

$$\vdash (A \to B) \to (A \to B \vee C). \tag{11}$$

Применив к (9) и (11) правило силлогизма, имеем

$$\vdash (A \sim B) \to (A \to B \vee C).$$

Подстановки в это последнее выражение дают

$$\vdash [\mathfrak{A}_1(\mathfrak{B}_1) \sim \mathfrak{A}_1(\mathfrak{B}_2)] \to [\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)],$$

откуда, используя (а), получаем по правилу силлогизма

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to [\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)]. \tag{12}$$

Аналогично доказывается

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to [\mathfrak{A}_2(\mathfrak{B}_1) \to \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)]. \tag{13}$$

Из (12) и (13), применив аксиому II. 3, получим

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to [\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)] \,\&\, [\mathfrak{A}_2(\mathfrak{B}_1) \to \\ \to \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)]. \tag{14}$$

С другой стороны, применив к аксиоме III. 3 правило соединения посылок и сделав подстановки, получим

$$\vdash [\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)] \,\&\, [\mathfrak{A}_2(\mathfrak{B}_1) \to \\ \to \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)] \to [\mathfrak{A}_1(\mathfrak{B}_1) \vee \mathfrak{A}_2(\mathfrak{B}_1) \to \\ \to \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)]. \tag{15}$$

Применив к (14) и (15) правило силлогизма, получим

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to [\mathfrak{A}_1(\mathfrak{B}_1) \vee \mathfrak{A}_2(\mathfrak{B}_1) \to \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)].$$

Из этого и из аналогично доказываемого утверждения

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to [\mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2) \to \mathfrak{A}_1(\mathfrak{B}_1) \vee \mathfrak{A}_2(\mathfrak{B}_1)]$$

следует, согласно аксиоме II. 3:

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to [\mathfrak{A}_1(\mathfrak{B}_1) \vee \mathfrak{A}_2(\mathfrak{B}_1) \sim \mathfrak{A}_1(\mathfrak{B}_2) \vee \mathfrak{A}_2(\mathfrak{B}_2)].$$

3. Из (a) применением аксиомы II. 2 и правила силлогизма получим

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_1 (\mathfrak{B}_2) \rightarrow \mathfrak{A}_1 (\mathfrak{B}_1)]. \tag{16}$$

Аналогично, из (b), применив аксиому II. 1 и правило силлогизма, получаем

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow [\mathfrak{A}_2 (\mathfrak{B}_1) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_2)]. \tag{17}$$

Переставив посылки в (16) и (17), получим

$$\vdash \mathfrak{A}_1 (\mathfrak{B}_2) \rightarrow [(\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow \mathfrak{A}_1 (\mathfrak{B}_1)] \tag{18}$$

и

$$\vdash \mathfrak{A}_2 (\mathfrak{B}_1) \rightarrow [(\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_2)]. \tag{19}$$

Соединив посылки в (18), получим

$$\vdash \mathfrak{A}_1 (\mathfrak{B}_2) \,\&\, (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow \mathfrak{A}_1 (\mathfrak{B}_1). \tag{20}$$

С другой стороны, подстановка в формулу

$$\vdash A \rightarrow A$$

дает

$$\vdash [\mathfrak{A}_1 (\mathfrak{B}_1) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_1)] \rightarrow [\mathfrak{A}_1 (\mathfrak{B}_1) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_1)],$$

откуда, переставив посылки, получаем

$$\vdash \mathfrak{A}_1 (\mathfrak{B}_1) \rightarrow \{[\mathfrak{A}_1 (\mathfrak{B}_1) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_1)] \rightarrow \mathfrak{A}_2 (\mathfrak{B}_1)\}. \tag{21}$$

Применением правила силлогизма к (20) и (21) получим

$$\vdash \mathfrak{A}_1 (\mathfrak{B}_2) \,\&\, (\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow \{[\mathfrak{A}_1 (\mathfrak{B}_1) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_1)] \rightarrow \mathfrak{A}_2 (\mathfrak{B}_1)\},$$

откуда по правилу соединения посылок следует

$$\vdash [\mathfrak{A}_1 (\mathfrak{B}_2) \,\&\, (\mathfrak{B}_1 \sim \mathfrak{B}_2)] \,\&\, [\mathfrak{A}_1 (\mathfrak{B}_1) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_1)] \rightarrow \mathfrak{A}_2 (\mathfrak{B}_1). \tag{22}$$

Из (22) и (19) по правилу силлогизма находим

$$\vdash [\mathfrak{A}_1 (\mathfrak{B}_2) \,\&\, (\mathfrak{B}_1 \sim \mathfrak{B}_2)] \,\&\, [\mathfrak{A}_1 (\mathfrak{B}_1) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_1)] \rightarrow \\ \rightarrow [(\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_2)]. \tag{23}$$

Применив к (23) правило разъединения посылок, получим

$$\vdash [\mathfrak{A}_1 (\mathfrak{B}_2) \,\&\, (\mathfrak{B}_1 \sim \mathfrak{B}_2)] \rightarrow \{[\mathfrak{A}_1 (\mathfrak{B}_1) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_1)] \rightarrow \\ \rightarrow [(\mathfrak{B}_1 \sim \mathfrak{B}_2) \rightarrow \mathfrak{A}_2 (\mathfrak{B}_2)]\},$$

откуда, еще раз применив то же правило и переставив посылки, получаем

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to (\mathfrak{A}_1(\mathfrak{B}_2) \to \{[\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_2(\mathfrak{B}_1)] \to \to [(\mathfrak{B}_1 \sim \mathfrak{B}_2) \to \mathfrak{A}_2(\mathfrak{B}_2)]\}).$$

Формула

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to ([\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_2(\mathfrak{B}_1)] \to \to \{\mathfrak{A}_1(\mathfrak{B}_2) \to [(\mathfrak{B}_1 \sim \mathfrak{B}_2) \to \mathfrak{A}_2(\mathfrak{B}_2)]\}) \quad (24)$$

получается из предыдущей применением правила перестановки посылок и правила силлогизма.

Точно так же получаем из (24)

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to ((\mathfrak{B}_1 \sim \mathfrak{B}_2) \to \{[\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_2(\mathfrak{B}_1)] \to \to [\mathfrak{A}_1(\mathfrak{B}_2) \to \mathfrak{A}_2(\mathfrak{B}_2)]\}), \quad (25)$$

пользуясь правилом перестановки посылок (дважды), правилом силлогизма (дважды) и монотонностью импликации. Из (25), соединив посылки и пользуясь формулой

$$\vdash A \to A \,\&\, A, \quad (26)$$

получим

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to \{[\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_2(\mathfrak{B}_1)] \to \to [\mathfrak{A}_1(\mathfrak{B}_2) \to \mathfrak{A}_2(\mathfrak{B}_2)]\}. \quad (27)$$

[Формулу (26) можно получить, заменив в аксиоме II.3 все переменные высказывания буквой A.]

Так же, как и (27), доказывается

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to \{[\mathfrak{A}_1(\mathfrak{B}_2) \to \mathfrak{A}_2(\mathfrak{B}_2)] \to [\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_2(\mathfrak{B}_1)]\}. \quad (28)$$

Из (27) и (28) следует аксиома (II.3)

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to \{[\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_2(\mathfrak{B}_1)] \sim [\mathfrak{A}_1(\mathfrak{B}_2) \to \mathfrak{A}_2(\mathfrak{B}_2)]\}.$$

4. Из (a) и из

$$\vdash [\mathfrak{A}_1(\mathfrak{B}_1) \to \mathfrak{A}_1(\mathfrak{B}_2)] \to [\overline{\mathfrak{A}_1(\mathfrak{B}_2)} \to \overline{\mathfrak{A}_1(\mathfrak{B}_1)}],$$

получаемого подстановками в аксиому IV. 1, по правилу силлогизма получаем утверждение 4:

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to [\overline{\mathfrak{A}_1(\mathfrak{B}_1)} \sim \overline{\mathfrak{A}_1(\mathfrak{B}_2)}].$$

Теорема эквивалентности полностью доказана.

Заметим, что ни в формулировке, ни в доказательстве этой теоремы мы *не предполагали и не использовали* того, что замена A соответственно на $\mathfrak{B}_1$ и $\mathfrak{B}_2$ в формуле $\mathfrak{A}(A)$ происходит *всюду*, где A входит в $\mathfrak{A}(A)$. Нужно только, чтобы при получении формул $\mathfrak{A}(\mathfrak{B}_1)$ и $\mathfrak{A}(\mathfrak{B}_2)$ в каждом месте, где A входит в $\mathfrak{A}$, такая замена на $\mathfrak{B}_1$ и $\mathfrak{B}_2$ либо происходила, либо нет — *одновременно*.

Это замечание позволяет сформулировать доказанный результат так:

Если в формуле $\mathfrak{A}$ *заменить какую-нибудь ее часть* $\mathfrak{B}_1$ *эквивалентной формулой* $\mathfrak{B}_2$, *то вновь полученная формула* $\mathfrak{A}(\mathfrak{B}_2)$ *будет эквивалентна прежней, именно*:

$$\vdash (\mathfrak{B}_1 \sim \mathfrak{B}_2) \to [\mathfrak{A}(\mathfrak{B}_1) \sim \mathfrak{A}(\mathfrak{B}_2)].$$

§ 7. Некоторые теоремы о выводимости

Теорема 1.

$$\vdash (A \sim \mathfrak{R}) \sim A.$$

Доказательство. По определению эквивалентности нужно доказать следующее:

$$\vdash [(A \sim \mathfrak{R}) \to A] \,\&\, [A \to (A \sim \mathfrak{R})].$$

Но для этого на основании теоремы 3 § 4 главы II достаточно доказать

$$\vdash (A \sim \mathfrak{R}) \to A \tag{1}$$

и

$$\vdash A \to (A \sim \mathfrak{R}). \tag{2}$$

Докажем (1). По определению выводимости имеем $\mathfrak{R} \to A \vdash A$, а потому на основании теоремы дедукции

$$\vdash (\mathfrak{R} \to A) \to A. \tag{3}$$

Из аксиомы II. 2 следует

$$\vdash [(A \to \mathfrak{R}) \,\&\, (\mathfrak{R} \to A)] \to (\mathfrak{R} \to A),$$

т. е.

$$\vdash (A \sim \mathfrak{R}) \to (\mathfrak{R} \to A). \tag{4}$$

Из (3) и (4) по правилу силлогизма заключаем, что

$$\vdash (A \sim \mathfrak{R}) \to A. \tag{1}$$

Докажем теперь (2). Имеем $\vdash \mathfrak{R}$ и тем более $A \vdash \mathfrak{R}$; теорема дедукции дает тогда $\vdash A \to \mathfrak{R}$ и тем более

$A \vdash A \to \mathfrak{R}$. Второй раз применяем теорему дедукции и получаем

$$\vdash A \to (A \to \mathfrak{R}). \tag{5}$$

Из аксиомы I. 1 имеем

$$\vdash A \to (\mathfrak{R} \to A). \tag{6}$$

Подстановками в аксиому II. 3 получим

$$\vdash [A \to (A \to \mathfrak{R})] \to \{[A \to (\mathfrak{R} \to A)] \to \\ \to [A \to (A \to \mathfrak{R}) \& (\mathfrak{R} \to A)]\}.$$

Используя (5) и (6) и применив дважды правило заключения, получим

$$\vdash A \to (A \to \mathfrak{R}) \& (\mathfrak{R} \to A),$$

т. е.

$$\vdash A \to (A \sim \mathfrak{R}), \tag{2}$$

что и требовалось доказать.

Теорема 2.

$$\vdash (A \sim \mathfrak{F}) \sim \overline{A}.$$

Докажем сначала

$$\vdash (A \sim \mathfrak{F}) \to \overline{A}.$$

Подстановка в аксиому IV.1 дает

$$\vdash (A \to \mathfrak{F}) \to (\overline{\mathfrak{F}} \to \overline{A}),$$

т. е.

$$\vdash (A \to \mathfrak{F}) \to (\mathfrak{R} \to \overline{A}). \tag{7}$$

Подставив в (3) $\overline{A}$ на место A, получим

$$\vdash (\mathfrak{R} \to \overline{A}) \to \overline{A}. \tag{8}$$

Из (7) и (8) следует по правилу силлогизма

$$\vdash (A \to \mathfrak{F}) \to \overline{A}. \tag{9}$$

Подстановками в аксиому II.1 получаем

$$\vdash (A \to \mathfrak{F}) \& (\mathfrak{F} \to A) \to (A \to \mathfrak{F}). \tag{10}$$

Из (9) и (10) получаем по правилу силлогизма

$$\vdash (A \to \mathfrak{F}) \& (\mathfrak{F} \to A) \to \overline{A},$$

т. е.

$$\vdash (A \sim \mathfrak{F}) \to \bar{A}. \tag{11}$$

Докажем теперь, что

$$\vdash \bar{A} \to (A \sim \mathfrak{F}),$$

т. е.

$$\vdash \bar{A} \to (A \to \mathfrak{F}) \mathbin{\&} (\mathfrak{F} \to A). \tag{12}$$

Подстановками в аксиомы I. 1 и IV. 1 получим

$$\vdash \bar{A} \to (\mathfrak{R} \to \bar{A}) \tag{13}$$

и

$$\vdash (\mathfrak{R} \to \bar{A}) \to (\bar{\bar{A}} \to \bar{\mathfrak{R}}). \tag{14}$$

Так как $\bar{\bar{A}} \sim A$, то по теореме эквивалентности формула, получаемая заменой $\bar{\bar{A}}$ на A, также выводима:

$$\vdash (\mathfrak{R} \to \bar{A}) \to (A \to \bar{\mathfrak{R}}),$$

т. е. (в силу того, что $\bar{\mathfrak{R}}$ есть $\mathfrak{F}$)

$$\vdash (\mathfrak{R} \to \bar{A}) \to (A \to \mathfrak{F}). \tag{15}$$

Из (13) и (15) по правилу силлогизма заключаем, что

$$\vdash \bar{A} \to (A \to \mathfrak{F}). \tag{16}$$

Так как $\vdash \mathfrak{F} \to A$ (теорема 4 § 4 главы II), то $\bar{A} \vdash \mathfrak{F} \to A$, и по теореме дедукции

$$\vdash \bar{A} \to (\mathfrak{F} \to A). \tag{17}$$

Подстановками в аксиому II. 3 получим

$$\vdash [\bar{A} \to (A \to \mathfrak{F})] \to \{[\bar{A} \to (\mathfrak{F} \to A)] \to$$
$$\to [\bar{A} \to (A \to \mathfrak{F}) \mathbin{\&} (\mathfrak{F} \to A)]\}.$$

Учитывая (16) и (17) и дважды применив правило заключения, получим

$$\vdash \bar{A} \to (A \to \mathfrak{F}) \mathbin{\&} (\mathfrak{F} \to A),$$

т. е.

$$\vdash \bar{A} \to (A \sim \mathfrak{F}). \tag{18}$$

Наконец, подставив в выводимую формулу $A \to$ $\to (B \to A \mathbin{\&} B)$ (см. теорему 3 § 4 главы II) формулу

(11) на место A и формулу (18) на место B и дважды применив правило заключения, получим

$$\vdash [(A \sim \mathfrak{F}) \to \overline{A}] \,\&\, [\overline{A} \to (A \sim \mathfrak{F})],$$

т. е.

$$\vdash (A \sim \mathfrak{F}) \sim \overline{A},$$

что и требовалось доказать.

Теорема 3.

$$\vdash \mathfrak{A}(\mathfrak{R}) \,\&\, \mathfrak{A}(\mathfrak{F}) \to [(A \sim \mathfrak{R}) \to \mathfrak{A}(A)] \,\&\, [(A \sim \mathfrak{F}) \to \mathfrak{A}(A)].$$

Доказательство. В силу теоремы эквивалентности

$$\vdash (A \sim B) \to [\mathfrak{A}(A) \sim \mathfrak{A}(B)]. \tag{19}$$

Из аксиомы II.2

$$\vdash [\mathfrak{A}(A) \sim \mathfrak{A}(B)] \to [\mathfrak{A}(B) \to \mathfrak{A}(A)]. \tag{20}$$

Из (19) и (20) по правилу силлогизма имеем

$$\vdash (A \sim B) \to [\mathfrak{A}(B) \to \mathfrak{A}(A)]$$

или, переставив посылки,

$$\vdash \mathfrak{A}(B) \to [(A \sim B) \to \mathfrak{A}(A)]. \tag{21}$$

Подставив в (21) $\mathfrak{R}$ и $\mathfrak{F}$ вместо B, получаем соответственно

$$\vdash \mathfrak{A}(\mathfrak{R}) \to [(A \sim \mathfrak{R}) \to \mathfrak{A}(A)] \tag{22}$$

и

$$\vdash \mathfrak{A}(\mathfrak{F}) \to [(A \sim \mathfrak{F}) \to \mathfrak{A}(A)]. \tag{23}$$

Но в силу аксиом II.1 и II.2

$$\vdash \mathfrak{A}(\mathfrak{R}) \,\&\, \mathfrak{A}(\mathfrak{F}) \to \mathfrak{A}(\mathfrak{R}) \tag{24}$$

и

$$\vdash \mathfrak{A}(\mathfrak{R}) \,\&\, \mathfrak{A}(\mathfrak{F}) \to \mathfrak{A}(\mathfrak{F}). \tag{25}$$

Применив правило силлогизма к двум парам формул (24), (22) и (23), получим соответственно

$$\vdash \mathfrak{A}(\mathfrak{R}) \,\&\, \mathfrak{A}(\mathfrak{F}) \to [(A \sim \mathfrak{R}) \to \mathfrak{A}(A)]$$

и

$$\vdash \mathfrak{A}(\mathfrak{R}) \,\&\, \mathfrak{A}(\mathfrak{F}) \to [(A \sim \mathfrak{F}) \to \mathfrak{A}(A)],$$

откуда по аксиоме II. 3 следует

$$\vdash \mathfrak{A}(\mathfrak{R}) \,\&\, \mathfrak{A}(\mathfrak{F}) \to [(A \sim \mathfrak{R}) \to \mathfrak{A}(A)] \,\&\, [(A \sim \mathfrak{F}) \to \mathfrak{A}(A)],$$

что и требовалось доказать.

Теорема 4.

$$\vdash [(A \sim \mathfrak{R}) \to \mathfrak{A}(A)] \,\&\, [(A \sim \mathfrak{F}) \to \mathfrak{A}(A)] \to$$
$$\to [(A \sim \mathfrak{R}) \vee (A \sim \mathfrak{F}) \to \mathfrak{A}(A)].$$

Доказательство получаем непосредственно, сделав подстановки в аксиоме III. 3:

$$\vdash [(A \sim \mathfrak{R}) \to \mathfrak{A}(A)] \to \{[(A \sim \mathfrak{F}) \to \mathfrak{A}(A)] \to$$
$$\to [(A \sim \mathfrak{R}) \vee (A \sim \mathfrak{F}) \to \mathfrak{A}(A)]\},$$

и применив к полученной формуле правило соединения посылок.

Теорема 5.

$$\vdash A \vee \bar{A}.$$

Доказательство. Из III. 1 и III. 2 подстановкой получаем

$$\vdash A \to A \vee \bar{A},$$
$$\vdash \bar{A} \to A \vee \bar{A}.$$

Далее, применив IV. 1 и правило заключения, находим

$$\vdash \overline{A \vee \bar{A}} \to \bar{A},$$
$$\vdash \overline{A \vee \bar{A}} \to \bar{\bar{A}}.$$

Подстановками в II. 3 получаем

$$\vdash (\overline{A \vee \bar{A}} \to \bar{\bar{A}}) \to ((\overline{A \vee \bar{A}} \to \bar{A}) \to (\overline{A \vee \bar{A}} \to \bar{\bar{A}} \,\&\, \bar{A})),$$

откуда, применив дважды правило заключения, находим

$$\vdash \overline{A \vee \bar{A}} \to \bar{\bar{A}} \,\&\, \bar{A}.$$

В силу эквивалентности A и $\bar{\bar{A}}$

$$\vdash \overline{A \vee \bar{A}} \to A \,\&\, \bar{A}.$$

Применив правило силлогизма к последней формуле и утверждению теоремы 6 § 4, находим

$$\vdash \overline{A \vee \bar{A}} \to \mathfrak{F}.$$

Подстановки в IV. 1 дают

$$\vdash (\overline{A \vee \bar{A}} \to \mathfrak{F}) \to (\bar{\mathfrak{F}} \to \overline{\overline{A \vee \bar{A}}}),$$

откуда, применяя правило заключения, получаем

$$\vdash \bar{\mathfrak{F}} \to \overline{\overline{A \vee \bar{A}}}.$$

Так как $\bar{\mathfrak{F}}$ есть $\mathfrak{R}$, а формула $\overline{\overline{A \vee \bar{A}}}$ эквивалентна $A \vee \bar{A}$, то имеем

$$\vdash \mathfrak{R} \to A \vee \bar{A}.$$

Так как $\mathfrak{R}$ выводимо, то, применив правило заключения, находим

$$\vdash A \vee \bar{A},$$

что и требовалось доказать.

Теорема 6.

$$\vdash (A \sim \mathfrak{R}) \vee (A \sim \mathfrak{F}).$$

Следует из теоремы 5 с помощью теорем 1 и 2.

Теорема 7.

$$\vdash \mathfrak{A}(\mathfrak{R}) \,\&\, \mathfrak{A}(\mathfrak{F}) \to \mathfrak{A}(A).$$

Доказательство. Применив правило силлогизма к формулам, доказанным в теоремах 3 и 4, получим

$$\vdash \mathfrak{A}(\mathfrak{R}) \,\&\, \mathfrak{A}(\mathfrak{F}) \to [(A \sim \mathfrak{R}) \vee (A \sim \mathfrak{F}) \to \mathfrak{A}(A)].$$

Отсюда, используя правило перестановки посылок, теорему 6 и правило заключения, находим

$$\vdash \mathfrak{A}(\mathfrak{R}) \,\&\, \mathfrak{A}(\mathfrak{F}) \to \mathfrak{A}(A),$$

что и требовалось доказать.

Введем теперь нужное для дальнейшего *сокращенное обозначение.*

Пусть формула $\mathfrak{A}$ содержит ровно n переменных высказываний:

$$\mathfrak{A} = \mathfrak{A}(A_1, A_2, \ldots, A_n).$$

Определим для нее по индукции формулу

$$\prod_{\delta_1, \ldots, \delta_n = \mathfrak{R}, \mathfrak{F}} \mathfrak{A}(\delta_1, \ldots, \delta_n). \qquad (*)$$

Если $n = 1$, то $\prod\limits_{\delta_1 = \mathfrak{N}, \mathfrak{F}} \mathfrak{A}(\delta_1)$ — это формула $\mathfrak{A}(\mathfrak{N}) \& \mathfrak{A}(\mathfrak{F})$. Пусть определены формулы (*) для всех $\mathfrak{A}$, для которых $n \leqslant k$. Пусть теперь формула $\mathfrak{A}(A_1, A_2, \ldots, A_k, A_{k+1})$ содержит ровно $k+1$ высказываний $A_1, \ldots, A_k, A_{k+1}$; через $\prod\limits_{\delta_1, \ldots, \delta_{k+1} = \mathfrak{N}, \mathfrak{F}} \mathfrak{A}(\delta_1, \ldots, \delta_k, \delta_{k+1})$ мы обозначим формулу

$$\left[\prod_{\delta_1, \ldots, \delta_k = \mathfrak{N}, \mathfrak{F}} \mathfrak{A}(\delta_1, \ldots, \delta_k, \mathfrak{N})\right] \& \left[\prod_{\delta_1, \ldots, \delta_k = \mathfrak{N}, \mathfrak{F}} \mathfrak{A}(\delta_1, \ldots, \delta_k, \mathfrak{F})\right].$$

Таким образом, мы определили формулу (*) для $\mathfrak{A}(A_1, \ldots, A_k, A_{k+1})$, содержащей $k+1$ высказываний, через формулы (*) для $\mathfrak{A}(A_1, \ldots, A_k, \mathfrak{N})$ и $\mathfrak{A}(A_1, \ldots, A_k, \mathfrak{F})$, содержащих по k переменных высказываний.

По существу, формула (*) может быть определена как конъюнкция (логическое произведение) всех возможных формул, полученных из $\mathfrak{A}(A_1, \ldots, A_n)$ всевозможными заменами переменных высказываний $A_1, A_2, \ldots, A_n$ на $\mathfrak{N}$ и $\mathfrak{F}$. Однако мы пока не доказали, что такое произведение ассоциативно и коммутативно, т. е. не зависит от способа расстановки скобок и от порядка сомножителей. Поэтому нам и пришлось определить формулу (*), задав некоторый определенный порядок сомножителей и определенный способ расстановки скобок.

Исходя из последней теоремы, легко доказать (по индукции) следующее утверждение.

Теорема 8.

$$\vdash \prod_{\delta_1, \ldots, \delta_n = \mathfrak{N}, \mathfrak{F}} \mathfrak{A}(\delta_1, \ldots, \delta_n) \to \mathfrak{A}(A_1, A_2, \ldots, A_n).$$

§ 8. Связь между формулами алгебры высказываний и исчисления высказываний

Формулы исчисления высказываний можно интерпретировать как формулы алгебры высказываний. Для этого мы будем трактовать свободные переменные исчисления высказываний как переменные алгебры высказываний, т. е. переменные в содержательном смысле, принимающие значения *И* и *Л*. Операции &, $\vee$ и $^{-}$ определим так же, как в алгебре высказываний; тогда всякая формула при любых значениях переменных сама будет принимать одно из значений *И* или *Л*, вычисляемое по правилам алгебры высказываний.

Произведем теперь в произвольной формуле исчисления высказываний $\mathfrak{A}$ замену входящих в нее переменных высказываний формулами $\mathfrak{R}$ и $\mathfrak{F}$. Если в той же формуле $\mathfrak{A}$, рассматривая ее как формулу алгебры высказываний, переменным высказываниям придать значения *И* и *Л*, причем значение *И* (или *Л*) придавать тем переменным, которые в $\mathfrak{A}$, как в формуле исчисления высказываний, были заменены соответственно $\mathfrak{R}$ (или $\mathfrak{F}$), то формула $\mathfrak{A}$ в алгебре высказываний примет одно из значений: *И* или *Л*. Мы докажем, что *если при этом значение* $\mathfrak{A}$ *есть И* (или есть *Л*), *то при соответствующей замене в* $\mathfrak{A}$, *как в формуле исчисления высказываний, получим* $\vdash \mathfrak{A}(\mathfrak{R}, \mathfrak{F}) \sim \mathfrak{R}$ (соответственно $\vdash \mathfrak{A}(\mathfrak{R}, \mathfrak{F}) \sim \mathfrak{F}$).

Достаточно доказать наше утверждение для простейших формул, полученных из переменных высказываний с помощью одной из операций: &, $\vee$, $\rightarrow$ или $^{-}$; действительно, тогда для любой формулы это утверждение доказывается по индукции на основании теоремы эквивалентности. Итак, докажем наше утверждение для простейших формул:

$$\text{a) } A \rightarrow B; \quad \text{b) } A \,\&\, B;$$

$$\text{c) } A \vee B; \quad \text{d) } \bar{A}.$$

Для каждой из этих формул нужно рассмотреть все возможные замены переменных высказываний формулами $\mathfrak{R}$ и $\mathfrak{F}$; однако мы рассмотрим лишь несколько случаев, так как доказательство в остальных проводится аналогично.

Рассмотрим сначала формулу d). Нужно доказать:

$$\text{d}_1) \ \vdash \bar{\mathfrak{F}} \sim \mathfrak{R};$$

$$\text{d}_2) \ \vdash \bar{\mathfrak{R}} \sim \mathfrak{F}.$$

Утверждение d_1) следует из определения формулы $\mathfrak{F}$ и из того, что всякие две истинные формулы исчисления высказываний эквивалентны.

d_2) $\vdash \mathfrak{L} \to \overline{\mathfrak{I}}$ получается из теоремы 4 § 4. Докажем

$$\vdash \overline{\mathfrak{I}} \to \mathfrak{L}.$$

Подстановка в аксиому IV. 1 дают

$$\vdash (\overline{\overline{\mathfrak{L}}} \to \mathfrak{I}) \to (\overline{\mathfrak{I}} \to \overline{\overline{\overline{\mathfrak{L}}}}).$$

Посылка этой формулы выводима в силу d_1). Применив правило заключения, находим

$$\vdash \overline{\mathfrak{I}} \to \overline{\overline{\overline{\mathfrak{L}}}}.$$

Так как из аксиомы IV. 3 имеем

$$\vdash \overline{\overline{\overline{\mathfrak{L}}}} \to \mathfrak{L},$$

то, применив правило силлогизма, получим

$$\vdash \overline{\mathfrak{I}} \to \mathfrak{L}.$$

a) Здесь мы рассмотрим все возможные замены и докажем, что

$$\begin{aligned}
&\mathrm{a}_1)\ \vdash (\mathfrak{I} \to \mathfrak{L}) \sim \mathfrak{L},\\
&\mathrm{a}_2)\ \vdash (\mathfrak{L} \to \mathfrak{I}) \sim \mathfrak{I},\\
&\mathrm{a}_3)\ \vdash (\mathfrak{I} \to \mathfrak{I}) \sim \mathfrak{I},\\
&\mathrm{a}_4)\ \vdash (\mathfrak{L} \to \mathfrak{L}) \sim \mathfrak{I}.
\end{aligned}$$

a_1) Достаточно доказать, что

$$\vdash \mathfrak{L} \to (\mathfrak{I} \to \mathfrak{L}) \qquad (1)$$

и

$$\vdash (\mathfrak{I} \to \mathfrak{L}) \to \mathfrak{L}. \qquad (2)$$

Но (1) получаем непосредственно подстановкой в формулу $\vdash \mathfrak{L} \to A$, доказанную в § 4.

Чтобы доказать (2), делаем подстановки в аксиоме IV. 1:

$$\vdash (\mathfrak{I} \to \mathfrak{L}) \to (\overline{\mathfrak{L}} \to \overline{\mathfrak{I}}),$$

откуда перестановкой посылок получаем

$$\vdash \overline{\mathfrak{L}} \to [(\mathfrak{I} \to \mathfrak{L}) \to \overline{\mathfrak{I}}].$$

Заметив теперь, что $\vdash \overline{\mathfrak{L}} \sim \mathfrak{I}$ и $\vdash \overline{\mathfrak{I}} \sim \mathfrak{L}$, и применив теорему эквивалентности (стр. 92) и правило заключения, получим требуемое:

$$\vdash (\mathfrak{I} \to \mathfrak{L}) \to \mathfrak{L}.$$

В остальных трех случаях доказательство немедленно следует из того, что формулы $\mathfrak{F} \to \mathfrak{R}$, $\mathfrak{R} \to \mathfrak{R}$ и $\mathfrak{F} \to \mathfrak{F}$ выводимые. Действительно, $\vdash \mathfrak{F} \to \mathfrak{R}$ получаем подстановкой в доказанную в § 4 истинную формулу

$$\vdash \mathfrak{F} \to A;$$

выводимость же формул $\mathfrak{R} \to \mathfrak{R}$ и $\mathfrak{F} \to \mathfrak{F}$ следует из теоремы 2 § 2, утверждающей, что $\vdash A \to A$.

Рассмотрим еще для примера один из возможных случаев замены в формуле $A \vee B$, а именно докажем, что

$$\vdash \mathfrak{R} \vee \mathfrak{F} \sim \mathfrak{R}.$$

Здесь $\vdash \mathfrak{R} \vee \mathfrak{F} \to \mathfrak{R}$ следует из теоремы 1 § 2, а

$$\vdash \mathfrak{R} \to \mathfrak{R} \vee \mathfrak{F}$$

есть результат подстановки в аксиому III. 1.

Доказательства в остальных случаях проводятся сходным образом и могут быть предложены читателю в качестве упражнений.

§ 9. Непротиворечивость исчисления высказываний

Проблема непротиворечивости возникает при рассмотрении любого исчисления; это одна из кардинальных проблем математической логики. Дадим определение непротиворечивости логического исчисления, которое относится не только к исчислению высказываний, но и ко всем логическим системам, изучаемым в математической логике.

Мы назовем логическое исчисление непротиворечивым, если в нем не выводимы никакие две формулы, из которых одна является отрицанием другой.

Иными словами, непротиворечивое исчисление — это такое исчисление, что, какова бы ни была формула $\mathfrak{A}$, никогда формулы $\mathfrak{A}$ и $\overline{\mathfrak{A}}$ не могут быть одновременно выведены из аксиом этого исчисления с помощью указанных в нем правил.

Проблема непротиворечивости состоит в следующем: является данное исчисление непротиворечивым или нет?

Если в исчислении обнаруживаются выводимые формулы вида $\mathfrak{A}$ и $\overline{\mathfrak{A}}$, то такое исчисление называется *противоречивым.* Такие исчисления никакой ценности не представляют. Все сколько-нибудь существенные логические системы таковы, что если бы какая-нибудь из них оказалась противоречивой, то это бы значило, что в ней все формулы выводимы, и поэтому такие системы не могут отражать в себе различие между истиной и ложью.

Если бы, например, в исчислении высказываний некоторые формулы $\mathfrak{A}$ и $\overline{\mathfrak{A}}$ оказались выводимыми, то в силу доказанных нами формул (см. теоремы 4 и 6 § 4)

$$\vdash \mathfrak{F} \rightarrow A \qquad \text{и} \qquad \vdash \mathfrak{A} \,\&\, \overline{\mathfrak{A}} \rightarrow \mathfrak{F}$$

мы имели бы

$$\vdash \mathfrak{A} \,\&\, \overline{\mathfrak{A}} \rightarrow A.$$

Но если $\mathfrak{A}$ и $\overline{\mathfrak{A}}$ выводимы, то в силу правила $\dfrac{\mathfrak{A}, \mathfrak{B}}{\mathfrak{A} \,\&\, \mathfrak{B}}$ также выводима $\mathfrak{A} \,\&\, \overline{\mathfrak{A}}$, и, следовательно, формула A также выводима в исчислении высказываний. Но если переменное высказывание A выводимо, то подстановкой в него можно вывести любую формулу.

Все сказанное об исчислении высказываний оказывается справедливым и для всех тех логических исчислений, которые мы будем рассматривать далее.

То обстоятельство, что в противоречивом исчислении всякая формула выводима, может быть использовано для доказательства непротиворечивости. Для этого достаточно показать, что существует по крайней мере одна невыводимая формула. Отсюда будет следовать непротиворечивость исчисления. Непротиворечивость исчисления высказываний устанавливается, однако, очень просто и без этого.

Теорема. *Исчисление высказываний непротиворечиво.*

Как мы уже говорили выше, каждую формулу исчисления высказываний можно рассматривать в то же время как формулу алгебры высказываний.

Покажем, что все формулы, выводимые в исчислении высказываний и рассмотренные как формулы алгебры высказываний, являются тождественно истинными, т. е. принимают значение *И* при всех значениях переменных высказываний.

Легко непосредственно проверить, что аксиомы исчисления высказываний таковы.

Покажем, что если формула $\mathfrak{A}(A)$, содержащая переменное высказывание A, тождественно истинна, то и формула $\mathfrak{A}(\mathfrak{B})$, получаемая из $\mathfrak{A}(A)$ подстановкой, также тождественно истинна. В самом деле, $\mathfrak{A}(A)$ при всех значениях переменных высказываний принимает значение $И$. В таком случае $\mathfrak{A}(И)$ и $\mathfrak{A}(Л)$ имеют значение $И$, каковы бы ни были значения других переменных высказываний. Но $\mathfrak{B}$ при любых значениях переменных высказываний может иметь только значение $И$ или $Л$. Отсюда ясно, что $\mathfrak{A}(\mathfrak{B})$ всегда будет иметь значение $И$.

Докажем, что если формулы $\mathfrak{A}$ и $\mathfrak{A} \to \mathfrak{B}$ тождественно истинны, то формула $\mathfrak{B}$ также тождественно истинна.

Если $\mathfrak{A}$ тождественно истинна, то она всегда имеет значение $И$. Так как формула $\mathfrak{A} \to \mathfrak{B}$ также всегда принимает значение $И$, то $\mathfrak{B}$ не может принять значение $Л$ ни при каких значениях переменных высказываний, иначе формула $\mathfrak{A} \to \mathfrak{B}$ приняла бы значение $И \to Л$, которое, по определению следования в алгебре высказываний, есть $Л$.

Итак, мы показали, что: 1) все аксиомы суть тождественно истинные формулы, 2) применяя к тождественно истинным формулам правила вывода, мы получаем также тождественно истинные формулы. Отсюда следует, что все выводимые формулы исчисления высказываний, рассматриваемые как формулы алгебры высказываний, являются тождественно истинными. В таком случае ясно, что если формула $\mathfrak{A}$ выводима в исчислении высказываний, то формула $\overline{\mathfrak{A}}$ не может быть выводима, так как $\mathfrak{A}$ — тождественно истинная формула, а $\overline{\mathfrak{A}}$ тогда, наоборот, принимает значение $Л$ при всех значениях входящих переменных высказываний. Итак, непротиворечивость исчисления высказываний доказана.

§ 10. Полнота исчисления высказываний

В § 8 мы уже отметили, что формулы исчисления высказываний могут быть интерпретированы как формулы алгебры высказываний. Доказывая непротиворечивость исчисления высказываний, мы показали, что всякая формула, выводимая в исчислении высказываний, является тождественно истинной, если ее рассматривать как формулу алгебры высказываний. Возникает обратный вопрос: *будет ли всякая тождественно истинная формула алгебры высказываний выводима в исчислении высказываний?*

Этот вопрос и представляет собой *проблему полноты в широком смысле* для исчисления высказываний.

Смысл такой постановки вопроса состоит в том, что при построении логического исчисления, предназначенного выражать содержательную логику, нам требуется знать, достаточно ли мы имеем аксиом и правил для того, чтобы вывести любую формулу, которая в содержательном понимании является тождественно истинной.

Проблема полноты в широком смысле слова решается положительным образом.

Теорема. *Всякая тождественно истинная формула алгебры высказываний выводима в исчислении высказываний.*

Для доказательства рассмотрим произвольную тождественно истинную в алгебре высказываний формулу $\mathfrak{A}$ и воспользуемся теоремой 8 § 7:

$$\vdash \prod_{\delta_1, \ldots, \delta_n = \mathfrak{R}, \mathfrak{F}} \mathfrak{A}(\delta_1, \ldots, \delta_n) \to \mathfrak{A}(A_1, \ldots, A_n). \qquad (1)$$

Так как формула $\mathfrak{A} = \mathfrak{A}(A_1, \ldots, A_n)$ тождественно истинна, то любая подстановка формул $\mathfrak{R}$, $\mathfrak{F}$ вместо $A_1, \ldots, A_n$ в формулу $\mathfrak{A}$ приводит к выводимой в исчислении высказываний формуле (это доказано в § 8). Следовательно, в формуле

$$\prod_{\delta_1, \delta_2, \ldots, \delta_n = \mathfrak{R}, \mathfrak{F}} \mathfrak{A}(\delta_1, \ldots, \delta_n),$$

являющейся посылкой в (1), все сомножители — выводимые формулы, а значит, и вся эта формула выводимая. Применив теперь к (1) правило заключения, получим, что формула $\mathfrak{A}(A_1, \ldots, A_n)$ выводима в исчислении высказываний. Таким образом, полнота в широком смысле исчисления высказываний доказана. Мы показали, что употреблявшийся нами ранее термин «выводимая в исчислении высказываний формула» совпадает с содержательным понятием тождественно истинной формулы. Одним из следствий теоремы о полноте является возможность непосредственно перенести в исчислении высказываний все «правила действий» с формулами, которые выполняются в алгебре высказываний. Например, отсюда следует, что в исчислении высказываний верны утверждения:

$$\vdash \mathfrak{A} \,\&\, \mathfrak{B} \sim \mathfrak{B} \,\&\, \mathfrak{A},$$

$$\vdash \mathfrak{A} \vee \mathfrak{B} \sim \mathfrak{B} \vee \mathfrak{A},$$

$$\vdash \mathfrak{A} \,\&\, (\mathfrak{B} \,\&\, \mathfrak{C}) \sim (\mathfrak{A} \,\&\, \mathfrak{B}) \,\&\, \mathfrak{C},$$

$$\vdash \mathfrak{A} \vee (\mathfrak{B} \vee \mathfrak{C}) \sim (\mathfrak{A} \vee \mathfrak{B}) \vee \mathfrak{C},$$

$$\vdash \mathfrak{A} \,\&\, (\mathfrak{B} \vee \mathfrak{C}) \sim \mathfrak{A} \,\&\, \mathfrak{B} \vee \mathfrak{A} \,\&\, \mathfrak{C},$$

$$\vdash \mathfrak{A} \vee \mathfrak{B} \,\&\, \mathfrak{C} \sim (\mathfrak{A} \vee \mathfrak{B}) \,\&\, (\mathfrak{A} \vee \mathfrak{C}),$$

$$\vdash (\mathfrak{A} \to \mathfrak{B}) \sim \overline{\mathfrak{A}} \vee \mathfrak{B},$$

$$\vdash \overline{\mathfrak{A} \vee \mathfrak{B}} \sim \overline{\mathfrak{A}} \,\&\, \overline{\mathfrak{B}},$$

$$\vdash \overline{\mathfrak{A} \,\&\, \mathfrak{B}} \sim \overline{\mathfrak{A}} \vee \overline{\mathfrak{B}}.$$

Не менее важное значение, чем понятие полноты в широком смысле, имеет понятие *полноты логического исчисления в узком смысле*. Логическое исчисление называется полным в узком смысле, если присоединение к его аксиомам какой-нибудь не выводимой в нем формулы приводит к противоречию.

Исчисление высказываний полно также в узком смысле. Доказательство этого факта нетрудно провести, используя конъюнктивные нормальные формы. Предоставляем читателю провести это доказательство.

§ 11. Независимость аксиом исчисления высказываний

Как мы уже говорили выше, всякое логическое исчисление может быть задано следующим образом: определяется понятие формулы и понятие выводимой формулы. Это делается путем указания, во-первых, некоторых исходных формул, объявленных выводимыми и называемых аксиомами, и, во-вторых, правил вывода, т. е. таких правил, с помощью которых из выводимых формул можно образовывать новые выводимые формулы. Для всякого такого исчисления возникает вопрос о независимости его аксиом. Вопрос этот ставится следующим образом:

Можно ли какую-нибудь аксиому вывести из остальных, применяя правила вывода данной системы?

Если оказывается, что некоторую аксиому можно таким образом вывести из остальных, то ее можно вычеркнуть из списка аксиом, и логическое исчисление при этом не изменится, т. е. запас его выводимых формул останется тот же.

Аксиома, не выводимая из остальных аксиом, называется независимой от этих аксиом, а система аксиом, в которой ни одна аксиома не выводима из остальных, называется независимой системой аксиом. В противном случае система аксиом называется зависимой. Ясно, что зависимая система аксиом в некотором смысле менее совершенна, чем независимая, так как она содержит лишние аксиомы. На первый взгляд кажется, что вопрос о независимости системы аксиом мало существен и имеет значение только с точки зрения технического удобства. Однако это не всегда так. Вопрос о независимости одной аксиомы некоторой системы от других аксиом часто бывает равносилен вопросу о возможности заменить без противоречия в рассматриваемой системе данную аксиому ее отрицанием. В качестве примера можно указать вопрос о независимости пятого постулата Евклида в системе аксиом геометрии. Вопрос этот, как известно, имел большое значение в развитии математики.

Мы докажем, что система аксиом исчисления высказываний независима. Метод доказательства этого положения сходен с тем, которым мы доказывали непротиворечивость исчисления высказываний (см. § 9). Тогда мы интерпретировали переменные высказывания в исчислении высказываний как переменные алгебры высказываний, способные принимать два значения *И* и *Л*. Операции &, $\vee$, $\rightarrow$, $^{-}$ мы при этом определяли так же, как в алгебре высказываний, и устанавливали, что всякая выводимая формула исчисления высказываний получает при всех значениях переменных значение *И*. Для решения вопроса о независимости некоторой аксиомы $\mathfrak{A}$ исчисления высказываний мы поставим себе задачу интерпретировать переменные высказывания как переменные с конечным набором значений, которые мы будем обозначать греческими буквами α, β, ... Операции &, $\vee$, $\rightarrow$, $^{-}$ определим с таким расчетом, чтобы соблюдались следующие условия:

1) Все аксиомы, кроме аксиомы $\mathfrak{A}$, при всех значениях переменных принимают значение α.

2) Каждая формула, выводимая из совокупности всех отличных от $\mathfrak{A}$ аксиом системы, также принимает значение α при всех значениях входящих переменных.

3) Аксиома $\mathfrak{A}$ принимает отличные от α значения при некоторых значениях входящих переменных.

Ясно, что если удастся привести такую интерпретацию, то независимость аксиомы $\mathfrak{A}$ от других аксиом будет доказана, так как если бы $\mathfrak{A}$ была выводима из них, то она имела бы значение α при всех значениях переменных. Заметим, что формулы, в которых вместо переменных подставлены некоторые их значения, также имеют смысл. Например,

$$\alpha \& \beta, \quad \bar{\alpha}, \quad A \rightarrow \alpha \quad \text{и т. д.}$$

То обстоятельство, что две формулы $\mathfrak{A}$ и $\mathfrak{B}$ принимают при всех заменах входящих в них переменных одинаковое значение α, β, ..., мы будем в дальнейшем ради краткости выражать знаком равенства:

$$\mathfrak{A} = \mathfrak{B}.$$

При этом мы будем всегда считать, что знак $=$ связывает слабее логических связок &, $\vee$, $\rightarrow$.

Легче всего доказать независимость аксиом групп II—IV. Мы докажем сейчас независимость аксиомы II. 1. Для этого будем интерпретировать переменные высказывания как переменные, принимающие два значения α и β. При этом α будет играть роль *И*, а β — роль *Л*. Все логические операции, кроме конъюнкции, определим так же, как в алгебре высказываний. Выпишем эту интерпретацию подробно:

$$\alpha \rightarrow \alpha = \alpha; \quad \beta \rightarrow \beta = \alpha; \quad \beta \rightarrow \alpha = \alpha; \quad \alpha \rightarrow \beta = \beta;$$

$$\alpha \vee \alpha = \alpha; \quad \alpha \vee \beta = \alpha; \quad \beta \vee \alpha = \alpha; \quad \beta \vee \beta = \beta;$$

$$\bar{\alpha} = \beta; \quad \bar{\beta} = \alpha.$$

Операцию же конъюнкции определим условием

$$A \& B = B.$$

Покажем, что тогда все формулы I—IV, кроме II. 1, принимают значение α при всех значениях входящих переменных. В формулы групп I, III и IV конъюнкция не входит; остальные же операции определены так же, как в алгебре высказываний. Так как в алгебре высказываний эти формулы являются тождественно истинными, то в нашей интерпретации они принимают значение α при всех значениях переменных. Рассмотрим отдельно формулы группы II. Формула II. 2 принимает всегда значение α, так как в нашей интерпретации она равносильна

$$B \to B.$$

Формула II. 3 равносильна формуле

$$(A \to B) \to ((A \to C) \to (A \to C)).$$

Эта формула не содержит конъюнкции и является тождественно истинной формулой алгебры высказываний. Поэтому она всегда принимает значение α.

Но формула II. 1 не является тождественно равной α. В самом деле, при $A = \beta$ и $B = \alpha$ она примет вид

$$\beta \& \alpha \to \beta.$$

Но, по определению операции &,

$$\beta \& \alpha = \alpha.$$

Поэтому наша формула принимает вид

$$\alpha \to \beta,$$

а это выражение имеет, по условию, значение β.

Покажем теперь, что формулы, получаемые путем правил вывода из таких, которые тождественно равны α, сами тождественно равны α.

Для правила подстановки это очевидно: если формула при всех значениях переменных принимает значение α, то такова же будет и формула, полученная из нее любой заменой переменных.

Рассмотрим правило заключения. Пусть формулы $\mathfrak{A}$ и $\mathfrak{A} \to \mathfrak{B}$ принимают значение α при всех значениях входящих переменных; но тогда

$$\mathfrak{A} \rightarrow \mathfrak{B} = \alpha \rightarrow \mathfrak{B}.$$

В таком случае $\mathfrak{B}$ не может принять значение β, так как в противном случае при соответствующей подстановке мы имели бы

$$\mathfrak{A} \rightarrow \mathfrak{B} = \alpha \rightarrow \beta = \beta,$$

чего не может быть. (Для правила заключения мы здесь, по существу, повторили рассуждение § 10, где доказывали, что правило заключения, применяемое к тождественно истинным формулам в смысле алгебры высказываний, приводит к таким же формулам.)

Таким образом, мы доказали независимость аксиомы II. 1.

Вообще независимость любой аксиомы из групп II—IV можно доказать по следующей схеме. Мы допускаем, что переменные могут принимать только два значения α и β. Все логические операции &, $\vee$, $\rightarrow$, $^{-}$, кроме одной из них, мы определяем так же, как и в алгебре высказываний, причем α играет роль *И*, а β — роль *Л*. Одну же из операций определяем так, чтобы та аксиома, независимость которой доказывается, не являлась тождественно равной α. Вместо того чтобы приводить все эти доказательства, мы дадим таблицу, в первом столбце которой стоит аксиома, независимость которой доказывается, во втором столбце помещено определение той операции &, $\vee$, $\rightarrow$ или $^{-}$, которая определяется иначе, чем в алгебре высказываний, и в третьем столбце указаны те значения переменных, при которых соответствующая аксиома принимает значение β.

При всех указанных интерпретациях аксиомы, входящие в группы, отличные от той, в которой находится исследуемая аксиома, принимают значение α при всех значениях переменных. Происходит это потому, что в аксиомы этих групп не входит та исключительная операция, которая определяется иначе, чем в алгебре высказываний, и, следовательно, интерпретация этих формул такая же, как и в алгебре высказываний. Поэтому все эти формулы принимают значение α при всех значениях переменных.

Аксиома	Исключительная операция	Значения переменных
II. 1. $A \& B \to A$	$A \& B = B$	$A = \beta$, $B = \alpha$
II. 2. $A \& B \to B$	$A \& B = A$	$A = \alpha$, $B = \beta$
II. 3. $(A \to B) \to$ $\to ((A \to C) \to (A \to B \& C))$	$A \& B = \beta$	$A = \alpha$, $B = \alpha$, $C = \alpha$
III. 1. $A \to A \vee B$	$A \vee B = B$	$A = \alpha$, $B = \beta$
III. 2. $B \to A \vee B$	$A \vee B = A$	$A = \beta$, $B = \alpha$
III. 3. $(A \to C) \to$ $\to ((B \to C) \to (A \vee B \to C))$	$A \vee B = \alpha$	$A = \beta$, $B = \beta$, $C = \beta$
IV. 1. $(A \to B) \to (\overline{B} \to \overline{A})$	$\overline{A} = A$	$A = \beta$, $B = \alpha$
IV. 2. $A \to \overline{\overline{A}}$	$\overline{A} = \beta$	$A = \alpha$
IV. 3. $\overline{\overline{A}} \to A$	$\overline{A} = \alpha$	$A = \beta$

Для аксиом той группы, куда входит исследуемая аксиома, можно убедиться непосредственной проверкой, что две из них также тождественно равны α, а сама исследуемая аксиома принимает значение β при значениях переменных, указанных в третьем столбце.

Доказательство того, что правила вывода, применяемые к формулам, тождественно равным α, порождают формулы, также тождественно равные α, для всех интерпретаций будет таким же, как и в случае приведенного выше доказательства независимости аксиомы II. 1. Таким образом, остается доказать независимость аксиом группы I. Доказательство независимости этих аксиом более трудно, так как знак $\to$ входит во все группы.

Интерпретации, которые мы будем употреблять для доказательства независимости аксиом группы I, удовлетворяют следующим общим условиям:

$$\left.\begin{array}{llll} A \to A = \alpha; & A \to \alpha = \alpha; & \beta \to A = \alpha; & \\ A \& B = B \& A; & A \& \alpha = A; & A \& \beta = \beta; & \\ A \vee B = B \vee A; & A \vee \alpha = \alpha; & A \vee \beta = A; & \\ \bar{\alpha} = \beta; & \bar{\beta} = \alpha; & A \& A = A; & A \vee A = A. \end{array}\right\} \quad (a)$$

Ясно, что эти условия совместны, так как им удовлетворяет, например, интепретация, являющаяся алгеброй высказываний, если α принять за *И*, а β за *Л*. Но эти условия, как мы сейчас увидим, не определяют интерпретацию однозначно.

Для доказательства независимости аксиомы I. 1 выберем следующую интерпретацию. Переменные принимают значения α, β, γ и δ, и, кроме условий (a), должны выполняться следующие условия:

$$\left.\begin{array}{llll} \alpha \to \beta = \beta; & \alpha \to \gamma = \beta; & \alpha \to \delta = \beta; & \\ \gamma \to \beta = \beta; & \gamma \to \delta = \beta; & & \\ \delta \to \beta = \beta; & \delta \to \gamma = \alpha; & & \\ \gamma \& \delta = \delta; & \gamma \vee \delta = \gamma; & \bar{\gamma} = \delta; & \bar{\delta} = \gamma. \end{array}\right\} \quad \text{(b)}$$

Легко видеть, что условия (a) и (b) уже полностью определяют интерпретацию. Например, операция $\to$ определяется условиями (a) и (b) однозначно. Действительно, когда первый из членов импликации есть β, или когда второй есть α, или когда оба члена равны, то операция $\to$ определяется условиями (a). Во всех остальных случаях значение формулы $A \to B$ определено условиями (b).

Операции & и $\vee$ также определяются из условий (a), когда один из членов или равен α, или равен β, или когда оба члена равны между собой.

Остается один случай, когда один из членов равен γ, а другой δ; в этом случае операции определяются полностью условиями $A \& B = B \& A$, $A \vee B = B \vee A$ из (a) и условиями (b). Операция отрицания очевидным образом определена условиями (a) и (b).

Из условий (a) и (b) вытекает, что применение правила заключения к формуле, тождественно равной α, приводит также к формуле, тождественно равной α.

В самом деле, если $\mathfrak{A} = \alpha$ и $\mathfrak{A} \to \mathfrak{B} = \alpha$, то $\alpha \to \mathfrak{B} = \alpha$. Но из условий (a) и (b) видно, что если значение $\mathfrak{B}$ отлично от α, то $\alpha \to \mathfrak{B}$ не равно α, поэтому $\mathfrak{B}$ также тождественно равно α.

То, что подстановка в формулу, тождественно равную α, приводит к формуле, тождественно равной α, остается, очевидно, верным для всех интерпретаций. Таким образом, правила вывода, применяемые к формулам, тождественно равным α, приводят к формулам, также тождественно равным α. Кроме того, приведенная интерпретация обладает тем свойством, что если переменные принимают значения α и β, то операции &, $\vee$, $\rightarrow$ и $\neg$ над ними таковы же, как в алгебре высказываний, если считать α за *И*, а β за *Л*.

В рассматриваемой интерпретации формула I. 1 при значениях переменных $A=\delta$, $B=\alpha$ принимает значение β. В самом деле, при этих значениях эта формула примет вид $\delta\rightarrow(\alpha\rightarrow\delta)$, но $\alpha\rightarrow\delta=\beta$ в силу условий (b), и формула примет вид $\delta\rightarrow\beta=\beta$.

Можно показать, что все остальные аксиомы при всех значениях переменных принимают значение α. Мы не будем проводить доказательства этого утверждения для всех аксиом. Истинность его может быть установлена непосредственной проверкой. Мы ограничимся тем, что докажем справедливость нашего утверждения для некоторых аксиом.

Рассмотрим аксиому I. 2. Выпишем ее:

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

Покажем сначала, что если

$$A\rightarrow B=\alpha, \quad B\rightarrow C=\alpha,$$

то и $A\rightarrow C=\alpha$, и, следовательно, аксиома I. 2 принимает значение α.

В самом деле, если $A\rightarrow B=\alpha$, то возможны только следующие случаи:

1) $A=\beta$;
2) $B=\alpha$;
3) $A=B$;
4) $A=\delta$; $B=\gamma$.

В первых трех случаях непосредственно видно, что

$$A\rightarrow C=\alpha,$$

так как при $B=\alpha$ из $B\rightarrow C=\alpha$ следует $C=\alpha$. В последнем случае в силу того, что $B\rightarrow C=\alpha$, для C возможны только два значения: γ и α. В обоих случаях $A\rightarrow C=\alpha$.

Остается рассмотреть случай, когда либо $A\rightarrow B$, либо $B\rightarrow C$ не равно α. Заметим, что импликация, как это легко видеть из (a) и (b), может принимать только значения α или β. Если $A \to B = \beta$, то

$$(A \to B) \to (A \to C) = \alpha$$

и вся формула I. 2 принимает значение α.

Остается рассмотреть случай, когда

$$B \to C = \beta.$$

Если при этом A принимает значение, отличное от β, то

$$A \to (B \to C) = \beta$$

и вся формула I. 2 примет значение α.

Если же $A = \beta$, то $A \to C = \alpha$ и формула I. 2 опять принимает значение α. Итак, I. 2 принимает значение α при любых значениях переменных.

Проверим аксиому II.1

$$A \& B \to A.$$

В случае, когда A или B принимает значение β,

$$A \& B = \beta,$$

и поэтому

$$A \& B \to A = \alpha.$$

Если же $A = \alpha$, то II. 1 также принимает значение α.

Если $B = \alpha$, то

$$A \& B = A, \quad A \& B \to A = A \to A = \alpha$$

и формула II. 1 опять принимает значение α. Если $A = B$, то II. 1 становится равной формуле

$$A \& A \to A.$$

Но в силу предпоследнего и первого из условий (а) имеем

$$A \& A \to A = \alpha.$$

Остается рассмотреть случай, когда A и B принимают значения δ и γ и при этом A не равно B.

Имея в виду коммутативность операции &, достаточно рассмотреть два случая:

$$\gamma \& \delta \to \gamma \quad \text{и} \quad \gamma \& \delta \to \delta.$$

Но $\gamma \& \delta = \delta$. Поэтому первое выражение равно

$$\delta \to \gamma,$$

а второе

$$\delta \to \delta.$$

В силу условий (а) и (b) оба эти выражения имеют значение α.

Рассмотрим еще аксиому IV. 1

$$(A \to B) \to (\bar{B} \to \bar{A}).$$

Импликация $A \to B$, как мы уже говорили выше, может принимать только значения α или β.

Если

$$A \to B = \beta,$$

то формула IV. 1 принимает значение α. Допустим, что

$$A \to B = \alpha.$$

Тогда возможны только следующие случаи:

1) $A = \beta$; 2) $B = \alpha$; 3) $A = B$; 4) $A = \delta$, $B = \gamma$.

Из (а) и (b) видно, что в каждом из этих случаев

$$\bar{B} \to \bar{A} = \alpha,$$

и, следовательно, формула IV. 1 принимает также значение α.

Перейдем к доказательству независимости аксиомы I. 2. Для этой цели мы выберем интерпретацию, в которой переменные принимают три значения: α, β, γ.

Операции определяются условиями (а) и дополнительными условиями:

$$\alpha \to \beta = \beta; \quad \alpha \to \gamma = \gamma; \quad \gamma \to \beta = \gamma; \quad \bar{\gamma} = \gamma. \tag{c}$$

Условиями (а) и (с) операции импликации и отрицания определены полностью.

Операции & и $\vee$ в этом случае полностью определены условиями (а). Рассмотрим, например, конъюнкцию $A \& B$. Если одна из переменных принимает значение α или β, то $A \& B$ определяется условиями (а). Если же обе переменные принимают значение γ, то $A \& B$ также равно γ.

При этой интерпретации аксиома I. 2

$$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$$

при некоторых значениях переменных принимает значение γ; остальные аксиомы принимают значение α при всех значениях переменных.

Покажем справедливость первого утверждения. Положим

$$A=\gamma, \quad B=\gamma, \quad C=\beta.$$

Получим

$$(\gamma \to (\gamma \to \beta)) \to ((\gamma \to \gamma) \to (\gamma \to \beta)) =$$
$$= (\gamma \to \gamma) \to (\alpha \to \gamma) = \alpha \to (\alpha \to \gamma) = \gamma.$$

Доказательство второго утверждения мы не будем проводить для всех остальных аксиом, но для примера проверим некоторые из них.

Рассмотрим аксиому I. 1

$$A \to (B \to A).$$

В случае, когда $A = B$, эта формула принимает значение α. В случае, когда $A = \alpha$, имеем $B \to A = \alpha$ и формула I. 1 принимает значение α. При $A = \beta$ также $A \to (B \to A) = \alpha$.

Остается рассмотреть случай $A = \gamma$. Тогда мы будем иметь

$$\gamma \to (B \to \gamma).$$

Но $B \to \gamma$ может принимать значения α или γ. В обоих случаях $\gamma \to (B \to \gamma) = \alpha$.

Рассмотрим аксиому III. 1

$$A \to A \vee B.$$

Если $A = \beta$, то эта формула принимает значение α.

Если $A = \alpha$, то $A \vee B = \alpha$ и формула III. 1 опять принимает значение α.

Допустим, что $A = \gamma$. Тогда будем иметь

$$\gamma \to \gamma \vee B.$$

Если $B = \alpha$ или $B = \gamma$, то последнее выражение равно α.

Если $B = \beta$, то $\gamma \vee B = \gamma$ и формула III. 1 принимает значение α.

Проверим еще аксиому IV. 1

$$(A \to B) \to (\overline{B} \to \overline{A}).$$

В случае, когда A и B равны α или β, формула IV. 1 принимает значение α, так как тогда имеют место законы алгебры высказываний.

Если $A = B$, то формула IV. 1 будет равна

$$\alpha \to \alpha = \alpha.$$

Допустим, что $A = \gamma$; получим

$$(\gamma \to B) \to (\bar{B} \to \bar{\gamma}).$$

Но $\bar{\gamma} = \gamma$; следовательно, последнее выражение равно

$$(\gamma \to B) \to (\bar{B} \to \gamma).$$

Если $B = \alpha$, то $\bar{B} = \beta$, $\bar{B} \to \gamma = \alpha$ и все выражение примет значение α.

Если $B = \beta$, то

$$(\gamma \to \beta) \to (\bar{\beta} \to \gamma) = (\gamma \to \beta) \to (\alpha \to \gamma) = \gamma \to \gamma = \alpha.$$

Если $B = \gamma$, а $A = \alpha$, то

$$(\alpha \to \gamma) \to (\bar{\gamma} \to \bar{\alpha}) = (\alpha \to \gamma) \to (\gamma \to \beta) = \gamma \to \gamma = \alpha.$$

Наконец, если $B = \gamma$, а $A = \beta$, то

$$(\beta \to \gamma) \to (\bar{\gamma} \to \bar{\beta}) = (\beta \to \gamma) \to (\gamma \to \alpha) = \alpha \to \alpha = \alpha.$$

Итак, формула IV. 1 принимает значение α при всех значениях переменных. Аналогично доказывается то же самое для всех остальных аксиом.

Таким образом, доказана независимость системы аксиом исчисления высказываний.

ЛОГИКА ПРЕДИКАТОВ

Мы видели выше, что можно дать два различных описания логики высказываний. В главе I мы дали ее содержательное описание, именуемое алгеброй высказываний, а в главе II изложили ее в виде аксиоматической системы.

Переходя к рассмотрению другой логической системы, которую мы будем называть логикой предикатов, опять сначала изложим ее содержательно, в духе алгебры высказываний. В главе IV мы изложим логику предикатов в виде аксиоматического исчисления.

Заметим, однако, что если для описания алгебры высказываний нам не потребовалось средств, выходящих за пределы конструктивных, то с логикой предикатов дело обстоит иначе. Чтобы изложить ее в содержательной форме, нам придется привлечь понятие актуальной бесконечности и принять, без всякого обоснования, способы проведения рассуждений, употребляемые в теории множеств. При таком изложении логики предикатов мы, конечно, не можем поставить задачи обоснования математики, так как то, что особенно нуждается в этом обосновании,— теорию множеств — мы принимаем за основу нашего изложения.

Содержательная трактовка логики предикатов обладает, однако, тем достоинством, что она очень облегчает изучение как исчисления предикатов, так и других абстрактных логических систем. Не являясь сама аксиоматической системой, она содержит богатые эвристические средства, позволяющие легко ориентироваться во многих вопросах, касающихся аксиоматических логических систем.

§ 1. Предикаты

Логика предикатов представляет собой развитие алгебры высказываний. Она содержит в себе всю алгебру высказываний, т. е. элементарные высказывания, рассматриваемые как величины, которые принимают два значения

И и *Л*, все операции алгебры высказываний и, следовательно, все ее формулы. Но, помимо этого, логика предикатов вводит в рассмотрение высказывания, отнесенные к предметам. В ней уже имеется расчленение высказывания на субъект и предикат.

Пусть $\mathfrak{M}$ — некоторое множество предметов и a, b, c, d — какие-то определенные предметы из этого множества. Тогда высказывания об этих предметах мы будем обозначать в виде

$$P(a), \quad Q(b), \quad R(c, d) \quad \text{и т. д.}$$

$P(a)$ обозначает высказывание о предмете a, $Q(b)$ — высказывание о предмете b, $R(c, d)$ — высказывание о предметах c и d и т. д. Пусть, например, $\mathfrak{M}$ представляет собой натуральный ряд чисел, а буквы a, b, c, d — соответственно числа 5, 8, 3, 1. Тогда $P(a)$ может быть, например, высказыванием: «5 есть простое число», $Q(b)$ — «8 есть нечетное число», $R(c, d)$ — «3 больше 1».

Такие высказывания могут быть как истинны, так и ложны. Как и в алгебре высказываний, мы будем рассматривать эти высказывания только с той точки зрения, что они представляют собой либо истину, либо ложь, обозначаемые соответственно символами *И* и *Л*. Но, в отличие от алгебры высказываний, здесь мы будем считать, что значения *И* и *Л* ставятся в соответствие определенным предметам или группам предметов. Так, в рассмотренных выше примерах $P(a)$ представляет собой *И*, поставленную в соответствие числу 5; $Q(b)$ — *Л*, поставленную в соответствие числу 8; $R(c, d)$ — *И*, поставленную в соответствие паре 3, 1.

Пусть $\mathfrak{M}$ — произвольное непустое множество, а x представляет собой произвольный предмет из этого множества. Тогда выражение $F(x)$ обозначает высказывание, которое становится определенным, когда x заменено определенным предметом из $\mathfrak{M}$. $F(a)$, $F(b)$, ... уже представляют собой вполне определенные высказывания. Например, если $\mathfrak{M}$ — натуральный ряд, то $F(x)$ может обозначать: «x есть простое число».

Это неопределенное высказывание становится определенным, если x заменить некоторым числом, например: «3 — простое число», «4 — простое число» и т. д.

Пусть $S(x, y)$ обозначает: «x меньше y».

Это высказывание становится определенным, если x и y заменить числами: «1 меньше 3», «5 меньше 2» и т. д.

Так как с нашей точки зрения каждое определенное высказывание представляет собой *И* или *Л*, то выражение $F(x)$ означает, что каждому предмету из $\mathfrak{M}$ поставлен в соответствие один из двух символов: *И* или *Л*. Иначе говоря, $F(x)$ представляет собой функцию, определенную на множестве $\mathfrak{M}$ и принимающую только два значения: *И* и *Л*. Таким же образом неопределенное высказывание о двух и более предметах $H(x, y)$, $G(x, y, z)$ и т. д. представляет собой функцию двух, трех и т. д. переменных. При этом переменные x, y, z пробегают множество $\mathfrak{M}$, а функция принимает значения *И* и *Л*. Эти неопределенные высказывания, или функции одной или нескольких переменных, мы будем называть *логическими функциями* или *предикатами*. Предикатом с одной переменной можно выразить *свойство* предмета, например: «x есть простое число», «x — прямоугольный треугольник» и т. д.

Понятие предиката в классической логике Аристотеля соответствует в нашей терминологии предикату с одной переменной. Понятие предиката, введенное нами, имеет более широкий объем. Предикатами мы называем также и логические функции нескольких переменных. Такими предикатами можно выразить *отношения* между предметами. Пусть, например, $\mathfrak{M}$ — множество действительных чисел, а переменные x, y, z, ... — предметы из $\mathfrak{M}$. Тогда можно посредством предикатов от двух и большего числа переменных выразить различные отношения между числами, как-то:

$$x < y, \quad x + y + z = 0$$

и другие, обозначив эти предикаты соответственно $A(x, y)$, $B(x, y, z)$ и т. д. Пусть $\mathfrak{M}$ — множество членов семьи. Тогда можно предикатами выразить родственные отношения, например: «быть отцом и сыном», «быть братом и сестрой» и т. д. Предикат $L(x, y)$ может обозначать «x — отец y», $M(x, y)$ — «x и y — братья» и т. д.

Мы увидим дальше, что введение в рассмотрение предикатов от нескольких переменных, способных выражать отношения между предметами, приносит существенно новое по сравнению с логикой предикатов от одной переменной. Оказывается, что во всех системах аксиом математических дисциплин существуют аксиомы, не выразимые посредством предикатов от одной переменной. Но с помощью предикатов от большего числа переменных все аксиомы этих систем могут быть выражены.

Все понятия, которые мы будем вводить, относятся всегда к некоторому произвольному множеству $\mathfrak{M}$, которое мы будем называть *предметной областью* или просто *областью*. Элементы этой области будем обозначать малыми латинскими буквами (иногда эти буквы мы будем снабжать индексами). Буквы конца латинского алфавита

$$x, \; y, \; z, \; u, \; v, \; x_1, \; x_2, \; \ldots$$

обозначают неопределенные элементы области. Их мы будем называть *предметными переменными*. Буквы начала алфавита

$$a, \; b, \; c, \; a_1, \; a_2, \; \ldots$$

обозначают определенные предметы области. Их мы будем называть *индивидуальными предметами* или *предметными постоянными*.

Большими латинскими буквами

$$A, \; B, \; \ldots, \; X, \; A_1, \; A_2, \; \ldots$$

мы будем, как и в алгебре высказываний, обозначать переменные, принимающие значения *И* и *Л*. Их мы назовем *переменными высказываниями*. Мы будем также рассматривать и постоянные высказывания. Их мы будем также обозначать большими латинскими буквами, как-нибудь отмеченными или просто с дополнительной оговоркой.

Выражения

$$F(x), \; G(x, y), \; P(x_1, \ldots, x_n), \; A(x, x), \; \ldots$$

обозначают предикаты, т. е. функции, аргументы которых принимают значения из области $\mathfrak{M}$, а сами функции могут принимать только два значения: *И* и *Л*. Если такое выражение ничем не отмечено и не сделано никакой оговорки, то оно означает переменный (т. е. произвольный) предикат на области $\mathfrak{M}$ от данного числа переменных. Определенный же предикат мы будем обозначать таким же символом с соответствующей оговоркой или какой-нибудь дополнительной отметкой. Впрочем, некоторые предикаты мы будем обозначать теми же символами, которые для них употребляются обычно.

Например, предикат «x меньше y» будем обозначать $x < y$, предикат «x равно y» будем обозначать $x = y$ и т. д.

Высказывания, выражаемые большими латинскими буквами, как переменные, так и постоянные, а также выражения

$$F(a),\ G(a,\ b),\ \ldots,$$

где F, G — предикаты, а a и b — индивидуальные предметы, мы будем называть *элементарными высказываниями.*

Большие латинские буквы и символы предикатов как от индивидуальных предметов, так и от предметных переменных мы будем называть элементарными формулами. Этот термин мы будем употреблять, чтобы отличить эти формулы от сложных, которые мы будем составлять из элементарных.

Символы предметов не являются формулами. Элементарные формулы, как высказывания, так и логические функции, всегда представляют собой величины, способные принимать только значения *И* и *Л*. Поэтому элементарные формулы можно связывать операциями алгебры высказываний:

$$\&,\ \vee,\ \rightarrow,\ \bar{}\ ,$$

сохраняя за этими операциями те определения, которые мы дали им в алгебре высказываний. Полученные таким образом формулы в свою очередь могут определять высказывания или предикаты. Например:

1) $A \vee F(x)$,
2) $A(x,\ y) \rightarrow (B \,\&\, \overline{A}(x,\ x))$,
3) $G(x,\ y) \rightarrow G(x,\ x)$,
4) $L(x) \sim L(y)$ и т. д.

Первая формула при фиксированных A и $F(x)$ определяет некоторый предикат. Четвертая формула при всяком L представляет собой предикат, зависящий от двух переменных x и y. Если x и y принимают одинаковые значения, то этот предикат принимает значение *И*.

§ 2. Кванторы

Кроме операций алгебры высказываний, мы будем употреблять еще две новые операции. Этих операций не было в алгебре высказываний, так как они связаны с особенностями логики предикатов. Операции эти выражают собой утверждения всеобщности и существования.

1. Квантор всеобщности. Пусть $R(x)$ — вполне определенный предикат, принимающий значение *И* или *Л* для каждого элемента x некоторой области $\mathfrak{M}$. Тогда под выражением

$$\forall x\, R(x)$$

мы будем подразумевать *высказывание истинное, когда $R(x)$ истинно для каждого элемента x области $\mathfrak{M}$, и ложное в противном случае.* Это высказывание уже не зависит от x. Соответствующее ему словесное выражение будет: «для всякого x $R(x)$ истинно».

Пусть теперь $\mathfrak{A}(x)$ — формула логики предикатов, принимающая определенное значение, если входящие в нее переменные предметы и переменные предикаты заменены вполне определенным образом. Формула $\mathfrak{A}(x)$ может содержать и другие переменные, кроме x. Тогда выражение $\mathfrak{A}(x)$ при замене всех переменных, как предметов, так и предикатов, кроме x, представляет собой конкретный предикат, зависящий только от x. А формула

$$\forall x\, \mathfrak{A}(x)$$

становится вполне определенным высказыванием. Следовательно, эта формула полностью определяется заданием значений всех переменных, кроме x, и, значит, от x не зависит. Символ $\forall x$ называется *квантором всеобщности.*

2. Квантор существования. Пусть $R(x)$ — некоторый предикат. Мы свяжем с ним формулу

$$\exists x\, R(x),$$

определив ее значение как *истину, если существует элемент области $\mathfrak{M}$, для которого $R(x)$ истинно, и как ложь в противном случае.* Тогда, если $\mathfrak{A}(x)$ — определенная формула логики предикатов, то формула

$$\exists x\, \mathfrak{A}(x)$$

также определена и от значения x не зависит. Знак $\exists x$ называется *квантором существования*.

Кванторы $\exists x$ и $\forall x$ называются *двойственными* друг другу.

Мы будем говорить, что в формулах

$$\forall x\, \mathfrak{A}(x) \quad \text{и} \quad \exists x\, \mathfrak{A}(x)$$

кванторы $\forall x$ и $\exists x$ относятся к переменной x или что *переменная x связана соответствующим квантором.*

Предметную переменную, не связанную никаким квантором, мы будем называть *свободной переменной*. Таким образом, мы описали все формулы логики предикатов.

Если две формулы $\mathfrak{A}$ и $\mathfrak{B}$, отнесенные к некоторой области $\mathfrak{M}$, при всех заменах переменных предикатов, переменных высказываний и свободных предметных переменных соответственно индивидуальными предикатами, определенными на $\mathfrak{M}$, индивидуальными высказываниями и индивидуальными предметами из $\mathfrak{M}$ принимают одинаковые значения И или Л, то мы будем говорить, что эти формулы равносильны на области $\mathfrak{M}$. (При заменах переменных предикатов, высказываний и предметов мы, конечно, те из них, которые в формулах $\mathfrak{A}$ и $\mathfrak{B}$ обозначены одинаковым образом, заменяем также одинаковым образом.)

Если две формулы равносильны на любых областях $\mathfrak{M}$, то мы будем их называть просто равносильными. Как и в алгебре высказываний, равносильные формулы могут быть заменены одна другой. Это позволяет в разных случаях приводить формулы к более удобному виду.

Очевидно, что все равносильности, имеющие место в алгебре высказываний, переносятся и на логику предикатов. В частности, имеет место

$$\mathfrak{A} \to \mathfrak{B} \text{ равносильно } \overline{\mathfrak{A}} \vee \mathfrak{B}.$$

Пользуясь этим, мы можем для любой формулы найти равносильную, в которой из операций алгебры высказываний имеются только &, $\vee$ и $^{-}$.

П р и м е р ы.

1. $\exists x(A(x) \to \forall y\, B(y))$ равносильна $\exists x\, (\overline{A}(x) \vee \forall y\, (B(y))$.

2. $\forall x\, A(x) \to (B(z) \to \forall x\, C(x))$ равносильна $\overline{\forall x\, A(x)} \vee \vee (\overline{B}(z) \vee \forall x\, C(x))$.

3. $(\exists x\, A(x) \to \forall y\, B(y)) \to C(z)$ равносильна

$$\overline{\exists x\, A(x) \to \forall y\, B(y)} \vee C(z).$$

Последняя равносильна

$$\overline{\overline{\exists x\, A(x)} \vee \forall y\, B(y)} \vee C(z).$$

Совершая преобразования алгебры высказываний, получим еще одну равносильную ей формулу:

$$\exists x\, A(x) \,\&\, \overline{\forall y\, B(y)} \vee C(z).$$

Кроме равносильностей алгебры высказываний, для логики предикатов имеются равносильности, связанные с кванторами.

Существуют знаки, связывающие кванторы со знаком отрицания. Рассмотрим выражение

$$\overline{\forall x\, \mathfrak{A}(x)}.$$

Высказывание «$\forall x\, \mathfrak{A}(x)$ ложно» равносильно высказыванию: «существует элемент y, для которого $\mathfrak{A}(y)$ ложно», или, что то же, «существует элемент y, для которого $\overline{\mathfrak{A}}(y)$ истинно». Следовательно, выражение $\overline{\forall x\, \mathfrak{A}(x)}$ равносильно выражению

$$\exists y\, \overline{\mathfrak{A}}(y).$$

Рассмотрим таким же образом выражение

$$\overline{\exists x\, \mathfrak{A}(x)}.$$

Это есть высказывание «$\exists x\, \mathfrak{A}(x)$ ложно». Но такое высказывание равносильно высказыванию: «для всех y высказывание $\mathfrak{A}(y)$ ложно» или «для всех y высказывание $\overline{\mathfrak{A}}(y)$ истинно». Итак, $\overline{\exists x\, \mathfrak{A}(x)}$ равносильно выражению

$$\forall y\, \overline{\mathfrak{A}}(y).$$

Мы получили, таким образом, следующее правило:

Знак отрицания можно ввести под знак квантора, заменив квантор на двойственный.

Мы уже видели, что для каждой формулы существует равносильная ей формула, которая из операций алгебры высказываний содержит только &, $\vee$ и $^{-}$.

Пользуясь последними равносильностями, связанными с кванторами, и законами алгебры высказываний, мы можем для каждой формулы найти равносильную, в которой знаки отрицания относятся только к элементарным высказываниям и элементарным предикатам. Доказательство этого утверждения мы здесь приводить не будем. Ограничимся только примером.

Рассмотрим формулу

$$\overline{\exists x\,(A\,(x) \rightarrow \forall y\,B\,(y))}.$$

Найдем для этой формулы равносильную ей формулу, в которой нет знака $\rightarrow$. Это будет

$$\overline{\exists x\,(\overline{A}\,(x) \vee \forall y\,B\,(y))}.$$

Применив рассмотренное выше правило к отрицанию над квантором $\exists x$, получим равносильную формулу:

$$\forall x\,\overline{(\overline{A}\,(x) \vee \forall y\,B\,(y))}.$$

Затем, совершая преобразования алгебры высказываний, получим

$$\forall x\,(A\,(x)\,\&\,\overline{\forall y\,B\,(y)}).$$

Применив опять правило внесения знака отрицания под знак квантора $\forall y$, получим окончательно

$$\forall x\,(A\,(x)\,\&\,\exists y\,\overline{B}\,(y)).$$

В этой формуле знак отрицания относится к элементарному предикату $B\,(y)$.

Формулы, в которых из операций алгебры высказываний имеются только операции &, $\vee$ и $^{-}$, а знаки отрицания относятся только к элементарным предикатам и высказываниям, будем называть приведенными формулами.

Из сказанного мы можем заключить, что *для каждой формулы существует равносильная ей приведенная формула.* Эту приведенную формулу мы будем называть *приведенной формой* данной формулы.

§ 3. Теоретико-множественный смысл предикатов

То обстоятельство, что две логические величины, будь то высказывания или предикаты, всегда принимают одинаковые значения *И* или *Л*, мы будем обозначать посредством знака $\equiv$. В настоящем параграфе мы рассмотрим некоторые множества, соответствующие логическим выражениям. Для обозначения равенства двух множеств мы будем употреблять знак $=$.

Пусть $\mathfrak{M}$ — некоторое множество, на котором определяются предикаты. Такое множество мы называем *областью*. Каждому предикату одной переменной $F(x)$ можно поставить в соответствие множество тех элементов a из области $\mathfrak{M}$, для которых $F(a)$ истинно. Обозначим это множество E_F. Обратно, каждому множеству E, содержащемуся в $\mathfrak{M}$, можно поставить в соответствие предикат $P(x)$, представляющий собой высказывание, истинное тогда и только тогда, когда $x \in E$. Предикат $P(x)$ принимает значение *И* на E и *Л* вне E. Следовательно, E есть E_P. Это соответствие между подмножествами $\mathfrak{M}$ и предикатами от одной переменной, определенными на ней, взаимно однозначно. В дальнейшем, если не оговорено противное, мы будем предполагать, что область $\mathfrak{M}$ непуста.

Как известно, теоретико-множественной суммой $E_1 \cup E_2$ двух множеств E_1 и E_2 называется множество, состоящее из всех элементов множества E_1 и всех элементов множества E_2. Теоретико-множественным произведением или пересечением $E_1 \cap E_2$ двух множеств E_1 и E_2 называется множество всех элементов, принадлежащих и множеству E_1 и множеству E_2. Аналогично определяются теоретико-множественная сумма и теоретико-множественное произведение любого конечного или бесконечного числа множеств.

Пусть

$$P(x) \equiv P_1(x) \vee P_2(x).$$

Тогда

$$E_P = E_{P_1} \cup E_{P_2},$$

т. е. E_P является теоретико-множественной суммой множеств E_{P_1} и E_{P_2}. В самом деле, если $x \in E_P$, то $P(x)$ истинно; значит, $P_1(x)$ или $P_2(x)$ истинно. В первом случае $x \in E_{P_1}$, во втором $x \in E_{P_2}$, следовательно,

$$x \in E_{P_1} \cup E_{P_2}.$$

Обратно, пусть $x \in E_{P_1} \cup E_{P_2}$. Тогда $x \in E_{P_1}$ или $x \in E_{P_2}$, т. е. $P_1(x)$ истинно или $P_2(x)$ истинно. Следовательно, $P(x)$ истинно и $x \in E_P$.

Аналогичным образом можно показать, что если

$$P(x) \equiv P_1(x) \,\&\, P_2(x),$$

то

$$E_P = E_{P_1} \cap E_{P_2},$$

где $E_{P_1} \cap E_{P_2}$ — теоретико-множественное произведение.

Множество, отвечающее предикату $\bar{P}(x)$, является дополнением к множеству, отвечающему предикату $P(x)$. В теоретико-множественных символах можно написать, что

$$E_{\bar{P}} = \boldsymbol{C}E_P,$$

где $\boldsymbol{C}E_P$ — совокупность элементов области $\mathfrak{M}$, не принадлежащих к E_P, или, как говорят, *дополнение* к множеству E_P.

Формулы алгебры высказываний, выражаемые большими латинскими буквами, присутствующие в логике предикатов, можно трактовать как предикаты, сохраняющие для всех предметов одно и то же значение *И* или *Л*. Таким предикатам мы должны в силу нашего условия поставить в соответствие в первом случае всю область $\mathfrak{M}$, во втором — пустое множество.

Логические законы, справедливые для величин алгебры высказываний, остаются справедливыми и для логических функций, так как значениями этих функций являются те же величины. В силу соответствия между логическими функциями и множествами законам логики предикатов соответствуют известные законы для теоретико-множественных операций.

Например, двум законам дистрибутивности для логических операций соответствуют законы дистрибутивности для теоретико-множественного сложения и умножения. Первому закону дистрибутивности

$$F(x)\,[G(x) \vee H(x)] \equiv F(x)\,G(x) \vee F(x)\,H(x)$$

соответствует теоретико-множественный закон

$$P \cap (Q \cup S) = P \cap Q \cup P \cap S,$$

где P, Q, S — произвольные множества.

Второму закону дистрибутивности

$$F(x) \vee G(x) H(x) \equiv (F(x) \vee G(x)) (F(x) \vee H(x))$$

соответствует теоретико-множественный закон

$$P \cup Q \cap S = (P \cup Q) \cap (P \cup S).$$

Мы установили связь между множествами и предикатами от одной переменной. Аналогичным образом это можно сделать и для логических функций большего числа переменных. Рассмотрим только случай функций двух переменных. Пусть $\mathfrak{M}^2$ — множество всех пар (x, y) множества $\mathfrak{M}$. При этом мы считаем, что пары различаются не только составом элементов, но и порядком.

Функции $P(x, y)$ поставим в соответствие множество тех пар (x, y), принадлежащих $\mathfrak{M}^2$, для которых $P(x, y)$ истинно; обозначим это множество по-прежнему E_P. Связь между функциями $P(x, y)$ и подмножествами множества $\mathfrak{M}^2$ такая же, как для случая функций одной переменной и подмножеств $\mathfrak{M}$.

Рассмотрим теперь теоретико-множественный смысл кванторов. Пусть

$$F(x) \equiv \exists y P(x, y).$$

Множество E_F, соответствующее предикату F, состоит из тех и только тех элементов области $\mathfrak{M}$, для которых истинно $F(x)$, т. е. $\exists y\ P(x, y)$. Но последнее выражение истинно для данного x_0, если существует такое y, что $P(x_0, y)$ истинно. Функции $P(x, y)$ отвечает часть E_P множества $\mathfrak{M}^2$. Итак, E_F состоит из всех трех элементов x области $\mathfrak{M}$, для каждого из которых найдется пара (x, y), принадлежащая E_P. Назовем x_0 проекцией любой пары (x_0, y), а проекцией множества — совокупность проекций принадлежащих ему пар. Легко видеть, что E_F есть *проекция* E_P. Пусть $\mathfrak{M}$ — множество действительных чисел. В соответствии с аналитической геометрией будем рассматривать $\mathfrak{M}^2$ как плоскость, точки которой имеют координаты x, y, а $\mathfrak{M}$ — как ось OX этой плоскости. В этом случае точка x является проекцией точки

(x, y) в буквальном геометрическом смысле. Поэтому множество E_F, отвечающее логической функции $F(x)$, равной $\exists y\; P(x, y)$, совпадает с обычной ортогональной проекцией множества E_P на ось OX. Обозначив проекцию произвольного множества H на $\mathfrak{M}$ символом $\text{пр}_x H$, мы можем записать, что

$$E_F = \text{пр}_x\, E_P.$$

Чтобы установить теоретико-множественный смысл квантора всеобщности, применим закон действия отрицания на квантор. Пусть

$$F(x) \equiv \forall y\, P(x, y).$$

Тогда

$$\forall y\, P(x, y) \equiv \overline{\exists y\, \overline{P}(x, y)}.$$

Операции отрицания, как известно, соответствует теоретико-множественная операция дополнения. Итак,

$$E_F = \boldsymbol{C}\, \text{пр}_x\, \boldsymbol{C} E_P,$$

т. е. множество, отвечающее функции $\forall y\, P(x, y)$, есть дополнение к проекции на $\mathfrak{M}$ дополнения к E_P.

Справедливо и обратное положение: всякое множество R, являющееся проекцией на $\mathfrak{M}$ множества D, содержащегося в $\mathfrak{M}^2$:

$$R = \text{пр}_x\, D,$$

может быть представлено как E_F, где $F(x)$ есть $\exists y\, P(x, y)$, причем $D = E_P$. Действительно, множеству R отвечает предикат $F(x)$, определенный на $\mathfrak{M}$, а множеству D — предикат $P(x, y)$, определенный на $\mathfrak{M}^2$, и, очевидно,

$$F(x) \equiv \exists y\, P(x, y).$$

Если же R' — дополнение к проекции D, то R' соответствует, очевидно, предикату $\forall y\, \overline{P}(x, y)$. В самом деле, предикату $\forall y\, \overline{P}(x, y)$ соответствует множество $\boldsymbol{C}\, \text{пр}_x\, \boldsymbol{C} E_{\overline{P}}$, но $\boldsymbol{C} E_{\overline{P}} = E_P = D$ и, следовательно,

$$\boldsymbol{C}\, \text{пр}_x\, \boldsymbol{C} E_{\overline{P}} = \boldsymbol{C}\, \text{пр}_x\, D.$$

Итак, кванторы связаны с геометрической операцией проектирования и, обратно, проектирование имеет указанный логический смысл.

§ 4. Аксиомы

Рассмотрим индивидуальные предикаты, которые мы обозначим $S(x)$ и $x = y$. Первый представляет собой функцию, принимающую значение *И* для всякого элемента области, а второй принимает значение *И*, когда x и y представляют собой один и тот же элемент, и *Л*, когда x и y различны. Предикат $S(x)$ может быть явно определен посредством формулы логики предикатов, например, в виде

$$F(x) \vee \overline{F}(x),$$

где $F(x)$ — произвольный предикат на той же области. В самом деле, это выражение имеет значение *И* для всякого x. Предикат $x = y$ нельзя представить непосредственно в виде формулы логики предикатов. Но посредством таких формул можно высказать условия, которые однозначно определяют этот предикат.

Допустим, что нам неизвестно, какой именно предикат изображается символом $x = y$. Напишем две формулы:

1. $x = x$,
2. $x = y \rightarrow (A(x) \rightarrow A(y))$,

и потребуем, чтобы для предиката $x = y$ эти формулы были истинны при всяком предикате A и для всех x и y. Легко видеть, что при этих условиях предикат $x = y$ может быть только предикатом тождества. В самом деле, если x и y заменены одним и тем же предметом, то предикат $x = y$ принимает значение *И* в силу формулы 1. Допустим, что x и y заменены различными предметами a и b. Заменим предикат $A(t)$ предикатом, принимающим значение *И*, если t есть a, и значение *Л*, если t не совпадает с a. Обозначим этот предикат через $A'(t)$. Формула

$$A'(a) \rightarrow A'(b)$$

имеет значение *Л*, так как $A'(a)$ есть *И*, а $A'(b)$ есть *Л*. Но формула

$$a = b \rightarrow (A'(a) \rightarrow A'(b))$$

должна быть истинна. Поэтому формула $a = b$ ложна. Итак, мы показали, что предикат $x = y$, удовлетворяющий нашим условиям, может быть только предикатом тождества.

Аналогичным образом можно характеризовать и другие индивидуальные предикаты. Часто такая характеристика не определяет однозначно характеризуемый предикат, но выделяет некоторый класс предикатов. Но и в этом случае мы будем называть символ характеризуемого предиката индивидуальным предикатом.

В некоторых случаях формулы характеризуют не только индивидуальный предикат, но и саму область. Это бывает тогда, когда не для всякой области существует индивидуальный предикат, удовлетворяющий этим формулам. Наконец, формулы могут вовсе не содержать индивидуальных предикатов; тогда они характеризуют только область. Например, формула

$$A(x) \to A(y),$$

где A — переменный предикат, характеризует области, состоящие из одного элемента. В самом деле, если область $\mathfrak{M}$ содержит только один предмет a, то при любой замене x и y предметами области мы получим формулу

$$A(a) \to A(a),$$

которая всегда истинна. Наоборот, если область содержит более одного предмета, то можно подобрать такой предикат, для которого наша формула ложна

Пример. Напишем формулы, характеризующие предикат, который мы обозначим $x < y$:

1. $\overline{x < x}$,
2. $x < y \to (y < z \to x < z)$.

Предикат, изображаемый символом $x < y$, должен быть таков, чтобы формулы 1 и 2 были для него истинны при всех значениях входящих свободных переменных x, y и z, или, иначе говоря, предикат $x < y$ должен удовлетворять условиям 1 и 2. Нетрудно указать пример такой области и такого предиката, для которых наши формулы истинны. Рассмотрим область из трех предметов a, b, c. Определим предикат для этой области следующим образом.

Пусть $a < b$ имеет значение *И*, $b < c$ — значение *И*, $a < c$ — значение *И*. При всех остальных заменах x и y

предикат имеет значение *Л*. Тогда формулы 1 и 2 для данной области выполнены, в чем легко убедиться непосредственной проверкой, осуществимой благодаря конечности области.

В теории множеств всякое отношение $x < y$, удовлетворяющее формулам 1 и 2, называется *отношением порядка*. Для элементов, находящихся в отношении порядка $x < y$, иногда употребляют выражение «x предшествует y». Мы также будем пользоваться этим термином. Говорят, что множество *упорядочено отношением* $x < y$, если это отношение, кроме формул 1 и 2, удовлетворяет еще одной формуле:

3. $\overline{x = y} \to (x < y \vee y < x)$.

Если понимать предикат $x = y$ содержательно, то для описания упорядоченного множества достаточно формул 1, 2 и 3. Иначе необходимо присоединить к формулам 1, 2 и 3 еще формулы, характеризующие равенство.

Введем еще одно понятие из теории множеств, которое мы используем в дальнейшем. *Упорядоченное множество называется вполне упорядоченным, если каждая его непустая часть содержит элемент, предшествующий всем другим элементам этой части.* В теории множеств доказывается «теорема Цермело»: *всякое множество может быть вполне упорядочено некоторым отношением порядка.* Отсюда следует, что для каждой области существует предикат, удовлетворяющий аксиомам 1, 2 и 3.

Формулы, характеризующие индивидуальные предикаты, область или то и другое, будем называть аксиомами. Здесь однако, нужно ввести точное определение.

Пусть $\mathfrak{A}_1, \mathfrak{A}_2, \ldots. \mathfrak{A}_n$ — формулы логики предикатов, содержащие символы предикатов $P_1, P_2, \ldots, P_k$ и $A_1, A_2, \ldots, A_s$ и символы индивидуальных предметов $a_1, a_2, \ldots, a_p$ и предметных переменных $x_1, x_2, \ldots, x_q$. *Если существуют такие предметы $a_1^0, \ldots, a_p^0$ области $\mathfrak{M}$ и такие предикаты $P_1^0, \ldots, P_k^0$, определенные на $\mathfrak{M}$, что после замены ими $a_1, \ldots, a_p$ и $P_1, \ldots, P_k$ во всех формулах $\mathfrak{A}$ эти формулы будут истинны при всех значениях свободных предметных переменных $x_1, \ldots, x_q$ из области $\mathfrak{M}$ и всевозможных заменах символов $A_1, \ldots$ $\ldots, A_s$ высказываниями или предикатами, определенными на области $\mathfrak{M}$, то мы скажем, что область $\mathfrak{M}$ и си-*

стема предикатов $P_1^0, \ldots, P_k^0$ *удовлетворяют системе аксиом* $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$.

Символы $P_1, P_2, \ldots, P_k$ в этих аксиомах мы будем называть *символами индивидуальных* (или *постоянных*) *предикатов*, а символы $A_1, A_2, \ldots, A_s$ — *символами переменных предикатов*.

Если какая-либо аксиома $\mathfrak{A}(x, y, \ldots)$ содержит свободные переменные $x, y, \ldots$, то ее можно заменить другой аксиомой:

$$\forall x \forall y \ldots \mathfrak{A}(x, y, \ldots).$$

При этом область $\mathfrak{M}$ и совокупность индивидуальных предикатов P_i^0, удовлетворяющих первоначальной системе аксиом, удовлетворяют и новой системе, так как если предикаты $P_1^0, \ldots, P_k^0$ удовлетворяют системе аксиом, то эти аксиомы должны быть истинны при всех значениях свободных переменных.

Область $\mathfrak{M}$ *с предикатами* $P_1^0, \ldots, P_k^0$, *удовлетворяющая системе аксиом* $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, *называется интерпретацией этой системы аксиом.*

§ 5. Непротиворечивость и независимость аксиом

Систему аксиом, для которой существует интерпретация, мы будем называть интерпретируемой или содержательно непротиворечивой. Систему аксиом, не допускающую никакой интерпретации, будем называть неинтерпретируемой или содержательно противоречивой. Определение содержательной непротиворечивости, или интерпретируемости, предполагает, что существует область предметов, из которых можно составлять множества (области) и определять на них предикаты так, чтобы с помощью этих множеств и предикатов мы могли находить интерпретации для исследуемых нами систем аксиом.

Круг предметов, употребляемый в математике для указанных целей, как мы уже говорили во введении, может представлять собой натуральный ряд чисел и все, что можно из него образовать путем общих теоретико-множественных построений, в частности рациональные числа, действительные числа, комплексные числа, различного рода функции и другие объекты.

Возможно и другое понимание непротиворечивости. *Будем считать систему аксиом непротиворечивой, если, получая из нее какие угодно логические следствия, мы никогда не придем к противоречию в том смысле, что никогда не выведем одновременно истинность и ложность одного и того же утверждения.*

Чтобы иметь возможность рассуждать о непротиворечивости в последнем смысле, необходимо иметь описание тех логических средств, которые мы употребляем для вывода следствий из аксиом. Описание логических выводов мы дадим в следующей главе; оно совершается посредством построения абстрактной логической системы. После этого определение непротиворечивости во втором смысле будет вполне точным. Чтобы различать введенные здесь различные понятия непротиворечивости, будем для непротиворечивости во втором смысле употреблять термин «*внутренняя непротиворечивость*». Примером внутренне непротиворечивой логической системы является рассмотренное в предыдущей главе исчисление высказываний. Не имея пока возможности рассуждать о введенных понятиях достаточно строго и точно, мы все же можем до некоторой степени сравнить эти определения непротиворечивости. Если считать, что область теоретико-множественных понятий, из которой мы черпаем интерпретации для систем аксиом, сама является внутренне непротиворечивой, то представляется ясным, что каждая интерпретируемая система аксиом также внутренне непротиворечива.

Таким образом, наличие интерпретации системы аксиом сводит вопрос о непротиворечивости этой системы к непротиворечивости используемой для интерпретации системы понятий. Если мы уверены, что эта система понятий внутренне непротиворечива, то факт наличия интерпретации устанавливает внутреннюю непротиворечивость исследуемой системы аксиом. Обратный вопрос: будет ли внутренне непротиворечивая система также интерпретируема — совсем не так ясен, и для его решения, по существу, необходимо иметь аксиоматическое описание средств вывода логических следствий из аксиом. Здесь мы не будем останавливаться на этом вопросе.

Рассмотрим произвольную систему аксиом

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n. \qquad (1)$$

Аксиома $\mathfrak{A}_i$ *называется независимой от остальных аксиом этой системы, если существует область* $\mathfrak{M}$ *с предикатами* F_j, *удовлетворяющая системе аксиом*

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_{i-1}, \mathfrak{A}_{i+1}, \ldots, \mathfrak{A}_n,$$

но не удовлетворяющая рассматриваемой системе (1).

Термин *независимость одной аксиомы от остальных*, так же как и *непротиворечивость*, употребляется еще в другом смысле. Будем говорить, что аксиома $\mathfrak{A}_i$ *внутренне независима от остальных аксиом, если она не может быть выведена из остальных аксиом.*

Как и в случае непротиворечивости, понятие внутренней независимости будет только тогда точным, когда мы дадим описание средств логического вывода следствий из аксиом. Используя и здесь нестрогие рассуждения, мы можем сравнить два определения независимости.

Допустим, что аксиома $\mathfrak{A}_i$ независима от остальных в первом смысле. В таком случае для системы аксиом

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_{i-1}, \mathfrak{A}_{i+1}, \ldots, \mathfrak{A}_n \tag{2}$$

существует интерпретация, которая не удовлетворяет системе из всех аксиом вместе с аксиомой $\mathfrak{A}_i$. В таком случае формула $\mathfrak{A}_i$ не может быть логически выведена из остальных аксиом. Если бы она была выводима из остальных аксиом, то этот вывод был бы справедлив и для любой интерпретации; для любой области с любыми предикатами из истинности аксиом $\mathfrak{A}_1, \ldots, \mathfrak{A}_{i-1}$, $\mathfrak{A}_{i+1}, \ldots, \mathfrak{A}_n$ вытекала бы и истинность аксиомы $\mathfrak{A}_i$. Но по предположению существует интерпретация, в которой аксиомы (2) истинны, а аксиома $\mathfrak{A}_i$ нет. Отсюда мы можем заключить, что если какая-либо аксиома независима от остальных в первом смысле, то она должна быть независима и во втором смысле.

Обратный вопрос: будет ли аксиома, внутренне независимая от остальных аксиом, также независимой в первом смысле — мы здесь не будем рассматривать.

Если аксиома не является независимой от остальных аксиом системы, то мы будем называть ее *зависимой* от них. Нам полезно, однако, иметь прямое определение зависимой аксиомы.

Аксиома $\mathfrak{A}_i$ *зависима от остальных аксиом*

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_{i-1}, \mathfrak{A}_{i+1}, \ldots, \mathfrak{A}_n,$$

если любая интерпретация этой системы удовлетворяет также и системе с аксиомой $\mathfrak{A}_i$.

Понятия непротиворечивости и независимости системы аксиом имеют большое значение для математики. Если мы пользуемся какой-то системой аксиом, то уверенность в ее внутренней непротиворечивости совершенно необходима, так как в противоречивой системе, как мы уже говорили раньше, нет отличия истины от лжи. В ней можно доказывать истинность произвольных утверждений.

Внутренняя независимость бывает нужна (об этом мы также раньше говорили) для того, чтобы в системе не было лишних аксиом. Эту независимость, как мы уже видели, также можно устанавливать посредством интерпретации. С вопросом независимости аксиом была связана хорошо известная история проблемы о пятом постулате Евклида, или «аксиоме о параллельных». После многочисленных неудачных попыток доказать этот постулат, т. е. вывести его из других принципов геометрии, Лобачевский высказал мысль о невыводимости этого постулата из других аксиом геометрии и дал этому предположению убедительное обоснование. В его исследованиях уже заключались элементы метода интерпретации, и впоследствии невыводимость пятого постулата на этом пути и была окончательно установлена. Была построена такая система объектов, которая удовлетворяет всем аксиомам геометрии, кроме аксиомы о параллельных, и не удовлетворяет этой последней. Метод интерпретации, однако, приложим к вопросам непротиворечивости и независимости только в известных границах. Другие методы уже связаны с рассмотрением абстрактных логических систем. В этой главе мы их затрагивать не будем.

§ 6. Взаимно однозначное соответствие областей

Введем одно понятие из теории множеств, которое нам в дальнейшем будет необходимо.

Рассмотрим два множества $\mathfrak{M}$ и $\mathfrak{M}'$.

Говорят, что между элементами этих множеств установлено взаимно однозначное соответствие, если каждому элементу множества $\mathfrak{M}$ некоторым способом поставлен в соответствие элемент множества $\mathfrak{M}'$, причем каждому элементу $\mathfrak{M}$ соответствует один и только один элемент из $\mathfrak{M}'$ и, обратно, каждому элементу из $\mathfrak{M}'$ соответствует один и только один элемент из $\mathfrak{M}$. Взаимно однозначное соответствие между элементами рассматриваемых множеств будем записывать в виде

$$x - x'.$$

Предположим, что между элементами двух множеств $\mathfrak{M}$ и $\mathfrak{M}'$ установлено взаимно однозначное соответствие. Пусть $F(x_1, \ldots, x_n)$ — произвольный предикат от n переменных, определенный на $\mathfrak{M}$. Определим на $\mathfrak{M}'$ предикат $F'(x'_1, \ldots, x'_n)$ следующим образом. Пусть a'_1, $a'_2, \ldots, a'_n$ — произвольная совокупность значений переменных $x'_1, \ldots, x'_n$. Каждому a'_i соответствует определенный элемент множества $\mathfrak{M}$, который мы обозначим a_i. Предикат $F(x_1, \ldots, x_n)$ определен для всех значений переменных, поэтому $F(a_1, \ldots, a_n)$ имеет вполне определенное значение *И* или *Л*. Это же значение мы дадим предикату $F'(x'_1, \ldots, x'_n)$, когда x'_1 есть $a'_1, \ldots, x'_n$ есть a'_n. Иными словами, $F'(x'_1, \ldots, x'_n)$ определим так, чтобы $F(a_1, \ldots, a_n)$ и $F'(a'_1, \ldots, a'_n)$ были одновременно истинны или ложны.

Таким образом, предикат $F'(x'_1, \ldots, x'_n)$ определен на области $\mathfrak{M}'$. Этот предикат мы поставим в соответствие предикату $F(x_1, \ldots, x_n)$. Из нашего определения следует, что и, обратно, любому предикату на $\mathfrak{M}'$ соответствует единственный предикат, определенный на $\mathfrak{M}$. Взаимная однозначность последнего соответствия очевидна, так как если два предиката, определенные на $\mathfrak{M}$ — $F_1(x_1, \ldots, x_n)$ и $F_2(x_1, \ldots, x_n)$, — различны, то найдется такая совокупность значений переменных $a_1, \ldots$ $\ldots, a_n$, для которой один из предикатов принимает значение *И*, а другой — значение *Л*. Пусть, например, $F_1(a_1, \ldots, a_n)$ имеет значение *И*, а $F_2(a_1, \ldots, a_n)$ — значение *Л*. Тогда, если F'_1 и F'_2 — предикаты, определенные на $\mathfrak{M}'$, соответствующие F_1 и F_2, то $F'_1(a'_1, \ldots, a'_n)$ имеет значение *И*, а $F'_2(a'_1, \ldots, a'_n)$ имеет значение *Л*. Поэтому предикаты F'_1 и F'_2 также различны.

Установленное соответствие между предикатами

$$F - F'$$

предполагает определенное соответствие между значениями предметных переменных:

$$x_1 - x_1',\ x_2 - x_2',\ \ldots,\ x_n - x_n'. \tag{1}$$

Если

$$F - F', \tag{2}$$

то с учетом соответствия (1) истинно соотношение

$$F(x_1, \ldots, x_n) \equiv F'(x_1', \ldots, x_n').$$

В силу взаимной однзначности соответствия (2) имеет место и обратное: если с учетом соответствия (1) имеем

$$F(x_1, \ldots, x_n) \equiv F'(x_1', \ldots, x_n'),$$

то

$$F - F'.$$

Пусть из некоторых индивидуальных предикатов, определенных на области $\mathfrak{M}$, образована какая-то формула $\mathfrak{A}$. При всякой замене свободных предметных переменных объектами из области $\mathfrak{M}$ эта формула принимает определенное значение *И* или *Л*. Если все предикаты, входящие в $\mathfrak{A}$, мы заменим соответствующими предикатами, определенными на $\mathfrak{M}'$, то получим формулу $\mathfrak{A}'$, отнесенную к области $\mathfrak{M}'$. Нетрудно видеть, что при соответствующих значениях переменных

$$\mathfrak{A}' \equiv \mathfrak{A}. \tag{3}$$

Если формула составлена только с помощью операций алгебры высказываний, то после замены предикатов на $\mathfrak{M}$ соответствующими предикатами на $\mathfrak{M}'$, а значений предметных переменных из $\mathfrak{M}$ соответствующими значениями из $\mathfrak{M}'$ значения предикатов, стоящих в формуле, не изменятся. Ясно, что операции алгебры высказываний после такой замены дадут тот же результат, что и до замены. Далее, легко видеть, что если формула $\mathfrak{A}(x_1, \ldots, x_n)$ при указанных заменах переходит в $\mathfrak{A}'(x_1', \ldots, x_n')$, причем

$$\mathfrak{A}(x_1, \ldots, x_n) \equiv \mathfrak{A}'(x_1', \ldots, x_n'),$$

то

$$\forall x_i \mathfrak{A}(x_1, \ldots, x_n) \equiv \forall x'_i \mathfrak{A}'(x'_1, \ldots, x'_n),$$

$$\exists x_i \mathfrak{A}(x_1, \ldots, x_n) \equiv \exists x'_i \mathfrak{A}'(x'_1, \ldots, x'_n).$$

Следовательно, как операции алгебры высказываний, так и операции связывания квантором, производимые над формулами, обладающими указанным свойством, приводят к формулам, обладающим тем же свойством. Из сказанного следует, что каждая формула, составленная из предикатов, определенных на области $\mathfrak{M}$, также обладает этим свойством, т. е. для нее имеет место соотношение (3).

§ 7. Изоморфизм областей и полнота систем аксиом

Рассмотрим некоторую область $\mathfrak{M}$ и систему предикатов

$$\begin{gathered} F_1(x_1, \ldots, x_{n_1}), \\ F_2(x_1, \ldots, x_{n_2}), \\ \cdots\cdots\cdots \\ F_k(x_1, \ldots, x_{n_k}), \end{gathered}$$

определенных на этой области, и другую область $\mathfrak{M}'$ с предикатами

$$\begin{gathered} F'_1(x'_1, \ldots, x'_{n_1}), \\ F'_2(x'_2, \ldots, x'_{n_2}), \\ \cdots\cdots\cdots \\ F'_k(x'_1, \ldots, x'_{n_k}). \end{gathered}$$

Мы скажем, что область $\mathfrak{M}$ с предикатами F_i изоморфна области $\mathfrak{M}'$ с предикатами F'_i, если между элементами $\mathfrak{M}$ и $\mathfrak{M}'$ можно установить такое взаимно однозначное соответствие

$$x - x',$$

что

$$F'_i(x'_1, \ldots, x'_n)$$

имеет то же значение (И или Л), что и

$$F_i(x_1, \ldots, x_n),$$

если x'_1 *соответствует* x_1, x'_2 *соответствует* x_2, ..., x'_n *соответствует* x_n.

Соответствие между элементами множеств $\mathfrak{M}$ и $\mathfrak{M}'$ мы будем называть *изоморфизмом, сохраняющим предикаты*

$$F_1(\ldots),\ F_2(\ldots),\ \ldots,\ F_n(\ldots).$$

Пример. Пусть область $\mathfrak{M}$ представляет собой совокупность натуральных чисел

$$1,\ 2,\ 3,\ 4,\ 5,$$

и пусть на этой области определен один предикат $F(x, y)$, который можно словами выразить так: разность чисел x и y делится на три, или, следуя терминологии теории чисел, «x сравнимо с y по модулю три». Записывается это выражение следующим образом:

$$x \equiv y \pmod 3.$$

Говоря точнее, $F(x, y)$ принимает значение *И*, если x сравнимо с y по модулю три, и значение *Л* в противном случае.

Область $\mathfrak{M}'$ будет совокупностью чисел

$$21,\ 22,\ 23,\ 24,\ 25.$$

Предикат $F'(x', y')$ для $\mathfrak{M}'$ определяется так же, как и для $\mathfrak{M}$: $F'(x', y')$ истинно тогда и только тогда, когда

$$x' \equiv y' \pmod 3.$$

Легко видеть, что область $\mathfrak{M}$ с предикатом $F(x, y)$ изоморфна области $\mathfrak{M}'$ с предикатом $F'(x', y')$.

Установим между $\mathfrak{M}$ и $\mathfrak{M}'$ следующее взаимно однозначное соответствие:

$$\begin{gathered} 1-21, \\ 2-22, \\ \cdot\ \cdot\ \cdot\ \cdot \\ 5-25. \end{gathered}$$

Разности между элементами области $\mathfrak{M}$ и между соответствующими элементами области $\mathfrak{M}'$ равны, поэтому, если $x \equiv y \pmod 3$, то и $x' \equiv y' \pmod 3$, и обратно.

Легко видеть, что если область $\mathfrak{M}$ с предикатами $F_1, \ldots, F_k$ изоморфна области $\mathfrak{M}'$ с предикатами $F'_1, \ldots, F'_k$, а область $\mathfrak{M}'$ в свою очередь изоморфна области $\mathfrak{M}''$ с предикатами $F''_1, \ldots, F''_k$, то области $\mathfrak{M}$ и $\mathfrak{M}''$ также изоморфны. Иначе говоря, *отношение изоморфизма областей транзитивно.*

Рассмотрим произвольную систему аксиом, которая содержит индивидуальные предикаты

$$F_1,\ F_2,\ \ldots,\ F_k$$

и только их. (Это условие не касается переменных предикатов; они могут входить в аксиомы как угодно.) Допустим, что область $\mathfrak{M}$ с предикатами

$$F_1^0,\ F_2^0,\ \ldots,\ F_k^0$$

удовлетворяет нашей системе аксиом. Пусть $\mathfrak{M}'$ — произвольная область с предикатами

$$F'_1,\ F'_2,\ \ldots,\ F'_k,$$

изоморфная области $\mathfrak{M}$. Ясно, что область $\mathfrak{M}'$ с предикатами F'_i также удовлетворяет той же системе аксиом. Иными словами, *если две области с некоторыми индивидуальными предикатами изоморфны и если одна из них вместе со своими предикатами удовлетворяет некоторой системе аксиом, то и другая область удовлетворяет той же системе аксиом.*

Возникает обратный вопрос: если две области с некоторыми предикатами удовлетворяют одной и той же системе аксиом, будут ли они изоморфны? Нетрудно убедиться, что ответ на этот вопрос отрицателен.

Рассмотренная выше система аксиом порядка:

1. $\overline{x < x}$,
2. $x < y \rightarrow (y < z \rightarrow x < z)$

представляет собой пример системы аксиом, для которой существуют не изоморфные между собой интерпретации. В самом деле, этой системе аксиом с предикатом $x < y$ удовлетворяет область $\mathfrak{M}$ из двух элементов a и b, если положить, что $a < b$ истинно, а $a < a$, $b < b$ и $b < a$ ложны. Вместе с тем той же системе аксиом удовлетворяет область $\mathfrak{M}'$ из трех элементов a, b, c, если предикат $x < y$ определить для этой области так, как это сделано в § 4. Но область $\mathfrak{M}$ не может быть изоморфна области $\mathfrak{M}'$, потому что области эти состоят из различного числа элементов.

Всякая система аксиом, для которой все интерпретации изоморфны, называется полной системой.

Теорема. *Пусть система аксиом*

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k, \mathfrak{A}_{k+1}$$

имеет некоторую интерпретацию и аксиомы

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k \tag{1}$$

образуют полную систему аксиом. Если при этом аксиома $\mathfrak{A}_{k+1}$ не содержит индивидуальных предикатов, отличных от тех, которые встречаются в (1), *то аксиома $\mathfrak{A}_{k+1}$ зависима от аксиом* (1).

Пусть в систему аксиом (1) входят индивидуальные предикаты

$$F_1, F_2, \ldots, F_p.$$

По условию аксиома $\mathfrak{A}_{k+1}$ иных индивидуальных предикатов не содержит.

Мы уже указывали, что если система аксиом удовлетворяется какой-либо областью с индивидуальными предикатами, то она удовлетворяется и всякой другой областью с индивидуальными предикатами, изоморфной первой области. Отсюда следует, что если система аксиом не удовлетворяется какой-либо областью с предикатами, то она не удовлетворяется и никакой другой областью с предикатами, изоморфной первой.

По условию теоремы существует какая-то интерпретация системы аксиом

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k, \mathfrak{A}_{k+1}. \tag{2}$$

Эта интерпретация представляет собой некоторую область $\mathfrak{M}'$ с предикатами $F'_1, \ldots, F'_p$, которыми заменяются в аксиомах предикаты $F_1, \ldots, F_p$. Эта область, очевидно, удовлетворяет и системе (1). В силу полноты системы (1) все ее интерпретации изоморфны. И так как эта система содержит те же индивидуальные предикаты, что и система (2), то всякая интерпретация системы (1) изоморфна данной интерпретации системы (2). Из свойств изоморфизма следует, что тогда произвольная интерпретация системы (1) удовлетворяет и системе (2). Итак, каждая интерпретация системы (1) является также интерпретацией системы (2). Значит, аксиома $\mathfrak{A}_{k+1}$ зависима от системы аксиом (1), что и требовалось доказать.

Конечно, для каждой непротиворечивой системы аксиом можно указать независимые от нее аксиомы. Можно взять, например, формулу

$$\forall x\, F^*(x),$$

где $F^*(x)$ — индивидуальный предикат, не содержащийся в данной системе аксиом, и присоединить ее к системе в качестве новой аксиомы. Если наша исходная система интерпретируется на области $\mathfrak{M}$ с предикатами

$$F_1, \ldots, F_p,$$

то, определив на этой области $F^*(x)$ так, чтобы формула $\forall x F^*(x)$ была ложной, мы можем заключить, что область с предикатами

$$F_1, \ldots, F_p, F^*$$

удовлетворяет исходной системе аксиом, но не удовлетворяет системе, полученной из нее присоединением аксиомы $\forall x\, F^*(x)$. Впрочем, вполне понятно, что аксиома, являющаяся не тавтологическим высказыванием о некоторых свойствах и отношениях вещей, не может зависеть от тех аксиом, в которых об этих свойствах и отношениях ничего не говорится.

Ранее нам уже приходилось употреблять термин «полнота системы аксиом» в другом смысле. В дальнейшем мы также будем употреблять этот термин в двух смыслах. Чтобы различать эти понятия, когда придется говорить о них в одном контексте, мы будем полноту, определенную в этом параграфе, называть *полнотой с точностью до изоморфизма* или *содержательной полнотой*, имея в виду, что здесь идет речь об изоморфизме, сохраняющем те индивидуальные предикаты, которые описываются рассматриваемой системой аксиом.

§ 8. Аксиомы натурального ряда

В целях краткости предикат

$$x < y \vee x = y$$

мы будем записывать в виде

$$x \leqslant y.$$

Предикат, имеющий вид

$$x < y \mathbin{\&} \forall u\,[u \leqslant x \lor y \leqslant u],$$

мы обозначим $\sigma(x, y)$. Смысл предиката $\sigma(x, y)$ можно выразить словами: «y непосредственно следует за x», так как истинность $\sigma(x, y)$ равносильна утверждению, что y следует за x и между ними никакого предмета не имеется.

Символ 0 означает индвидуальный предмет области.

Аксиомы

I

1. $x = x$.
2. $x = y \to (A(x) \to A(y))$.

II

1. $\overline{x < x}$.
2. $x < y \to (y < z \to x < z)$.
3. $\forall x\, \exists y\, [\sigma(x, y) \mathbin{\&} \forall u\, (\sigma(x, u) \to u = y)]$.

III

$$A(0) \mathbin{\&} \forall x\, \forall y\, [A(x) \mathbin{\&} \sigma(x, y) \to A(y)] \to A(z).$$

Как видно из этих аксиом, характеризуемая ими область содержит индивидуальный предмет 0.

Аксиомы I определяют предикат равенства. Две первые аксиомы второй группы определяют предикат предшествования $<$.

Аксиома II. 3 выражает утверждение, что для каждого предмета области существует единственный непосредственно за ним следующий предмет.

Аксиома III представляет собой аксиому полной индукции. Она состоит в утверждении: «*если предложение верно для предмета* 0 *и из того, что оно верно для* x, *следует, что оно верно для непосредственно следующего предмета области, то это предложение верно для произвольного* z».

Заметим, что предикат $x = y$ во всех интерпретациях не может быть не чем иным, как тождеством объектов x и y, так как только этот предикат и может удовлетворять аксиомам I—III. Нетрудно убедиться, что натуральный ряд

$$0,\ 1,\ 2,\ \ldots,\ n,\ \ldots$$

(мы здесь и в дальнейшем будем считать 0 натуральным числом), в котором предикат $x < y$ означает, что «натуральное число x меньше натурального числа y» в обычном смысле слова, удовлетворяет аксиомам I, II, III. Таким образом, эта система аксиом содержательно непротиворечива.

Введем одно понятие из теории множеств. Рассмотрим два упорядоченных множества $\mathfrak{M}_1$ и $\mathfrak{M}_2$, на каждом из которых определен предикат, представляющий отношение порядка (в первом $x_1 < y_1$, во втором $x_2 < y_2$). Мы будем говорить, что *два упорядоченных множества подобны, если между ними можно установить взаимно однозначное соответствие*

$$x_1 — x_2,$$

сохраняющее порядковые отношения между элементами, т. е. всякий раз, когда $x_1 < y_1$ истинно, то $x_2 < y_2$ для соответствующих элементов также истинно. В таком случае в силу упорядоченности рассматриваемых множеств, если $x_1 < y_1$ ложно, то для соответствующих элементов $x_2 < y_2$ также ложно. В самом деле, если $x_1 < y_1$ ложно, то или $x_1 = y_1$, или $y_1 < x_1$ истинно. В первом случае $x_2 = y_2$, так как наше соответствие взаимно однозначно, и, значит, $x_2 < y_2$ ложно. Во втором случае $y_2 < x_2$ истинно. Но тогда $x_2 < y_2$ ложно, так как иначе мы бы пришли к противоречию с аксиомами порядка.

Мы можем, таким образом, высказать следующее положение: *упорядоченные множества подобны тогда и только тогда, когда они вместе со своими предикатами порядка изоморфны.*

Натуральный ряд есть упорядоченное множество и удовлетворяет аксиомам I, II, III. Во все эти аксиомы входят только два индивидуальных предиката—предикат равенства и предикат порядка. Предикат равенства сохраняется при всяком взаимно однозначном соответствии. Так как при подобии сохраняется и предикат порядка, то отсюда следует, что *всякое подобное и, следовательно, изоморфное натуральному ряду множество удовлетворяет системе аксиом* I, II, III.

Докажем обратное: *всякое множество с определенным на нем предикатом порядка, удовлетворяющее аксиомам* I, II, III, *подобно натуральному ряду.*

В самом деле, пусть область $\mathfrak{M}$ удовлетворяет аксиомам I, II, III. Рассмотрим, с другой стороны, натуральный ряд

$$0,\ 1,\ 2,\ \ldots,\ n,\ \ldots,$$

в котором отношением порядка является отношение «n меньше m» в обычном смысле этого слова. Натуральному числу 0 поставим в соответствие элемент из области $\mathfrak{M}$, обозначенный тем же символом. Обозначим этот элемент еще через x_0. Единице поставим в соответствие элемент, непосредственно следующий за x_0; обозначим его через x_1. Если числу n мы поставили в соответствие элемент x_n, то числу $n+1$ поставим в соответствие элемент области $\mathfrak{M}$, непосредственно следующий за x_n. В силу аксиомы II. 3 такой элемент существует, и притом только один. Обозначим его x_{n+1}. Таким образом, мы каждому натуральному числу n поставим в соответствие элемент x_n области $\mathfrak{M}$. Имеем, очевидно,

$$x_0 < x_1,\ x_1 < x_2,\ \ldots,\ x_n < x_{n+1},\ \ldots$$

Из этих соотношений следует, что

$$\text{если } n < m, \text{ то } x_n < x_m.$$

Отсюда следует, что множество элементов $x_0, x_1, \ldots$ $\ldots, x_n, \ldots$, которое мы обозначим $\mathfrak{M}'$, упорядочено и подобно натуральному ряду.

Покажем, что это множество представляет собой всю область $\mathfrak{M}$, т. е. $\mathfrak{M}'$ совпадает с $\mathfrak{M}$.

Справедливость этого утверждения мы докажем, применив аксиому полной индукции, которой удовлетворяет область $\mathfrak{M}$. Выскажем положение: «элемент z из области $\mathfrak{M}$ принадлежит множеству $\mathfrak{M}'$». Это положение справедливо, если этот элемент есть x_0 (или 0). Если это положение верно для некоторого элемента x, то оно верно и для непосредственно следующего элемента. В самом деле, пусть x — какой-то элемент x_n; тогда x_{n+1} — элемент, непосредственно следующий за x_n. На основании аксиомы II. 3 для каждого элемента x_n существует единственный элемент, непосредственно за ним следующий. В таком случае элемент x_{n+1}, непосредственно следующий за элементом x_n, также принадлежит $\mathfrak{M}'$. На основании аксиомы полной индукции мы можем теперь заключить, что всякий элемент области $\mathfrak{M}$ есть также элемент области $\mathfrak{M}'$, т. е. $\mathfrak{M}$ и $\mathfrak{M}'$ совпадают.

Итак, мы доказали, что всякая область, удовлетворяющая аксиомам I, II, III, упорядочена и подобна натуральному ряду. Мы можем формулировать полученный результат следующим образом: *всякая интерпретация аксиом* I, II, III *изоморфна натуральному ряду*. Отсюда следует, что любые две интерпретации аксиом I, II, III изоморфны. Это значит, что *рассматриваемая система аксиом является полной*. Вместе с тем надо сказать, что аксиомы I, II, III не описывают всех свойств натурального ряда. В них, например, не содержатся арифметические действия сложения и умножения. Аксиомы I, II и III определяют только порядковые отношения натурального ряда, и полнота этой системы аксиом в некотором смысле ограничена. Ее, как мы согласились выше, можно назвать полнотой с точностью до изоморфизма, сохраняющего порядковые отношения.

Можно доказать, что каждая из аксиом рассматриваемой системы независима от остальных. Мы здесь ограничимся доказательством независимости аксиомы полной индукции. Для этого надо найти интерпретацию, удовлетворяющую системе аксиом I и II и не удовлетворяющую системе из всех аксиом.

Пусть область $\mathfrak{M}$ представляет собой совокупность рациональных чисел, имеющих вид $\frac{i}{i+1}$ и $1+\frac{i}{i+1}$, где i принимает все возможные значения из натурального ряда. Таким образом, рассматриваемая совокупность состоит из следующих чисел:

$$0,\ \frac{1}{2},\ \frac{2}{3},\ \ldots,\ \frac{i}{i+1},\ \ldots,\ 1,\ 1\frac{1}{2},\ 1\frac{2}{3},\ \ldots,\ 1+\frac{i}{i+1},\ \ldots$$

Пусть индивидуальный объект, обозначенный в системе символом «0», для данной области является рациональным числом 0, а предикат $x < y$ означает: «рациональное число x меньше рационального числа y» в обычном смысле этого слова.

Нетрудно убедиться, что рассматриваемая интерпретация удовлетворяет системе аксиом I и II.

В самом деле, для предиката, являющегося тождеством объектов, аксиомы I истинны при всякой замене переменного предиката A. Аксиомы II.1 и II.2 также истинны, так как предикат «число x меньше числа y» им удовлетворяет.

Рассмотрим аксиому II.3. В этой аксиоме утверждается, что для каждого объекта существует единственный объект, непосредственно за ним следующий. Но для числа вида $\frac{i}{i+1}$ число $\frac{i+1}{i+2}$ является непосредственно следующим, так как $\frac{i}{i+1} < \frac{i+1}{i+2}$ и в нашей области $\mathfrak{M}$ не существует числа, заключенного между $\frac{i}{i+1}$ и $\frac{i+1}{i+2}$. Кроме того, $\frac{i+1}{i+2}$ является единственным числом, непосредственно следующим за $\frac{i}{i+1}$, так как всякое число, большее $\frac{i}{i+1}$ и не совпадающее с $\frac{i+1}{i+2}$, больше $\frac{i+1}{i+2}$ и потому не может быть непосредственно следующим за $\frac{i}{i+1}$. Точно так же устанавливается, что для числа $1+\frac{i}{i+1}$ число $1+\frac{i+1}{i+2}$ является единственным непосредственно за ним следующим. Таким образом, область $\mathfrak{M}$ с предикатом $x < y$ удовлетворяет системе аксиом I и II.

Покажем, что при некоторых заменах предиката A и предметной переменной z аксиома III является ложной в нашей интерпретации. Выберем для замены предиката A предикат $A^0(x)$, имеющий значение *И* для чисел вида $\frac{i}{i+1}$ и *Л* для чисел вида $1+\frac{i}{i+1}$. В таком случае $A^0(0)$ истинно.

$$A^0(x) \,\&\, \sigma(x, y) \to A^0(y) \qquad (1)$$

также истинно для всяких x и y из нашей области. В самом деле, если $A^0(x)$ или $\sigma(x, y)$ ложны, то формула (1) истинна, так как посылка ложна. Допустим, что $A^0(x)$ и $\sigma(x, y)$ истинны. Тогда x — число вида $\frac{i}{i+1}$, а y — непосредственно за ним следующее число. Но тогда y — число $\frac{i+1}{i+2}$, являющееся числом того же самого вида. Поэтому $A^0\left(\frac{i+1}{i+2}\right)$ также истинно, и, следовательно, $A^0(y)$ истинно. В таком случае формула (1) опять истинна. Итак, формула (1) истинна для каждого x и каждого y из области $\mathfrak{M}$. Следовательно, формула

$$\forall x \, \forall y \, (A^0(x) \,\&\, \sigma(x, y) \to A^0(y))$$

также истинна, и, значит, формула

$$A^0(0) \,\&\, \forall x \, \forall y \, (A^0(x) \,\&\, \sigma(x, y) \to A^0(y))$$

истинна для области $\mathfrak{M}$. Но если z — число вида $1 + \frac{i}{i+1}$, то $A^0(z)$ ложно; поэтому формула

$$A^0(0) \,\&\, \forall x \, \forall y \, (A^0(x) \,\&\, \sigma(x, y) \to A^0(y)) \to A^0(z)$$

ложна, если z — число вида $1 + \frac{i}{i+1}$.

Мы видим, что аксиома III при некоторой замене переменного предиката A и предметной переменной z ложна, и поэтому область $\mathfrak{M}$ не удовлетворяет системе аксиом I, II и III.

По определению независимости аксиом мы заключаем, что аксиома III независима от остальных аксиом рассматриваемой системы.

§ 9. Нормальные формулы и нормальные формы

Как мы уже видели (см. § 2), для каждой формулы существует равносильная ей приведенная формула. Среди приведенных формул мы выделим некоторый класс формул, которые будем называть *нормальными.*

Приведенная формула называется нормальной, если она не содержит кванторов или если при образовании ее из элементарных формул операции связывания *кванторов следуют за всеми операциями алгебры высказываний.*

В записи нормальной формулы кванторы, если они есть, предшествуют всем остальным логическим символам. Например, приведенная формула

$$\forall x_1 \forall x_2 \exists x_3 \forall x_4 \mathfrak{A}(x_1, \ldots, x_4)$$

нормальна, если $\mathfrak{A}(x_1, \ldots, x_4)$ не содержит кванторов.

Теорема. *Для каждой формулы существует равносильная ей нормальная формула.*

Для доказательства этой теоремы нам будут нужны равносильности **1**—**4**, которые мы докажем сначала. В них предполагается, что формула H не содержит свободной переменной x.

1. $\forall x \mathfrak{A}(x) \vee H$ равносильно $\forall x (\mathfrak{A}(x) \vee H)$.

Пусть, в самом деле, формула $\forall x \mathfrak{A}(x) \vee H$ истинна для некоторой области $\mathfrak{M}$ и при некоторых фиксированных заменах свободных переменных как предметных, так и предикатных. Тогда либо $\forall x \mathfrak{A}(x)$ истинно при этих заменах, либо H истинно. В первом случае $\mathfrak{A}(x)$ истинно для каждого x, принадлежащего $\mathfrak{M}$. Но тогда

$$\mathfrak{A}(x) \vee H \tag{1}$$

также истинно для всякого x из $\mathfrak{M}$ и, следовательно, истинна формула

$$\forall x [\mathfrak{A}(x) \vee H]. \tag{2}$$

Во втором случае, если истинно H, то формулы (1) и (2) также истинны на $\mathfrak{M}$ при данных заменах свободных переменных.

Пусть формула $\forall x \mathfrak{A}(x) \vee H$ при данных заменах ложна. Тогда $\forall x \mathfrak{A}(x)$ ложно и H ложно. Следовательно, существует такой элемент x_0 области $\mathfrak{M}$, что $\mathfrak{A}(x_0)$ ложно. Но для этого элемента $\mathfrak{A}(x_0) \vee H$ ложно, следовательно, формула (5) ложна.

2. Формула $\forall x \mathfrak{A}(x) \& H$ равносильна $\forall x [\mathfrak{A}(x) \& H]$.

3. Формула $\exists x \mathfrak{A}(x) \& H$ равносильна $\exists x [\mathfrak{A}(x) \& H]$.

4. Формула $\exists x \mathfrak{A}(x) \vee H$ равносильна $\exists x [\mathfrak{A}(x) \vee H]$.

Равносильности **2**, **3** и **4** доказываются так же, как и **1**. Очевидно, верны также соответствующие утверждения для случая, когда квантором связано второе слагаемое (множитель).

Случай, когда формула содержит константы, охватывается рассмотренными случаями, так как константы a, b, c, входящие в формулы $\mathfrak{A}$ и H, можно рассматривать как результаты замены свободных переменных y, z, t элементами a, b, c.

Мы докажем теорему по индукции, следуя закону построения формул логики предикатов. Для элементарных формул, представляющих собой либо буквы A, B, ..., либо элементарные предикаты $A(x)$, $B(x, y)$, ..., наше утверждение истинно, так как эти формулы сами нормальны. Пусть для формул $\mathfrak{A}_1$ и $\mathfrak{A}_2$ имеются нормальные формы соответственно $\mathfrak{A}_1^*$ и $\mathfrak{A}_2^*$. Пусть, например, $\mathfrak{A}_1^*$ имеет вид

$$\forall x_1 \forall x_2 \ldots \exists x_i \ldots \exists x_n \mathfrak{B}_1(x_1, \ldots, x_n),$$

а $\mathfrak{A}_2^*$ имеет вид

$$\exists y_1 \forall y_2 \ldots \forall y_m \mathfrak{B}_2(y_1, \ldots, y_m).$$

Так как при переименовании связанной переменной формула переходит в равносильную, то мы можем считать, что переменные x_i не входят в формулу $\mathfrak{A}_2^*$, а y_i не входят в $\mathfrak{A}_1^*$.

Докажем, что для формулы $\mathfrak{A}_1 \vee \mathfrak{A}_2$ также существует равносильная ей нормальная формула. Формула $\mathfrak{A}_1^* \vee \mathfrak{A}_2^*$ равносильна формуле $\mathfrak{A}_1 \vee \mathfrak{A}_2$, но она, вообще говоря, еще не представляет собой нормальную формулу. Однако, пользуясь доказанными выше равносильностями, можно преобразовать ее в нормальную формулу.

Во-первых, формулу $\mathfrak{A}_1^* \vee \mathfrak{A}_2^*$ можно заменить формулой

$$\forall x_1 [\forall x_2 \ldots \exists x_n \mathfrak{B}_1(x_1, \ldots, x_n) \vee \\ \vee \exists y_1 \forall y_2 \ldots \forall y_m \mathfrak{B}_2(y_1, \ldots, y_m)],$$

внеся $\mathfrak{A}_2^*$ под знак первого квантора формулы $\mathfrak{A}_1^*$. В силу **1** эта формула равносильна формуле $\mathfrak{A}_1^* \vee \mathfrak{A}_2^*$. Далее можно производить равносильные преобразования под знаком квантора $\forall x_1$, так как в результате связывания квантором по одной и той же переменной x_1

двух равносильных формул мы получим также две равносильные формулы. На том же основании формулу $\mathfrak{A}_2^*$ можно ввести под знак второго квантора $\forall x_2$ и т. д. Допустим, что формула $\mathfrak{A}_2^*$ уже введена под знаки всех кванторов формулы $\mathfrak{A}_1^*$. Тогда получим формулу

$$\forall x_1 \forall x_2 \ldots \exists x_n [\mathfrak{B}_1(x_1, \ldots, x_n) \vee \\ \vee \exists y_1 \forall y_2 \ldots \forall y_m \mathfrak{B}_2(y_1, \ldots, y_m)].$$

Таким же образом можно слагаемое $\mathfrak{B}_1(x_1, \ldots, x_n)$ ввести последовательно под все кванторы формулы $\mathfrak{A}_2^*$. После этого мы получим нормальную формулу

$$\forall x_1 \forall x_2 \ldots \exists x_n \exists y_1 \forall y_2 \ldots \forall y_m [\mathfrak{B}_1(x_1, \ldots, x_n) \vee \\ \vee \mathfrak{B}_2(y_1, \ldots, y_m)],$$

равносильную формуле $\mathfrak{A}_1 \vee \mathfrak{A}_2$.

Аналогичным образом при помощи равносильностей **3** и **4** можно построить нормальную формулу, равносильную формуле $\mathfrak{A}_1 \mathbin{\&} \mathfrak{A}_2$, если известны нормальные формулы $\mathfrak{A}_1^*$ и $\mathfrak{A}_2^*$, равносильные соответственно $\mathfrak{A}_1$ и $\mathfrak{A}_2$.

Пусть $\mathfrak{A}^*$ — нормальная формула, равносильная формуле $\mathfrak{A}$, и пусть $\mathfrak{A}^*$ имеет, например, вид

$$\forall x_1 \exists x_2 \forall x_3 \ldots \forall x_n H(x_1, \ldots, x_n).$$

Формула $\overline{\mathfrak{A}^*}$ равносильна формуле $\overline{\mathfrak{A}}$. Но формула $\overline{\mathfrak{A}^*}$ в свою очередь равносильна формуле

$$\exists x_1 \forall x_2 \exists x_3 \ldots \exists x_n \overline{H}(x_1, \ldots, x_n),$$

которая является нормальной формулой. Итак, зная нормальную формулу, равносильную $\mathfrak{A}$, мы можем построить нормальную формулу, равносильную $\overline{\mathfrak{A}}$.

Формула $\forall x \mathfrak{A}^*(x)$, очевидно, равносильна формуле $\forall x \mathfrak{A}(x)$, а формула $\exists x \mathfrak{A}^*(x)$ равносильна формуле $\exists x \mathfrak{A}(x)$. Но формулы $\forall x \mathfrak{A}^*(x)$ и $\exists x \mathfrak{A}^*(x)$ — нормальные формулы.

Итак, для элементарных формул существуют равносильные нормальные формулы; если формула $\mathfrak{A}$ получена с помощью операций &, $\vee$, $^{-}$ и связывания квантором из формул, для которых существуют равносильные нормальные формулы, то и для $\mathfrak{A}$ существует равносильная нормальная формула.

Но так как каждая формула алгебры предикатов получается из элементарных формул с помощью указанных операций, то для каждой формулы алгебры предикатов существует равносильная ей нормальная формула, что и требовалось доказать.

Нормальную формулу, равносильную формуле $\mathfrak{A}$, мы будем называть *нормальной формой формулы* $\mathfrak{A}$.

§ 10. Проблема разрешения

Эту проблему мы будем ставить для формул исчисления предикатов, *лишенных символов постоянных предметов* и *символов индивидуальных предикатов.* В последующем изложении этой главы мы будем предполагать, что рассматриваемые формулы таковы (если не сделано специальных оговорок).

Каждая такая формула представляет собой определенное утверждение, истинное или ложное, когда оно относится к определенной области $\mathfrak{M}$, и предикаты, в нее входящие, заменены индивидуальными предикатами, определенными на $\mathfrak{M}$.

Если такая формула истинна для некоторой области $\mathfrak{M}$ *и некоторых предикатов, на ней определенных, мы будем называть ее выполнимой.*

Если формула истинна для данной области $\mathfrak{M}$ *и для всех предикатов, определенных на* $\mathfrak{M}$, *мы будем называть ее тождественно истинной для области* $\mathfrak{M}$.

Если формула истинна для всякой области $\mathfrak{M}$ *и для всяких предикатов, будем называть ее тождественно истинной или просто истинной.*

Формула называется ложной или невыполнимой, если ни для какой области ни при каких заменах предикатов она не является истинной. Легко показать, что если формула $\mathfrak{A}$ тождественно истинна, то формула $\overline{\mathfrak{A}}$ ложна, и наоборот.

Постановка проблемы разрешения для логики предикатов аналогична постановке этой проблемы для алгебры высказываний. Она ставится следующим образом: *указать единый эффективный способ (алгоритм) для определения по произвольной формуле, выполнима она или нет.*

Умея решать вопрос о выполнимости, мы тем самым сможем решать и вопрос об истинности любой формулы. В самом деле, если формула $\mathfrak{A}$ истинна, то формула $\overline{\mathfrak{A}}$ невыполнима, и обратно. Поэтому, проверив выполнимость или невыполнимость $\mathfrak{A}$ и $\overline{\mathfrak{A}}$, мы тем самым проверим истинность $\mathfrak{A}$. Проблема разрешения для логики предикатов является обобщением проблемы разрешения для исчисления высказываний, так как все формулы исчисления высказываний входят в число формул логики предикатов. Однако в то время как решение проблемы разрешения для исчисления высказываний никаких трудностей не представляет, проблема разрешения для логики предикатов оказалась связанной с серьезными трудностями.

Современные исследования пролили свет на природу этих затруднений. После того как в 30-х годах XX века в математической логике было дано точное определение понятия алгоритма, появилась возможность доказать, что проблема разрешения для логики предикатов неразрешима, т. е. искомый в этой проблеме алгоритм невозможен. Это впервые было доказано А. Чёрчем (см. также § 15 главы V).

Для некоторых частных типов формул, однако, проблема разрешения решается. Мы рассмотрим наиболее важный тип формул, для которых решение проблемы разрешения может быть осуществлено.

§ 11. Логика предикатов с одной переменной

Мы будем рассматривать формулы логики предикатов, содержащие предикаты, которые зависят только от одной переменной. Логика, в которой употребляются только такие выражения, соответствует той, которая описана Аристотелем и вошла как традиционный элемент в систему гуманитарного образования. Известные формы высказываний этой логики и формы умозаключений, так называемые «модусы силлогизмов», выражаются полностью в символике логики предикатов от одной переменной.

Теорема. *Если формула логики предикатов, содержащая только предикаты от одной переменной, выпол-*

нима на некоторой области $\mathfrak{M}$, то она выполнима на области $\mathfrak{M}'$, содержащей не более 2^n элементов, где n — число предикатов, входящих в рассматриваемую формулу.

Пусть формула $\mathfrak{A}(A_1, \ldots, A_n)$, содержащая только символы предикатов $A_1, \ldots, A_n$, каждый из которых зависит от одной переменной, выполнима на некоторой области $\mathfrak{M}$. Эту формулу мы можем предполагать представленной в нормальной форме, а все предметные переменные в ней связанными. В самом деле, какова бы ни была формула $\mathfrak{A}$, мы можем, произведя над ней преобразования, указанные в § 9, привести ее к виду, в котором все кванторы предшествуют остальным символам формулы, при этом состав ее предикатов и предметных переменных не изменяется. Если в $\mathfrak{A}$ есть свободные предметные переменные, то мы можем связать их квантором всеобщности.

Итак, допустим, что $\mathfrak{A}$ — нормальная формула. Тогда мы можем представить ее следующим образом:

$$\mathrm{Q}x_1 \mathrm{Q}x_2 \ldots \mathrm{Q}x_p \mathfrak{B}(A_1, \ldots, A_n, x_1, \ldots, x_p),$$

где каждый из символов $\mathrm{Q}x_i$ обозначает квантор $\forall x$ или $\exists x_i$, а формула

$$\mathfrak{B}(A_1, \ldots, A_n, x_1, \ldots, x_p)$$

кванторов не содержит.

В формуле $\mathfrak{B}(A_1, \ldots, A_n, x_1 \ldots, x_p)$ все переменные $x_1, \ldots, x_p$ входят в предикаты $A_1, \ldots, A_n$, и ее можно записать в виде

$$\mathfrak{B}(A_1(x_{i_1}), \ldots, A_n(x_{i_n})),$$

где $i_1, \ldots, i_n$ — числа от 1 до p. Нам будет, однако, удобнее пользоваться выражением

$$\mathfrak{B}(A_1, \ldots, A_n, x_1, \ldots, x_p),$$

если иметь в виду, что $\mathfrak{B}$ является логической функцией предикатов A_k, а каждый предикат A_k зависит от какой-то одной переменной x_{i_k}.

Покажем, что если для некоторой области $\mathfrak{M}$ существуют индивидуальные предикаты

$$A_1^0, \ldots, A_n^0,$$

для которых формула $\mathfrak{A}(A_1^0, \ldots, A_n^0)$ истинна, то эта формула истинна и на некотором подмножестве этой области, содержащем не более 2^n элементов. Этим теорема будет доказана. Можно предполагать, что область $\mathfrak{M}$ содержит более 2^n элементов, так как иначе наше утверждение тривиально. Разобьем элементы множества $\mathfrak{M}$ на классы следующим образом. Для каждой последовательности, содержащей n символов *И* и *Л* в произвольном порядке (*И*, *Л*, *Л*, ..., *И*), существует часть (может быть, пустая) множества $\mathfrak{M}$, содержащая те и только те элементы x, для которых последовательность значений предикатов $A_1^0(x)$, $A_2^0(x)$, ..., $A_n^0(x)$ совпадает с данной последовательностью символов *И* и *Л*.

Обозначим через

$$\delta_1, \delta_2, \ldots, \delta_n$$

последовательность символов *И* и *Л*, где δ_i представляют собой *И* или *Л*, а соответствующий этой последовательности класс элементов x обозначим

$$\alpha_{\delta_1, \delta_2, \ldots, \delta_n}.$$

Некоторые из этих классов могут оказаться пусты, так как может случиться, что для некоторой последовательности $\delta_1, \ldots, \delta_n$ не существует такого элемента, для которого предикаты $A_1^0, \ldots, A_n^0$ принимают соответствующие значения $\delta_1, \ldots, \delta_n$. Вместе с тем каждый элемент множества $\mathfrak{M}$ принадлежит одному из классов α и различные классы общих элементов не имеют. Число всех классов (пустых и непустых) равно числу последовательностей $\delta_1, \ldots, \delta_n$, т. е. 2^n. Следовательно, число q непустых классов α не превышает 2^n. Выберем из каждого непустого класса по одному элементу и обозначим эти элементы

$$a_1, a_2, \ldots, a_q.$$

Множество всех этих элементов обозначим $\mathfrak{M}'$. Докажем, что если формула $\mathfrak{A}(A_1^0, \ldots, A_n^0)$ истинна на области $\mathfrak{M}$, то она истинна и на области $\mathfrak{M}'$ (так как $\mathfrak{M}'$ — часть области $\mathfrak{M}$, то предикаты A_i^0 определены на $\mathfrak{M}'$). Каждому элементу x области $\mathfrak{M}$ поставим в соответствие элемент из $\mathfrak{M}'$, принадлежащий тому же классу, что и x. В $\mathfrak{M}'$ существует один и только один такой элемент. Элемент из $\mathfrak{M}'$, поставленный в соответствие x, обозначим $\varphi(x)$. Можно сказать, что мы построили функцию, определенную на множестве $\mathfrak{M}$ и принимающую значения из множества $\mathfrak{M}'$.

Легко видеть, что имеет место следующая равносильность:

$$A_i^0(x) \sim A_i^0(\varphi(x)).$$

Действительно, $\varphi(x)$ принадлежит тому же классу α, что и x. Но, по определению для элементов одного и того же класса каждый предикат A_i^0 принимает одно и то же значение. Отсюда следует, что если в формуле $\mathfrak{A}(A_1^0, \ldots, A_n^0)$ для каждой предметной переменной t заменить каждое выражение $A_i^0(t)$ через $A_i^0(\varphi(t))$, то формула $\mathfrak{A}(A_1^0, \ldots, A_n^0)$ перейдет в формулу $\mathfrak{A}'(A_1^0, \ldots, A_n^0)$. равносильную первой. Написание формулы $\mathfrak{A}'$ отличается от $\mathfrak{A}$ только тем, что все предметные переменные $x, y, z, \ldots, u$ формулы $\mathfrak{A}$ заменены соответственно на $\varphi(x), \varphi(y), \ldots, \varphi(u)$. Это следует из того, что по условию формула $\mathfrak{A}(A_1^0, \ldots, A_n^0)$ содержит только предикаты A_i^0, и поэтому всякая предметная переменная входит только под знаком одного из этих предикатов.

Пусть $R(x, y, \ldots, u)$ — предикат, определенный на области $\mathfrak{M}$. Под выражением

$$\widehat{\forall x}\, R(x, y, \ldots, u)$$

будем понимать предикат, зависящий от $y, z, \ldots, u$ (или высказывание, если $y, z, \ldots, u$ отсутствуют) и принимающий значение *И*, когда $R(x, y, z, \ldots, u)$ имеет значение *И* для данных $y, z, \ldots, u$ и для всех x, принадлежащих области $\mathfrak{M}'$, и принимающий значение *Л* в противном случае. Введем также выражение

$$\widehat{\exists x}\, R(x, y, \ldots, u),$$

которое представляет собой предикат от $y, \ldots, u$ и принимает значение *И*, когда $R(x, y, \ldots, u)$ имеет значение *И* для $y, \ldots, u$ и по крайней мере для одного значения x из области $\mathfrak{M}'$, и значение *Л* в противном случае. Символы $\widehat{\forall x}$ и $\widehat{\exists x}$ будем называть *ограниченными* *кванторами.* Если мы все переменные предиката $R(x, y, \ldots, u)$ свяжем ограниченными кванторами, например

$$\widehat{\forall x}\, \widehat{\exists y} \ldots \widehat{\forall y}\, R(x, y, \ldots, u),$$

то получим формулу, отнесенную к области $\mathfrak{M}'$. Покажем, что выражение

$$\forall x\, R(\varphi(x), y, \ldots, u)$$

равносильно выражению

$$\widehat{\forall x}\, R(x, y, \ldots, u). \tag{1}$$

Пусть $\forall x\, R(\varphi(x), y, \ldots, u)$ имеет при некоторых значениях переменных $y, \ldots, u$ значение *И*. В таком случае $R(\varphi(x), y, \ldots, u)$ имеет значение *И* для данных $y, \ldots, u$ и для каждого x. Но так как функция $\varphi(x)$ пробегает всю область $\mathfrak{M}'$, когда x пробегает область $\mathfrak{M}$, то $R(x, y, \ldots, u)$ имеет значение *И* для данных $y, \ldots, u$ и для всех x из $\mathfrak{M}'$. В силу определения $\widehat{\forall x}\, R(x, y, \ldots, u)$ также принимает значение *И*. Обратно, если $\widehat{\forall x} R(x, y, \ldots, u)$ принимает значение *И*, то $R(x, y, \ldots, u)$ имеет значение *И* для данных $y, \ldots, u$ и для каждого x из $\mathfrak{M}'$. В таком случае выражение $R(\varphi(x), y, \ldots, u)$ имеет значение *И* для данных $y, \ldots, u$ и для каждого x из $\mathfrak{M}$, так как $\varphi(x)$ для любого x принадлежит $\mathfrak{M}'$.

Аналогичным образом можно показать, что выражения

$$\exists x\, R(\varphi(x), y, \ldots, u) \quad \text{и} \quad \widehat{\exists x}\, R(x, y, \ldots, u) \tag{2}$$

также равносильны.

Рассмотрим формулу $\mathfrak{A}(A_1^0, \ldots, A_n^0)$, которую можно представить в форме

$$\mathrm{Q}x_1\, \mathrm{Q}x_2 \ldots \mathrm{Q}x_p\, \mathfrak{B}(A_1^0, \ldots, A_n^0, x_1, \ldots, x_p),$$

где $\mathfrak{B}(A_1^0, \ldots, A_n^0, x_1, \ldots, x_p)$ представляет собой предикат, определенный на области $\mathfrak{M}$ и зависящий от p переменных $x_1, \ldots, x_p$. Каждая из этих переменных входит в формулу $\mathfrak{B}$ только через предикаты $A_1^0, \ldots, A_n^0$. С другой стороны, мы видели, что предикаты $A_i^0(x)$ и $A_i^0(\varphi(x))$ равносильны. Поэтому, если в формуле

$\mathfrak{B}(A_1^0, \ldots, A_n^0, x_1, \ldots, x_p)$ мы заменим x_i на $\varphi(x_i)$, то получим равносильное выражение:

$$\mathfrak{B}(A_1^0, \ldots, A_n^0, x_1, \ldots, x_p) \sim \\ \sim \mathfrak{B}(A_1^0, \ldots, A_n^0, \varphi(x_1), \ldots, \varphi(x_p)).$$

Отсюда следует, что

$$\mathrm{Q}x_p \mathfrak{B}(A_1^0, \ldots, A_n^0, x_1, \ldots, x_p) \sim \\ \sim \mathrm{Q}x_p \mathfrak{B}(A_1^0, \ldots, A_n^0, \varphi(x_1), \ldots, \varphi(x_p)).$$

Далее можно заключить, что

$$\mathrm{Q}x_p \mathfrak{B}(A_1^0, \ldots, A_n^0, \varphi(x_1), \ldots, \varphi(x_p)) \sim \\ \sim \widehat{\mathrm{Q}x_p} \mathfrak{B}(A_1^0, \ldots, A_n^0, \varphi(x_1), \ldots, \varphi(x_{p-1}), x_p).$$

Действительно, фиксируя произвольным образом в выражении $\mathfrak{B}(A_1^0, \ldots, A_n^0, \varphi(x_1), \ldots, \varphi(x_p))$ переменные $x_1, \ldots, x_{p-1}$, мы получим предикат от одной переменной x_p. Применив к нему равносильность (1) или (2), получим требуемую равносильность. Из двух последних равносильностей вытекает

$$\mathrm{Q}x_p \mathfrak{B}(A_1^0, \ldots, A_n^0, x_1, \ldots, x_p) \sim \\ \sim \widehat{\mathrm{Q}x_p} \mathfrak{B}(A_1^0, \ldots, A_n^0, \varphi(x_1), \ldots, \varphi(x_{p-1}), x_p).$$

Рассуждая аналогичным образом, мы получим

$$\mathrm{Q}x_{p-1} \mathrm{Q}x_p \mathfrak{B}(A_1^0, \ldots, A_n^0, x_1, \ldots, x_{p-1}, x_p) \sim \\ \sim \widehat{\mathrm{Q}x_{p-1}} \widehat{\mathrm{Q}x_p} \mathfrak{B}(A_1^0, \ldots, A_n^0, \varphi(x_1), \ldots, \varphi(x_{p-2}), x_{p-1}, x_p)$$

и, наконец, придем к следующему:

$$\mathrm{Q}x_1 \ldots \mathrm{Q}x_p \mathfrak{B}(A_1^0, \ldots, A_n^0, x_1, \ldots, x_p) \sim \\ \sim \widehat{\mathrm{Q}x_1} \ldots \widehat{\mathrm{Q}x_p} \mathfrak{B}(A_1^0, \ldots, A_n^0, x_1, \ldots, x_p).$$

Правая часть последней равносильности, согласно смыслу символа $\widehat{\mathrm{Q}x}$, представляет не что иное, как формулу

$$\mathrm{Q}x_1 \ldots \mathrm{Q}x_p \mathfrak{B}(A_1^0, \ldots, A_n^0, x_1, \ldots, x_p),$$

отнесенную к области $\mathfrak{M}'$.

Таким образом, мы доказали, что формула $\mathfrak{A}(A_1^0, \ldots \ldots, A_n^0)$ сохраняет свое значение, если ее отнести к области $\mathfrak{M}'$, и теорема, таким образом, доказана.

Следствие. *Если формула $\mathfrak{A}$, содержащая только предикаты, зависящие от одной переменной, является тождественно истинной для всякой области, не превышающей 2^n элементов, где n — число предикатов в $\mathfrak{A}$, то формула $\mathfrak{A}$ тождественно истинна* (т. е. истинна для любой области).

В самом деле, допустим, что $\mathfrak{A}$ не является тождественно истинной формулой. В таком случае ее отрицание $\overline{\mathfrak{A}}$ выполнимо на некоторой области. Так как $\overline{\mathfrak{A}}$ также удовлетворяет условиям теоремы, то найдется область, содержащая не более 2^n элементов, на которой формула $\overline{\mathfrak{A}}$ выполнима. Следовательно, $\mathfrak{A}$ не может быть истинной на этой области, что противоречит условию. Итак, предположение, что $\mathfrak{A}$ не является тождественно истинной, приводит к противоречию, что и требовалось доказать.

Доказанная теорема позволяет решать проблему разрешения для формул, содержащих только предикаты, зависящие от одной переменной. Из следствия видно, что для того, чтобы установить, является ли формула $\mathfrak{A}$ тождественно истинной или нет, достаточно проверить, является ли она тождественно истинной на всякой области, содержащей не более чем 2^n элементов.

Заметим, что достаточно проверить, является ли данная формула $\mathfrak{A}'$ тождественно истинной на области, состоящей ровно из 2^n элементов. Это следует из того, что для формул рассматриваемого типа имеет место следующее: если формула $\mathfrak{A}$ тождественно истинна на некоторой области, то она тождественно истинна на всякой ее части.

Рассмотрим произвольную область, содержащую ровно 2^n элементов: $x_1, x_2, \ldots, x_{2^n}$. Легко видеть, что всякая формула, имеющая вид

$$\forall x \mathfrak{B}(x),$$

отнесенная к данной области, равносильна формуле

$$\mathfrak{B}(x_1) \& \mathfrak{B}(x_2) \& \ldots \& \mathfrak{B}(x_{2^n}).$$

А формула, имеющая вид

$$\exists x\, \mathfrak{B}(x),$$

равносильна формуле

$$\mathfrak{B}(x_1) \vee \mathfrak{B}(x_2) \vee \ldots \vee \mathfrak{B}(x_{2^n}).$$

В таком случае произвольная формула $\mathfrak{A}$, отнесенная к области $\{x_1, \ldots, x_{2^n}\}$, равносильна формуле $\mathfrak{A}'$, в которой все кванторы заменены операциями конъюнкции и дизъюнкции. Если в $\mathfrak{A}$ входили только предикаты $A_1, \ldots, A_n$, зависящие от одной переменной, то $\mathfrak{A}'$ представляет собой формулу, образованную только операциями алгебры высказываний над выражениями $A_i(x_j)$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant 2^n$. Так как предикаты $A_i(x)$ совершенно произвольны, то выражения $A_i(x_j)$ представляют собой произвольные высказывания. Формулу $\mathfrak{A}'$ тогда можно рассматривать как формулу алгебры высказываний, у которой $A_i(x_j)$ являются элементарными переменными высказываниями. Тогда вопрос о тождественной истинности $\mathfrak{A}$ на области $x_1, x_2, \ldots, x_{2^n}$ оказывается эквивалентным вопросу о тождественной истинности $\mathfrak{A}'$ как формулы алгебры высказываний с переменными высказываниями $A_i(x_j)$.

Заметим, что формула алгебры высказываний $\mathfrak{A}'$, по существу, не зависит от того, каковы элементы области $\{x_1, \ldots, x_p\}$, а зависит только от их числа, так как если мы возьмем другую область $\{x'_1, \ldots, x'_p\}$, то в $\mathfrak{A}'$ произойдет только перемена обозначений переменных высказываний $A_i(x_j)$ на $A_i(x'_j)$. В силу этого мы можем сказать, что если $\mathfrak{A}'$ тождественно истинна как формула алгебры высказываний, то формула $\mathfrak{A}$ тождественно истинна на любой области из 2^n элементов, и обратно. С другой стороны, в главе I мы получили конструктивный способ определять, является произвольная формула алгебры высказываний тождественно истинной или нет. Применяя этот критерий, мы можем установить, будет ли произвольная формула $\mathfrak{A}$, содержащая только предикаты от одной переменной, тождественно истинной на любой области, содержащей 2^n элементов. В таком случае в силу высказанного выше положения мы решим также и вопрос о том, будет формула $\mathfrak{A}$ тождественно истинной или нет.

§ 12. Конечные и бесконечные области

Чтобы выяснить вопрос, какие области могут характеризоваться аксиомами, содержащими только предикаты с одной переменной, мы должны несколько усилить теорему предыдущего параграфа. Именно, мы докажем следующую теорему.

Теорема. *Пусть формула* $\mathfrak{A}$, *не содержащая свободных предметных переменных, содержит только индивидуальные предметы* $c_1, \ldots, c_q$, *индивидуальные предикаты* $A_1, \ldots, A_n$ *и переменные предикаты* $B_1, \ldots, B_m$, *причем каждый из предикатов* A_i *и* B_j *зависит только от одной переменной; и пусть на некоторой области* $\mathfrak{M}$ *с определенными на ней индивидуальными предикатами* $A_1^0, \ldots, A_n^0$ *формула* $\mathfrak{A}$ *истинна при любых заменах символов* $B_1, \ldots, B_m$ *предикатами. Тогда существует область* $\mathfrak{M}'$, *содержащая не более* 2^n *элементов, с определенными на ней индивидуальными предикатами* $A_1', \ldots, A_n'$, *на которой формула* $\mathfrak{A}$ *также истинна.*

Выражение «формула $\mathfrak{A}$ истинна на области $\mathfrak{M}$ с предикатами A_i» употребляется здесь в том смысле, как и в § 4. Только в настоящем случае система аксиом состоит из одной аксиомы $\mathfrak{A}$. Это обстоятельство, впрочем, не является существенным, так как любую систему аксиом

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$$

мы всегда можем заменить одной аксиомой

$$\mathfrak{A}_1 \,\&\, \mathfrak{A}_2 \,\&\, \ldots \,\&\, \mathfrak{A}_n,$$

которая, как это непосредственно ясно по смыслу операции &, удовлетворяется теми же областями и предикатами, что и система $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$.

Перейдем к доказательству теоремы. Рассмотрим классы α, определенные так же, как и в предыдущем параграфе в связи с предикатами $A_1^0, \ldots, A_n^0$. Пусть $a_1, \ldots, a_p$ — элементы, выделенные из каждого непустого класса α. Совокупность всех этих элементов обозначим $\mathfrak{M}'$. Рассмотрим на области $\mathfrak{M}$ такие предикаты B' с одной переменной, которые для элементов, принадлежащих одному и тому же классу α, имеют одинаковое значение. Пусть $\varphi(x)$ так же, как и в предыдущей теореме, представляет собой элемент a_i, принадлежащий тому классу α, в который входит x. Мы уже знаем, что

$$A_i^0(x) \sim A_i^0(\varphi(x)).$$

Предикаты $B'(x)$, по условию, также обладают этим свойством, т. е.

$$B'(x) \sim B'(\varphi(x)),$$

так как x и $\varphi(x)$ всегда принадлежат одному и тому же классу α. Тогда, рассуждая так же, как при доказательстве предыдущей теоремы, можно показать, что если формула

$$\mathfrak{A}(c_1, \ldots, c_q, A_1, \ldots, A_n, B_1, \ldots, B_m)$$

истинна при некоторых определенных заменах предметов c и предикатов A и B предметами и предикатами из $\mathfrak{M}$, то формула

$$\mathfrak{A}(\varphi(c_1), \ldots, \varphi(c_q), A_1, \ldots, A_n, B_1', \ldots, B_m')$$

также истинна.

По условию формула $\mathfrak{A}$ удовлетворяется областью $\mathfrak{M}$ с предикатами $A_1^0, \ldots, A_n^0$. Поэтому существуют такие предметы $c_1^0, \ldots, c_q^0$, что формула

$$\mathfrak{A}(c_1^0, \ldots. c_q^0, A_1^0, \ldots, A_n^0, B_1, \ldots, B_m)$$

истинна при всяких заменах предикатов B_i предикатами, определенными на $\mathfrak{M}$. В таком случае формула

$$\mathfrak{A}(c_1^0, \ldots, c_q^0, A_1^0, \ldots, A_n^0, B_1', \ldots, B_m')$$

истинна при всевозможных предикатах B_i'. Из сказанного следует, что формула

$$\mathfrak{A}(\varphi(c_1^0), \ldots, \varphi(c_q^0), A_1^0, \ldots, A_n^0, B_1', \ldots, B_m')$$

истинна на области $\mathfrak{M}'$ при всевозможных предикатах B_i'. Но совокупность возможных предикатов B_i' на области $\mathfrak{M}'$ совпадает с множеством всех предикатов этой области, так как значения предикатов B_i' для элементов различных классов α не связаны никаким условием, а в $\mathfrak{M}'$ из каждого класса α присутствует только один элемент. Поэтому формула

$$\mathfrak{A}(\varphi(c_1^0), \ldots, \varphi(c_q^0), A_1^0, \ldots, A_n^0, B_1, \ldots, B_m)$$

истинна для всевозможных B_i из области $\mathfrak{M}'$; следовательно, область $\mathfrak{M}'$ с предикатами $A_1^0, \ldots, A_n^0$ удовлетворяет этой формуле. Теорема доказана.

Рассмотрим вопрос о том, какие множества могут характеризоваться аксиомами, содержащими предикаты только от одной переменной. Пусть

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$$

— система аксиом, содержащая предикаты только от одной переменной. Как мы указывали в § 4, всегда можно предполагать, что аксиомы $\mathfrak{A}_i$ не содержат свободных переменных. Кроме того, эту систему аксиом можно заменить одной аксиомой:

$$\mathfrak{A}_1 \& \mathfrak{A}_2 \& \ldots \& \mathfrak{A}_n,$$

которую мы обозначим буквой $\mathfrak{A}$ без индекса. Из доказанной теоремы следует, что если формула $\mathfrak{A}$ интерпретируется какой-либо областью, то она интерпретируется и конечной областью. То же самое справедливо и для системы аксиом $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$.

Из всего этого следует, что *не существует совместной системы аксиом, содержащей предикаты только от одной переменной и такой, чтобы из нее вытекала бесконечность характеризуемой ею области.*

Иными словами, посредством аксиом с предикатами, зависящими от одной переменной, невозможно отличить бесконечное множество от конечного. Это значит, что бесконечное множество нельзя отличить от конечного, если делать высказывания только о свойствах его элементов, а не об отношениях между ними. Следовательно, чтобы достаточно полно охарактеризовать такие множества, как, например, натуральный ряд чисел, совокупность всех действительных чисел, без которых математика немыслима, необходимо употреблять предикаты, зависящие более чем от одной переменной.

Аксиомы, в которых допускаются предикаты, зависящие от любого числа переменных, могут характеризовать бесконечные множества. Примером может служить система аксиом натурального ряда в § 8. Область, удовлетворяющая этим аксиомам, подобна натуральному ряду и поэтому не может быть конечной.

Можно привести простую формулу, которая невыполнима на конечной области, но выполнима на бесконечной области:

$$\forall x \forall y \forall z \exists u [F(x, x) \,\&\, (\overline{F}(x, y) \to \\ \to (\overline{F}(y, z) \to \overline{F}(x, z))) \,\&\, \overline{F}(x, u)].$$

Допустим, что эта формула выполняется на некоторой области $\mathfrak{M}$. В таком случае должен существовать предикат $F^0(x, y)$, для которого эта формула на области $\mathfrak{M}$ истинна. Нетрудно убедиться, что в таком случае предикат $\overline{F}^0(x, y)$ представляет собой предикат, устанавливающий отношение порядка между элементами области $\mathfrak{M}$. Из формулы видно, что предикат $\overline{F}^0(x, y)$ в самом деле удовлетворяет аксиомам порядка:

1. $\overline{\overline{F}}{}^0(x, x)$,
2. $\overline{F}^0(x, y) \to (\overline{F}^0(y, z) \to \overline{F}^0(x, z))$.

Условимся $\overline{F}^0(x, y)$ выражать словами «x предшествует y». Как видно из формулы, для каждого x должно существовать u такое, что истинно $\overline{F}(x, u)$, т. е. «x предшествует u». Возьмем произвольный элемент области x_1; среди элементов области должен найтись такой элемент x_2, что «x_1 предшествует x_2». Точно так же должен найтись такой элемент x_3, что «x_2 предшествует x_3», и т. д. Получаем последовательность элементов

$$x_1, x_2, \ldots, x_n.$$

В силу аксиом 1 и 2 каждый элемент этой последовательности отличен от каждого элемента с меньшим индексом, так как будет иметь место «x_1 предшествует x_n», «x_2 предшествует x_n», «x_{n-1} предшествует x_n». Но это значит, что любые два элемента нашей последовательности различны и область $\mathfrak{M}$ бесконечна. Мы доказали, таким образом, что если рассматриваемая формула выполняется на некоторой области, то эта область бесконечна.

Покажем, что существует область, на которой данная формула выполняется. Пусть $\mathfrak{M}$ — натуральный ряд, а $F(x, y)$ означает, что «x больше или равно y». Тогда $\overline{F}(x, y)$ означает $x < y$. При такой замене предиката $F(x, y)$ формула примет вид

$$\forall x \forall y \forall z \exists u [\overline{x < x} \,\&\, ((x < y) \to (y < z \to x < z)) \,\&\, x < u].$$

Легко видеть, что для натурального ряда это выражение в самом деле истинно.

Чтобы рассмотреть некоторые вопросы, касающиеся формул, выполнимых на бесконечных областях, нам необходимо ввести одно понятие из теории множеств, представляющее собой обобщение понятия «числа элементов конечного множества» и позволяющее различать бесконечные множества так, что это различие не связано ни с природой элементов, ни с отношениями между элементами рассматриваемых множеств.

Мы будем называть два множества $\mathfrak{M}$ *и* $\mathfrak{M}'$ *равномощными, если между их элементами можно установить взаимно однозначное соответствие.* В силу этого определения множества входят в классы равномощных между собой множеств, и выражение «мощность данного множества» или «число элементов данного множества» означает принадлежность данного множества к тому или другому классу.

Множества, равномощные натуральному ряду чисел, называются *счетными* множествами. Бесконечные множества, не равномощные натуральному ряду, называются *несчетными* множествами. Примером несчетного множества является множество действительных чисел.

Счетные множества имеют наименьшую мощность среди всех бесконечных множеств. (Смысл термина «мощность множества $\mathfrak{M}$ меньше мощности множества $\mathfrak{M}'$» определяется в теории множеств следующим образом: мощность $\mathfrak{M}$ меньше мощности $\mathfrak{M}'$, если $\mathfrak{M}$ и $\mathfrak{M}'$ неравномощны и $\mathfrak{M}$ равномощно части $\mathfrak{M}'$.)

Для выполнимости формул логики предикатов имеет место следующая теорема, которую мы докажем в § 14.

Теорема Лёвенгейма. *Если формула выполнима на каком-нибудь бесконечном множестве, то она выполнима и на счетном множестве.*

§ 13. Разрешающие функции (функции Сколема)

Рассмотрим формулу вида

$$\exists x_1 \ldots \exists x_{n_1} \forall y_1 \ldots \forall y_i \ldots \exists z_1 \ldots \forall u_1 \ldots \exists v_1 \ldots \\ \ldots \mathfrak{B}(x_1, \ldots, y_1, \ldots, v_1, \ldots), \qquad (1)$$

где $\mathfrak{B}$ — индивидуальный предикат, определенный на некоторой области $\mathfrak{M}$, и предположим, что все переменные в формуле (1) связаны. Расположение и число кванторов, стоящих перед $\mathfrak{B}$, совершенно произвольно, и то, что в выражении (1) мы поставили первым квантор существования, не имеет никакого значения. Однако, не уменьшая общности, мы можем предположить, что в выражении (1) всегда присутствует квантор существования, и даже, более того, можем предположить, что последним является квантор существования. Для этого только надо заметить, что если $I(t)$, где t не входит свободно в $\mathfrak{B}$, представляет собой тождественно истинный предикат на области $\mathfrak{M}$, то имеет место

$$\mathfrak{B}(x_1, \ldots. v_1, \ldots) \sim \exists t\, (\mathfrak{B}(x_1, \ldots, v_1, \ldots) \,\&\, I(t))$$

при всех значениях переменных, входящих в $\mathfrak{B}$. В таком случае, если в формуле (1) последний квантор есть квантор всеобщности, мы можем заменить выражение $\mathfrak{B}$ равносильным выражением $\exists t\, (\mathfrak{B} \,\&\, I(t))$. Тогда получится формула, в которой последний квантор есть квантор существования. В дальнейшем мы и будем предполагать, что последний квантор является квантором существования.

Разобьем кванторы в формуле (1) на группы так, чтобы к каждой группе относились непосредственно следующие один за другим кванторы одного и того же рода (существования или всеобщности). Так, в выражении (1) мы будем иметь следующие группы:

первая

$$\exists x_1, \ldots, \exists x_{n_1},$$

вторая

$$\forall y_1, \ldots, \forall y_{n_2},$$

третья

$$\exists z_1, \ldots, \exists z_{n_3}$$

и т. д.

Поставим в соответствие каждой переменной, связанной квантором существования, какую-нибудь функцию, определенную на области $\mathfrak{M}$, принимающую значения из области $\mathfrak{M}$ и зависящую только от переменных, связанных квантором всеобщности и предшествующих данному квантору существования. Если же квантору существования не предшествует ни один квантор всеобщности, то мы ему поставим в соответствие какой-нибудь индивидуальный предмет области. (Можно сказать, что в этом случае функция вырождается в константу.) Для формулы (1), таким образом, переменным x_i будут поставлены в соответствие некоторые индивидуальные предметы x_i^0, переменным z_i — функции $\varphi_i(y_1, \ldots, y_{n_2})$ и т. д., переменным v_i — функции $\psi_i\left(y_1, \ldots, y_{n_2}, \ldots \ldots, u_1, \ldots, u_{n_{k-1}}\right)$. Если эти предметы и функции таковы, что в результате замены ими соответствующих переменных в предикате

$$\mathfrak{B}(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}, \ldots)$$

полученный предикат

$$\mathfrak{B}\left(x_1^0, \ldots, x_{n_1}^0, y_1, \ldots, y_{n_2}, \varphi_1\left(y_1, \ldots, y_{n_2}\right), \ldots \right.$$
$$\ldots, \varphi_{n_3}\left(y_1, \ldots, y_{n_2}\right), \ldots$$
$$u_1, \ldots, u_{n_{k-1}}, \psi_{n_1}\left(y_1, \ldots, u_1, \ldots, u_{n_{k-1}}\right), \ldots$$
$$\left. \ldots, \psi_{n_k}\left(y_1, \ldots, u_1, \ldots, u_{n_{k-1}}\right)\right) \quad (2)$$

окажется истинным для всех значений входящих в него переменных, то мы будем называть указанные предметы и функции

$$x_1^0, \ldots, x_{n_1}^0, \varphi_1\left(y_1, \ldots, y_{n_2}\right), \ldots, \psi_{n_k}\left(y_1, \ldots, u_{n_{k-1}}\right)$$

разрешающими функциями (или функциями Сколема) *для формулы* (1). Причем это название будем относить и к предметам x_i^0, чтобы не вводить для них особого термина.

Л е м м а. *Чтобы формула* (1) *была истинна на области* $\mathfrak{M}$, *необходимо и достаточно, чтобы для этой формулы существовали разрешающие функции.*

Прежде всего, очевидно, что для того, чтобы (1) было истинно, необходимо и достаточно, чтобы существовали предметы $x_1^0, \ldots, x_{n_1}^0$ области $\mathfrak{M}$ такие, что

$$\forall y_1 \ldots \forall y_{n_2} \exists z_1 \ldots \exists v_{n_k} \mathfrak{B}\left(x_1^0, \ldots, x_{n_1}^0, y_1, \ldots, v_{n_k}\right)$$

— истинная на $\mathfrak{M}$ формула.

Проведем доказательство нашей леммы индукцией по числу групп кванторов.

В случае, когда в формуле (1) имеется только одна группа кванторов, эта формула имеет вид

$$\exists x_1 \ldots \exists x_{n_1} \mathfrak{B}(x_1, \ldots, x_{n_1}),$$

так как согласно нашему предположению последний квантор должен быть квантором существования. Очевидно, что в этом случае, для того чтобы формула была истинна, необходимо и достаточно, чтобы в $\mathfrak{M}$ существовали элементы

$$x_1^0, x_2^0, \ldots, x_{n_1}^0$$

такие, что формула

$$\mathfrak{B}(x_1^0, x_2^0, \ldots, x_{n_1}^0)$$

истинна. В этом случае разрешающей системой функций является система элементов $x_1^0, \ldots, x_{n_1}^0$.

Допустим, что формула (1) имеет $p+1$ групп кванторов. Возможны два случая:

1) первая группа состоит из кванторов существования;

2) первая группа состоит из кванторов всеобщности.

В первом случае формула (1) имеет вид

$$\exists x_1 \ldots \exists x_{n_1} \forall y_1 \ldots \forall y_{n_2} \ldots \mathfrak{B}(x_1, \ldots, x_{n_1}, y_1, \ldots). \qquad (3)$$

Для того чтобы формула была истинна, необходимо и достаточно, чтобы в области $\mathfrak{M}$ существовали предметы

$$x_1^0, x_2^0, \ldots, x_{n_1}^0,$$

для которых

$$\forall y_1 \ldots \forall y_{n_2} \ldots \mathfrak{B}(x_1^0, \ldots, x_{n_1}^0, y_1, \ldots)$$

истинна. Но эта последняя формула сама является формулой вида (1) и содержит уже только p групп кванторов. На основании индуктивного предположения для истинности этой формулы необходимо и достаточно существования разрешающей системы функций

$$\varphi_1(y_1, \ldots, y_{n_2}), \ldots, \varphi_{n_3}(y_1, \ldots, y_{n_2}), \ldots$$
$$\ldots, \psi_{n_k}(y_1, \ldots, y_{n_2}, \ldots, u_{n_{k-1}}), \qquad (4)$$

т. е. такой системы функций, что выражение

$$\mathfrak{B}\left(x_1^0, \ldots, x_{n_1}^0, y_1, \ldots, y_{n_2}, \varphi_1(y_1, \ldots, y_{n_2}), \ldots \right.$$
$$\left. \ldots, \psi_{n_k}\left(y_1, \ldots, y_{n_{k-1}}\right)\right) \qquad (5)$$

истинно для всех значений переменных на области $\mathfrak{M}$. Но тогда для истинности формулы (3) необходимым и достаточным условием является существование предметов $x_1^0, x_2^0, \ldots, x_{n_1}^0$ и функций $\varphi_1(y_1, \ldots, y_{n_2}), \ldots$ $\ldots, \psi_{n_k}\left(y_1, \ldots, u_{n_{k-1}}\right)$, для которых выражение (5) истинно при всех значениях переменных. Но это и означает, что предметы $x_1^0, \ldots, x_{n_1}^0$ и функции (4) образуют систему разрешающих функций для формулы (1).

Итак, мы доказали, что в рассматриваемом случае для истинности формулы (1) необходимо и достаточно существование системы разрешающих функций.

Перейдем к второму случаю, когда первая группа кванторов состоит из кванторов всеобщности. В этом случае формула (1) имеет вид

$$\forall x_1 \ldots \forall x_{n_1} \exists y_1 \ldots \exists y_{n_2} \ldots \mathfrak{B}\left(x_1, \ldots, y_1, \ldots, v_{n_k}\right), \qquad (6)$$

причем число групп кванторов этой формулы равно, по условию, $p+1$.

Для того чтобы формула была истинна, необходимо и достаточно, чтобы формула

$$\exists y_1 \ldots \exists y_{n_2} \ldots \mathfrak{B}\left(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}, \ldots, v_{n_k}\right)$$

была истинна при всех значениях переменных $x_1, \ldots, x_{n_1}$ из $\mathfrak{M}$. Возьмем произвольную группу значений переменных из области $\mathfrak{M}$:

$$x_1^0, x_2^0, \ldots, x_{n_1}^0.$$

Формула

$$\exists y_1 \ldots \exists y_{n_2} \forall z_1 \ldots \mathfrak{B}\left(x_1^0, \ldots, x_{n_1}^0, y_1, \ldots, y_{n_2}, \ldots, v_{n_k}\right) \qquad (7)$$

при фиксированных таким образом значениях переменных $x_1, \ldots, x_{n_1}$ не имеет свободных предметных переменных и представляет собой выражение вида (1). Число различных групп одноименных кванторов в этой формуле равно p. Согласно индуктивному предположению, для того чтобы эта формула была истинна, необходимо и достаточно существование разрешающей системы функций

$$y_1^0, \ldots, y_{n_2}^0, \chi_1(z_1, z_2, \ldots, z_{n_3}), \ldots, \psi_{n_k}(z_1, \ldots, u_{n_{k-1}}).$$

Допустим, что формула (6) истинна. Тогда для каждой совокупности значений переменных $x_1^0, \ldots, x_{n_1}^0$ должна существовать разрешающая система функций формулы (7). Выберем для каждой совокупности значений переменных $x_1^0, \ldots, x_{n_1}^0$ вполне определенную разрешающую систему функций формулы (7) и обозначим ее

$$y_1^0(x_1^0, \ldots, x_{n_1}^0), \ldots, y_{n_2}^0(x_1^0, \ldots, x_{n_1}^0),$$
$$\chi_1(x_1^0, \ldots, x_{n_1}^0, z_1, \ldots, z_{n_3}), \ldots \tag{8}$$

Выражение

$$\mathfrak{B}(x_1^0, \ldots, x_{n_1}^0, y_1^0(x_1^0, \ldots, x_{n_1}^0), \ldots, \psi_{n_k}(x_1^0, \ldots, x_{n_1}^0, z_1, \ldots))$$

истинно при всех значениях входящих в него свободных переменных, каковы бы ни были $x_1^0, x_2^0, \ldots, x_{n_1}^0$ из области $\mathfrak{M}$. Но мы можем рассмотреть $y_i^0(x_1^0, \ldots, x_{n_1}^0)$ как функцию, определенную на области $\mathfrak{M}$, принимающую значения из $\mathfrak{M}$ и зависящую от переменных $x_1, \ldots, x_n$. Обозначим ее $\varphi_i(x_1, \ldots, x_n)$. Точно так же мы можем рассмотреть $\chi_i(x_1^0, \ldots, x_{n_1}^0, z_1, \ldots, z_{n_3})$ как функцию, зависящую от переменных $x_1, \ldots, x_{n_1}, z_1, \ldots, z_{n_3}$, и записать ее в виде

$$\chi_i(x_1, \ldots, x_{n_1}, z_1, \ldots, z_{n_3}),$$

и так для всех функций системы (8).

В таком случае предикат

$$\mathfrak{B}(x_1, \ldots, x_{n_1}, \varphi_1(x_1, \ldots, x_{n_1}), \ldots, \psi_{n_k}(x_1, \ldots, u_{n_{k-1}}))$$

истинен при всех значениях входящих в него переменных. Но тогда система функций

$$\varphi_1(x_1, \ldots, x_{n_1}), \ldots, \varphi_{n_2}(x_1, \ldots, x_{n_1}), \ldots$$
$$\ldots, \psi_{n_k}(x_1, \ldots, u_{n_{k-1}}) \tag{9}$$

является разрешающей системой функций для формулы (6). (Легко видеть, что зависимость входящих в эту систему функций от переменных такая, какая требуется для разрешающей системы.)

Обратно, допустим, что для формулы (6) существует разрешающая система функций (9). В таком случае

$$\mathfrak{B}\left(x_1, \ldots, x_{n_1}, \varphi_1\left(x_1, \ldots, x_{n_1}\right), \ldots, \psi_{n_k}\left(x_1, \ldots, u_{n_{k-1}}\right)\right)$$

истинно при всех значениях входящих переменных. Тогда для каждой совокупности значений переменных $x_1^0, \ldots, x_{n_1}^0$

$$\mathfrak{B}\left(x_1^0, \ldots, x_{n_1}^0, \varphi_1\left(x_1^0, \ldots, x_{n_1}^0\right), \ldots, \psi_{n_k}\left(x_1^0, \ldots, u_{n_{k-1}}\right)\right)$$

истинно и, следовательно, система функций

$$\varphi_1\left(x_1^0, \ldots, x_{n_1}^0\right), \ldots, \psi_{n_k}\left(x_1^0, \ldots, x_{n_1}^0, z_1, \ldots, u_{n_{k-1}}\right),$$

получающаяся из данной нам системы функций фиксированием переменных $x_1, \ldots, x_{n_1}$, является разрешающей системой для формулы (7).

На основании сказанного выше мы можем заключить, что тогда и формула (7) для любых значений переменных $x_1, \ldots, x_{n_1}$, и формула (6) будут истинны. Так как лемма верна в случае, если в формуле (1) есть только одна группа кванторов, и, будучи верной для p групп кванторов, остается верной для $p+1$ групп кванторов, то лемма полностью доказана.

§ 14. Теорема Лёвенгейма

Все рассуждения предыдущего параграфа не зависят от того, входят ли в рассматриваемые формулы индивидуальные предметы или нет. Поэтому доказанные в этом параграфе положения мы можем применять и к выполнимости в расширенном смысле слова, которую мы сейчас определим.

Понятие выполнимости формулы в § 10 было определено только для формул, не содержащих символов индивидуальных предметов и предикатов. Расширим понятие выполнимости так, чтобы оно было применимо к случаю, когда в формуле имеются символы индивидуальных предметов.

Пусть формула $\mathfrak{A}$ удовлетворяет всем ранее высказанным условиям, кроме требования отсутствия символов индивидуальных предметов. *Будем называть формулу $\mathfrak{A}$ выполнимой на области $\mathfrak{M}$, если все предикаты, входящие в $\mathfrak{A}$, можно заменить предикатами, определенными на $\mathfrak{M}$, а символы индивидуальных предметов — предметами из области $\mathfrak{M}$ так, чтобы полученная таким образом формула была истинна.*

Теорема Лёвенгейма. *Если формула, не содержащая свободных предметных переменных (но, быть может, содержащая символы индивидуальных предметов), выполнима на некоторой области, то она выполнима на конечной или на счетной области.*

В доказательстве этой теоремы мы можем ограничиться рассмотрением нормальных формул, так как нормальная форма любой формулы одновременно с ней выполнима или невыполнима на каждой области. Рассмотрим произвольную нормальную формулу, все предметные переменные которой связаны. Она может содержать символы индивидуальных предметов. Например,

$$\forall x_1 \ldots \forall x_{n_1} \exists y_1 \ldots \exists y_{n_2} \ldots$$
$$\ldots \mathfrak{B}(x_1, \ldots, a_1, \ldots, a_p, A_1, \ldots, A_q), \quad (1)$$

где $a_1, \ldots, a_p$ — символы индивидуальных предметов, а $A_1, \ldots, A_q$ — элементарные предикаты, входящие в формулу. То, что первыми стоят кванторы всеобщности, не имеет никакого значения для наших рассуждений. Допустим, что эта формула выполнима на некоторой области $\mathfrak{M}$. В таком случае найдутся такие предметы $a_1^0, \ldots, a_p^0$, принадлежащие данной области, и предикаты $A_1^0, \ldots, A_q^0$, определенные на этой области, что формула

$$\forall x_1 \ldots \forall x_{n_1} \exists y_1 \ldots \exists y_{n_2} \ldots$$
$$\ldots \mathfrak{B}(x_1, \ldots, x_{n_1}, \ldots, a_1^0, \ldots, a_p^0, A_1^0, \ldots, A_q^0) \quad (2)$$

будет истинным высказыванием.

Применив условия истинности, доказанные в предыдущем параграфе, мы можем сказать, что для формулы

(2) существует система разрешающих функций

$$\varphi_i(x_1, \ldots, x_{n_1}), \quad \psi_j(x_1, \ldots, x_{n_1}, z_1, \ldots, z_{n_3}), \ldots$$

В таком случае выражение

$$\mathfrak{B}(x_1, \ldots, x_{n_1}, \varphi_1(x_1, \ldots, x_{n_1}), \ldots, z_1, \ldots \\ \ldots, z_{n_3}, \psi_1(x_1, \ldots, x_{n_1}, z_1, \ldots, z_{n_3}), \ldots \\ \ldots, a_1^0, \ldots, a_p^0, A_1^0, \ldots, A_q^0$$

является предикатом, принимающим при всех значениях входящих в него переменных значение *И*.

Обозначим, ради краткости, этот предикат через

$$R(x_1, \ldots, x_{n_1}, z_1, \ldots, z_{n_3}, \ldots),$$

где переменные $x_1, \ldots, x_{n_1}, z_1, \ldots$ являются переменными, связанными в формуле (2) кванторами всеобщности. Построим некоторое множество $\mathfrak{M}'$, являющееся частью области $\mathfrak{M}$. Это множество мы определим как теоретико-множественную сумму последовательности конечных множеств

$$\mathfrak{M}_1', \mathfrak{M}_2', \ldots, \mathfrak{M}_n', \ldots$$

Множество $\mathfrak{M}_1'$ состоит из всех индивидуальных элементов $a_1^0, \ldots, a_p^0$, а если формула (2) не содержала индивидуальных предметов, то $\mathfrak{M}_1'$ состоит из одного произвольным образом выбранного элемента области $\mathfrak{M}$.

Допустим, что мы определили множество $\mathfrak{M}_n'$. Определим тогда множество $\mathfrak{M}_{n+1}'$. Включим в $\mathfrak{M}_{n+1}'$ все элементы множества $\mathfrak{M}_n'$ и присоединим к ним все те значения каждой разрешающей функции, которые она принимает при всевозможных заменах ее переменных предметами из множества $\mathfrak{M}_n'$. Очевидно, если множество $\mathfrak{M}_n'$ конечно, то множество $\mathfrak{M}_{n+1}'$ также конечно. Таким образом, мы определим последовательность конечных множеств

$$\mathfrak{M}_1', \mathfrak{M}_2', \ldots, \mathfrak{M}_n', \ldots$$

Очевидно, их теоретико-множественная сумма представляет собой множество счетное или конечное.

Обозначим теоретико-множественную сумму

$$\mathfrak{M}'_1 \cup \mathfrak{M}'_2 \cup \ldots \cup \mathfrak{M}'_n \cup \ldots \tag{3}$$

через $\mathfrak{M}'$. Множество $\mathfrak{M}'$ обладает следующим свойством. Если аргументы любой из разрешающих функций

$$\ldots, \varphi_i, \ldots, \psi_j, \ldots$$

принимают значения из $\mathfrak{M}'$, то и значение самой функции также является элементом из $\mathfrak{M}'$. Пусть $\theta(x_1, \ldots \ldots, x_{n_1}, z_1, \ldots, z_{n_3}, \ldots)$ — произвольная функция из системы $\varphi_i, \psi_j, \ldots$ Пусть x_1 принимает значение x_1^0, x_2 — значение $x_2^0, \ldots, z_1$ — значение $z_1^0, \ldots, z_{n_3}$ — значение $z_{n_3}^0, \ldots$, причем $x_1^0, x_2^0, \ldots, z_1^0, \ldots, z_{n_3}^0, \ldots$ принадлежат области $\mathfrak{M}'$. Каждый из этих элементов входит в одно из слагаемых $\mathfrak{M}'_i$. Допустим, что

$$x_1^0 \in \mathfrak{M}'_{k_1}, \quad x_2^0 \in \mathfrak{M}'_{k_2}, \ldots, z_1^0 \in \mathfrak{M}'_{g_1}, \ldots$$

Возьмем из всех множеств $\mathfrak{M}'_{k_1}, \ldots, \mathfrak{M}'_{g_1}, \ldots$ то, у которого номер наибольший. Пусть это будет $\mathfrak{M}'_t$. Множества $\mathfrak{M}'_n$ определены так, что каждое последующее содержит все элементы предыдущего. Поэтому все элементы $x_1^0, \ldots, x_n^0, z_1^0, \ldots, z_{n_3}^0, \ldots$ входят в $\mathfrak{M}'_t$. Но в таком случае $\theta(x_1^0, \ldots)$ является элементом множества $\mathfrak{M}'_{t+1}$ и поэтому также входит в $\mathfrak{M}'$.

Рассмотрим опять формулу (2), но предположим, что теперь она относится к области $\mathfrak{M}'$. Это сделать вполне возможно, так как область $\mathfrak{M}'$ представляет собой часть $\mathfrak{M}$. Предикаты $A_1^0, \ldots, A_q^0$, определенные на $\mathfrak{M}$, определены и для всех элементов $\mathfrak{M}'$, а предметы $a_1^0, \ldots, a_p^0$ принадлежит к $\mathfrak{M}'$ по построению. Разрешающие функции

$$\ldots, \varphi_i(x_1, \ldots, x_{n_1}), \ldots, \psi_j(x_1, \ldots, x_{n_1}, z_1, \ldots, z_{n_3}), \ldots$$

принимают значения из $\mathfrak{M}'$, если их аргументы принадлежат к $\mathfrak{M}'$. Поэтому тождественная истинность предиката

$$\mathfrak{B}(x_1, \ldots, x_{n_1}, \varphi_1(x_1, \ldots, x_{n_1}), \ldots)$$

на области $\mathfrak{M}'$ является также необходимым и достаточным условием истинности формулы (2) на области

$\mathfrak{M}'$. Так как этот предикат действительно является истинным на $\mathfrak{M}'$, то мы можем заключить, что формула (2) истинна для области $\mathfrak{M}'$. В таком случае формула (1) выполнима на $\mathfrak{M}'$.

Таким образом, мы доказали утверждение, что если формула (1) выполнима на некоторой области, то она выполнима на ее конечной или счетной части, что и составляет теорему Лёвенгейма.

Аксиоматическая характеристика бесконечных множеств. Мы видели, что если аксиомы содержат только предикаты с одной переменной, то они не могут характеризовать бесконечной области, потому что такой системе аксиом всегда будет удовлетворять также и конечная область.

Аксиомы с предикатами, которые зависят от двух и большего числа переменных, могут характеризовать бесконечные области, и возникает вопрос: могут ли они характеризовать несчетные области? Пусть

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$$

— система аксиом, содержащих только символы индивидуальных предикатов. Как мы уже указывали выше, мы всегда можем заменить эту систему одной аксиомой

$$\mathfrak{A}_1 \,\&\, \mathfrak{A}_2 \,\&\, \ldots \,\&\, \mathfrak{A}_n$$

и рассуждать всегда только об одной аксиоме. В рассматриваемом случае понятие интепретируемости аксиомы совпадает с понятием выполнимости этой формулы на некоторой области (см. § 10). Однако если эта формула выполнима на некоторой области, то в силу теоремы Лёвенгейма она выполнима и на некоторой конечной или счетной области. Из этого следует, что посредством аксиом рассматриваемого типа невозможно отличить несчетную область от счетной или конечной.

Оказывается, однако, что аксиомы, содержащие символы переменных предикатов, могут характеризовать несчетные множества и даже множества заданной несчетной мощности в том смысле, что все удовлетворяющие им области несчетны и имеют в точности данную мощность.

ИСЧИСЛЕНИЕ ПРЕДИКАТОВ

В настоящей главе мы приведем аксиоматическое описание логики предикатов, которую мы рассмотрели в предшествующей главе с содержательной точки зрения. Заметим, что, в отличие от алгебры высказываний, логика предикатов имеет явно неконструктивный характер. Все ее понятия определяются для произвольной области или произвольного множества объектов. Ввиду этого при содержательном изложении логики предикатов нам приходилось опираться на неконструктивные принципы теории множеств. Описание логики предикатов, которое мы дадим в настоящей главе, вполне удовлетворяет требованиям финитизма Гильберта.

Исчисление предикатов, как и всякая аксиоматическая система, содержит символы, из которых составляются формулы. Затем среди всех формул выделяются формулы, называемые выводимыми. Выделение выводимых формул в исчислении предикатов, так же как и в исчислении высказываний, осуществляется путем указания некоторой конечной совокупности формул, которые называются аксиомами, и указанием правил вывода, позволяющих из выводимых формул получать новые выводимые формулы.

§ 1. Формулы исчисления предикатов

Каждая формула исчисления предикатов представляет собой некоторую конечную последовательность символов этого исчисления. Опишем символы исчисления предикатов.

1) Малые латинские буквы с индексами или без них:

$$a,\ b,\ c,\ \ldots,\ x,\ y,\ z,\ \ldots,\ a_1,\ a_2,\ \ldots,\ x_1,\ x_2,\ \ldots$$

Эти символы носят название *переменных предметов.*

2) Большие латинские буквы с индексами внизу или без них:

$$A,\ B,\ \ldots,\ A_1,\ A_2,\ \ldots,$$

называются *переменными высказываниями.*

3) Большие латинские буквы с индексами вверху:

$$F^p,\ G^p,\ \ldots,\ S^p,\ T^p,\ \ldots,$$

и эти же символы с индексами внизу:

$$F_1^p,\ F_2^p,\ \ldots,\ G_1^p,\ G_2^p,\ \ldots,\ S_1^p,\quad S_2^p,\ \ldots$$

Эти символы носят название *переменных предикатов от p переменных* ($p = 1, 2, \ldots$).

4) Символы исчисления высказываний:

$$\&,\ \vee,\ \rightarrow,\ -.$$

5) Скобки

$$(\quad).$$

6) Символы $\forall$ и $\exists$.

Определение формул. Как мы уже указывали, каждая формула является конечной последовательностью символов или, иначе говоря, словом в алфавите, содержащем все указанные выше символы. Однако этим понятие формулы еще не определено. Мы должны определить, какие слова называются формулами.

1°. Каждое переменное высказывание есть формула.

2°. Если F^p — символ переменного предиката, $a_1, a_2, \ldots, a_p$ — символы предметных переменных, не обязательно различных, то слово

$$F^p(a_1,\ a_2,\ \ldots,\ a_p)$$

есть формула. За такими формулами мы сохраним название *переменного предиката.* Формулы, определенные в 1° и 2°, мы будем называть *элементарными формулами.*

Для дальнейшего определения формулы нам необходимо различать входящие в формулу предметные переменные. Одни из них мы будем называть *связанными,* другие — *свободными.* Различие это мы будем устанавливать параллельно определению формулы. В элементарных формулах все предметные переменные являются свободными.

3°. Пусть формула $\mathfrak{A}$ содержит свободную переменную x. Тогда слова

$$\forall x\,\mathfrak{A} \quad \text{и} \quad \exists x\,\mathfrak{A} \tag{1}$$

также являются формулами. Символы $\forall x$ и $\exists x$ носят название кванторов: первый — *квантор всеобщности*, второй — *квантор существования*. Переменная x в формулах (1) называется *связанной переменной*. Именно, мы будем говорить, что в формуле $\forall x\,\mathfrak{A}$ переменная x связана квантором $\forall x$, а в формуле $\exists x\,\mathfrak{A}$ переменная x связана квантором $\exists x$. Остальные же предметные переменные, которые в формуле $\mathfrak{A}$ свободны, остаются свободными и в обеих формулах (1). Переменные, которые связаны в формуле $\mathfrak{A}$, остаются связанными в формулах (1).

4°. Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — формулы, причем в них нет таких предметных переменных, которые связаны в одной формуле и свободны в другой. Тогда слова

$$(\mathfrak{A}\,\&\,\mathfrak{B}), \quad (\mathfrak{A} \vee \mathfrak{B}), \quad (\mathfrak{A} \rightarrow \mathfrak{B}), \quad \overline{}\mathfrak{A} \tag{2}$$

являются формулами. При этом свободные переменные в формулах $\mathfrak{A}$ и $\mathfrak{B}$ остаются свободными во всех формулах (2), а связанные переменные в формулах $\mathfrak{A}$ и $\mathfrak{B}$ остаются связанными в формулах (2).

Определение формулы исчисления предикатов имеет тот же индуктивный характер, как и определение формулы исчисления высказываний. Оно может быть высказано следующим образом.

Формулой называется слово из символов, которое может быть построено, исходя из элементарных формул, операциями перехода от формулы $\mathfrak{A}$ к формулам $\forall x\,\mathfrak{A}$ и $\exists x\,\mathfrak{A}$, от формул $\mathfrak{A}$ и $\mathfrak{B}$ к формулам $(\mathfrak{A}\,\&\,\mathfrak{B})$, $(\mathfrak{A} \vee \mathfrak{B})$, $(\mathfrak{A} \rightarrow \mathfrak{B})$ и $\overline{}\mathfrak{A}$.

В таком случае для доказательства каких-либо утверждений о формулах можно применять принцип полной индукции. Такое доказательство имеет следующий вид. Утверждение доказывается для элементарных формул. Затем доказывается, что из предположения истинности этого утверждения для $\mathfrak{A}$ следует его истинность для $\forall x\,\mathfrak{A}$ и $\exists x\,\mathfrak{A}$, а из истинности его для $\mathfrak{A}$ и $\mathfrak{B}$ следует его истинность для формул (2). Отсюда делается заключение, что наше утверждение истинно для любой формулы.

Из 1° — 4° видно, что все формулы исчисления высказываний являются также формулами исчисления предикатов. В самом деле, в числе формул исчисления предикатов находятся переменные высказывания, и мы можем, исходя из них, образовывать формулы, пользуясь теми же операциями, что и в исчислении высказываний. При этом к формулам, построенным только из переменных высказываний (т. е. не включающим символов предикатов), ограничения, указанные в 4°, не относятся, так как они относятся только к формулам, содержащим предметные переменные.

Примеры формул.

1. $\exists x (F^1(x) \rightarrow \forall y\, G^2(y, z))$.

Это слово является формулой. В самом деле, $G^2(y, z)$ — переменный предикат, содержащий две свободные переменные y, z, т. е. элементарная формула. В силу 3° слово $\forall y\, G^2(y, z)$ — также формула, содержащая свободную переменную z и переменную y, связанную квантором всеобщности. В формулах $F^1(x)$ и $\forall y\, G^2(y, z)$ нет переменных, связанных в одной формуле и свободных в другой; поэтому слово $(F^1(x) \rightarrow \forall y\, G^2(y, z))$ в силу 4° является формулой, в которой x и z — свободные переменные, а y связана квантором $\forall y$. Наконец, в силу 3° слово

$$\exists x (F^1(x) \rightarrow \forall y\, G^2(y, z))$$

также является формулой, в которой переменная x связана квантором $\exists x$, переменная y связана квантором $\forall y$, а переменная z свободна.

2. $(\forall x\, F^1(x) \vee \forall x\, \exists y\, G^2(x, y))$.

Легко видеть, что $\forall x\, F^1(x)$ является формулой, в которой x — связанная переменная, а $\forall x\, \exists y G^2(x, y)$ — формула, в которой обе переменные связаны. Формулы эти удовлетворяют условию из 4°, так как в них все переменные связаны. Поэтому исходное слово является формулой.

3. $(\exists x\; F^1(x)\; \&\; \exists y\, G^2(x, y))$.

Это слово не является формулой. Оба слова $\exists x\, F^1(x)$ и $\exists y\, G^2(x, y)$ являются формулами, но в первом переменная x связана, а во втором свободна. Следовательно, эти формулы не удовлетворяют условию из 4°, и, соединив их знаком &, мы не получим формулы.

Для формул исчисления предикатов можно, как и в исчислении высказываний, определить понятие *части формулы.*

Частью элементарной формулы является она сама.

Частью формулы $\forall x\mathfrak{A}$ (или $\exists x\mathfrak{A}$) является сама формула и всякая часть формулы $\mathfrak{A}$.

Частями формул $(\mathfrak{A}\,\&\,\mathfrak{B})$, $(\mathfrak{A}\vee\mathfrak{B})$ и $(\mathfrak{A}\to\mathfrak{B})$ являются сами эти формулы и все части формул $\mathfrak{A}$ и $\mathfrak{B}$.

Частями формулы $\neg\mathfrak{A}$ является сама эта формула и все части формулы $\mathfrak{A}$.

В записи формул мы внесем некоторые изменения. Во-первых, мы будем опускать некоторые скобки. Правила опускания скобок здесь остаются те же, что и в исчислении высказываний. Во-вторых, опускаются внешние скобки. Например, формулу $(A\,\&\,F^1(x))$ мы будем записывать в виде

$$A\,\&\,F^1(x),$$

формулу $(\forall x\,G^1(x)\vee A)$ — в виде

$$\forall x\,G^1(x)\vee A$$

и т. д. Далее, будем опускать скобки, сообразуясь с правилом, что & связывает сильнее, чем $\vee$ и $\to$, а $\vee$ связывает сильнее, чем $\to$. Например, формулу

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

будем записывать в виде

$$A\,\&\,B\vee C,$$

а формулу

$$(B\to(F^1(x)\vee G^1(y)))$$

будем писать в виде

$$B\to F^1(x)\vee G^1(y).$$

Чтобы облегчить чтение длинных формул, мы разрешим заменять некоторые круглые скобки прямыми. Например, выражение

$$\exists x\,[F(x)\to\forall y\,G(y,z)]$$

также будем считать формулой.

Знак отрицания будем ставить над формулой, т. е. вместо $-\mathfrak{A}$ будем писать $\overline{\mathfrak{A}}$. При этом, если $\mathfrak{A}$ имеет внешние скобки, то в формуле $\overline{\mathfrak{A}}$ будем их опускать.

Наконец, в записи предиката $F^p(x_1, \ldots, x_p)$ мы будем опускать индекс p, а знак отрицания, относящийся к предикату, будем ставить над символом предиката, например: $\bar{A}(x, y)$.

Мы условимся только, что в формуле буквы, изображающие предикаты с разным числом переменных, различны. В записи формулы предикат нельзя спутать с переменным высказыванием, так как он в формуле всегда входит в слово вида $F^p(x_1, \ldots, x_p)$, т. е. вместе с переменными предметами, чего никогда не бывает с переменным высказыванием.

Примеры.

1. Формула $(-\forall y\, \forall x\, A^2(x, y)) \vee (C \,\&\, -\exists y\, B^1(y))$ сокращенно может быть записана в виде

$$\overline{\forall y\, \forall x\, A(x, y)} \vee C \,\&\, \overline{\exists y\, B(y)}.$$

2. Формула $-\forall x - \exists y\, F^2(x, y)$ запишется в виде

$$\overline{\forall x\, \overline{\exists y\, F(x, y)}}.$$

3. Формула $(\exists x\, \forall y - (\forall z(H^1(x) - G^2(y, z))))$ запишется так:

$$\exists x\, \forall y\, \overline{\forall z\, (H(x) \to G(y, z))}.$$

Мы могли бы, как и для исчисления высказываний, дать такое определение формулы, при котором получится сразу та запись, к которой мы пришли после указанных изменений. Однако такая форма создала бы большие неудобства для определения формулы.

Введем понятие области действия квантора. Пусть формула имеет вид $\forall x\, \mathfrak{A}$ или $\exists x\, \mathfrak{A}$. *Тогда областью действия квантора* $\forall x$ (соответственно $\exists x$) *называется формула* $\mathfrak{A}$.

Из условия 4° относительно несовпадения обозначений свободных и связанных переменных следует:

а) *в формуле свободные и связанные переменные обозначены разными буквами*;

b) *если какой-либо квантор находится в области действия другого квантора, то переменные, связанные этими кванторами, обозначены разными буквами.*

Докажем утверждения a) и b). Утверждение a) очевидно для элементарных формул, так как в них нет связанных переменных. Допустим, что a) справедливо для формулы $\mathfrak{A}(x)$, содержащей свободую переменную x. Тогда a) справедливо и для формул $\forall x\, \mathfrak{A}$ и $\exists x\, \mathfrak{A}$. Действительно, все связанные переменные, входящие в $\forall x\, \mathfrak{A}$ и $\exists x\, \mathfrak{A}$, кроме x, связаны и в формуле $\mathfrak{A}$ и поэтому, по условию, отличаются от свободных переменных формулы $\mathfrak{A}$. Тем более они отличны от свободных переменных в $\forall x\, \mathfrak{A}$ и $\exists x\, \mathfrak{A}$.

Допустим, что a) справедливо для формул $\mathfrak{A}$ и $\mathfrak{B}$. Тогда a) справедливо для формул $\mathfrak{A} \,\&\, \mathfrak{B}$, $\mathfrak{A} \vee \mathfrak{B}$, $\mathfrak{A} \rightarrow \mathfrak{B}$, если только эти выражения являются формулами. В самом деле, для того чтобы можно было составить эти формулы, необходимо, чтобы свободные переменные в $\mathfrak{A}$ отличались от связанных переменных в $\mathfrak{B}$ и наоборот. Но тогда, если в $\mathfrak{A}$ и в $\mathfrak{B}$ не было одинаковых свободных и связанных переменных, то их не будет и во вновь образованных формулах $\mathfrak{A} \,\&\, \mathfrak{B}$, $\mathfrak{A} \vee \mathfrak{B}$ и $\mathfrak{A} \rightarrow \mathfrak{B}$. Если утверждение a) справедливо для $\mathfrak{A}$, то оно, очевидно, справедливо и для $\overline{\mathfrak{A}}$.

Таким образом, мы доказали по индукции справедливость утверждения a).

Докажем утверждение b). Оно, очевидно, справедливо для элементарных формул.

Допустим, что b) справедливо для формулы $\mathfrak{A}$, содержащей свободную переменную x. В силу индуктивного предположения, если один квантор в $\mathfrak{A}$ входит в область действия другого квантора, то связанные этими кванторами переменные различны. В формулах $\forall x\, \mathfrak{A}$ и $\exists x\, \mathfrak{A}$ появляется еще один квантор, в область действия которого входят все остальные кванторы. Но переменная x отличается от всех остальных связанных переменных в этих формулах, так как x в $\mathfrak{A}$ свободна и, следовательно, не совпадает ни с какой связанной переменной. Если b) справедливо для формул $\mathfrak{A}$ и $\mathfrak{B}$, то b) справедливо и для формул $\mathfrak{A} \,\&\, \mathfrak{B}$, $\mathfrak{A} \vee \mathfrak{B}$ и $\mathfrak{A} \rightarrow \mathfrak{B}$, так как если один квантор такой формулы входит в область действия другого, то оба эти квантора принадлежат одной из формул $\mathfrak{A}$ или $\mathfrak{B}$ и в силу индуктивного предположения связанные этими кванторами переменные различны. Таким образом, и утверждение b) доказано.

Итак, для того чтобы слово из символов исчисления предикатов было формулой, необходимо, чтобы соблюдались свойства a) и b). Нарушение этих условий мы будем называть *коллизией переменных*.

Пример.

$$\forall x\, [F(x) \to \exists x\, G(x, y)].$$

Это слово не является формулой, так как для него не удовлетворяется b). Легко видеть, что оно не может быть построено операциями 3° и 4° из элементарных формул. В самом деле, из формул $F(x)$ и $\exists x\, G(x, y)$ нельзя составить формулы $F(x) \to \exists x\, G(x, y)$, так как эти формулы не удовлетворяют условию из 4°. Но слово

$$\forall x\, F(x)\, \&\, \exists x\, G(x, y)$$

является формулой, так как мы не требовали, чтобы при составлении формул $\mathfrak{A}\, \&\, \mathfrak{B}$, $\mathfrak{A} \vee \mathfrak{B}$ и $\mathfrak{A} \to \mathfrak{B}$ из $\mathfrak{A}$ и $\mathfrak{B}$ переменные, связанные различными кванторами в формулах $\mathfrak{A}$ и $\mathfrak{B}$, были различными.

§ 2. Замена переменных в формулах

Теорема. *Если в формуле $\mathfrak{A}$ переменить обозначения переменных как свободных, так и связанных, меняя букву на другую всюду, где она входит, так, чтобы при этом удовлетворялись условия* a) *и* b), *то полученное таким образом слово будет формулой.*

Это справедливо для элементарных формул, например для $F(x, y, z)$, так как, заменяя произвольным образом предметные переменные, входящие в предикат, мы снова получим предикат, т. е. элементарную формулу. Допустим, что наше утверждение справедливо для формулы $\mathfrak{A}$, содержащей свободную переменную x. Переменим обозначения предметных переменных в формуле $\forall x\, \mathfrak{A}$, не нарушая условий a) и b). Если при этом буква x заменена новой буквой, например y, то y должно отличаться от переменных, которыми заменены все остальные переменные формулы $\mathfrak{A}$, так как всякая отличная от x переменная либо свободна в $\forall x\, \mathfrak{A}$, либо связана квантором, находящимся в области действия квантора $\forall x$. Так как произведенное нами переименование переменных в формуле $\forall x\, \mathfrak{A}$, а следовательно, и в формуле $\mathfrak{A}$ удовлетворяет условиям a) и b), то в силу индуктивного предположения выражение $\mathfrak{A}'(y)$, полученное в результате этого переименования переменных из $\mathfrak{A}(x)$, является формулой. И так как все связанные переменные, входящие в $\mathfrak{A}'(y)$, отличны от y, то слово $\forall y\, \mathfrak{A}'(y)$ является формулой, что и требовалось доказать.

Таким же образом можно показать, что если наше утверждение верно для $\mathfrak{A}$, то оно верно и для $\exists x\, \mathfrak{A}$.

Допустим, что наше утверждение справедливо для формул $\mathfrak{A}$ и $\mathfrak{B}$ таких, что связанные переменные одной формулы отличны от свободных переменных другой. Докажем, что оно справедливо и для формулы $\mathfrak{A} \,\&\, \mathfrak{B}$. Переименуем переменные этой формулы так, чтобы удовлетворялись условия a) и b). После этого части $\mathfrak{A}$ и $\mathfrak{B}$ нашей формулы превращаются в $\mathfrak{A}'$ и $\mathfrak{B}'$. В силу индуктивного предположения слова $\mathfrak{A}'$ и $\mathfrak{B}'$, полученные из $\mathfrak{A}$ и $\mathfrak{B}$ переименованием переменных, удовлетворяющим условиям a) и b), являются формулами. В силу условия a) связанные переменные в $\mathfrak{A}'$ отличаются от свободных переменных в $\mathfrak{B}'$ и наоборот. Поэтому слово $\mathfrak{A}' \,\&\, \mathfrak{B}'$, составленное из $\mathfrak{A}'$ и $\mathfrak{B}'$, является формулой, что и требовалось доказать.

Таким же образом можно показать, что наше утверждение верно для формул $\mathfrak{A} \vee \mathfrak{B}$ и $\mathfrak{A} \rightarrow \mathfrak{B}$, если оно верно для $\mathfrak{A}$ и для $\mathfrak{B}$. Для операции отрицания наше утверждение очевидно.

Таким образом, теорема доказана для любой формулы.

Заметим, что указанные выше способы переименования предметных переменных не исчерпывают всех тех, при которых формула остается формулой. Например, в формуле

$$\forall x\, [F(x) \vee G(y)]$$

переименование буквы y в букву x не допускается нашими требованиями, так как переменная y свободна, а x связана. Однако если такую замену произвести, то получится слово

$$\forall x\,[F(x) \vee G(x)],$$

которое является формулой. Таким образом, условия a) и b) не являются необходимыми для того, чтобы в результате переименования переменных из формулы снова получилась формула. В дальнейшем нам понадобятся только переименования переменных, удовлетворяющие условиям a) и b), и мы не будем искать более широких.

§ 3. Аксиомы исчисления предикатов

Определение выводимых формул мы будем формулировать тем же способом, который мы применяли при описании исчисления высказываний. Условимся считать некоторые определенные формулы, заданные в конечном числе, выводимыми и будем их называть аксиомами исчисления предикатов. Затем укажем правила образования новых выводимых формул из тех, которые уже получены, или же из аксиом. Те и только те формулы, которые можно получить применением этих правил, исходя из аксиом, мы будем считать выводимыми.

Аксиомы исчисления предикатов

I

1. $A \to (B \to A)$.
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.

II

1. $A \& B \to A$.
2. $A \& B \to B$.
3. $(A \to B) \to ((A \to C) \to (A \to B \& C))$.

III

1. $A \to A \vee B$.
2. $B \to A \vee B$.
3. $(A \to C) \to ((B \to C) \to (A \vee B \to C))$.

IV

1. $(A \to B) \to (\overline{B} \to \overline{A})$.
2. $A \to \overline{\overline{A}}$.
3. $\overline{\overline{A}} \to A$.

V

1. $\forall x\, F(x) \to F(y)$.
2. $F(y) \to \exists x\, F(x)$.

Первые четыре группы аксиом представляют собой не что иное, как аксиомы исчисления высказываний (см. стр. 72). К ним добавляются еще две новые аксиомы, составляющие группу V. Этим и исчерпывается система аксиом исчисления предикатов.

§ 4. Правила образования выводимых формул

1. Правило заключения. *Если G и $G \to H$ — выводимые формулы, то H — также выводимая формула.*

Это правило формулируется так же, как и в исчислении высказываний. Только объем формул, к которым применяется это правило, здесь шире.

2. Правило подстановки в переменное высказывание и переменный предикат. Это правило аналогично правилу подстановки, которое мы имели для исчисления высказываний (см. главу II). Там оно сводилось к тому, что, заменяя переменные высказывания в выводимой формуле любой формулой, мы получали выводимую формулу. В логике предикатов мы будем иметь дело с заменой переменных высказываний и переменных предикатов формулами. Но в то время как в исчислении высказываний формула, которой заменяется переменное высказывание в выводимой формуле, могла быть совершенно произвольной, здесь необходимо наложить некоторые дополнительные условия на эти формулы, так как иначе в результате подстановки может получиться выражение, даже не являющееся формулой.

Мы сначала опишем нужные нам операции замены для любой формулы независимо от того, выводима она или нет, и притом пока не строгим, но более наглядным образом.

Замена переменного высказывания. Пусть формула $\mathfrak{A}(A)$ содержит переменное высказывание A. Тогда мы можем заменить в формуле $\mathfrak{A}$ букву A всюду, где она входит, любой формулой $\mathfrak{B}$, удовлетворяющей следующим условиям.

$\mathfrak{b}^1$. *Свободные переменные в $\mathfrak{B}$ обозначены буквами, отличными от связанных переменных в $\mathfrak{A}$, и связанные переменные в $\mathfrak{B}$ — буквами, отличными от свободных переменных в $\mathfrak{A}$.*

$\mathfrak{b}^2$. *Если A в $\mathfrak{A}$ находится в области действия квантора, обозначенного какой-то буквой, то эта буква не входит в $\mathfrak{B}$.*

Такая замена называется *подстановкой формулы $\mathfrak{B}$ в переменную A.*

Пример. Пусть $\mathfrak{A}(A)$ есть формула

$$\forall x \forall y [A \vee \forall z H(z, x) \& (\bar{A} \vee F(x, y))].$$

В таком случае A нельзя заменить формулой $\forall x \mathfrak{B}(x)$ или формулой $\exists x \mathfrak{C}(x)$, так как при такой замене не соблюдено условие $\mathfrak{b}^2$. Если все же произвести эту замену, то полученное слово не будет формулой, так как в нем два квантора, один из которых находится в области действия другого, обозначены одинаковыми буквами. Замена буквы A формулой

$$\forall z \forall t [A \& H(z, t) \vee B \& F(z, t)]$$

возможна, так как в этом случае условия $\mathfrak{b}^1$, $\mathfrak{b}^2$ выполнены. Полученное в результате такой замены слово

$$\forall x \forall y \{\forall z \forall t (A \& H(z, t) \vee B \& F(z, t)) \vee \forall z H(z, x) \& \\ \& [\overline{\forall z \forall t (A \& H(z, t) \vee B \& F(z, t))} \vee F(x, y)]$$

является формулой.

Замена переменного предиката. Пусть формула $\mathfrak{A}(F)$ содержит переменный предикат F от n переменных, и пусть имеется формула $\mathfrak{B}(t_1, t_2, \ldots, t_n)$, содержащая n свободных переменных $t_1, t_2, \ldots, t_n$ (вообще говоря, $\mathfrak{B}$ может содержать и другие переменные), где $t_1, t_2, \ldots, t_n$ — буквы, отличные от всех предметных переменных формулы $\mathfrak{A}$. Если для формулы $\mathfrak{B}$ соблюдено условие $\mathfrak{b}^1$ и еще условие:

$\mathfrak{b}_2^2$. *Если F в $\mathfrak{A}$ находится в области действия квантора, связывающего какую-либо букву, то эта буква не входит в* $\mathfrak{B}$, то возможна подстановка формулы $\mathfrak{B}$ в $\mathfrak{A}$ вместо предиката F. Операция подстановки формулы $\mathfrak{B}(t_1, \ldots, t_n)$ в формулу $\mathfrak{A}(F)$ вместо $F(\ldots)$ представляет собой замену каждой элементарной формулы вида $F(x_1, x_2, \ldots, x_n)$ (где $x_1, x_2, \ldots, x_n$ — какие-то переменные, не обязательно различные), входящей в $\mathfrak{A}(F)$, выражением, полученным из $\mathfrak{B}$ переименованием переменных $t_1, t_2, \ldots, t_n$ буквами $x_1, x_2, \ldots, x_n$ соответственно. При этом должно быть жестко указано, какой из переменных $t_1, t_2, \ldots, t_n$ соответствует каждое пустое место в $F(\ldots)$.

Пример. Пусть формула $\mathfrak{A}$ имеет вид

$$\forall x \exists y \exists z [F(x, y) \vee \overline{F}(x, z)].$$

Требуется произвести подстановку, заменив F формулой

$$\forall u \exists v [H(u, t_1) \vee H(v, t_2)].$$

Пусть при этом первое пустое место в $F(\ldots)$ соответствует переменной t_1, а второе — переменной t_2. Условия $\mathfrak{b}^1$ и $\mathfrak{b}_2^2$ здесь выполнены, и результатом подстановки будет формула

$$\forall x \exists y \exists z \{\forall u \exists v [H(u, x) \vee H(v, y)] \vee \\ \vee \overline{\forall u \exists v [H(u, x) \vee H(v, z)]}\}$$

Легко видеть, что если условия $\mathfrak{b}^1$, $\mathfrak{b}^2$ или $\mathfrak{b}_2^2$ не выполнены, то, вообще говоря, в результате замены будут получаться выражения, не являющиеся формулами.

Примеры.

1. Требуется в формулу

$$A \vee \forall x F(x)$$

подставить $U(x)$ вместо A. Получится слово

$$U(x) \vee \forall x F(x),$$

которое не является формулой в силу возникшей коллизии переменных; здесь не соблюдено условие $\mathfrak{b}^1$.

2. Требуется в формулу

$$\forall x (A \to F(x))$$

подставить $\forall x U(x)$ вместо A. Получится слово

$$\forall x (\forall x U(x) \to F(x)),$$

которое не является формулой. В рассматриваемой подстановке не соблюдено условие $\mathfrak{b}^2$.

Другое определение операции подстановки. Операцию подстановки мы будем изображать символом

$$R_A^{\mathfrak{B}} \left(\text{соответственно } R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}\right),$$

поставленным перед той формулой, в которую производится подстановка, например:

$$R_A^{\mathfrak{B}}(\mathfrak{A}) \left(\text{соответственно } R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A})\right),$$

где A представляет собой переменное высказывание, а F — переменный предикат от n переменных. Формула $\mathfrak{B}(t_1, \ldots, t_n)$ в числе своих свободных предметных переменных содержит особо отмеченные переменные $t_1, \ldots, t_n$, число которых равно числу переменных предиката F, т. е. n.

Если формула $\mathfrak{A}$ содержит переменное высказывание A (соответственно переменный предикат F), то операция подстановки

$$R_A^{\mathfrak{B}}(\mathfrak{A}) \left(\textit{соответственно } R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A})\right)$$

применяется, если для формул $\mathfrak{B}$ и $\mathfrak{A}$ (соответственно для $\mathfrak{B}(t_1, \ldots, t_n)$ и $\mathfrak{A}$) выполнены условия $\mathfrak{b}^1$ и $\mathfrak{b}^2$ (соответственно $\mathfrak{b}^1$ и $\mathfrak{b}_2^2$) и, кроме того, условие: отмеченные переменные $t_1, \ldots, t_n$ не должны входить в формулу $\mathfrak{A}$.

Определение операции подстановки мы проведем по индукции, начиная с элементарных формул:

$$R_A^{\mathfrak{B}}(A) \quad \textit{есть} \quad \mathfrak{B},$$

$$R_A^{\mathfrak{B}}(C) \quad \textit{есть} \quad C,$$

если C — переменное высказывание, отличное от A;

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(F(x_1, \ldots, x_n)) \quad \textit{есть} \quad \mathfrak{B}(x_1, \ldots, x_n);$$

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(G(x_1, \ldots, x_m)) \quad \textit{есть} \quad G(x_1, \ldots, x_m),$$

если $G(x_1, \ldots, x_m)$ — *переменный предикат, отличный от* $F(x_1, \ldots, x_n)$.

Допустим, что операция подстановки определена для формул $\mathfrak{A}_1$ *и* $\mathfrak{A}_2$. *Тогда операция подстановки для формул* $\mathfrak{A}_1 \& \mathfrak{A}_2$, $\mathfrak{A}_1 \vee \mathfrak{A}_2$, $\mathfrak{A}_1 \to \mathfrak{A}_2$ *и* $\overline{\mathfrak{A}}$ *определяется следующим образом:*

$$R_A^{\mathfrak{B}}(\mathfrak{A}_1 \& \mathfrak{A}_2) \quad \text{есть} \quad R_A^{\mathfrak{B}}(\mathfrak{A}_1) \& R_A^{\mathfrak{B}}(\mathfrak{A}_2);$$

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_1 \& \mathfrak{A}_2) \quad \text{есть}$$

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_1) \& R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_2);$$

$$R_A^{\mathfrak{B}}(\mathfrak{A}_1 \vee \mathfrak{A}_2) \quad \text{есть} \quad R_A^{\mathfrak{B}}(\mathfrak{A}_1) \vee R_A^{\mathfrak{B}}(\mathfrak{A}_2);$$

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_1 \vee \mathfrak{A}_2) \quad \text{есть}$$

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_1) \vee R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_2);$$

$$R_A^{\mathfrak{B}}(\mathfrak{A}_1 \to \mathfrak{A}_2) \quad \text{есть} \quad R_A^{\mathfrak{B}}(\mathfrak{A}_1) \to R_A^{\mathfrak{B}}(\mathfrak{A}_2);$$

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_1 \to \mathfrak{A}_2) \quad \text{есть}$$

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_1) \to R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_2);$$

$$R_A^{\mathfrak{B}}(\overline{\mathfrak{A}}) \quad \text{есть} \quad \overline{R_A^{\mathfrak{B}}(\mathfrak{A})},$$

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\overline{\mathfrak{A}}) \quad \text{есть} \quad \overline{R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A})}.$$

Пусть операции $R_A^{\mathfrak{B}}(\mathfrak{A}(x))$ *и соответственно* $R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}(x))$ *определены. Тогда*

$$R_A^{\mathfrak{B}}(\forall x\, \mathfrak{A}(x)) \quad \text{есть} \quad \forall x\, R_A^{\mathfrak{B}}(\mathfrak{A}(x))$$

и

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\forall x\, \mathfrak{A}(x)) \quad \text{есть} \quad \forall x\, R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}(x)).$$

Аналогичным образом

$$R_A^{\mathfrak{B}}(\exists x\, \mathfrak{A}(x)) \quad \text{есть} \quad \exists x\, R_A^{\mathfrak{B}}(\mathfrak{A}(x))$$

и

$$R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\exists x\, \mathfrak{A}(x)) \quad \text{есть} \quad \exists x\, R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}(x)).$$

Этими соотношениями операция подстановки полностью определена.

Нетрудно доказать, что если операция подстановки применяется с соблюдением всех указанных условий, то в результате опять получается формула. Мы на этом не будем останавливаться.

3. Правило замены свободной предметной переменной. *Пусть формула $\mathfrak{A}$ является выводимой формулой в исчислении предикатов и формула $\mathfrak{A}'$ получена из $\mathfrak{A}$ заменой любой свободной предметной переменной другой свободной предметной переменной, так что заменяемая переменная заменяется одинаковым образом всюду, где она в формулу $\mathfrak{A}$ входит; тогда $\mathfrak{A}'$ является выводимой формулой исчисления предикатов.*

Конечно, мы предполагаем, что указанная замена переменных не должна приводить к коллизии переменных. Это, впрочем, уже вытекает из предположения, что $\mathfrak{A}'$ также должна быть формулой.

Пример. Рассмотрим формулу

$$\forall x\,(F(x) \to G(y))\,\&\,(\overline{F}(y) \to \exists x\,G(x)).$$

Произведем в ней подстановку, заменив переменную y переменной z; получим формулу

$$\forall x\,(F(x) \to G(z))\,\&\,(\overline{F}(z) \to \exists x\,G(x)).$$

Переменную y мы заменили, как это и требуется, всюду, где она входит. Заметим, что нельзя заменить переменную y переменной x, так как, согласно определению, свободная переменная y должна заменяться только свободной переменной.

4. Правило переименования связанных предметных переменных. *Если формула $\mathfrak{A}$ является выводимой формулой исчисления предикатов, то формула $\mathfrak{A}'$, полученная из $\mathfrak{A}$ заменой связанных переменных другими связанными переменными, отличными от всех свободных переменных формулы $\mathfrak{A}$, также является выводимой формулой. При этом заменяемая связанная переменная в формуле $\mathfrak{A}$ должна заменяться одинаковым образом всюду в области действия квантора, связывающего данную переменную, и в самом кванторе.*

Операция переименования связанных переменных существенно отличается от операции подстановки в свободные переменные. Производя переименование связанных переменных, мы уже не обязаны переименовывать их всюду, где они входят в формулу $\mathfrak{A}$, а лишь только в области действия квантора, связывающего данную переменную. Это значит, что такие одинаковые переменные, для которых связывающие их кванторы имеют разные области действия, могут переименовываться разным образом или одна из них может переименовываться, а другая нет.

Примеры.

1. Рассмотрим формулу

$$\exists x\, F(x) \to \forall x\, G(x).$$

Применив операцию переименования связанных переменных, мы можем из данной формулы получить следующую:

$$\exists y\, F(y) \to \forall z\, G(z).$$

Здесь мы переменную x в области действия одного квантора заменили переменной y, а в области действия другого квантора — переменной z.

Поскольку области действия этих кванторов различны, мы совершили переименование связанных переменных правильно. Переименовывая иначе связанные переменные, мы из той же формулы можем получить формулу

$$\exists x\, F(x) \to \forall z\, G(z).$$

2. Рассмотрим формулу

$$\exists v\, \exists x\, \forall y\, [(F(x, y) \vee \exists z\, G(z))\, \&\, G(y) \vee H(v)].$$

Переименовывая в этой формуле переменную y, мы должны заменить ее одинаковым образом всюду, где она входит. Переименование, приводящее к формуле

$$\exists v\, \exists x\, \forall u\, [(F(x, u) \vee \exists z G(z))\, \&\, G(u) \vee H(v)],$$

является вполне правильным, но замена переменной y, приводящая к формуле

$$\exists v\, \exists x\, \forall u\, [(F(x, u) \vee \exists z G(z))\, \&\, G(v) \vee H(v)],$$

не является правильным переименованием связанных переменных, так как в этом случае мы переменную y в области действия одного и того же квантора $\forall y$ переименовали разным образом, в одном месте заменив ее переменной u, а в другом переменной v.

5. Правила связывания квантором. Первое правило связывания квантором.

Если

$$\mathfrak{B} \to \mathfrak{A}(x)$$

— выводимая формула и $\mathfrak{B}$ не содержит переменной x, то

$$\mathfrak{B} \to \forall x\, \mathfrak{A}(x)$$

— также выводимая формула.

Второе правило связывания квантором.

Если

$$\mathfrak{A}(x) \to \mathfrak{B}$$

— выводимая формула и $\mathfrak{B}$ не содержит переменной x, то

$$\exists x\, \mathfrak{A}(x) \to \mathfrak{B}$$

— также выводимая формула *).

Заметим, что *среди выводимых формул исчисления предикатов находятся все выводимые формулы исчисления высказываний.* В самом деле, исчисление предикатов содержит в числе своих аксиом все аксиомы исчисления высказываний, а в числе правил образования выводимых формул — оба правила вывода исчисления высказываний: правило заключения и правило подстановки. В применении к формулам исчисления высказываний эти два правила исчисления предикатов совпадают с теми же правилами исчисления высказываний (см. главу II). Таким образом, мы можем, применяя эти правила к аксиомам, получить все выводимые формулы исчисления высказываний. Вопрос о том, существуют ли формулы исчисления высказываний, выводимые в исчислении предикатов, но не выводимые в исчислении высказываний, решается отрицательно. Это легко следует из непротиворечивости исчисления предикатов и полноты исчисления высказываний в узком смысле. Об этом мы будем говорить в следующем параграфе.

*) В первом и втором правилах связывания квантором речь идет о вполне определенной предметной переменной x. Однако посредством правил подстановки в свободную предметную переменную и переименования связанных переменных она легко распространяется на любую предметную переменную.

Поставим вопрос о соотношении между понятием выводимой формулы описанного исчисления и рассмотренным в главе III содержательным понятием тождественно истинной формулы. Нетрудно видеть, что *каждая выводимая формула исчисления предикатов является в то же время и тождественно истинной в наивном теоретико-множественном смысле.* Во-первых, очевидно, что аксиомы исчисления предикатов тождественно истинны. Во-вторых, применение правил вывода исчисления предикатов к тождественно истинным формулам приводит к тождественно истинным формулам. Это очевидно для правила заключения. Для правил переименования свободных и связанных переменных это также очевидно.

Рассмотрим правило подстановки. $R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A})$ есть результат замены в формуле $\mathfrak{A}$ элементарного предиката $F(\ldots)$ формулой $\mathfrak{B}(t_1, \ldots, t_n)$ всюду, где он входит в $\mathfrak{A}$. При этом всякий раз переменные $t_1, \ldots$ $\ldots, t_n$ заменяются соответствующими переменными заменяемого символа $F(\ldots)$. Но формулу $\mathfrak{B}(t_1, \ldots, t_n)$ можно также рассмотреть как предикат от n переменных, если фиксировать значения всех остальных свободных переменных. Так как по условию формула $\mathfrak{A}$ истинна для каждой области и при любой замене переменных предикатов индивидуальными, то, очевидно, она истинна и при замене F формулой $\mathfrak{B}(t_1, \ldots, t_n)$. Случай правила подстановки в переменное высказывание очевиден.

Рассмотрим правила связывания квантором. Пусть

$$\mathfrak{B} \to \mathfrak{A}(x) \tag{1}$$

— тождественно истинная формула и $\mathfrak{B}$ не содержит переменной x. Тогда в содержательном смысле $\mathfrak{B}$ для любой области и любых предикатов не зависит от x. Если формула $\mathfrak{B}$ оказалась при некоторой замене переменных истинной, то она истинна для каждого значения x при данной замене остальных переменных. Так как формула (1) по условию истинна, то и $\mathfrak{A}(x)$ истинна при любом x и данной замене остальных переменных. Но тогда и формула $\forall x\, \mathfrak{A}(x)$, а следовательно, и формула

$$\mathfrak{B} \to \forall x\, \mathfrak{A}(x) \tag{2}$$

истинны при данной замене остальных переменных. Если же при некоторой замене переменных формула $\mathfrak{B}$ ложна, то формула (2) также истинна. Итак, формула (2) является тождественно истинной формулой, что и требовалось доказать.

Таким же образом доказывается, что применение второго правила связывания квантором к тождественно истинной формуле приводит к тождественно истинной формуле.

Итак, мы показали, что всякая формула, выведенная из аксиом по правилам исчисления предикатов, является тождественно истинной формулой в содержательном смысле. Заметим, что мы вместе с тем получаем и доказательство непротиворечивости исчисления предикатов на основе наивной теории множеств.

В самом деле, если каждая доказуемая в исчислении предикатов формула тождественно истинна, то две формулы, из которых одна является отрицанием другой, не могут быть обе доказуемы, так как не могут быть одновременно тождественно истинными. Однако приведенное доказательство непротиворечивости опирается на понятие актуальной бесконечности. Оно не может быть употреблено при решении вопроса о непротиворечивости самой теории множеств, так как это привело бы к порочному кругу. Впрочем, строгое доказательство непротиворечивости исчисления предикатов, которое мы рассмотрим в следующем параграфе, основано на той же идее, что и приведенное здесь.

§ 5. Непротиворечивость исчисления предикатов

Вопрос о непротиворечивости исчисления предикатов легко решается в положительном смысле. Постановка вопроса о непротиворечивости исчисления предикатов та же самая, что и для исчисления высказываний: *противоречивым называется такое исчисление, в котором какая-либо формула доказуема вместе со своим отрицанием.*

Для исчисления предикатов и для любой логической системы, полученной из исчисления предикатов присоединением в качестве аксиом новых формул, так же, как и для исчисления высказываний, можно утверждать, что если бы эта системы была противоречивой, то в ней была бы выводима произвольная формула. В самом деле, допустим, что мы доказали в исчислении предикатов как формулу $\mathfrak{A}$, так и формулу $\overline{\mathfrak{A}}$. Формула

$$A \mathbin{\&} \overline{A} \to B$$

является выводимой формулой исчисления предикатов, так как она выводима в исчислении высказываний. Выполнив подстановку, получим выводимую формулу

$$\mathfrak{A} \mathbin{\&} \overline{\mathfrak{A}} \to B.$$

На основании правила заключения утверждаем, что B — выводимая формула. Произведя подстановку в B произвольной формулы $\mathfrak{B}$, находим, что $\mathfrak{B}$ — выводимая формула. Таким образом, и для исчисления предикатов обнаружение какой-либо невыводимой формулы является доказательством ее непротиворечивости.

Схема доказательства непротиворечивости состоит в следующем. Мы будем рассматривать формулы содержательным образом и понимать их так, как это делалось в предыдущей главе. Именно, мы будем считать, что все предикаты, входящие в формулы, определены на некоторой области $\mathfrak{M}$. Если эта область состоит из одного элемента, то кванторы можно отбросить, так как оба высказывания $\forall x \mathfrak{A}(x)$ и $\exists x \mathfrak{A}(x)$ для области, состоящей из одного элемента a, равносильны высказыванию $\mathfrak{A}(a)$. При такой интерпретации все формулы исчисления предикатов заменяются формулами исчисления высказываний. При этом все аксиомы исчисления предикатов будут выводимыми формулами исчисления высказываний, а правила исчисления предикатов преобразуются в правила исчисления высказываний, основные или выводимые. Если бы в исчислении предикатов была доказуема формула, являющаяся буквой A, то в преобразованной системе она также была бы доказуема. Но тогда преобразованная система была бы противоречива. Но преобразованная система является исчислением высказываний, которое, как известно (см. § 9 главы II), непротиворечиво. После этих предварительных замечаний дадим формальное доказательство непротиворечивости исчисления предикатов.

Поставим в соответствие каждой формуле исчисления предикатов формулу $\mathfrak{A}^*$ по следующему закону: переменному высказыванию ставим в соответствие это же переменное высказывание.

Элементарной формуле вида $F(x, y, \ldots, u)$ ставим в соответствие букву F.

Если формулам $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}$, $\mathfrak{B}(x)$ поставлены в соответствие формулы $\mathfrak{A}_1^*$, $\mathfrak{A}_2^*$, $\mathfrak{A}^*$, $\mathfrak{B}^*(x)$, то формулам

$$1)\ \mathfrak{A}_1 \,\&\, \mathfrak{A}_2, \qquad 2)\ \mathfrak{A}_1 \vee \mathfrak{A}_2, \qquad 3)\ \mathfrak{A}_1 \to \mathfrak{A}_2,$$
$$4)\ \overline{\mathfrak{A}}, \qquad 5)\ \forall x\, \mathfrak{B}(x), \qquad 6)\ \exists x\, \mathfrak{B}(x)$$

поставим в соответствие формулы

$$1')\ \mathfrak{A}_1^* \,\&\, \mathfrak{A}_2^*, \qquad 2')\ \mathfrak{A}_1^* \vee \mathfrak{A}_2^*, \qquad 3')\ \mathfrak{A}_1^* \to \mathfrak{A}_2^*,$$
$$4')\ \overline{\mathfrak{A}}^*, \qquad 5')\ \mathfrak{B}^*, \qquad 6')\ \mathfrak{B}^*.$$

Мы видим, что наличие кванторов в формуле исчисления предикатов никак не сказывается на формуле, которая ей поставлена в соответствие. Формулам $\mathfrak{B}(x)$, $\forall x\, \mathfrak{B}(x)$ и $\exists x\, \mathfrak{B}(x)$ ставится в соответствие одна и та же формула. Можно кратко описать формулу $\mathfrak{A}^*$, соответствующую формуле $\mathfrak{A}$, следующим образом: *формула $\mathfrak{A}^*$ получится из формулы $\mathfrak{A}$, если в последней зачеркнуть все кванторы и удалить ее предметные переменные, оставив от каждого элементарного предиката $F(x, y, \ldots, u)$, входящего в формулу, только букву F.* Из этого закона соответствия следует, что формулы, которые мы ставим в соответствие формулам исчисления предикатов, являются формулами исчисления высказываний. Для элементарных формул исчисления предикатов это непосредственно ясно. Составляя из элементарных формул произвольную формулу исчисления предикатов, мы применяем операции 3° и 4°, описанные в § 1 (стр. 185). Но тогда соответствующая ей формула составляется из формул, соответствующих элементарным, только операциями 4°, т. е. для всякой формулы исчисления предикатов соответствующая ей формула составляется из переменных высказываний с помощью операций исчисления высказываний и, следовательно, является сама формулой исчисления высказываний.

Покажем, что *выводимым формулам исчисления предикатов соответствуют выводимые формулы исчисления высказываний.* Доказательство проведем по индукции.

Аксиомам исчисления предикатов соответствуют выводимые формулы исчисления высказываний.

В самом деле, аксиомам групп I—IV соответствуют они сами. Эти формулы являются также аксиомами исчисления высказываний. Обеим же аксиомам группы V соответствует формула

$$F \rightarrow F,$$

которая является выводимой формулой исчисления высказываний.

Теперь мы рассмотрим все правила образования формул исчисления предикатов и докажем, что они переводят формулы, которым соответствуют выводимые формулы исчисления высказываний, в формулы, которым также соответствуют выводимые формулы исчисления высказываний.

Правило заключения в исчислении предикатов: если $\mathfrak{A}$ и $\mathfrak{A} \rightarrow \mathfrak{B}$ — выводимые формулы, то и $\mathfrak{B}$ является выводимой формулой. Но если соответствующие формулы $\mathfrak{A}^*$ и $\mathfrak{A}^* \rightarrow \mathfrak{B}^*$ — выводимые формулы исчисления высказываний, то и формула $\mathfrak{B}^*$ является выводимой формулой исчисления высказываний, так как правило заключения есть и в исчислении высказываний.

Правило подстановки в свободную предметную переменную и правило переименования связанной переменной. Заметим, что если формулы $\mathfrak{A}$ и $\mathfrak{A}'$ отличаются одна от другой только предметной переменной, то соответствующие им формулы совпадают между собой. Это непосредственно следует из того краткого описания соответствующей формулы, которое было сделано выше. Отсюда следует, что если формуле $\mathfrak{A}$ исчисления предикатов соответствует выводимая формула исчисления высказываний $\mathfrak{A}^*$, то формуле $\mathfrak{A}'$, полученной из $\mathfrak{A}$ переименованием предметных переменных или подстановкой в свободную переменную, соответствует та же выводимая формула $\mathfrak{A}^*$.

Правило подстановки. Докажем сначала, что *если H — формула, получившаяся в результате подстановки,* *при которой в формуле $\mathfrak{A}$ буква A или же предикат $F(\ldots)$ заменены формулой $\mathfrak{B}$, то соответствующая H формула H^* получается в результате замены в формуле $\mathfrak{A}^*$ буквы A или F формулой $\mathfrak{B}^*$.* Применяя символ операции подстановки, наше утверждение можно записать так:

$$\left[R_A^{\mathfrak{B}}(\mathfrak{A})\right]^* \quad \text{есть} \quad R_A^{\mathfrak{B}^*}(\mathfrak{A}^*)$$

и

$$\left[R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A})\right]^* \quad \text{есть} \quad R_F^{\mathfrak{B}^*}(\mathfrak{A}^*)\ {}^{*)}.$$

Это утверждение, очевидно, справедливо, если $\mathfrak{A}$ — элементарная формула A или F.

Будем далее рассматривать операции образования новых формул и докажем по индукции, что если наше утверждение справедливо для формул $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}(x)$, то оно справедливо и для формул, полученных из этих применением логических операций конъюнкции, дизъюнкции, импликации, отрицания и связывания квантором. Это можно сделать кратко, пользуясь свойством перестановочности операций $R_A^{\mathfrak{B}}$ и $R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}$ с этими логическими операциями. Мы проведем доказательство только для оператора подстановки $R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}$ и логических операций конъюнкции и связывания квантором.

Требуется доказать, что формула

$$\left[R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_1 \mathbin{\&} \mathfrak{A}_2)\right]^*$$

совпадает с

$$R_F^{\mathfrak{B}^*}(\mathfrak{A}_1^* \mathbin{\&} \mathfrak{A}_2^*),$$

если известно, что наше утверждение справедливо для формул $\mathfrak{A}_1$ и $\mathfrak{A}_2$. В силу свойств оператора $R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}$

$$\left[R_{F(\ldots)}^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}_1 \mathbin{\&} \mathfrak{A}_2)\right]^*$$

---

*) Заметим, что операция $R_F^{\mathfrak{B}^*}(\mathfrak{A}^*)$, представляющая собой подстановку в формулу исчисления высказываний $\mathfrak{A}^*$ другой формулы $\mathfrak{B}^*$, которая также является формулой исчисления высказываний, всегда выполнима.

есть

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}_1)\,\&\,R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}_2)\right]^*. \qquad (1)$$

Но в силу соответствия между 1) и 1′) (см. стр. 204)

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}_1)\,\&\,R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}_2)\right]^*$$

есть

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}_1)\right]^*\,\&\,\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}_2)\right]^*. \qquad (2)$$

В силу индуктивного предположения

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}_1)\right]^* \quad \text{есть} \quad R_F^{\mathfrak{B}^*}(\mathfrak{A}_1^*)$$

и (3)

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}_2)\right]^* \quad \text{есть} \quad R_F^{\mathfrak{B}^*}(\mathfrak{A}_2^*).$$

Из (1), (2) и (3) следует, что

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}_1\,\&\,\mathfrak{A}_2)\right]^* \quad \text{есть} \quad R_F^{\mathfrak{B}^*}(\mathfrak{A}_1^*)\,\&\,R_F^{\mathfrak{B}^*}(\mathfrak{A}_2^*),$$

т. е. в силу свойств оператора $R_F^{\mathfrak{B}^*}$

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}_1\,\&\,\mathfrak{A}_2)\right]^* \quad \text{есть} \quad R_F^{\mathfrak{B}^*}(\mathfrak{A}_1^*\,\&\,\mathfrak{A}_2^*).$$

Рассмотрим теперь операцию связывания квантором $\forall x$. Надо доказать, что

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}\forall x\,\mathfrak{A}(x)\right]^* \quad \text{есть} \quad R_F^{\mathfrak{B}^*}[\forall x\,\mathfrak{A}(x)]^*.$$

В самом деле,

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}\forall x\,\mathfrak{A}(x)\right]^* \quad \text{есть} \quad \left[\forall x\,R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}(x))\right]^*$$

или

$$\forall x\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}(x))\right]^*.$$

В силу индуктивного предположения

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}(x))\right]^* \quad \text{есть} \quad R_F^{\mathfrak{B}^*}(\mathfrak{A}^*)$$

или, что то же,

$$\forall x\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\mathfrak{A}(x))\right]^* \quad \text{есть} \quad R_F^{\mathfrak{B}^*}[\forall x\,\mathfrak{A}(x)]^*,$$

откуда следует:

$$\left[R_{F\,(\ldots)}^{\mathfrak{B}\,(t_1,\ldots,t_n)}(\forall x\,\mathfrak{A}(x))\right]^* \quad \text{есть} \quad R_F^{\mathfrak{B}^*}[\forall x\,\mathfrak{A}(x)]^*,$$

что и требовалось доказать.

Для остальных логических операций наше утверждение доказывается точно так же.

Пусть теперь H — формула исчисления предикатов, полученная из выводимой формулы $\mathfrak{A}$ в результате подстановки формулы $\mathfrak{B}$ в $F(\ldots)$ (или в A). По предположению формуле $\mathfrak{A}$ соответствует выводимая формула исчисления высказываний $\mathfrak{A}^*$, а формуле $\mathfrak{B}$ — формула исчисления высказываний $\mathfrak{B}^*$. Но тогда, по доказанному, формуле H соответствует формула H^*, полученная в результате подстановки в выводимую формулу исчисления высказываний $\mathfrak{A}^*$ вместо F (или A) формулы $\mathfrak{B}^*$. Следовательно, H^* есть выводимая формула исчисления высказываний, что и требовалось доказать.

Правила связывания квантором. Пусть $\mathfrak{B} \to \mathfrak{A}(x)$ — выводимая формула и $\mathfrak{B}$ не содержит переменной x. Ей соответствует формула $\mathfrak{B}^* \to \mathfrak{A}^*$. Допустим, что эта формула выводима. Формуле

$$\mathfrak{B} \to \forall x\, \mathfrak{A}(x), \tag{4}$$

которая получена из $\mathfrak{B} \to \mathfrak{A}(x)$ с помощью правила связывания квантором $\forall x$, соответствует формула

$$\mathfrak{B}^* \to [\forall x\, \mathfrak{A}(x)]^*$$

или, что то же,

$$\mathfrak{B}^* \to \mathfrak{A}^*.$$

Следовательно, формуле (4) соответствует та же формула, что и формуле $\mathfrak{B} \to \mathfrak{A}(x)$, т. е. выводимая формула исчисления высказываний.

Таким же образом наше утверждение доказывается для второго правила связывания квантором.

Таким образом, мы показали:

Если формулам исчисления предикатов

$$\mathfrak{A},\ \mathfrak{B},\ \ldots \tag{5}$$

соответствуют выводимые формулы исчисления высказываний

$$\mathfrak{A}^*,\ \mathfrak{B}^*,\ \ldots,$$

то и формулам, полученным из формул (5) *применением правил заключения, подстановки, переименования переменных и связывания квантором, соответствуют формулы, выводимые в исчислении высказываний.*

Так как аксиомам исчисления предикатов соответствуют выводимые формулы исчисления высказываний, то отсюда следует, что *всякой выводимой формуле исчисления предикатов соответствует выводимая формула исчисления высказываний.*

Отсюда немедленно следует внутренняя непротиворечивость исчисления предикатов. В самом деле, если бы исчисление предикатов было противоречиво, то в нем всякая формула была бы выводимой. В частности, формула, состоящая из одной буквы A, была бы в ней выводимой. Но тогда соответствующая A формула, т. е. она сама, была бы выводимой в исчислении высказываний. А это, как известно, неверно, так как исчисление высказываний непротиворечиво.

Теперь мы можем ответить на вопрос, поставленный выше: может ли формула исчисления высказываний, не являющаяся выводимой в исчислении высказываний, быть выводимой в исчислении предикатов? Докажем, что такой формулы не может быть. Пусть $\mathfrak{A}$ — формула исчисления высказываний, выводимая в исчислении предикатов; тогда соответствующая ей формула $\mathfrak{A}^*$ выводима в исчислении высказываний. Но так как $\mathfrak{A}$ — сама формула исчисления высказываний, то $\mathfrak{A}^*$ совпадает с $\mathfrak{A}$ и, значит, $\mathfrak{A}$ выводима в исчислении высказываний, что и требовалось доказать.

Мы показали, таким образом, что *всякая формула исчисления высказываний, выводимая в исчислении предикатов, является выводимой формулой исчисления высказываний.*

§ 6. Полнота в узком смысле

Относительно исчисления предикатов также возникает вопрос о полноте в широком и узком смысле (см. главу II, § 10). Вопрос о полноте в широком смысле мы будем рассматривать в дальнейшем. Вопрос же о полноте в узком смысле легко решается отрицательно. Мы его сейчас рассмотрим.

Напомним определение полноты в узком смысле. *Логическая система называется полной в узком смысле, если нельзя без противоречия присоединить к ее аксиомам в качестве новой аксиомы никакую не выводимую* *в ней формулу так, чтобы полученная при этом система была непротиворечива.* В отличие от исчисления высказываний, исчисление предикатов оказывается неполным в узком смысле. К его аксиомам можно присоединить без противоречия недоказуемую в нем формулу:

$$\exists x F(x) \rightarrow \forall x F(x). \qquad (1)$$

Доказательство этого осуществляется на основании того же соответствия, в силу которого мы каждой формуле $\mathfrak{A}$ исчисления предикатов отнесли формулу $\mathfrak{A}^*$ исчисления высказываний. Из рассуждений § 5 вытекает, что каждая формула, которой соответствует выводимая формула исчисления высказываний, может быть присоединена без противоречия к аксиомам исчисления предикатов. Формуле (1) соответствует в исчислении высказываний формула

$$F \rightarrow F,$$

которая является выводимой формулой исчисления высказываний.

Итак, формула (1) может быть присоединена к аксиомам исчисления предикатов. Может показаться странным, что такую формулу, явно неверную, можно без противоречия присоединить к аксиомам исчисления предикатов. Для выяснения этого вопроса обратимся к содержательному смыслу формул исчисления предикатов. Дело в том, что из общих логических аксиом ничего не вытекает относительно того, какие предметы и сколько их существует в той области $\mathfrak{M}$, к которой относятся наши высказывания и предикаты. Из общелогических положений нельзя, например, заключить, что область $\mathfrak{M}$ содержит более одного элемента. Если же область $\mathfrak{M}$ содержит только один элемент, то формула (1) для нее истинна. Вместе с тем наш прием доказательства непротиворечивости тех или других аксиом в том и состоял, что мы интерпретировали все наши формулы на области, состоящей из одного элемента.

Чтобы доказать, что исчисление предикатов неполно в узком смысле, нам еще нужно показать, что формула (1) не выводима из аксиом исчисления предикатов. С содержательной точки зрения этот вопрос представляется совершенно ясным. Ведь из всеобщей истинности формулы (1) вытекала бы невозможность существования в области более одного элемента. И если из общелогических положений нельзя доказать существование более чем одного предмета, то существование только одного предмета тоже доказать нельзя.

Однако можно дать и вполне строгое доказательство того, что формула (1) не может быть формально выведена из аксиом исчисления предикатов. Мы не будем приводить этого доказательства подробно, а ограничимся тем, что изложим основную идею. Идея эта состоит в том, что используется интерпретация формул исчисления предикатов на области, состоящей из двух элементов, в качестве которых можно взять числа 1 и 2. Поставим в соответствие каждой формуле $\mathfrak{A}$ исчисления предикатов такую формулу $\mathfrak{A}^{**}$, в которой операции связывания квантором заменены следующим образом:

$$\begin{array}{lcl} \forall x\, \mathfrak{A}(x) & \text{заменяется} & \mathfrak{A}(1) \,\&\, \mathfrak{A}(2), \\ \exists x\, \mathfrak{A}(x) & \text{»} & \mathfrak{A}(1) \vee \mathfrak{A}(2). \end{array}$$

Назовем не содержащую кванторов формулу исчисления предикатов правильной, если при любых заменах свободных переменных числами 1 и 2 она является выводимой формулой исчисления высказываний. Докажем, что для каждой выводимой формулы $\mathfrak{A}$ исчисления предикатов поставленная ей в соответствие формула $\mathfrak{A}^{**}$ является выводимой формулой исчисления высказываний.

Для аксиом это можно непосредственно проверить. Аксиомы групп I—IV не содержат ни переменных, ни кванторов; поэтому соответствующими им формулами являются они сами, т. е. выводимые формулы исчисления высказываний.

Рассмотрим аксиому V. 1

$$\forall x\, F(x) \rightarrow F(y).$$

Заменив в ней посылку конъюнкцией, получим

$$F(1) \,\&\, F(2) \rightarrow F(y).$$

Эта формула правильная, так как она становится выводимой формулой исчисления высказываний при замене переменной y числами 1 и 2.

Аналогичным образом можно убедиться, что и аксиоме V. 2 поставлена в соответствие правильная формула.

Дальше можно показать, что правила получения выводимых формул исчисления предикатов для соответствующих формул без кванторов переходят в правила, в силу которых из правильных формул получаются снова правильные формулы исчисления предикатов.

Рассмотрим, например, первое правило связывания квантором. Предположим, что формула

$$\mathfrak{A} \to \mathfrak{B}(x),$$

где $\mathfrak{A}$ не содержит переменной x, выводима, а соответствующая ей формула является правильной формулой исчисления предикатов. Эта формула имеет вид

$$\mathfrak{A}^{**} \to \mathfrak{B}^{**}(x), \tag{2}$$

где $\mathfrak{A}^{**}$ и $\mathfrak{B}^{**}$ — формулы, соответствующие $\mathfrak{A}$ и $\mathfrak{B}$. Так как формула (2) по предположению правильная, то формулы

$$\mathfrak{A}^{**} \to \mathfrak{B}^{**}(1) \quad \text{и} \quad \mathfrak{A}^{**} \to \mathfrak{B}^{**}(2)$$

также правильные. Но тогда и формула

$$\mathfrak{A}^{**} \to \mathfrak{B}^{**}(1) \mathbin{\&} \mathfrak{B}^{**}(2)$$

правильная, а это и есть формула, соответствующая формуле

$$\mathfrak{A} \to \forall x \, \mathfrak{B}(x).$$

Проведя доказательство для всех правил исчисления предикатов, мы тем самым покажем, что каждой выводимой формуле исчисления предикатов соответствует правильная формула.

Рассмотрим теперь формулу, соответствующую исследуемой формуле (1). Это, очевидно, формула

$$F(1) \vee F(2) \to F(1) \mathbin{\&} F(2). \tag{3}$$

Так как формула (1) свободных переменных не содержит, то формула (3), если она правильная, должна быть выводимой формулой исчисления высказываний. Однако легко видеть, что формула (3) не является выводимой. В самом деле, для предиката F, для которого $F(1)$ имеет значение *И*, а $F(2)$ — значение *Л*, формула

(3) перейдет в

$$И \vee Л \rightarrow И \,\&\, Л,$$

т. е. примет значение $Л$. Отсюда следует, что формула (1) не является выводимой в исчислении предикатов, что и требовалось доказать.

§ 7. Некоторые теоремы исчисления предикатов

Утверждение о том, что формула $\mathfrak{A}$ является выводимой в исчислении предикатов, мы будем обозначать так же, как и в исчислении высказываний:

$$\vdash \mathfrak{A}.$$

Так как все формулы, выводимые в исчислении высказываний, являются также выводимыми в исчислении предикатов, то, совершая подстановки в выводимые формулы исчисления высказываний, мы будем получать выводимые формулы исчисления предикатов.

Примеры.

1. Заменяя в выводимой формуле исчисления высказываний

$$\vdash A \vee \bar{A}$$

A на $F(x)$, получим выводимую формулу исчисления предикатов:

$$\vdash F(x) \vee \bar{F}(x).$$

2. Заменяя в выводимой формуле

$$\vdash A \rightarrow A \vee B$$

A на $F(x)$, B на $\forall y\, G(y)$, получим

$$\vdash F(x) \rightarrow F(x) \vee \forall y\, G(y).$$

3. Заменяя в выводимой формуле

$$\vdash A \rightarrow (B \,\&\, C \rightarrow B) \,\&\, A$$

B на $\exists x\, F(x)$, C на $\forall y\, H(y)$, получим

$$\vdash A \rightarrow (\exists x\, F(x) \,\&\, \forall y\, H(y) \rightarrow \exists x\, F(x)) \,\&\, A.$$

Заметим, что обнаружить выводимость формулы в исчислении высказываний не представляет никакого труда. Для этого нет необходимости проводить ее вывод, как доказано в главе II. Для этого достаточно лишь установить, что формула является тождественно истинной в смысле алгебры высказываний.

Подстановкой в выводимые формулы исчисления высказываний можно легко получить многие выводимые формулы исчисления предикатов; однако таким образом всякую выводимую формулу исчисления предикатов вывести нельзя.

Все производные правила, выведенные для исчисления высказываний, остаются справедливыми и для исчисления предикатов. Правило сложной подстановки (см. стр. 78), а также правило сложного заключения складываются из последовательного применения основного правила подстановки (соответственно основного правила заключения) и поэтому остаются верными и для исчисления предикатов.

Мы не будем приводить выводы всех этих правил, так как они получаются повторением соответствующих доказательств для исчисления высказываний. Для примера докажем только справедливость правила силлогизма

$$\frac{\mathfrak{A} \to \mathfrak{B},\ \mathfrak{B} \to \mathfrak{C}}{\mathfrak{A} \to \mathfrak{C}}$$

(в предположении, что $\mathfrak{A} \to \mathfrak{C}$ есть формула).

В исчислении высказываний мы вывели это правило из выводимой формулы

$$\vdash (A \to B) \to ((B \to C) \to (A \to C)).$$

Но так как правило подстановки в исчислении предикатов также имеет место, то формула

$$\vdash (\mathfrak{A} \to \mathfrak{B}) \to ((\mathfrak{B} \to \mathfrak{C}) \to (\mathfrak{A} \to \mathfrak{C}))$$

является выводимой, каковы бы ни были формулы исчисления предикатов $\mathfrak{A}$, $\mathfrak{B}$ и $\mathfrak{C}$. Коллизия переменных при образовании этой формулы не может возникнуть, так как иначе имела бы место коллизия переменных в какой-нибудь из формул $\mathfrak{A}$, $\mathfrak{B}$ или $\mathfrak{C}$ либо между переменными какой-нибудь пары этих формул. Но так как каждая пара формул $\mathfrak{A}$, $\mathfrak{B}$ и $\mathfrak{C}$ входит в одну из формул $\mathfrak{A} \to \mathfrak{B}$, $\mathfrak{B} \to \mathfrak{C}$ и $\mathfrak{A} \to \mathfrak{C}$, то коллизия переменных имела бы место по крайней мере в одной из этих формул, чего, по предположению, нет.

Формулы $\mathfrak{A} \rightarrow \mathfrak{B}$ и $\mathfrak{B} \rightarrow \mathfrak{C}$, по условию, выводимы. Применив правило силлогизма, мы получим, что формула $\mathfrak{A} \rightarrow \mathfrak{C}$ также выводима.

В исчислении предикатов выводимы формулы

$$\vdash A \rightarrow \mathfrak{R}$$

и

$$\vdash \mathfrak{F} \rightarrow A,$$

где через $\mathfrak{R}$ обозначена любая выводимая формула, а через $\mathfrak{F}$ — любая формула вида $\overline{\mathfrak{R}}$.

Выведем для исчисления предикатов следующее *производное правило.*

Если формула $\mathfrak{A}(x)$, *содержащая свободную предметную переменную* x, *выводима, то и формула*

$$\forall x\, \mathfrak{A}(x)$$

также выводима в исчислении предикатов.

Итак, допустим, что имеет место

$$\vdash \mathfrak{A}(x).$$

В силу того, что имеет место

$$\vdash A \rightarrow \mathfrak{R},$$

где $\mathfrak{R}$ — произвольная выводимая формула, имеем

$$\vdash A \rightarrow \mathfrak{A}(x).$$

Применив первое правило связывания квантором, получим

$$\vdash A \rightarrow \forall x\, \mathfrak{A}(x).$$

Можно предполагать, что A не входит в формулу $\mathfrak{A}$ (его всегда так можно выбрать). Заменив в последней формуле A произвольной выводимой формулой, имеем

$$\vdash \mathfrak{R} \rightarrow \forall x\, \mathfrak{A}(x).$$

Применив правило заключения, получим

$$\vdash \forall x\, \mathfrak{A}(x).$$

Итак, если имеет место $\vdash \mathfrak{A}(x)$, то имеет место и $\vdash \forall x\, \mathfrak{A}(x)$, и мы доказали правило, которое можно записать так:

$$\frac{\mathfrak{A}(x)}{\forall x\, \mathfrak{A}(x)}.$$

Полученное правило мы будем называть *производным правилом связывания квантором.* Оно, очевидно, применимо к любой предметной переменной.

Применяя это правило, мы имеем возможность вывести еще новые выводимые формулы.

Примеры.

1. Применив к формуле

$$\vdash F(x) \vee \overline{F}(x)$$

правило $\frac{\mathfrak{A}(x)}{\forall x\, \mathfrak{A}(x)}$, мы получим

$$\vdash \forall x\, (F(x) \vee \overline{F}(x)).$$

2. Из выводимой формулы

$$\vdash F(x) \to (G(y) \to F(x)),$$

которая является результатом подстановок в аксиому II. 1, применив производное правило связывания квантором, получим

$$\vdash \forall y\, (F(x) \to (G(y) \to F(x))).$$

Применив к последней формуле еще раз то же правило, будем иметь

$$\vdash \forall x\, \forall y\, (F(x) \to (G(y) \to F(x))).$$

§ 8. Теорема дедукции

Мы докажем для исчисления предикатов теорему, аналогичную теореме дедукции, которую мы имели для исчисления высказываний. Эта теорема позволит нам получать выводимые формулы исчисления предикатов, не производя для них всех операций формальной дедукции, что в значительной степени сокращает непосредственный путь вывода выводимых формул. За этой теоремой мы и в исчислении предикатов сохраним название «*теоремы дедукции*».

Введем сначала следующее определение:

Мы будем говорить, что *формула* $\mathfrak{B}$ *выводима из формулы* $\mathfrak{A}$, если $\mathfrak{A} \to \mathfrak{B}$ есть формула и формула $\mathfrak{B}$ выводима из совокупности всех выводимых формул исчисления предикатов и формулы $\mathfrak{A}$ посредством применения всех правил исчисления предикатов, причем оба правила связывания квантором, правила подстановки вместо переменных предикатов и вместо свободных предметных переменных должны применяться только к таким переменным предикатам или предметам, которые в формулу $\mathfrak{A}$ не входят.

Мы высказали предварительное, не вполне точное определение «выводимости формулы $\mathfrak{B}$ из формулы $\mathfrak{A}$». Дадим теперь точное определение этого понятия. Оно складывается из следующих пунктов.

1. Каждая выводимая формула $\mathfrak{B}$ исчисления предикатов выводима из $\mathfrak{A}$, если только выражение $\mathfrak{A} \to \mathfrak{B}$ не содержит коллизии переменных.

2. Формула $\mathfrak{A}$ выводима из $\mathfrak{A}$.

3. Если формулы

$$\mathfrak{B}_1 \quad \text{и} \quad \mathfrak{B}_1 \to \mathfrak{B}_2$$

выводимы из формулы $\mathfrak{A}$, то и формула $\mathfrak{B}_2$ выводима из формулы $\mathfrak{A}$.

4. Если формула

$$\mathfrak{B}_1 \to \mathfrak{B}_2(x)$$

выводима из $\mathfrak{A}$, причем $\mathfrak{B}_1$ и $\mathfrak{A}$ не содержат переменной x, то и формула

$$\mathfrak{B}_1 \to \forall x\, \mathfrak{B}_2(x)$$

выводима из формулы $\mathfrak{A}$.

5. Если формула

$$\mathfrak{B}_2(x) \to \mathfrak{B}_1$$

выводима из $\mathfrak{A}$, причем x не входит ни в $\mathfrak{B}_1$, ни в $\mathfrak{A}$, то и формула

$$\exists x\, \mathfrak{B}_2(x) \to \mathfrak{B}_1$$

выводима из $\mathfrak{A}$.

6. Если $\mathfrak{B}$ выводима из $\mathfrak{A}$, то и формула $\mathfrak{B}'$, полученная из $\mathfrak{B}$ любым переименованием связанных переменных, не приводящим к коллизии переменных с $\mathfrak{A}$, выводима из $\mathfrak{A}$.

7. Если $\mathfrak{B}$ выводима из $\mathfrak{A}$, то и формула $\mathfrak{B}'$, полученная из $\mathfrak{B}$ подстановкой в свободную предметную переменную, не входящую в $\mathfrak{A}$, также выводима из $\mathfrak{A}$, если эта подстановка не приводит к коллизии переменных с $\mathfrak{A}$.

8. Если $\mathfrak{B}$ выводима из $\mathfrak{A}$ и если формула $\mathfrak{B}'$ получена из $\mathfrak{B}$ посредством подстановки в переменное высказывание или переменный предикат, причем это переменное высказывание или предикат не содержатся в формуле $\mathfrak{A}$, и если, кроме того, подстановка не приводит к коллизии переменных с $\mathfrak{A}$, то $\mathfrak{B}'$ также выводима из $\mathfrak{A}$.

Теорема дедукции. *Если формула $\mathfrak{B}$ выводима из формулы $\mathfrak{A}$, то формула $\mathfrak{A} \to \mathfrak{B}$ выводима в исчислении предикатов.*

Мы при этом, конечно, предполагаем, что $\mathfrak{A}$ и $\mathfrak{B}$ таковы, что $\mathfrak{A} \to \mathfrak{B}$ является формулой, т. е. между $\mathfrak{A}$ и $\mathfrak{B}$ не возникает коллизии переменных. Впрочем, какова бы ни была формула $\mathfrak{B}$, можно так переименовать предметные переменные, что полученная при этом формула $\mathfrak{B}'$ не приводит к коллизии переменных с $\mathfrak{A}$ и позволяет образовать формулу $\mathfrak{A} \to \mathfrak{B}'$. В таком случае теорема дедукции может быть сформулирована для формул $\mathfrak{A}$ и $\mathfrak{B}'$.

Для доказательства теоремы дедукции достаточно показать, что верны следующие утверждения.

a). Для любой выводимой в исчислении предикатов формулы теорема дедукции имеет место.

b) Для формулы $\mathfrak{A}$ она имеет место.

c) Если теорема справедлива для формул $\mathfrak{B}_1$ и $\mathfrak{B}_1 \to \mathfrak{B}_2$, то она справедлива и для формулы $\mathfrak{B}_2$.

d) Если теорема справедлива для формулы

$$\mathfrak{B}_1 \to \mathfrak{B}_2(x),$$

причем x не входит ни в $\mathfrak{B}_1$, ни в $\mathfrak{A}$, то она справедлива и для формулы

$$\mathfrak{B}_1 \to \forall x\, \mathfrak{B}_2(x).$$

e) Если теорема справедлива для формулы

$$\mathfrak{B}_2(x) \to \mathfrak{B}_1,$$

причем x не входит ни в $\mathfrak{B}_1$, ни в $\mathfrak{A}$, то она справедлива и для формулы

$$\exists x\, \mathfrak{B}_2(x) \to \mathfrak{B}_1.$$

f) Если теорема справедлива для $\mathfrak{B}$, то она справедлива и для любой формулы $\mathfrak{B}'$, полученной из $\mathfrak{B}$ переименованием связанных переменных, если только это переименование не приводит к коллизии переменных с формулой $\mathfrak{A}$.

g) Если теорема справедлива для формулы $\mathfrak{B}$, то она справедлива и для $\mathfrak{B}'$, полученной из $\mathfrak{B}$ подстановкой в свободную предметную переменную, не входящую в $\mathfrak{A}$, если только эта подстановка не приводит к коллизии переменных с формулой $\mathfrak{A}$.

h) Если теорема справедлива для формулы $\mathfrak{B}$, то она справедлива и для формулы $\mathfrak{B}'$, полученной из $\mathfrak{B}$ подстановкой в переменное высказывание или переменный предикат, не содержащиеся в $\mathfrak{A}$, при условии, что между $\mathfrak{A}$ и $\mathfrak{B}'$ не возникает коллизии переменных.

Справедливость a) следует из того, что всякая формула вида

$$A \to \mathfrak{R},$$

где $\mathfrak{R}$ — выводимая формула, также выводима. Следовательно, если $\mathfrak{B}$ — выводимая формула, то и

$$\mathfrak{A} \to \mathfrak{B}$$

— также выводимая формула.

Справедливость b) очевидна.

Докажем c). Пусть $\mathfrak{B}_1$ и $\mathfrak{B}_1 \to \mathfrak{B}_2$ — выводимые из $\mathfrak{A}$ формулы, для которых справедлива теорема дедукции.

Возьмем аксиому I. 2:

$$(A \to (B \to C)) \to ((A \to B) \to (A \to C)).$$

Подстановками в эту аксиому мы получим следующую выводимую формулу исчисления предикатов:

$$\vdash (\mathfrak{A} \to (\mathfrak{B}_1 \to \mathfrak{B}_2)) \to ((\mathfrak{A} \to \mathfrak{B}_1) \to (\mathfrak{A} \to \mathfrak{B}_2)).$$

Так как по предположению мы имеем

$$\vdash \mathfrak{A} \to (\mathfrak{B}_1 \to \mathfrak{B}_2) \quad \text{и} \quad \vdash \mathfrak{A} \to \mathfrak{B}_1,$$

то, применив сложное правило заключения, получим

$$\vdash \mathfrak{A} \to \mathfrak{B}_2.$$

d) Допустим, что для выводимой из $\mathfrak{A}$ формулы $\mathfrak{B}_1 \to \mathfrak{B}_2(x)$ (причем x в $\mathfrak{B}_1$ и в $\mathfrak{A}$ не входит) наша теорема верна. Это значит, что имеет место

$$\vdash \mathfrak{A} \to (\mathfrak{B}_1 \to \mathfrak{B}_2(x)).$$

Применив правило соединения посылок

$$\frac{\mathfrak{A} \to (\mathfrak{B}_1 \to \mathfrak{B}_2(x))}{\mathfrak{A} \,\&\, \mathfrak{B}_1 \to \mathfrak{B}_2(x)},$$

получим

$$\vdash \mathfrak{A} \,\&\, \mathfrak{B}_1 \to \mathfrak{B}_2(x).$$

Применив первое правило связывания квантором, будем иметь

$$\vdash \mathfrak{A} \,\&\, \mathfrak{B}_1 \to \forall x\, \mathfrak{B}_2(x).$$

Применив правило разъединения посылок

$$\frac{\mathfrak{A} \,\&\, \mathfrak{B}_1 \to \forall x\, \mathfrak{B}_2(x)}{\mathfrak{A} \to (\mathfrak{B}_1 \to \forall x\, \mathfrak{B}_2(x))},$$

получим требуемую формулу:

$$\vdash \mathfrak{A} \to (\mathfrak{B}_1 \to \forall x\, \mathfrak{B}_2(x)).$$

e) Справедливость этого утверждения доказывается так же, как и d); только в этом случае надо воспользоваться еще правилом перестановки посылок:

$$\frac{\mathfrak{A} \to (\mathfrak{B} \to \mathfrak{C})}{\mathfrak{B} \to (\mathfrak{A} \to \mathfrak{C})}.$$

Справедливость f) и g) очевидна.

h) Справедливость этого утверждения также ясна. Действительно, для выводимой из $\mathfrak{A}$ формулы $\mathfrak{B}$ имеет место

$$\vdash \mathfrak{A} \to \mathfrak{B}.$$

Если $\mathfrak{B}'$ является результатом подстановки в переменное высказывание или переменный предикат, не входящий в $\mathfrak{A}$, то

$$\mathfrak{A} \to \mathfrak{B}'$$

является результатом той же подстановки в формулу

$$\mathfrak{A} \to \mathfrak{B}.$$

Поэтому $\mathfrak{A} \to \mathfrak{B}'$ — также выводимая формула исчисления предикатов.

§ 9. Дальнейшие теоремы исчисления предикатов

Теорема 1.

$$\vdash \forall x\, F(x) \to \exists x\, F(x).$$

Возьмем аксиомы V. 1 и V. 2:

$$\forall x\, F(x) \to F(y) \quad \text{и} \quad F(y) \to \exists x\, F(x).$$

Применив правило силлогизма, получим требуемую формулу.

Введем знак $\sim$, определив его так же, как и в исчислении высказываний, т. е. будем считать, что выражение

$$\mathfrak{A} \sim \mathfrak{B}$$

представляет собой формулу

$$(\mathfrak{A} \to \mathfrak{B}) \,\&\, (\mathfrak{B} \to \mathfrak{A}).$$

За знаком $\sim$ сохраним название *знака эквивалентности*, а формулы вида $\mathfrak{A} \sim \mathfrak{B}$ будем называть *эквивалентностями.*

Теорема 2.

$$\forall x\, \forall y\, F(x, y) \sim \forall y\, \forall x\, F(x, y).$$

Применив дважды аксиому V. 1, находим

$$\forall x\, \forall y\, F(x, y) \to F(u, v).$$

Применим к этой формуле первое правило связывания квантором, связывая сначала переменную u, а затем переменную v. Тогда получим

$$\forall x\, \forall y\, F(x, y) \to \forall v\, \forall u\, F(u, v).$$

Произведя в этой формуле переименование переменных, заменив u на x и v на y, получаем формулу

$$\forall x\, \forall y\, F(x, y) \to \forall y\, \forall x\, F(x, y).$$

Таким же образом доказывается и обратное следование. Применив, наконец, правило

$$\frac{\mathfrak{A},\ \mathfrak{B}}{\mathfrak{A} \,\&\, \mathfrak{B}},$$

получим требуемую эквивалентность.

Теорема 3.

$$\exists x \forall y F(x, y) \to \forall y \exists x F(x, y).$$

Путем подстановки в аксиому V. 1 и замены свободных переменных получаем

$$\vdash \forall y F(x, y) \to F(x, v).$$

Таким же образом из аксиомы V. 2 имеем

$$\vdash F(x, v) \to \exists w F(w, v).$$

Применив правило силлогизма к полученным формулам, находим

$$\vdash \forall y F(x, y) \to \exists w F(w, v).$$

К последней формуле применим сначала второе правило связывания квантором, а затем первое, получим

$$\vdash \exists x \forall y F(x, y) \to \forall v \exists w F(w, v).$$

Наконец, применив правило переименования связанных переменных, получим требуемую формулу.

Обратное следование

$$\forall x \exists y F(x, y) \to \exists y \forall x F(x, y)$$

не является выводимым.

Легко видеть, что предположение общелогической истинности этой формулы немедленно приводит к противоречию. Применим ее к натуральному ряду чисел. Пусть $F(x, y)$ означает, что «натуральное число x меньше натурального числа y». В таком случае в посылке рассматриваемого следования утверждается, что для всякого натурального числа x существует большее натуральное число y. Это утверждение, очевидно, справедливо для натурального ряда. В таком случае должно быть верным и следствие, т. е.

$$\exists y \forall x F(x, y).$$

Это утверждение в нашем случае выражает следующее: «существует такое натуральное число y, что каждое натуральное число x меньше числа y». Это утверждение, очевидно, неверно.

Наше рассуждение не является строгим доказательством невыводимости формулы

$$\forall x\, \exists y\, F(x,\ y) \to \exists y\, \forall x\, F(x,\ y)$$

в исчислении предикатов. Но нетрудно доказать и строго, что эта формула действительно невыводима; мы не будем останавливаться на этом.

Теорема 4.

$$\vdash \forall x\, (F(x) \to G(x)) \to (\forall x\, F(x) \to \forall x\, G(x)).$$

Для доказательства выводимости этой формулы применим теорему дедукции. Покажем, что формула $\forall x\ F(x) \to \forall x\, G(x)$ выводима из формулы

$$\forall x\, (F(x) \to G(x)). \tag{1}$$

В самом деле, формула

$$\forall x\, (F(x) \to G(x)) \to (F(y) \to G(y))$$

получается подстановкой в аксиому V. 1 и поэтому является выводимой в исчислении предикатов. Следовательно, эта формула выводима из любой формулы и, в частности, из формулы (1). Применив правило заключения, мы найдем, что формула

$$F(y) \to G(y)$$

выводима из формулы (1).

Напишем выводимую формулу исчисления высказываний:

$$(A \to B) \to ((B \to C) \to (A \to C)).$$

Из нее путем подстановок получаем

$$\vdash (\forall x\, F(x) \to F(y)) \to ((F(y) \to G(y)) \to (\forall x\, F(x) \to G(y)).$$

Обе посылки этой формулы выводимы из формулы (1) (первая является аксиомой V. 1). Применив два раза правило заключения 3, находим, что формула

$$\forall x\, F(x) \to G(y)$$

выводима из формулы (1).

Наконец, применив к последней формуле первое правило связывания квантором и переименовав затем связанную переменную y, найдем, что формула

$$\forall x\, F(x) \rightarrow \forall x\, G(x)$$

выводима из формулы (1). Применив теорему дедукции, получим требуемую формулу.

Может показаться странным, что мы в одном пункте доказательства теоремы 4 не применили правила силлогизма, а вместо этого использовали формулу

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

Мы сделали это потому, что не доказали справедливости правила силлогизма для понятия выводимости из данной формулы, которое мы ввели при доказательстве теоремы дедукции. Однако и для выводимости в смысле теоремы дедукции это правило верно, и его доказательство можно провести в самом общем виде совершенно так же, как оно фактически проведено выше для частного случая. Учитывая это, в дальнейшем мы будем применять правило силлогизма и для выводимости в смысле теоремы дедукции.

Теорема 5.

$$\vdash \forall x\, (F(x) \rightarrow G(x)) \rightarrow (\exists x\, F(x) \rightarrow \exists x\, G(x)).$$

Покажем, что правая часть следования выводима из левой. Из

$$\vdash \forall x\, (F(x) \rightarrow G(x)) \rightarrow (F(y) \rightarrow G(y)),$$

применив правило заключения, мы найдем, что формула

$$F(y) \rightarrow G(y)$$

выводима из формулы

$$\forall x\, (F(x) \rightarrow G(x)). \tag{2}$$

Из формул

$$G(y) \rightarrow \exists x\, G(x)$$

и

$$F(y) \rightarrow G(y),$$

которые выводимы из формулы (2) (первая потому, что она выводимая), применив правило силлогизма, получим формулу

$$F(y) \rightarrow \exists x\, G(x), \tag{3}$$

которая, следовательно, также выводима из формулы (2).

Применив второе правило связывания квантором по переменной y к формуле (3), получим после переименования связанных переменных формулу

$$\exists x\, F(x) \to \exists x\, G(x),$$

которая, следовательно, также выводима из формулы (2). [Мы можем применить правило связывания квантором к формуле (3), так как переменная y не входит в формулу (2).]

В результате на основании теоремы дедукции можно заключить, что имеет место

$$\vdash \forall x\,(F(x) \to G(x)) \to (\exists x\, F(x) \to \exists x\, G(x)),$$

и теорема доказана.

Замечание к теореме 5. Легко видеть, что выводима следующая формула:

$$\vdash \forall x\,(F(x) \sim G(x)) \to (\exists x\, F(x) \sim \exists x\, G(x)).$$

В самом деле, при доказательстве теоремы 5 мы показали, что из формулы $F(y) \to G(y)$ выводима формула $\exists x\, F(x) \to \exists x\, G(x)$. Ясно, что из формулы $G(y) \to F(y)$ выводима формула

$$\exists x\, G(x) \to \exists x\, F(x).$$

Но обе формулы

$$F(y) \to G(y) \quad \text{и} \quad G(y) \to F(y)$$

выводимы, как легко видеть, из формулы

$$\forall x\,(F(x) \sim G(x)).$$

В таком случае из этой формулы выводимы также и формулы

$$\exists x\, G(x) \to \exists x\, F(x) \quad \text{и} \quad \exists x\, F(x) \to \exists x\, G(x).$$

Подстановками в выводимую формулу исчисления высказываний

$$A \to (B \to A \,\&\, B)$$

получим

$$\vdash (\exists x\, F(x) \to \exists x\, G(x)) \to ((\exists x\, G(x) \to \exists x\, F(x)) \to \\ \to (\exists x\, F(x) \sim \exists x\, G(x))).$$

Применив два раза правило заключения, получим, что формула

$$\exists x\, F(x) \sim \exists x\, G(x)$$

выводима из формулы $\forall x\,(F(x) \sim G(x))$, откуда в силу теоремы дедукции следует

$$\vdash \forall x\,(F(x) \sim G(x)) \to (\exists x\, F(x) \sim \exists x\, G(x)).$$

Теорема 6.

$$\vdash \forall x\,(F(x) \sim G(x)) \to (\forall x\, F(x) \sim \forall x\, G(x)).$$

Покажем, что следование в одну сторону выводимо из посылки. Из формулы

$$\forall x\,(F(x) \sim G(x)) \tag{4}$$

выводима формула

$$F(y) \sim G(y).$$

Последнюю формулу можно записать в виде

$$(F(y) \to G(y))\,\&\,(G(y) \to F(y)).$$

Рассмотрим две выводимые формулы:

$$(F(y) \to G(y))\,\&\,(G(y) \to F(y)) \to (F(y) \to G(y)),$$
$$(F(y) \to G(y))\,\&\,(G(y \to F(y)) \to (G(y) \to F(y)).$$

Применяя правило заключения, легко показать, что обе формулы $F(y) \to G(y)$ и $G(y) \to F(y)$ выводимы из формулы (4). Из выводимой формулы $\forall x\, F(x) \to F(y)$ и выводимой из посылки (4) формулы $F(y) \to G(y)$, применяя правило силлогизма, получаем, что формула $\forall x\, F(x) \to G(y)$ выводима из формулы (4). Применяя первое правило связывания квантором и переименовывая переменные, найдем, что формула

$$\forall x\, F(x) \to \forall x\, G(x)$$

выводима из формулы (4). Таким же образом доказывается, что обратное следование

$$\forall x\, G(x) \to \forall x\, F(x)$$

выводимо из формулы (4).

Рассмотрим выводимую формулу исчисления высказываний

$$A \to (B \to A \,\&\, B).$$

Из нее путем сложной подстановки получим выводимую формулу

$$(\forall x\, F(x) \to \forall x\, G(x)) \to [(\forall x\, G(x) \to \forall x\, F(x)) \to$$
$$\to (\forall x\, F(x) \to \forall x\, G(x)) \,\&\, (\forall x\, G(x) \to \forall x\, F(x))].$$

Обе посылки этой формулы выводимы из формулы (4). Применяя два раза правило заключения, находим, что формула

$$(\forall x\, F(x) \to \forall x\, G(x)) \,\&\, (\forall x\, G(x) \to \forall x\, F(x))$$

или, что то же самое, формула

$$\forall x\, F(x) \sim \forall x\, G(x)$$

выводима из формулы (4). Отсюда, применив теорему дедукции, получаем теорему 6.

Теорема 7.

a. $\exists x\, F(x) \sim \overline{\forall x\, \overline{F}(x)}$;

b. $\exists x\, \overline{F}(x) \sim \overline{\forall x\, F(x)}$;

c. $\overline{\exists x\, F(x)} \sim \forall x\, \overline{F}(x)$;

d. $\overline{\exists x\, \overline{F}(x)} \sim \forall x\, F(x)$.

Докажем 7а.

Подстановкой в аксиому V. 1 получаем

$$\vdash \forall x\, \overline{F}(x) \to \overline{F}(y).$$

Обращая следование $\left(\text{правило } \dfrac{\mathfrak{A} \to \mathfrak{B}}{\overline{\mathfrak{B}} \to \overline{\mathfrak{A}}}\right)$, имеем

$$\vdash \overline{\overline{F}}(y) \to \overline{\forall x\, \overline{F}(x)}.$$

Из последней формулы и из истинной формулы

$$\vdash F(y) \to \overline{\overline{F}}(y),$$

применив правило силлогизма, получим

$$\vdash F(y) \to \overline{\forall x\, \overline{F}(x)}.$$

Применив второе правило связывания квантором и переименовав связанные переменные, имеем

$$\vdash \exists x\, F(x) \rightarrow \overline{\forall x\, \overline{F}(x)}. \qquad (5)$$

Выведем обратное следование. Применив к аксиоме V. 2 правило обращения следования, получим

$$\vdash \overline{\exists x\, F(x)} \rightarrow \overline{F}(y).$$

Применив первое правило связывания квантором и переименовав связанные переменные, будем иметь

$$\vdash \overline{\exists x\, F(x)} \rightarrow \forall x\, \overline{F}(x).$$

Обращая следование, получим

$$\overline{\forall x\, \overline{F}(x)} \rightarrow \overline{\overline{\exists x\, F(x)}}.$$

Применив к последней формуле и к выводимой формуле

$$\overline{\overline{\exists x\, F(x)}} \rightarrow \exists x\, F(x)$$

правило силлогизма, имеем

$$\overline{\forall x\, \overline{F}(x)} \rightarrow \exists x\, F(x). \qquad (6)$$

Применив к формулам (5) и (6) правило

$$\frac{\mathfrak{A},\ \mathfrak{B}}{\mathfrak{A}\ \&\ \mathfrak{B}},$$

получим 7а.

Докажем 7b. Рассмотрим истинную формулу

$$\vdash F(x) \sim \overline{\overline{F}}(x).$$

Применив к ней производное правило связывания квантором, будем иметь

$$\vdash \forall x\, (F(x) \sim \overline{\overline{F}}(x)).$$

Сделав подстановку в выводимую формулу, доказанную в теореме 6, получим

$$\vdash \forall x\, (F(x) \sim \overline{\overline{F}}(x)) \rightarrow (\forall x\, F(x) \sim \forall x\, \overline{\overline{F}}(x)).$$

Применив правило заключения к последним формулам, будем иметь

$$\vdash \forall x\, F(x) \sim \forall x\, \overline{\overline{F}}(x).$$

Рассмотрим оба следования, заключенные в этой формуле:

$$\forall x\, F(x) \to \forall x\, \bar{\bar{F}}(x) \text{ и } \forall x\, \bar{\bar{F}}(x) \to \forall x\, F(x).$$

Обратим оба эти следования и соединим полученные обращения в виде формулы

$$\vdash \overline{\forall x\, F(x)} \sim \overline{\forall x\, \bar{\bar{F}}(x)}.$$

Сделаем подстановку в формулу 7a; заменив $F(x)$ на $\bar{F}(x)$, получим

$$\vdash \exists x \bar{F}(x) \sim \overline{\forall x\, \bar{\bar{F}}(x)}.$$

Применив к двум последним формулам правило

$$\frac{\mathfrak{A} \sim \mathfrak{B},\ \mathfrak{B} \sim \mathfrak{C}}{\mathfrak{A} \sim \mathfrak{C}},$$

получим формулу 7b.

Выводимость формул 7c и 7d легко доказывается посредством правила обращения следования из формул 7a и 7b.

Теорема 8.

$$\vdash (A \to \forall x\, F(x)) \sim \forall x\, (A \to F(x)).$$

Докажем первое следование:

$$(A \to \forall x\, F(x)) \to \forall x\, (A \to F(x)).$$

Сначала докажем, что $F(y)$ выводимо из формулы

$$(A \to \forall x\, F(x))\ \&\ A. \tag{7}$$

В самом деле, из формулы (7) выводимы, очевидно, формулы $A \to \forall x\, F(x)$ и A. Применив к этим формулам правило заключения, мы видим, что формула $\forall x\, F(x)$ выводима из формулы (7). Аксиома V. 1 $\forall x\, F(x) \to F(y)$ выводима из (7). Применив правило заключения к формулам $\forall x\, F(x)$ и $\forall x\, F(x) \to F(y)$, находим, что $F(y)$ выводима из (7).

На основании теоремы дедукции мы можем заключить, что

$$\vdash (A \to \forall x\, F(x))\ \&\ A \to F(y).$$

Применив правило $\dfrac{\mathfrak{A}\ \&\ \mathfrak{B} \to \mathfrak{C}}{\mathfrak{A} \to (\mathfrak{B} \to \mathfrak{C})}$, получим

$$\vdash (A \to \forall x\, F(x)) \to (A \to F(y)),$$

откуда, применив правило связывания квантором и переименовав затем связанные переменные, имеем

$$\vdash (A \to \forall x\, F(x)) \to \forall x\, (A \to F(x)). \tag{8}$$

Докажем обратное следование:

$$\vdash \forall x\, (A \to F(x)) \to (A \to \forall x\, F(x)).$$

Покажем, что следствие выводимо из посылки. В самом деле, из формулы

$$\forall x\, (A \to F(x)) \tag{9}$$

и выводимой формулы

$$\vdash \forall x\, (A \to F(x)) \to (A \to F(y)),$$

применив правило заключения, находим, что формула

$$A \to F(y)$$

выводима из формулы (9). Применив первое правило связывания квантором и переименовав связанные переменные, найдем, что формула

$$A \to \forall x\, F(x)$$

выводима из формулы (9).

На основании теоремы дедукции мы можем заключить, что

$$\vdash \forall x\, (A \to F(x)) \to (A \to \forall x\, F(x)).$$

Из выводимости доказанных следований вытекает выводимость эквивалентности

$$\vdash \forall x\, (A \to F(x)) \sim (A \to \forall x\, F(x)).$$

§ 10. Эквивалентные формулы

Так же, как и в исчислении высказываний, мы будем говорить, что *формулы $\mathfrak{A}$ и $\mathfrak{B}$ эквивалентны, если имеет место*

$$\vdash \mathfrak{A} \sim \mathfrak{B}.$$

Так как в исчислении предикатов также справедливы правила

$$\frac{\mathfrak{A} \sim \mathfrak{B},\ \mathfrak{B} \sim \mathfrak{C}}{\mathfrak{A} \sim \mathfrak{C}} \quad \text{и} \quad \frac{\mathfrak{A} \sim \mathfrak{B}}{\mathfrak{B} \sim \mathfrak{A}},$$

то отношение эквивалентности симметрично и транзитивно. Покажем, что *если в формуле исчисления предикатов $\mathfrak{A}$ заменить любую часть эквивалентной формулой и если полученное вследствие этой замены выражение $\mathfrak{A}'$ также является формулой и содержит все свободные предметные переменные формулы $\mathfrak{A}$, то $\mathfrak{A}$ и $\mathfrak{A}'$ эквивалентны.*

Мы не будем проводить полностью доказательство этого утверждения, так как оно в значительной части представляет собой повторение доказательства аналогичного предложения в исчислении высказываний (см. главу II § 6). Доказательство это проводится индукцией по схеме образования формул.

Сначала заметим, что наше утверждение имеет место для элементарных формул, т. е. для переменных высказываний и переменных предикатов. Это в самом деле очевидно, так как каждая элементарная формула имеет только одну часть — именно самое себя.

Допустим, что наше утверждение справедливо для формул $\mathfrak{A}$ и $\mathfrak{B}$ Тогда оно справедливо и для формул $\mathfrak{A} \& \mathfrak{B}$, $\mathfrak{A} \vee \mathfrak{B}$, $\mathfrak{A} \rightarrow \mathfrak{B}$ и $\overline{\mathfrak{A}}$. Доказательство этого пункта представляет собой дословное повторение рассуждений, проводившихся в исчислении высказываний.

Докажем, что если наше утверждение справедливо для формулы $\mathfrak{A}(x)$, то оно справедливо и для формул

$$\forall x\, \mathfrak{A}(x) \text{ и } \exists x\, \mathfrak{A}(x).$$

Доказательство проведем сначала для формулы $\forall x\, \mathfrak{A}(x)$. Заменяемая часть этой формулы, по определению, является либо ею самой, либо частью формулы $\mathfrak{A}(x)$. В первом случае наше утверждение очевидно Во втором случае в силу индуктивного предположения формула $\mathfrak{A}(x)$ перейдет в формулу $\mathfrak{A}'(x)$, эквивалентную формуле $\mathfrak{A}(x)$. [Переменная x должна сохраниться в формуле $\mathfrak{A}'(x)$, иначе выражение $\forall x\, \mathfrak{A}'(x)$ не было бы формулой.] Итак, $\mathfrak{A}(x)$ и $\mathfrak{A}'(x)$ эквивалентны; это значит, что формула $\mathfrak{A}(x) \sim \mathfrak{A}'(x)$ выводима. Сделав подстановку в формулу теоремы 6 § 9, получим

$$\vdash \forall x\, (\mathfrak{A}(x) \sim \mathfrak{A}'(x)) \rightarrow (\forall x\, \mathfrak{A}(x) \sim \forall x\, \mathfrak{A}'(x)).$$

Кроме того, применив производное правило связывания квантором к формуле $\mathfrak{A}(x) \sim \mathfrak{A}'(x)$, имеем

$$\vdash \forall x\, (\mathfrak{A}(x) \sim \mathfrak{A}'(x)).$$

Применив к двум последним формулам правило заключения, получим

$$\vdash \forall x\, \mathfrak{A}(x) \sim \forall x\, \mathfrak{A}'(x),$$

и, следовательно, для формулы $\forall x\, \mathfrak{A}(x)$ наше утверждение доказано.

Докажем то же самое для формулы $\exists x\, \mathfrak{A}(x)$.

Пусть $\mathfrak{A}(x) \sim \mathfrak{A}'(x)$. Тогда имеем

$$\vdash \overline{\mathfrak{A}}'(x) \sim \overline{\mathfrak{A}}(x).$$

Исходя из этой формулы, мы, так же как и в предыдущем случае, выведем

$$\vdash \forall x\, \overline{\mathfrak{A}}'(x) \sim \forall x\, \overline{\mathfrak{A}}(x),$$

и, следовательно,

$$\vdash \overline{\forall x\, \overline{\mathfrak{A}}(x)} \sim \overline{\forall x\, \overline{\mathfrak{A}}'(x)}. \qquad (1)$$

Подстановкой в 7а получим

$$\vdash \exists x\, \mathfrak{A}(x) \sim \overline{\forall x\, \overline{\mathfrak{A}}(x)}, \qquad (2)$$

$$\vdash \exists x\, \mathfrak{A}'(x) \sim \overline{\forall x\, \overline{\mathfrak{A}}'(x)}. \qquad (3)$$

Из (1), (2) и (3) непосредственно следует

$$\vdash \exists x\, \mathfrak{A}(x) \sim \exists x\, \mathfrak{A}'(x).$$

Таким образом, наше утверждение доказано для всех формул.

Эквивалентность формул $\mathfrak{A} \to \mathfrak{B}$ *и* $\overline{\mathfrak{A}} \vee \mathfrak{B}$, *т. е. истинность утверждения*

$$\vdash (\mathfrak{A} \to \mathfrak{B}) \sim \overline{\mathfrak{A}} \vee \mathfrak{B}, \qquad (4)$$

справедливая для исчисления высказываний, имеет место и для исчисления предикатов.

Доказательство этого в исчислении предикатов можно получить подстановками в формулу (4) исчисления высказываний.

На основании того, что при замене любых частей формулы эквивалентными мы переведем данную формулу в эквивалентную, *мы можем исключить знак* $\rightarrow$ *из формулы, заменив в ней каждую часть вида* $\mathfrak{A} \rightarrow \mathfrak{B}$ *формулой* $\overline{\mathfrak{A}} \vee \mathfrak{B}$. После такой замены мы получим формулу, эквивалентную данной.

Кроме того, *мы можем для каждой формулы, не содержащей знака* $\rightarrow$, *найти такую эквивалентную ей формулу, в которой знаки отрицания относятся только к элементарным частям.*

В самом деле, если какая-нибудь формула имеет вид $\overline{\forall x\, \mathfrak{A}(x)}$ (соответственно $\overline{\exists x\, \mathfrak{A}(x)}$), то формула $\exists x\, \overline{\mathfrak{A}}(x)$ (соответственно $\forall x\, \overline{\mathfrak{A}}(x)$) ей эквивалентна. Поэтому мы можем всегда знак отрицания, стоящий над квантором, ввести под знак квантора, изменив при этом квантор всеобщности на квантор существования и обратно. Эквивалентности

$$\vdash \overline{\mathfrak{A} \,\&\, \mathfrak{B}} \sim \overline{\mathfrak{A}} \vee \overline{\mathfrak{B}},$$

$$\vdash \overline{\mathfrak{A} \vee \mathfrak{B}} \sim \overline{\mathfrak{A}} \,\&\, \overline{\mathfrak{B}},$$

$$\vdash \overline{\overline{\mathfrak{A}}} \sim \mathfrak{A},$$

которые мы доказали для исчисления высказываний, имеют место и для исчисления предикатов [их доказательство в исчислении предикатов таково же, как и в исчислении высказываний (см. главу II)]. Отсюда следует, что знак отрицания, стоящий над логической суммой, можно внести внутрь, только при этом сумма перейдет в произведение; знак отрицания над логическим произведением также вносится внутрь формулы, причем произведение переходит в сумму. Если же знак отрицания стоит над знаком отрицания, то оба эти знака уничтожаются.

В силу сказанного мы можем последовательно вносить знак отрицания внутрь формулы, заменяя при этом формулу на эквивалентную. Очевидно, что в результате таких операций мы придем к формуле, у которой знак отрицания относится только к ее элементарным частям.

Формулы, не содержащие знака $\rightarrow$ *и такие, что знак отрицания относится только к элементарным частям, мы будем называть приведенными.* Из изложенного следует, что для каждой формулы $\mathfrak{A}$ существует эквивалентная ей приведенная формула. Эту формулу мы будем называть *приведенной формой формулы* $\mathfrak{A}$.

Рассмотрим пример приведения формулы к приведенной форме:

$$\overline{\exists x (A (x) \rightarrow B (x))}.$$

Исключим сначала знак $\rightarrow$. Заменив $A(x) \rightarrow B(x)$ на $\bar{A}(x) \vee B(x)$, имеем

$$\overline{\exists x (\bar{A} (x) \vee B (x))}.$$

Затем внесем внешний знак отрицания под квантор:

$$\forall x \,(\overline{\bar{A} (x) \vee B (x)}).$$

Далее внесем знак отрицания внутрь суммы:

$$\forall x \,(\bar{\bar{A}} (x) \,\&\, \bar{B} (x)).$$

Уничтожим двойной знак отрицания:

$$\forall x \,(A (x) \,\&\, \bar{B} (x)).$$

Полученная формула эквивалентна данной нам формуле и является приведенной формулой. Следовательно, она является приведенной формой исходной формулы.

Эквивалентности, выражающие ассоциативность и коммутативность логической суммы и логического произведения и два дистрибутивных закона, которые мы доказали в исчислении высказываний:

a. $(A \vee B) \vee C \sim A \vee (B \vee C)$;
b. $A \vee B \sim B \vee A$;
c. $(A \,\&\, B) \,\&\, C \sim A \,\&\, (B \,\&\, C)$;
d. $A \,\&\, B \sim B \,\&\, A$;
e. $A \,\&\, (B \vee C) \sim A \,\&\, B \vee A \,\&\, C$;
f. $A \vee B \,\&\, C \sim (A \vee B) \,\&\, (A \vee C)$,

справедливы и для исчисления предикатов (см. главу II). Поэтому в исчислении предикатов, в вопросах, для которых эквивалентные формулы равноправны, мы также иногда будем в выражениях, в которых члены соединены только знаком & или только знаком $\vee$, опускать скобки. Например, выражение

$$(\mathfrak{A} \& \mathfrak{B}) \& \mathfrak{C}$$

будем писать в виде

$$\mathfrak{A} \& \mathfrak{B} \& \mathfrak{C},$$

а выражение

$$\mathfrak{A} \vee (\mathfrak{B} \vee \mathfrak{C}) \vee (\mathfrak{G} \vee \mathfrak{H})$$

в виде

$$\mathfrak{A} \vee \mathfrak{B} \vee \mathfrak{C} \vee \mathfrak{G} \vee \mathfrak{H}.$$

Конечно, это выражение не является формулой. Мы будем подразумевать под таким выражением любую формулу, которую можно из него получить, расставив надлежащим образом скобки.

§ 11. Закон двойственности

Для формул, не содержащих символа $\rightarrow$, установим понятие «*двойственных формул*». Назовем знаки $\&$ и $\vee$ двойственными друг другу. Назовем кванторы $\forall x$ и $\exists x$ также двойственными. Будем говорить, что *формула* $\mathfrak{B}$ *двойственна формуле* $\mathfrak{A}$, *если она может быть получена из формулы* $\mathfrak{A}$ *изменением каждого из символов* $\&$, $\vee$, $\forall x$, $\exists x$ *на двойственный.*

Из определения следует, что понятие двойственности симметрично, т. е. если $\mathfrak{B}$ двойственна $\mathfrak{A}$, то и $\mathfrak{A}$ двойственна $\mathfrak{B}$.

Примеры двойственных формул.

1. $\forall x\,(A \vee B(x) \& (B(y) \vee \overline{B}(x)))$;

двойственной для данной является формула

$$\exists x\,(A \& (B(x) \vee B(y) \& \overline{B}(x))).$$

2. $\forall x\,\exists y\,(A(x,\ y) \vee \forall z\,A(x,\ z) \& \exists z\,\overline{A}(y,\ z))$;

двойственной формулой будет

$$\exists x\,\forall y\,(A(x,\ y) \& (\exists z\,A(x,\ z) \vee \forall z\,\overline{A}(y,\ z))).$$

Дадим понятию «двойственная формула» еще индуктивное определение, которое нам будет в дальнейшем более удобно при доказательствах.

а) Для элементарной формулы двойственной является она сама.

b) Если $\mathfrak{A}^*$ двойственна $\mathfrak{A}$, а $\mathfrak{B}^*$ двойственна $\mathfrak{B}$, то для формулы $\mathfrak{A} \& \mathfrak{B}$ двойственной формулой является $\mathfrak{A}^* \vee \mathfrak{B}^*$, а для $\mathfrak{A} \vee \mathfrak{B}$ — формула $\mathfrak{A}^* \& \mathfrak{B}^*$.

c) Если $\mathfrak{A}^*$ двойственна для $\mathfrak{A}$, то для $\overline{\mathfrak{A}}$ двойственной формулой является $\overline{\mathfrak{A}}^*$.

d) Если $\mathfrak{A}^*(x)$ двойственна формуле $\mathfrak{A}(x)$, то для $\forall x\, \mathfrak{A}(x)$ [соответственно для $\exists x\, \mathfrak{A}(x)$] двойственной формулой будет $\exists x\, \mathfrak{A}^*(x)$ [соответственно $\forall x\, \mathfrak{A}^*(x)$]. Так как по предположению рассматриваемые формулы не содержат знака $\rightarrow$, то понятие «двойственная формула» определено полностью.

Симметричность отношения двойственности является следствием данного определения и легко доказывается по индукции. Формулу, двойственную $\mathfrak{A}$, будем обозначать $\mathfrak{A}^*$.

Лемма. *Пусть $\mathfrak{A}(A_1, \ldots, A_n, F_1, \ldots, F_m)$ — формула исчисления предикатов, не содержащая знака $\rightarrow$, $A_1, \ldots, A_n$ суть все элементарные высказывания, входящие в $\mathfrak{A}$, а $F_1, \ldots, F_m$ — все элементарные предикаты, входящие в $\mathfrak{A}$. Тогда имеет место*

$$\vdash \overline{\mathfrak{A}}(A_1, \ldots, A_n, F_1, \ldots, F_m) \sim \\ \sim \mathfrak{A}^*(\overline{A}_1, \ldots, \overline{A}_n, \overline{F}_1, \ldots, \overline{F}_m).$$

Докажем эту лемму по индукции, соответствующей индуктивному определению двойственной формулы.

Для элементарной формулы справедливость леммы очевидна, так как элементарная формула представляет собой либо высказывание, либо предикат и двойственная ей формула с ней совпадает.

Пусть лемма верна для формул

$$\mathfrak{B}(B_1, \ldots, B_p, G_1, \ldots, G_q) \text{ и } \mathfrak{A}(A_1, \ldots, A_n, F_1, \ldots, F_m),$$

т. е. имеем

$$\vdash \overline{\mathfrak{A}}(A_1, \ldots, A_n, F_1, \ldots, F_m) \sim \\ \sim \mathfrak{A}^*(\overline{A}_1, \ldots, \overline{A}_n, \overline{F}_1, \ldots, \overline{F}_m),$$

$$\vdash \overline{\mathfrak{B}}(B_1, \ldots, B_p, G_1, \ldots, G_q) \sim \\ \sim \mathfrak{B}^*(\overline{B}_1, \ldots, \overline{B}_p, \overline{G}_1, \ldots, \overline{G}_q).$$

Покажем, что тогда лемма верна и для конъюнкции и дизъюнкции формул $\mathfrak{A}$ и $\mathfrak{B}$. В самом деле, имеем

$$\vdash \overline{\mathfrak{A} \& \mathfrak{B}} \sim \overline{\mathfrak{A}} \vee \overline{\mathfrak{B}}.$$

Заменяя $\overline{\mathfrak{A}}$ и $\overline{\mathfrak{B}}$ на основании написанных выше эквивалентностей, получим

$$\vdash \overline{\mathfrak{A} \& \mathfrak{B}} \sim \mathfrak{A}^*(\overline{A}_1, \ldots, \overline{A}_n, \overline{F}_1, \ldots, \overline{F}_m) \vee \\ \vee \mathfrak{B}^*(\overline{B}_1, \ldots, \overline{B}_p, \overline{G}_1, \ldots, \overline{G}_q),$$

но

$$\mathfrak{A}^*(\overline{A}_1, \ldots, \overline{A}_n, \overline{F}_1, \ldots, \overline{F}_m) \vee \\ \vee \mathfrak{B}^*(\overline{B}_1, \ldots, \overline{B}_p, G_1, \ldots, \overline{G}_q)$$

представляет собой, по определению,

$$(\mathfrak{A}(\overline{A}_1, \ldots, \overline{A}_n, \overline{F}_1, \ldots, \overline{F}_m) \& \\ \& \mathfrak{B}(\overline{B}_1, \ldots, \overline{B}_p, \overline{G}_1, \ldots, \overline{G}_q))^*,$$

поэтому

$$\vdash \overline{\mathfrak{A} \& \mathfrak{B}} \sim (\mathfrak{A}(\overline{A}_1, \ldots, \overline{A}_n, \overline{F}_1, \ldots, \overline{F}_m) \& \\ \& \mathfrak{B}(\overline{B}_1, \ldots, \overline{B}_p, \overline{G}_1, \ldots, \overline{G}_q))^*.$$

Справедливость леммы для $\mathfrak{A} \vee \mathfrak{B}$ доказывается аналогичным образом.

Допустим, что лемма верна для $\mathfrak{A}(A_1, \ldots, A_n, F_1, \ldots, F_m)$. Покажем, что она верна и для $\overline{\mathfrak{A}}$. В силу допущения мы будем иметь

$$\vdash \overline{\mathfrak{A}}(A_1, \ldots, A_n, F_1, \ldots, F_m) \sim \\ \sim \mathfrak{A}^*(\overline{A}_1, \ldots, \overline{A}_n, \overline{F}_1, \ldots, \overline{F}_m).$$

Если формулы эквивалентны, то их отрицания также эквивалентны. Поэтому имеем

$$\vdash \overline{\overline{\mathfrak{A}}}(A_1, \ldots, A_n, F_1, \ldots, F_m) \sim \\ \sim \overline{\mathfrak{A}^*}(\overline{A}_1, \ldots, \overline{A}_n, \overline{F}_1, \ldots, \overline{F}_m).$$

Но по определению $\overline{\mathfrak{A}}^*$ есть $(\overline{\mathfrak{A}})^*$. Следовательно,

$$\vdash \overline{\overline{\overline{\mathfrak{A}}}}(A_1, \ldots, A_n, F_1, \ldots, F_m) \sim \\ \sim (\overline{\mathfrak{A}}(\overline{A}_1, \ldots, \overline{A}_n, \overline{F}_1, \ldots, \overline{F}_m))^*,$$

и мы, таким образом, получили требуемую эквивалентность.

Пусть для формулы $\mathfrak{A}(x, A_1, \ldots, F_m)$ лемма верна. Покажем, что тогда она верна для формул

$$\forall x \mathfrak{A}(x, A_1, \ldots, F_m) \text{ и } \exists x \mathfrak{A}(x, A_1, \ldots, F_m).$$

На основании индуктивного предположения имеем

$$\vdash \overline{\mathfrak{A}}(x, A_1, \ldots, F_m) \sim \mathfrak{A}^*(x, \bar{A}_1, \ldots, \bar{F}_m),$$

но тогда

$$\vdash \exists x \overline{\mathfrak{A}}(x, A_1, \ldots, F_m) \sim \exists x \mathfrak{A}^*(x, \bar{A}_1, \ldots, \bar{F}_m).$$

На основании теоремы 7 § 9 имеем

$$\vdash \exists x \overline{\mathfrak{A}}(x, A_1, \ldots, F_m) \sim \overline{\forall x \mathfrak{A}(x, A_1, \ldots, F_m)}.$$

Из двух последних эквивалентностей выводим

$$\vdash \overline{\forall x \mathfrak{A}(x, A_1, \ldots, F_m)} \sim \exists x \mathfrak{A}^*(x, \bar{A}_1, \ldots, \bar{F}_m).$$

В силу определения правая часть этой формулы представляет собой

$$(\forall x \mathfrak{A}(x, \bar{A}_1, \ldots, \bar{F}_m))^*;$$

следовательно,

$$\vdash \overline{\forall x \mathfrak{A}(x, A_1, \ldots, F_m)} \sim (\forall x \mathfrak{A}(x, \bar{A}_1, \ldots, \bar{F}_m))^*.$$

Для формулы $\exists x \mathfrak{A}(x, A_1, \ldots, F_m)$ лемма доказывается аналогичным образом. Итак, мы доказали справедливость леммы для всех формул, не включающих знака $\to$.

Теорема. *Если формулы $\mathfrak{A}$ и $\mathfrak{B}$ эквивалентны, то двойственные им формулы также эквивалентны.*

Пусть $\mathfrak{A}(A_1, \ldots, A_n, F_1, \ldots, F_m)$ и $\mathfrak{B}(B_1, \ldots, B_p, G_1, \ldots, G_q)$ — эквивалентные формулы, $A_1, \ldots, A_n, B_1, \ldots, B_p$ — все входящие в них переменные высказывания, а $F_1, \ldots, F_m, G_1, \ldots, G_q$ — все предикаты. Двойственные формулы будем по-прежнему изображать посредством звездочки.

Если формулы $\mathfrak{A}$ и $\mathfrak{B}$ эквивалентны, то их отрицания также эквивалентны. Поэтому имеем

$$\vdash \overline{\mathfrak{A}}(A_1, \ldots, F_m) \sim \overline{\mathfrak{B}}(B_1, \ldots, G_q).$$

На основании предыдущей леммы формула $\mathfrak{A}(A_1, \ldots, F_m)$ эквивалентна формуле $\mathfrak{A}^*(\overline{A}_1, \ldots, \overline{F}_m)$, а формула $\mathfrak{B}(B_1, \ldots, G_q)$ эквивалентна формуле $\mathfrak{B}^*(\overline{B}_1, \ldots, \overline{G}_q)$. Заменив обе части полученной нами выводимой формулы эквивалентными формулами, получим также выводимую формулу:

$$\vdash \mathfrak{A}^*(\overline{A}_1, \ldots, \overline{F}_m) \sim \mathfrak{B}^*(\overline{B}_1, \ldots, \overline{G}_q).$$

Сделаем подстановки в эту формулу, заменив A_i на $\overline{A}_i$, B_i на $\overline{B}_i$, F_i на $\overline{F}_i$, G_i на $\overline{G}_i$. Получим тогда

$$\vdash \mathfrak{A}^*(\overline{\overline{A}}_1, \ldots, \overline{\overline{F}}_m) \sim \mathfrak{B}^*(\overline{\overline{B}}_1, \ldots, \overline{\overline{G}}_q).$$

Заменив в этой формуле каждую часть вида $\overline{\overline{A}}_i$ на эквивалентную ей A_i, $\overline{\overline{B}}_i$ на B_i, $\overline{\overline{F}}_i$ на F_i и $\overline{\overline{G}}_i$ на G_i, получим

$$\vdash \mathfrak{A}^*(A_1, \ldots, F_m) \sim \mathfrak{B}^*(B_1, \ldots, G_q).$$

Доказанная теорема носит название *закона двойственности*. Она позволяет из эквивалентностей, выводимость которых установлена, получать другие выводимые эквивалентности. Она, как и теорема дедукции, облегчает доказательство выводимости некоторых формул. Например, мы доказали (теорема 2 § 9), что

$$\vdash \forall x \forall y F(x, y) \sim \forall y \forall x F(x, y).$$

В силу закона двойственности мы можем утверждать выводимость следующей формулы:

$$\vdash \exists x \exists y F(x, y) \sim \exists y \exists x F(x, y).$$

Из этих эквивалентностей можно вывести следующее правило.

Если непосредственно друг за другом стоящие однородные кванторы переставить, то формула при этом превратится в эквивалентную.

§ 12. Нормальные формы

Нормальные формулы и нормальные формы мы уже рассматривали в главе III при содержательном описании логики предикатов. Те же понятия мы введем и для исчисления предикатов.

Будем называть приведенную формулу нормальной, если в последовательности символов, образующих формулу, кванторы предшествуют всем остальным символам.

Можно доказать, что для каждой формулы существует эквивалентная ей нормальная формула.

Для доказательства этого утверждения необходимо установить справедливость некоторых преобразований эквивалентности, аналогичных преобразованиям равносильности, которые мы употребляли в содержательной логике предикатов для той же цели (глава III, § 2).

Теорема 1.

$$\vdash \forall x (A \vee F(x)) \sim A \vee \forall x F(x).$$

В теореме 8 § 9 было доказано

$$\vdash \forall x (A \to F(x)) \sim A \to \forall x F(x).$$

На основании эквивалентности $\mathfrak{A} \to \mathfrak{B} \sim \overline{\mathfrak{A}} \vee \mathfrak{B}$ мы, заменив обе части рассматриваемой формулы, получим

$$\vdash \forall x (\overline{A} \vee F(x)) \sim \overline{A} \vee \forall x F(x).$$

Подставив в эту формулу $\bar{A}$ вместо A, будем иметь

$$\vdash \forall x (\overline{\overline{A}} \vee F(x)) \sim \overline{\overline{A}} \vee \forall x F(x).$$

Заменив $\overline{\overline{A}}$ на эквивалентную ей элементарную формулу A, получим требуемую формулу.

Теорема 2.

$$\vdash \forall x (A \& F(x)) \sim A \& \forall x F(x).$$

Для доказательства применим теорему дедукции. Рассмотрим формулу

$$\forall x (A \& F(x)) \to A \& \forall x F(x).$$

Покажем, что следствие выводимо из посылки. В самом деле, приемом, который мы неоднократно употребляли, доказываем выводимость из посылки формул $\forall x F(x)$ и A. Формула

$$\forall x F(x) \to (A \to A \& \forall x F(x))$$

выводима в исчислении предикатов. Поэтому она выводима из формулы $\forall x (A \& F(x))$. Применяя дважды правило заключения к формулам $\forall x F(x)$, A и $\forall x F(x) \to (A \to A \& \forall x F(x))$, видим, что формула $A \& \forall x F(x)$ также выводима из $\forall x (A \& F(x))$. Тогда в силу теоремы дедукции получим

$$\vdash \forall x (A \& F(x)) \to A \& \forall x F(x). \qquad (1)$$

Докажем выводимость обратного следования. Для этого покажем, что формула $\forall x (A \& F(x))$ выводима из формулы $A \& \forall x F(x)$. В самом деле, формулы A и $F(y)$, как мы видели, выводимы из формулы $A \& \forall x F(x)$. В силу этого выводима и формула $A \& F(y)$. Из выводимой формулы

$$A \& F(y) \to (A \to A \& F(y)),$$

применив правило заключения, получим, что формула $A \to A \& F(y)$ выводима из формулы $A \& \forall x F(x)$. Применив правило связывания квантором и переименовав связанные переменные, заключаем, что формула

$$A \to \forall x (A \& F(x))$$

выводима из формулы $A \& \forall x F(x)$. Удалив на основании правила заключения посылку A, найдем, что формула $\forall x (A \& F(x))$ выводима из формулы $A \& \forall x F(x)$. Тогда на основании теоремы дедукции заключаем, что

$$\vdash A \& \forall x F(x) \to \forall x (A \& F(x)). \qquad (2)$$

Из выводимости следований (1) и (2) следует выводимость эквивалентности

$$\vdash A \& \forall x F(x) \sim \forall x (A \& F(x)).$$

Из теорем 1 и 2, на основании закона двойственности, вытекают следующие теоремы.

Теорема 1'.

$$\vdash \exists x (A \& F(x)) \sim A \& \exists x F(x).$$

Теорема 2'.

$$\vdash \exists x (A \vee F(x)) \sim A \vee \exists x F(x).$$

Из теорем 1, 2, 1' и 2' можно вывести правила, позволяющие производить преобразования эквивалентности приведенных формул, состоящие в вынесении за скобки и внесении в скобки кванторов всеобщности и существования.

Выпишем эти правила:

$$\text{a.}\ \frac{\forall x\,(\mathfrak{A} \vee \mathfrak{B}(x))}{\mathfrak{A} \vee \forall x\,\mathfrak{B}(x)}, \qquad \text{a}'.\ \frac{\mathfrak{A} \vee \forall x\,\mathfrak{B}(x)}{\forall x\,(\mathfrak{A} \vee \mathfrak{B}(x))},$$

$$\text{b.}\ \frac{\forall x\,(\mathfrak{A} \,\&\, \mathfrak{B}(x))}{\mathfrak{A} \,\&\, \forall x\,\mathfrak{B}(x)}, \qquad \text{b}'.\ \frac{\mathfrak{A} \,\&\, \forall x\,\mathfrak{B}(x)}{\forall x\,(\mathfrak{A} \,\&\, \mathfrak{B}(x))},$$

$$\text{c.}\ \frac{\exists x\,(\mathfrak{A} \,\&\, \mathfrak{B}(x))}{\mathfrak{A} \,\&\, \exists x\,\mathfrak{B}(x)}, \qquad \text{c}'.\ \frac{\mathfrak{A} \,\&\, \exists x\,\mathfrak{B}(x)}{\exists x\,(\mathfrak{A} \,\&\, \mathfrak{B}(x))},$$

$$\text{d.}\ \frac{\exists x\,(\mathfrak{A} \vee \mathfrak{B}(x))}{\mathfrak{A} \vee \exists x\,\mathfrak{B}(x)}, \qquad \text{d}'.\ \frac{\mathfrak{A} \vee \exists x\,\mathfrak{B}(x)}{\exists x\,(\mathfrak{A} \vee \mathfrak{B}(x))},$$

в предположении, что формула $\mathfrak{A}$ не содержит x в качестве свободной переменной.

Предоставляем читателю доказать (используя теорему дедукции) следующие теоремы:

$$\vdash \forall x\,\mathfrak{A}(x) \vee \forall x\,\mathfrak{B}(x) \to \forall x\,(\mathfrak{A}(x) \vee \mathfrak{B}(x)),$$

$$\vdash \forall x\,(\mathfrak{A}(x) \,\&\, \mathfrak{B}(x)) \sim \forall x\,\mathfrak{A}(x) \,\&\, \forall x\,\mathfrak{B}(x),$$

и двойственные им теоремы:

$$\vdash \exists x\,(\mathfrak{A}(x) \,\&\, \mathfrak{B}(x)) \to \exists x\,\mathfrak{A}(x) \,\&\, \exists x\,\mathfrak{B}(x),$$

$$\vdash \exists x\,(\mathfrak{A}(x) \vee \mathfrak{B}(x)) \sim \exists x\,\mathfrak{A}(x) \vee \exists x\,\mathfrak{B}(x).$$

Этим теоремам соответствуют правила:

$$\frac{\forall x\,\mathfrak{A}(x) \vee \forall x\,\mathfrak{B}(x)}{\forall x\,(\mathfrak{A}(x) \vee \mathfrak{B}(x))},$$

$$\frac{\forall x\,(\mathfrak{A}(x) \,\&\, \mathfrak{B}(x))}{\forall x\,\mathfrak{A}(x) \,\&\, \forall x\,\mathfrak{B}(x)}, \qquad \frac{\forall x\,\mathfrak{A}(x) \,\&\, \forall x\,\mathfrak{B}(x)}{\forall x\,(\mathfrak{A}(x) \,\&\, \mathfrak{B}(x))},$$

$$\frac{\exists x\,(\mathfrak{A}(x) \,\&\, \mathfrak{B}(x))}{\exists x\,\mathfrak{A}(x) \,\&\, \exists x\,\mathfrak{B}(x)},$$

$$\frac{\exists x\,(\mathfrak{A}(x) \vee \mathfrak{B}(x))}{\exists x\,\mathfrak{A}(x) \vee \exists x\,\mathfrak{B}(x)}, \qquad \frac{\exists x\,\mathfrak{A}(x) \vee \exists x\,\mathfrak{B}(x)}{\exists x\,(\mathfrak{A}(x) \vee \mathfrak{B}(x))}.$$

В главе III, при изложении алгебры предикатов, мы установили преобразования равносильности, аналогичные тем преобразованиям эквивалентности, которые выражены в виде правил a — d′. Пользуясь этими преобразованиями равносильности в главе III, мы доказали, что для каждой формулы существует равносильная ей нормальная формула. Мы теперь можем, исходя из преобразований эквивалентности a — d′, точно таким же образом доказать, что для всякой приведенной формулы (а следовательно, и для произвольной формулы) существует эквивалентная ей нормальная формула. Доказательство при этом может быть взято из главы III. Хотя мы там и не ставили себе задачи ограничиваться конструктивными средствами, тем не менее фактически доказательство было конструктивным. Поэтому мы не будем приводить его во всем подробностях. Напомним только, что так как можно производить преобразования вынесения кванторов за скобки, то можно добиться того, что все кванторы окажутся предшествующими остальным символам формулы.

Нормальную формулу, эквивалентную данной формуле, мы будем называть *нормальной формой данной формулы.*

§ 13. Дедуктивная эквивалентность

Введем понятие «дедуктивной эквивалентности формул». *Две формулы $\mathfrak{A}$ и $\mathfrak{B}$ называются дедуктивно эквивалентными в исчислении, если из аксиом этого исчисления и формулы $\mathfrak{A}$ посредством правил исчисления можно вывести формулу $\mathfrak{B}$ и, обратно, из аксиом исчисления и формулы $\mathfrak{B}$ посредством правил исчисления выводима формула $\mathfrak{A}$.*

Для исчисления предикатов понятия «эквивалентные формулы» и «дедуктивно эквивалентные» не равнозначны.

Если $\mathfrak{A}$ и $\mathfrak{B}$ эквивалентны в исчислении предикатов, то они и дедуктивно эквивалентны. В самом деле, пусть $\mathfrak{A}$ эквивалентна $\mathfrak{B}$. Это значит, что формула $\mathfrak{A} \sim \mathfrak{B}$ выводима в исчислении предикатов. В таком случае формула $\mathfrak{A} \rightarrow \mathfrak{B}$ также выводима. Если мы присоединим к аксиомам исчисления предикатов формулу $\mathfrak{A}$, то из формул $\mathfrak{A}$ и $\mathfrak{A} \rightarrow \mathfrak{B}$, применив правило заключения, можно вывести формулу $\mathfrak{B}$. Присоединив к аксиомам формулу $\mathfrak{B}$, таким же образом можно вывести формулу $\mathfrak{A}$. Отсюда следует что эквивалентные формулы $\mathfrak{A}$ и $\mathfrak{B}$ являются также дедуктивно эквивалентными.

Обратное утверждение, однако, неверно. Рассмотрим элементарные формулы A и B. Они дедуктивно эквивалентны. В самом деле, если мы присоединим к аксиомам исчисления предикатов формулу A, то любая формула и, в частности, B станет выводимой посредством подстановки в формулу A. То же самое будет, если мы присоединим к аксиомам формулу B. Отсюда следует, что формулы A и B дедуктивно эквивалентны в исчислении предикатов. Однако эти формулы, очевидно, не эквивалентны, так как формула $A \sim B$ не является выводимой в исчислении высказываний. Поэтому, как мы знаем (см. § 4), она не является выводимой и в исчислении предикатов.

Заметим, что для исчисления высказываний понятие дедуктивной эквивалентности мало интересно. В силу полноты этого исчисления в узком смысле для каждой формулы имеет место одно из двух: или она выводима в исчислении высказываний, или присоединение ее к аксиомам ведет к противоречию (глава II). Рассмотрим две произвольные формулы исчисления высказываний $\mathfrak{A}$ и $\mathfrak{B}$. Если обе они выводимы в исчислении высказываний, то они просто эквивалентны. Если одна выводима, а другая нет, то они не могут быть дедуктивно эквивалентны, так как присоединение к аксиомам выводимой формулы новых выводимых формул не дает и другая формула поэтому останется невыводимой. Если обе формулы невыводимы, то они дедуктивно эквивалентны, но тогда присоединение каждой из них к аксиомам образует противоречивую систему.

§ 14. Нормальные формулы Сколема

Сколем установил весьма интересный вид формул, к которому можно привести любую формулу исчисления предикатов.

Формула называется нормальной формулой Сколема, если она, во-первых, является нормальной формулой и, во-вторых, в ней все кванторы существования, если они есть, предшествуют всем кванторам всеобщности. Например, формулы

$$\exists x \exists y \forall z \forall u A(x, y, z, u),$$
$$\forall x \forall y A(x, y)$$

являются нормальными формулами Сколема. Но формулы

$$\forall x \exists y A(x, y), \quad \exists x \forall y \exists z A(x, y, z)$$

не являются нормальными формулами Сколема.

Теорема Сколема. *Для всякой формулы исчисления предикатов существует дедуктивно эквивалентная ей нормальная формула Сколема.*

Для доказательства этой теоремы нам придется доказать предварительно некоторые леммы.

Лемма 1. *Формула*

$$\exists x_1 \ldots \exists x_n \forall y \mathfrak{A},$$

где $\mathfrak{A}$ — нормальная формула, дедуктивно эквивалентна формуле

$$\exists x_1 \ldots \exists x_n [\forall y (\mathfrak{A} \to A(y)) \to \forall y A(y)],$$

где A — переменный предикат, не содержащийся в $\mathfrak{A}$.

Для доказательства этой леммы мы воспользуемся следующими формулами, доказанными выше (см. § 9, теоремы 4 и 5):

$$\forall x [A(x) \to B(x)] \to [\forall x A(x) \to \forall x B(x)], \tag{1}$$

$$\forall x [A(x) \to B(x)] \to [\exists x A(x) \to \exists x B(x)]. \tag{2}$$

Предположим, что формула

$$\exists x_1 \ldots \exists x_n \forall y \mathfrak{A}(x_1, \ldots, x_n, y) \tag{3}$$

присоединена в качестве аксиомы к исчислению предикатов или же выводима в нем. Формула

$$\vdash \mathfrak{A}(x_1, \ldots, x_n, t) \to ((\mathfrak{A} \to A(t)) \to A(t))$$

выводима, так как она, как легко проверить, получается подстановками из выводимой формулы исчисления высказываний. Из этой формулы и из выводимой формулы

$$\forall y \mathfrak{A}(x_1, \ldots, x_n, y) \to \mathfrak{A}(x_1, \ldots, x_n, t)$$

с помощью правила силлогизма получим формулу

$$\vdash \forall y \mathfrak{A}(x_1, \ldots, x_n, y) \to ((\mathfrak{A} \to A(t)) \to A(t)).$$

Далее, применяя первое правило связывания квантором и переименовывая переменные, получим

$$\vdash \forall y\, \mathfrak{A}(x_1, \ldots, x_n, y) \to \forall y\, ((\mathfrak{A} \to A(y)) \to A(y)).$$

Затем на основании формулы (1), пользуясь правилом силлогизма, получим

$$\vdash \forall y\, \mathfrak{A}(x_1, \ldots, x_n, y) \to [\forall y\, (\mathfrak{A} \to A(y)) \to \forall y\, A(y)].$$

Применив к этой формуле производное правило связывания квантором, получим

$$\vdash \forall x_n [\forall y\, \mathfrak{A}(x_1, \ldots, x_n, y) \to \\ \to (\forall y\, (\mathfrak{A} \to A(y)) \to \forall y A(y))]. \quad (4)$$

Совершив подстановку в формулу (2) вместо предиката $A(x)$ формулы

$$\forall y\, \mathfrak{A}(x_1, \ldots, x_{n-1}, x, y),$$

а вместо предиката $B(x)$ — формулы

$$\forall y\, (\mathfrak{A}(x_1, \ldots, x_{n-1}, x, y) \to A(y)) \to \forall y\, A(y)$$

и заменив x на x_n, получим

$$\vdash \forall x_n [\forall y\, \mathfrak{A}(x_1, \ldots, x_n, y) \to (\forall y\, (\mathfrak{A}(x_1, \ldots, x_n, y) \to \\ \to A(y)) \to \forall y\, A(y)) \to (\exists x_n \forall y\, \mathfrak{A}(x_1, \ldots, x_n, y) \to \\ \to \exists x_n (\forall y\, (\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall y\, A(y))].$$

Посылка в этой формуле есть выводимая формула (4). Поэтому на основании правила заключения следствие также является выводимой формулой, т. е.

$$\vdash \exists x_n \forall y\, \mathfrak{A}(x_1, \ldots, x_n, y) \to \\ \to \exists x_n (\forall y\, (\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall y\, A(y)).$$

Аналогичным образом из этой формулы, связав сначала ее квантором $\forall x_{n-1}$, при помощи формулы (2) получим

$$\vdash \exists x_{n-1} \exists x_n \forall y\, \mathfrak{A}(x_1, \ldots, x_n, y) \to \\ \to \exists x_{n-1} \exists x_n [\forall y\, (\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall y\, A(y)].$$

Продолжая подробные рассуждения далее, мы придем к выводимой формуле

$$\vdash \exists x_1 \ldots \exists x_n \forall y\, \mathfrak{A}(x_1, \ldots, x_n, y) \to \\ \to \exists x_1 \ldots \exists x_n [\forall y\, (\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall y\, A(y)].$$

Отсюда следует, что из посылки, т. е. формулы (3), выводима формула

$$\exists x_1 \ldots \exists x_n [(\forall y\, \mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall y\, A(y)]. \quad (5)$$

Таким образом, мы показали, что если к аксиомам исчисления предикатов присоединить в качестве аксиомы формулу (3), то формула (5) станет выводимой. Тем самым лемма в одну сторону доказана.

Допустим теперь, что формула (5) присоединена к аксиомам исчисления предикатов. Сделаем в ней подстановку, заменив предикат $A(t)$ формулой $\mathfrak{A}(x_1, \ldots \ldots, x_n, t)$. Получим выводимую в новой системе аксиом формулу

$$\exists x_1 \ldots \exists x_n [\forall y (\mathfrak{A}(x_1, \ldots, x_n, y) \to \mathfrak{A}(x_1, \ldots, x_n, y)) \to \\ \to \forall y\, \mathfrak{A}(x_1, \ldots, x_n, y)]. \quad (6)$$

Формула

$$(\mathfrak{R} \to \forall y\, \mathfrak{A}(y)) \to \forall y\, \mathfrak{A}(y),$$

где $\mathfrak{R}$ — любая выводимая формула, также выводима, так как получается подстановкой в выводимую формулу исчисления высказываний. Так как $\forall y (\mathfrak{A} \to \mathfrak{A})$ — выводимая формула, то выводима и формула

$$(\forall y (\mathfrak{A} \to \mathfrak{A}) \to \forall y\, \mathfrak{A}(y)) \to \forall y\, \mathfrak{A}(y).$$

Связывая эту формулу квантором $\forall x_n$, получим выводимую формулу

$$\forall x_n [(\forall y (\mathfrak{A} \to \mathfrak{A}) \to \forall y\, \mathfrak{A}(y)) \to \forall y\, \mathfrak{A}(y)].$$

Применяя к этой формуле те же рассуждения, что и в первой части доказательства, получим выводимую формулу

$$\exists x_n (\forall y (\mathfrak{A} \to \mathfrak{A}) \to \forall y\, \mathfrak{A}(y)) \to \exists x_n \forall y\, \mathfrak{A}(y).$$

Связывая затем, последовательно, эту формулу кванторами $\forall x_{n-1}, \ldots, \forall x_1$ и повторяя те же рассуждения, мы, наконец, получим

$$\vdash \exists x_1 \ldots \exists x_n (\forall y (\mathfrak{A} \to \mathfrak{A}) \to \forall y\, \mathfrak{A}(y)) \to \\ \to \exists x_1 \ldots \exists x_n \forall y\, \mathfrak{A}(y).$$

Посылкой этого следования является формула (6), выводимая в системе аксиом исчисления предикатов после присоединения к ней формулы (5). А тогда на основании правила заключения и следствие выводимо после присоединения формулы (5). Таким образом, дедуктивная эквивалентность формул (3) и (5) доказана.

Лемма 2. *Предположим, что формула* $\mathfrak{A}$ *имеет вид*

$$\mathrm{Q}_1 z_1 \mathrm{Q}_2 z_2 \ldots \mathrm{Q}_m z_m \mathfrak{C},$$

где $\mathrm{Q}_i z_i$ *— условное общее обозначение для кванторов* $\forall z_i$ *и* $\exists z_i$, *а* $\mathfrak{C}$ *кванторов не содержит*. [Кванторы $\mathrm{Q}_i z_i$ могут также отсутствовать.] *Тогда имеет место*

$$\vdash ((\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall z\, A(z)) \sim \mathrm{Q}_1 z_1 \ldots$$
$$\ldots \mathrm{Q}_m z_m \forall z ((\mathfrak{C}(z_1, \ldots, z_m, x_1, \ldots, x_n, y) \to A(y)) \to A(z)). \quad (7)$$

Чтобы доказать эквивалентность (7), мы преобразуем ее левую часть. Выпишем сначала в $\mathfrak{A}$ кванторы. Получим

$$(\mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \mathfrak{C} \to A(y)) \to \forall z\, A(z).$$

Затем исключим знак $\to$ посредством известных нам эквивалентных преобразований:

$$\overline{\overline{\mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \mathfrak{C}} \vee A(y)} \vee \forall z\, A(z).$$

После этого преобразуем левую часть, введя верхний знак отрицания внутрь дизъюнкции, и уничтожим сразу получающееся при этом двойное отрицание. Тогда имеем

$$\mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \mathfrak{C} \mathbin{\&} \overline{A}(y) \vee \forall z\, A(x).$$

Затем вынесем за общие скобки кванторы $\mathrm{Q}_1 z_1, \ldots$ $\ldots, \mathrm{Q}_m z_m$ и $\forall z$. Это, как мы уже знаем, можно сделать (см. § 12). Получим

$$\mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \forall z (\mathfrak{C} \mathbin{\&} \overline{A}(y) \vee A(z)).$$

Формула, стоящая под всеми знаками кванторов $\mathrm{Q}_i z_i$ и $\forall z$, эквивалентна формуле

$$(\mathfrak{C} \to A(y)) \to A(z).$$

Заменив ее этой эквивалентной формулой, имеем

$$\mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \forall z ((\mathfrak{C} \to A(y)) \to A(z)).$$

Эта формула представляет собой правую часть эквивалентности (7), которую нам требовалось доказать. Но так как мы получили ее посредством эквивалентных преобразований из левой части эквивалентности (7), то эта эквивалентность имеет место, и лемма доказана.

Лемма 3. *Формула*

$$\exists x_1 \ldots \exists x_n (\forall y (\mathfrak{A} \to A(y)) \to \forall z\, A(z)), \tag{8}$$

где $\mathfrak{A}$ *имеет вид, указанный в лемме* 2, *эквивалентна формуле*

$$\exists x_1 \ldots \exists x_n \exists y\, \mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \forall z [(\mathfrak{C}(z_1, \ldots, z_n, y) \to \\ \to A(y)) \to A(z)]. \tag{9}$$

Доказательство. В силу леммы 2 имеет место

$$\vdash [(\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall z\, A(z)] \to \mathrm{Q}_1 z_1 \ldots \\ \ldots \mathrm{Q}_m z_m \forall z [(\mathfrak{C}(z_1, \ldots, z_m, x_1, \ldots, x_n, y) \to A(y)) \to A(z)].$$

Связывая эту выводимую формулу квантором, получим

$$\vdash \forall y [[(\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall z\, A(z)] \to \mathrm{Q}_1 z_1 \ldots \\ \ldots \mathrm{Q}_m z_m \forall z [(\mathfrak{C}(z_1, \ldots, z_m, x_1, \ldots, x_n, y) \to A(y)) \to A(z)]].$$

Используя формулу (2) так же, как и в лемме 1, мы получим отсюда

$$\vdash \exists y [(\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall z\, A(z)] \to \exists y\, \mathrm{Q}_1 z_1 \ldots \\ \ldots \mathrm{Q}_m z_m \forall z [(\mathfrak{C}(z_1, \ldots, z_m, x_1, \ldots, x_n, y) \to \\ \to A(y)) \to A(z)]. \tag{10}$$

Рассмотрев истинное в силу леммы 2 обратное следование

$$\vdash \mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \forall z [(\mathfrak{C}(z_1, \ldots, z_m, x_1, \ldots, x_n, y) \to \\ \to A(y)) \to A(z)] \to [(\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall z\, A(z)],$$

мы таким же образом получим

$$\vdash \exists y\, \mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \forall z [(\mathfrak{C}(z_1, \ldots, z_m, x_1, \ldots, x_n, y) \to \\ \to A(y)) \to A(z)] \to \exists y [(\mathfrak{C}(x_1, \ldots, x_n, y) \to \\ \to A(y)) \to \forall z\, A(z)]. \tag{11}$$

Сопоставляя взаимно обратные следования (10) и (11), мы получим

$$\vdash \exists y\, [\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall z\, A(z)] \sim \exists y\, Q_1 z_1 \ldots$$
$$\ldots Q_m z_m \forall z\, [(\mathfrak{C}(z_1, \ldots, z_m, x_1, \ldots, x_n, y) \to A(y)) \to A(z)].$$

Очевидно, исходя из этой формулы, мы можем повторить наше рассуждение последовательно для кванторов $\exists x_n, \exists x_{n-1}, \ldots, \exists x_1$. В результате мы придем к эквивалентности

$$\vdash \exists x_1 \ldots \exists x_n \exists y\, [(\mathfrak{A}(x_1, \ldots, x_n, y) \to A(y)) \to \forall z\, A(z)] \sim$$
$$\sim \exists x_1 \ldots \exists x_n \exists y\, Q_1 z_1 \ldots Q_m z_m \forall z\, [(\mathfrak{C}(z_1, \ldots$$
$$\ldots, z_m, x_1, \ldots, x_n, y) \to A(y)) \to A(z)]. \qquad (12)$$

Покажем, что имеет место следующее утверждение:

$$\vdash [\forall y\, (\mathfrak{A} \to A(y)) \to \forall z\, A(z)] \sim$$
$$\sim \exists y\, [(\mathfrak{A} \to A(y)) \to \forall z\, A(z)]. \qquad (13)$$

Чтобы доказать выводимость этой эквивалентности, достаточно посредством эквивалентных преобразований из ее левой части получить правую Для этого сначала исключим знак $\to$ из левой части; получим формулу

$$\overline{\forall y\, (\overline{\mathfrak{A}} \vee A(y))} \vee \forall z\, A(z).$$

Внося знак отрицания под знак квантора $\forall y$, получим

$$\exists y\, \overline{(\overline{\mathfrak{A}} \vee A(y))} \vee \forall z\, A(z).$$

Вынося квантор $\exists y$, имеем

$$\exists y\, [\overline{\overline{\mathfrak{A}} \vee A(y)} \vee \forall z\, A(z)].$$

Вводя опять знак $\to$, получим левую часть эквивалентности (13):

$$\exists y\, [(\mathfrak{A} \to A(y)) \to \forall z\, A(z)].$$

Таким образом, выводимость эквивалентности (13) доказана.

Применив к этой эквивалентности те же рассуждения, которые мы уже неоднократно употребляли в этом параграфе, мы получим

$$\vdash \exists x_1 \ldots \exists x_n [\forall y (\mathfrak{A} \to A(y)) \to \forall z\, A(z)] \sim$$
$$\sim \exists x_1 \ldots \exists x_n \exists y [(\mathfrak{A} \to A(y)) \to \forall z\, A(z)]. \quad (14)$$

Рассматривая эквивалентности (14) и (12), мы с помощью правила силлогизма получим требуемую эквивалентность формул (8) и (9), и лемма, таким образом, доказана.

§ 15. Доказательство теоремы Сколема

Из лемм 1 и 3 легко получаем следующее заключение.

Формула

$$\exists x_1 \ldots \exists x_n \forall y\, \mathfrak{A}(x_1, \ldots, x_n, y)$$

или, что то же, формула

$$\exists x_1 \ldots \exists x_n \forall y\, \mathrm{Q}_1 z_1 \ldots$$
$$\ldots \mathrm{Q}_m z_m \mathfrak{C}(z_1, \ldots, z_m, x_1, \ldots, x_n, y) \quad (1)$$

дедуктивно эквивалентна формуле

$$\exists x_1 \ldots \exists x_n \exists y\, \mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \forall z\, \mathfrak{C}_1, \quad (2)$$

где $\mathfrak{C}_1$ *представляет собой формулу*

$$(\mathfrak{C} \to A(y)) \to A(z),$$

$\mathfrak{C}$ *и* $\mathfrak{C}_1$ *кванторов не содержат.*

Первый по порядку квантор всеобщности формулы (1) в дедуктивно эквивалентной формуле (2) заменился квантором существования, и вместе с тем в (2) появился новый квантор всеобщности — последний по порядку. Если в формуле (2) среди кванторов $\mathrm{Q}_i z_i$ есть кванторы всеобщности, то, применив к (2) те же рассуждения, мы можем получить дедуктивно эквивалентную ей, а следовательно, и формуле (1) формулу, у которой первый из кванторов всеобщности $\mathrm{Q}_r z_r$ заменится квантором существования и появится опять новый, последний по порядку квантор всеобщности. Если формула (2) имеет вид

$$\exists x_1 \ldots \exists x_n \exists y \exists z_1 \ldots \exists z_{r-1} \forall z_r\, \mathrm{Q}_{r+1} z_{r+1} \ldots \mathrm{Q}_m z_m \forall z\, \mathfrak{C}_1,$$

то дедуктивно эквивалентная ей формула имеет вид

$$\exists x_1 \ldots \exists x_n \exists y \exists z_1 \ldots \exists z_r \mathrm{Q}_{r+1} z_{r+1} \ldots \mathrm{Q}_m z_m \forall z \forall z' \mathfrak{C}_2.$$

Продолжая далее этот процесс, мы получим, наконец, формулу

$$\exists x_1 \ldots \exists x_n \exists y \exists z_1 \ldots \exists z_m \forall z \forall z' \ldots \forall z^{(p-1)} \mathfrak{C}_p, \qquad (3)$$

дедуктивно эквивалентную формуле (1), т. е. формуле

$$\exists x_1 \ldots \exists x_n \forall y \mathfrak{A}. \qquad (4)$$

Вместе с тем (3) является нормальной формулой Сколема. Теорема будет доказана, если мы покажем, что всякая формула дедуктивно эквивалентна формуле вида (1).

Мы знаем, что для каждой формулы существует эквивалентная ей нормальная формула. Поэтому достаточно доказать, что всякая нормальная формула эквивалентна формуле вида (1).

Рассмотрим произвольную нормальную формулу

$$\mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \mathfrak{B}, \qquad (5)$$

где $\mathfrak{B}$ кванторов не содержит. Кванторов $\mathrm{Q}_i z_i$ может и не быть. Пусть x и y — переменные, не входящие в эту формулу. Формула

$$\exists x \forall y \mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m [\mathfrak{B} \mathbin{\&} (A(x) \vee \bar{A}(x)) \mathbin{\&} (A(y) \vee \bar{A}(y))] \qquad (6)$$

является формулой вида (1). Внеся в ней все кванторы $\mathrm{Q}_i z_i$ в скобки, получим эквивалентную формулу

$$\exists x \forall y [\mathrm{Q}_1 z_1 \ldots \mathrm{Q}_m z_m \mathfrak{B} \mathbin{\&} (A(x) \vee \bar{A}(x)) \mathbin{\&} (A(y) \vee \bar{A}(y))].$$

Легко видеть, что эта формула эквивалентна формуле (5), так как для любой формулы $\mathfrak{A}$, не содержащей x и y, имеет место

$$\vdash \exists x \forall y [\mathfrak{A} \mathbin{\&} (A(x) \vee \bar{A}(x)) \mathbin{\&} (A(y) \vee \bar{A}(y))] \sim \mathfrak{A}.$$

Доказательство этой эквивалентности очень просто, и мы предоставляем его читателю. В результате получается, что произвольная нормальная формула (5) эквивалентна формуле (6) вида (1). А выше мы показали, что для доказательства теоремы Сколема этого достаточно. Итак, мы доказали, что для каждой формулы существует дедуктивно эквивалентная ей нормальная формула Сколема. Нормальную формулу Сколема, дедуктивно эквивалентную данной формуле $\mathfrak{A}$, будем называть *ее нормальной формой Сколема.*

§ 16. Теорема Мальцева

Содержательная трактовка исчисления высказываний, или алгебра высказываний, позволяет обобщить определение логической суммы и произведения на случай бесконечного числа высказываний и ввести, таким образом, бесконечные формулы.

Определим логические понятия индуктивным образом, исходя из элементарных переменных высказываний, которых теперь может существовать бесконечное множество любой мощности. Эти элементарные переменные высказывания могут принимать два и только два значения: *И* и *Л*. Обозначать эти переменные высказывания будем либо, как и раньше, большими латинскими буквами:

$$A,\ B,\ C,\ \ldots,$$

либо буквами с индексами:

$$A_{\xi},\ X_{\delta},\ \ldots,\ P_n,\ \ldots,$$

где индексы могут принимать значения из произвольного множества объектов. Пусть дано некоторое множество формул, уже определенных и представляющих собой функции входящих в них переменных высказываний. Обозначим это множество через $\{\mathfrak{A}\}$, где $\mathfrak{A}$ — символ общего элемента данного множества формул.

Логическое произведение $\prod \mathfrak{A}$ представляет собой формулу, принимающую значение *И* тогда и только тогда, когда все $\mathfrak{A}$ принимают значение *И*. Следовательно, $\prod \mathfrak{A}$ принимает значение *Л*, если хотя бы одна из формул $\mathfrak{A}$ принимает значение *Л*.

Логическая сумма $\sum \mathfrak{A}$ определяется аналогично: формула $\sum \mathfrak{A}$ принимает значение *И* тогда и только тогда, когда хотя бы одна из формул $\mathfrak{A}$ принимает значение *И*.

В том случае, когда $\{\mathfrak{A}\}$ — счетное множество формул и может быть, следовательно, представлено в виде последовательности элементов, занумерованных целыми числами:

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n, \ldots,$$

формулу $\prod \mathfrak{A}_n$ можно написать в виде

$$\mathfrak{A}_1 \,\&\, \mathfrak{A}_2 \,\&\, \ldots \,\&\, \mathfrak{A}_n \,\&\, \ldots,$$

а формулу $\sum \mathfrak{A}_n$ — в виде

$$\mathfrak{A}_1 \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_n \vee \ldots$$

Закон двойственности для бесконечных формул такой же, как и для конечных:

$$\overline{\prod \mathfrak{A}} \quad \textit{эквивалентно} \quad \sum \overline{\mathfrak{A}};$$

$$\overline{\sum \mathfrak{A}} \quad \textit{эквивалентно} \quad \prod \overline{\mathfrak{A}}.$$

Мы не останавливаемся на доказательстве этих положений, так как оно получается дословным повторением приведенного выше доказательства закона двойственности в исчислении высказываний.

Точно так же, как и выше, пользуясь этим законом, можно все операции заменить двумя операциями: & и — (или же $\vee$ и —). Советский математик А. И. Мальцев доказал интересную теорему, связывающую некоторые бесконечные формулы исчисления высказываний с конечными формулами исчисления высказываний и имеющую дальнейшие приложения.

Теорема Мальцева. *Пусть* $\sum \mathfrak{A}$ — *произвольная логическая сумма, все слагаемые которой* $\mathfrak{A}$ — *конечные формулы. Если* $\sum \mathfrak{A}$ — *тождественно истинная формула, то найдется конечное число ее слагаемых, сумма которых* $\mathfrak{A}_1 \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_N$ *также тождественно истинна.*

Теорема эта справедлива для произвольного множества конечных логических слагаемых. Однако для доказательства ее в полном виде необходимо обращение к трансфинитным числам. Мы проведем доказательство этой теоремы в предположении, что множество формул $\mathfrak{A}$ счетно. Для дальнейших приложений нам такого результата будет достаточно. Итак, нам дана счетная логическая сумма конечных формул:

$$\mathfrak{A}_1 \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_n \vee \ldots$$

Она, по условию теоремы, тождественно истинна. Мы докажем, что тогда существует такое число N, что сумма

$$\mathfrak{A}_1 \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_N$$

— тождественно истинная формула. Предположим противное; тогда ни одна сумма $\sum\limits_{i=1}^{n} \mathfrak{A}_i$ не является тождественно истинной, т. е. можно найти такие значения входящих в нее переменных высказываний, при которых она принимает значение $Л$. Пусть

$$A_1^n,\ A_2^n,\ \ldots,\ A_{k_n}^n \tag{1}$$

— переменные высказывания, входящие в формулу $\sum\limits_{i=1}^{n} \mathfrak{A}_i$, а

$$\alpha_1^n,\ \alpha_2^n,\ \ldots,\ \alpha_{k_n}^n \tag{2}$$

— те значения этих переменных высказываний, при которых она принимает значение $Л$. Каждое α_i^n представляет собой или $И$, или $Л$. Число всевозможных распределений значений, которые могут принимать переменные высказывания (1), равно 2^{k_n}, т. е. конечно. Рассмотрим

$$\mathfrak{A}_1(A_1^1,\ A_2^1,\ \ldots,\ A_{k_1}^1).$$

Все переменные высказывания A_i^1 содержатся в каждой формуле $\sum\limits_{i=1}^{n} \mathfrak{A}_i$ и находятся, следовательно, среди переменных высказываний (1), каково бы ни было n. Обозначим их через

$$A_1^{1,n},\ A_2^{1,n},\ \ldots,\ A_{k_1}^{1,n}.$$

Таким образом, $A_i^{1,n}$, $i \leqslant k_n$, представляет собой не что иное, как A_i^1. Значения, которые переменные высказывания $A_i^{1,n}$ приняли в группе переменных высказываний (1) и которые мы обозначили α_i^n, будем теперь обозначать $\alpha_i^{1,n}$. Хотя $A_i^{1,n}$ и совпадает с A_i^1, значение $\alpha_i^{1,n}$ не будет, вообще говоря, совпадать со значением α_i^1. Действительно, подставляя в формулу $\sum_{i=1}^{n} \mathfrak{A}_i$ значения переменных высказываний так, чтобы эта формула принимала значение *Л*, мы не имеем основания думать, что переменные высказывания $A_1^1, \ldots, A_{k_1}^1$ формулы $\mathfrak{A}_1$, входящие в формулу $\sum_{i=1}^{n} \mathfrak{A}_i$, примут при этом те же самые значения $\alpha_1^1, \ldots, \alpha_{k_1}^1$, которые были выбраны для формулы $\mathfrak{A}_1$. Вообще если $n < m$, то переменные высказывания формулы $\sum_{i=1}^{n} \mathfrak{A}_i$, находящиеся среди переменных высказываний формулы $\sum_{i=1}^{m} \mathfrak{A}_i$, мы будем обозначать также через

$$A_1^{n,m},\ A_2^{n,m},\ \ldots,\ A_{k_n}^{n,m},$$

а их значения в группе $\left(\alpha_1^m, \ldots, \alpha_{k_m}^m\right)$ — через

$$\alpha_1^{n,m},\ \alpha_2^{n,m},\ \ldots,\ \alpha_{k_n}^{n,m}.$$

При значениях переменных высказываний (2) формула $\sum_{i=1}^{n} \mathfrak{A}_i$ ложна; следовательно, каждое слагаемое этой формулы при этих значениях также ложно. Следовательно, формула $\mathfrak{A}_1$ при значениях переменных высказываний

$$\alpha_1^{1,n},\ \alpha_2^{1,n},\ \ldots,\ \alpha_{k_1}^{1,n}$$

должна быть ложной, каково бы ни было n.

Рассмотрим последовательность групп значений k_1 переменных, входящих в формулу $\mathfrak{A}_1$:

$$\left(\alpha_1^{1,1}, \ldots, \alpha_{k_1}^{1,1}\right), \left(\alpha_1^{1,2}, \ldots, \alpha_{k_1}^{1,2}\right), \ldots, \left(\alpha_1^{1,n}, \ldots, \alpha_{k_1}^{1,n}\right), \ldots \quad (3)$$

В этой последовательности может быть только конечное число (не больше 2^{k_1}) различных между собой групп

Поэтому одна из этих групп повторяется в последовательности (3) бесконечное число раз. Мы можем, следовательно, выделить из последовательности (3) бесконечную подпоследовательность одинаковых групп:

$$\left(\alpha_1^{1,n_1}, \ldots, \alpha_{k_1}^{1,n_1}\right), \quad \left(\alpha_1^{1,n_2}, \ldots, \alpha_{k_1}^{1,n_2}\right), \ldots$$
$$\ldots, \left(\alpha_1^{1,n_j}, \ldots, \alpha_{k_1}^{1,n_j}\right), \ldots, \qquad (\mathrm{a}_1)$$

где $\alpha_i^{1,n_r} = \alpha_i^{1,n_j}$ при любых r и j. При значениях переменных высказываний A_i^1, равных α_i^{1,n_j}, формула $\mathfrak{A}_1$ принимает значение $Л$.

Вместе с тем мы имеем бесконечную последовательность формул

$$\sum_{i=1}^{n_1} \mathfrak{A}_i, \quad \sum_{i=1}^{n_2} \mathfrak{A}_i, \ldots, \sum_{i=1}^{n_j} \mathfrak{A}_i, \ldots,$$

где каждая формула $\sum_{i=1}^{n_j} \mathfrak{A}_i$ принимает значение $Л$, когда входящие в нее переменные высказывания принимают значения

$$\alpha_1^{n_j}, \ \alpha_2^{n_j}, \ldots, \ \alpha_{k_{n_j}}^{n_j}.$$

При замене в формуле $\sum_{i=1}^{n_j} \mathfrak{A}_i$ переменных высказываний этими значениями каждое переменное высказывание A_i^1 принимает одно и то же значение, каково бы ни было n_j. Остальные же переменные высказывания, входящие в $\sum_{i=1}^{n_j} \mathfrak{A}_i$ и не входящие в $\mathfrak{A}_1$, принимают, вообще говоря, различные значения $\alpha_i^{n_j}$ для различных n_j.

Рассмотрим формулу $\sum_{i=1}^{2} \mathfrak{A}_i$ или, что то же, $\mathfrak{A}_1 \vee \mathfrak{A}_2$. Для каждого $n_j \geqslant 2$ переменные этой формулы находятся в числе переменных высказываний формулы $\sum_{i=1}^{n_j} \mathfrak{A}_i$. Группы значений переменных высказываний A_i^2, входящих в $\sum_{i=1}^{n_j} \mathfrak{A}_i$ $(j=1, 2, \ldots)$, при которых эти формулы принимают значение $Л$, образуют бесконечную последовательность

$$\left(\alpha_1^{2, n_1}, \ldots, \alpha_{k_2}^{2, n_1}\right), \quad \left(\alpha_1^{2, n_2}, \ldots, \alpha_{k_2}^{2, n_2}\right), \ldots$$
$$\ldots, \left(\alpha_1^{2, n_j}, \ldots, \alpha_{k_2}^{2, n_j}\right), \ldots, \tag{4}$$

причем значения каждого переменного высказывания, входящего в $\mathfrak{A}_1$, одни и те же во всех группах последовательности (4). Они совпадают со значениями в последовательности (a_1).

Рассуждая так же, как для случая $n=1$, мы можем выделить из последовательности (4) подпоследовательность одинаковых групп

$$\left(\alpha_1^{2, m_1}, \ldots, \alpha_{k_2}^{2, m_1}\right), \quad \left(\alpha_1^{2, m_2}, \ldots, \alpha_{k_2}^{2, m_2}\right), \ldots$$
$$\ldots, \left(\alpha_1^{2, m_j}, \ldots, \alpha_{k_2}^{2, m_j}\right), \ldots, \tag{a_2}$$

где

$$\alpha_i^{2, m_j} = \alpha_i^{2, m_k} \quad \text{при} \quad i = 1, 2, \ldots, k_2;$$
$$j, k = 1, 2, \ldots, n, \ldots; \quad m_j, m_k \geqslant 2.$$

Каждая группа значений переменных высказываний A_i^2 из последовательности (a_2) обращает формулу $\mathfrak{A}_1 \vee \mathfrak{A}_2$ в $Л$. Значения переменных высказываний A_i^2, входящих в $\mathfrak{A}_1$, в последовательности (a_2) те же, что в последовательности (a_1). Рассуждая таким же образом далее, мы получим счетное множество последовательностей

$$\left(\alpha_1^{3, p_1}, \ldots, \alpha_{k_3}^{3, p_1}\right), \quad \left(\alpha_1^{3, p_2}, \ldots, \alpha_{k_3}^{3, p_2}\right), \ldots$$
$$\ldots, \left(\alpha_1^{3, p_j}, \ldots, \alpha_{k_3}^{3, p_j}\right), \ldots \tag{a_3}$$

. . . .

$$\left(\alpha_1^{n, q_1}, \ldots, \alpha_{k_n}^{n, q_1}\right), \quad \left(\alpha_1^{n, q_2}, \ldots, \alpha_{k_n}^{n, q_2}\right), \ldots$$
$$\ldots, \left(\alpha_1^{n, q_j}, \ldots, \alpha_{k_n}^{n, q_j}\right), \ldots \tag{a_n}$$

. . . .

где $\alpha_i^{n, q_j} = \alpha_i^{n, q_r}$. Группы, входящие в последовательность (a_n), — это группы значений всех переменных высказываний, входящих в формулу $\sum_{i=1}^{n} \mathfrak{A}_i$. Они обращают эту формулу в $Л$.

Рассмотрим теперь следующую последовательность:

$$\left(\alpha_1^{1, n_1}, \ldots, \alpha_{k_1}^{1, n_1}\right), \quad \left(\alpha_1^{2, m_1}, \ldots, \alpha_{k_2}^{2, m_1}\right), \ldots$$
$$\ldots, \left(\alpha_1^{n, q_1}, \ldots, \alpha_{k_n}^{n, q_1}\right), \ldots \qquad \text{(b)}$$

Первая группа состоит из значений переменных высказываний A_i^1, обращающих $\mathfrak{A}_1$ в $Л$, вторая — из значений переменных высказываний A_i^2, обращающих $\mathfrak{A}_1 \vee \mathfrak{A}_2$ в $Л$, и т. д.

Эти группы обладают следующим свойством. *Каково бы ни было переменное высказывание X_i, входящее в некоторые формулы $\sum_{i=1}^{n} \mathfrak{A}_i$, значение его одинаково во всех группах последовательности* (b), *в которые оно входит*. В самом деле, пусть переменное высказывание X при некоторых n входит в формулу $\sum_{i=1}^{n} \mathfrak{A}_i$. Пусть n_0 — наименьшее значение n, для которого X входит в такую формулу. Тогда для каждого $n \geqslant n_0$ переменное высказывание X совпадает с каким-то $A_r^{n_0, n}$, т. е. $A_r^{n_0, n}$ есть обозначение переменного высказывания X в формуле $\sum_{i=1}^{n} \mathfrak{A}_i$. По построению значения $\alpha_r^{n_0, n}$ переменного высказывания $A_r^{n_0, n}$ во всех группах последовательности (a_{n_0}) одни и те же. Но значение переменного высказывания $A_r^{n_0, n}$, входящего в $\sum_{i=1}^{n_0} \mathfrak{A}_i$, во всех группах последовательности (a_n) при $n > n_0$ такое же, как в группах последовательности (a_{n_0}). Следовательно, и значение переменного высказывания $A_r^{n_0, n}$, т. е. X, во всех группах последовательности (b) одно и то же.

Каждому переменному высказыванию, входящему в какую-либо формулу $\sum_{i=1}^{n} \mathfrak{A}_i$, *посредством* *последовательности* (b) *поставлено в соответствие какое-то его значение.*

Группы последовательности (b) состоят из значений всех переменных высказываний, входящих соответственно в формулы

$$\mathfrak{A}_1,\ \mathfrak{A}_1 \vee \mathfrak{A}_2,\ \ldots,\ \mathfrak{A}_1 \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_n,\ \ldots \tag{5}$$

Группа последовательности (b) с номером n состоит, таким образом, из значений всех переменных высказываний, входящих в $\sum\limits_{i=1}^{n} \mathfrak{A}_i$. Поэтому, если переменное высказывание X входит в $\sum\limits_{i=1}^{n} \mathfrak{A}_i$, то в группе номера n имеется его значение. Значение X, как мы видели, одно и то же во всех группах, в которые оно входит. Это значение мы и поставим в соответствие переменному высказыванию X.

Дадим каждому переменному высказыванию, входящему в бесконечную формулу

$$\mathfrak{A}_1 \vee \mathfrak{A}_2 \vee \ldots \mathfrak{A}_n \vee \ldots, \tag{6}$$

то значение, которое ему поставлено в соответствие посредством последовательности (b). Эти значения таковы, что формулы (5) при замене каждого переменного высказывания соответствующим ему значением принимают значение *Л*. Но тогда, каково бы ни было n, формула $\mathfrak{A}_n$ при замене всех переменных высказываний соответствующими им значениями принимает также значение *Л*. Итак, каждое слагаемое суммы (6) при данной подстановке значений переменных высказываний принимает значение *Л*. Но тогда и сама сумма (6) также принимает значение *Л* и, значит, не является тождественно истинной, что противоречит условию теоремы. Таким образом, предположение, что все суммы $\sum\limits_{i=1}^{N} \mathfrak{A}_i$ не являются тождественно истинными формулами, приводит к противоречию. Следовательно, существует по крайней мере одна конечная тождественно истинная сумма $\sum\limits_{i=1}^{N} \mathfrak{A}_i$, что и требовалось доказать.

Доказанную теорему можно сформулировать следующим образом:

Если все конечные произведения $\prod_{i=1}^{n} \mathfrak{A}_i$ *множителей бесконечного произведения* $\prod_{n=1}^{\infty} \mathfrak{A}_n$ *конечных формул* $\mathfrak{A}_i$ *выполнимы, то и* $\prod_{n=1}^{\infty} \mathfrak{A}_n$ *является выполнимой формулой.*

В самом деле, если бы $\prod_{n=1}^{\infty} \mathfrak{A}_n$ оказалась невыполнимой формулой, то $\sum_{n=1}^{\infty} \overline{\mathfrak{A}}_n$ была бы тождественно истинной. Но тогда в силу доказанной теоремы существует такое N, что и сумма $\sum_{n=1}^{N} \overline{\mathfrak{A}}_n$ тождественно истинна. А тогда отрицание этой формулы, равносильное формуле $\prod_{n=1}^{N} \mathfrak{A}_n$, было бы невыполнимой формулой, что противоречит условию.

§ 17. Проблема полноты исчисления предикатов в широком смысле

При рассмотрении логики предикатов с содержательной точки зрения (глава III) мы ввели понятие тождественно истинной формулы, отвечающей, по своему смыслу, понятию «тавтологически истинного высказывания». С другой стороны, в исчислении предикатов мы имеем также понятие выводимой формулы. Возникает вопрос о сравнении этих двух понятий. Как мы указывали выше, всякая выводимая в исчислении предикатов формула является также и тождественно истинной в содержательном смысле (см. § 4).

Возникает обратный вопрос: *будет ли всякая тождественно истинная формула выводима в исчислении предикатов*? Этот вопрос носит название проблемы полноты исчисления предикатов в широком смысле. Мы увидим в § 19, что проблема полноты в широком смысле решается положительным образом. Надо, однако, заметить, что при решении вопроса о полноте исчисления предикатов в широком смысле мы не можем ограничиться средствами рассуждения финитной металогики ввиду того, что в самую постановку вопроса входит понятие «тождественно истинной формулы», включающее в себя рассмотрение всех интерпретаций.

Сделаем еще одно замечание технического порядка. *Если две формулы дедуктивно эквивалентны, то из того, что одна из них тождественно истинна, следует, что и другая также тождественно истинна.* В самом деле, пусть $\mathfrak{A}$ и $\mathfrak{B}$ — дедуктивно эквивалентные формулы и $\mathfrak{A}$ — тождественно истинная формула. Как мы видели, все формулы, выводимые из тождественно истинных формул, также являются тождественно истинными формулами. В силу дедуктивной эквивалентности $\mathfrak{B}$ выводима из аксиом исчисления предикатов и формулы $\mathfrak{A}$; поэтому $\mathfrak{B}$ также является тождественно истинной формулой. Кроме того, если $\mathfrak{A}$ и $\mathfrak{B}$ дедуктивно эквивалентны и $\mathfrak{A}$ — выводимая в исчислении предикатов формула, то $\mathfrak{B}$ также выводима в исчислении предикатов. Последнее вытекает из определения дедуктивной эквивалентности.

Из всего сказанного следует, что при решении вопроса о полноте исчисления предикатов в широком смысле можно ограничиться рассмотрением только нормальных формул Сколема. В самом деле, допустим, что мы доказали, что всякая тождественно истинная нормальная формула Сколема выводима в исчислении предикатов. Пусть $\mathfrak{A}$ — произвольная формула, а $\mathfrak{A}^*$ — ее нормальная форма Сколема. Если $\mathfrak{A}$ тождественно истинна, то $\mathfrak{A}^*$ также тождественно истинна. Но тогда $\mathfrak{A}^*$ выводима в исчислении предикатов, а следовательно, дедуктивно эквивалентная ей формула $\mathfrak{A}$ также выводима в исчислении предикатов.

§ 18. Замечание о формулах без кванторов

Формула исчисления предикатов, которая не содержит кванторов, может быть в известном смысле рассмотрена как формула исчисления высказываний и как формула алгебры высказываний. Для этого надо только входящие в нее переменные предикаты рассматривать как переменные высказывания, только обозначенные особым образом. При этом мы будем считать, что такие переменные высказывания, представляемые переменными предикатами, одинаковы тогда и только тогда, когда выражающие их предикаты полностью одинаковы, т. е. совпадают графически.

Примеры.

1. Формулу

$$F(x) \to F(x) \,\&\, F(y)$$

мы будем представлять себе как формулу исчисления высказываний, где $F(x)$ и $F(y)$ — переменные высказывания и при этом различные. В обычном написании такая формула имела бы вид

$$A \to A \,\&\, B.$$

2. $(F(x, y) \to F(x, x)) \vee (\overline{F}(y, y) \to \overline{F}(x, y))$.

Эта формула, рассмотренная как формула исчисления высказываний, в обычном написании имела бы вид

$$(A \to B) \vee (\overline{C} \to \overline{A}).$$

3. $(A \vee F(x)) \,\&\, (B \vee \overline{F}(y))$.

Этой формуле, рассматривая ее как формулу алгебры высказываний, мы могли бы дать такой вид:

$$(A \vee C) \,\&\, (B \vee D).$$

Пусть $\mathfrak{A}$ — формула исчисления предикатов, не содержащая кванторов. *Допустим, что эта формула, рассмотренная как формула алгебры высказываний, является выполнимой.* Это значит, что при некоторых значениях переменных высказываний она принимает значение *И*. Тогда можно так заменить переменные высказывания и переменные предикаты значениями *И* и *Л*, соблюдая условие, что одинаковые высказывания и предикаты заменяются одинаковым образом, что получится формула, принимающая значение *И*. В таком случае, возвращаясь к рассмотрению этой формулы как формулы исчисления предикатов, мы можем утверждать:

Заменив предметные переменные формулы предметами любой области с таким условием, что разные *переменные заменяются разными предметами, можно найти такие предикаты, определенные на этой области, для которых полученная формула принимает значение И.*

Выбор области ограничен только тем, что число содержащихся в ней предметов должно быть не меньше, чем число различных предметных переменных, входящих в формулу. Таким образом, произвольная область, содержащая бесконечное множество предметов, может быть использована в указанном смысле для любой формулы, не содержащей кванторов.

Если формула $\mathfrak{A}$, рассмотренная как формула алгебры высказываний, является тождественно истинной, то как формула исчисления высказываний она выводима в исчислении высказываний. Но тогда эта формула, рассмотренная вновь как формула исчисления предикатов, выводима и в исчислении предикатов, так как она получается подстановками в выводимую формулу исчисления высказываний.

В дальнейшем для краткости, вместо того чтобы говорить «*формула* $\mathfrak{A}$, *рассмотренная как формула исчисления высказываний, выводима в исчислении высказываний*», мы будем говорить: «*формула* $\mathfrak{A}$ *выводима в исчислении высказываний*».

§ 19. Теорема Гёделя

Теорема Гёделя. *Всякая тождественно истинная формула логики предикатов является выводимой в исчислении предикатов.*

Для доказательства этой теоремы мы введем некоторые обозначения и докажем предварительно лемму. Из теоремы Сколема и замечания, сделанного в § 17, следует, что для доказательства теоремы Гёделя достаточно рассмотреть только нормальные формулы Сколема.

Пусть $\mathfrak{A}$ — нормальная формула Сколема. Тогда она имеет вид

$$\exists x_1 \ldots \exists x_k \forall y_1 \ldots \forall y_m \mathfrak{M}(x_1, \ldots, x_k, y_1, \ldots, y_m). \quad (1)$$

Введем последовательность новых символов предметных переменных:

$$t_0, t_1, \ldots, t_n, \ldots$$

Рассмотрим всевозможные группы $(t_{i_1}, \ldots, t_{i_k})$ из k символов этой последовательности и расположим эти группы в последовательность так, чтобы группы с большей суммой индексов $i_1 + i_2 + \ldots + i_k$ следовали за группами с меньшей суммой индексов, а группы с одинаковой суммой индексов были упорядочены как-нибудь, например лексикографически:

$$(t_0, t_0, \ldots, t_0,), (t_0, \ldots, t_0, t_1), (t_0, \ldots, t_1, t_0), \ldots$$
$$\ldots, (t_{i_1}, \ldots, t_{i_k}), \ldots$$

Пусть j-я группа этой последовательности есть $(t_{i_1}, t_{i_2}, \ldots, t_{i_k})$. Введем следующие обозначения:

$$\left.\begin{array}{l} \mathfrak{B}_j \text{ обозначает формулу} \\ \mathfrak{M}(t_{i_1}, \ldots, t_{i_k}, t_{(j-1)m+1}, t_{(j-1)m+2}, \ldots, t_{jm}), \\ \mathfrak{C}_j \text{ обозначает формулу } \mathfrak{B}_1 \vee \mathfrak{B}_2 \vee \ldots \vee \mathfrak{B}_j, \\ \mathfrak{D}_j \text{ обозначает формулу } \forall t_0 \ldots \forall t_{jm} \mathfrak{C}_j. \end{array}\right\} \quad (2)$$

Выпишем подробнее формулу $\mathfrak{D}_j$:

$$\forall t_0 \ldots \forall t_{jm} (\mathfrak{B}_1 (t_0, \ldots., t_0, t_1, \ldots, t_m) \vee$$
$$\vee \mathfrak{B}_2 (t_0, \ldots, t_1, t_{m+1}, \ldots, t_{2m}) \vee \ldots$$
$$\ldots \vee \mathfrak{B}_j (t_{i_1}, \ldots, t_{i_k}, t_{(j-1)m+1}, \ldots, t_{jm})). \quad (3)$$

Легко видеть, что при данном способе нумерации групп $t_{i_1}, \ldots, t_{i_k}$ индекс $(j-1)m+1$ превосходит индексы $i_1, \ldots, i_k$ элементов j-й группы. Действительно, индекс каждого элемента, входящего в группу, всегда меньше, чем номер группы. Таким образом, формула $\mathfrak{C}_{j-1}$, т. е. $\mathfrak{B}_1 \vee \mathfrak{B}_2 \vee \ldots \vee \mathfrak{B}_{j-1}$, не содержит переменных $t_{(j-1)m+1}, \ldots, t_{jm}$, а формула $\mathfrak{C}_j$ содержит только переменные $t_0, t_1, \ldots, t_{jm}$. С другой стороны, $\mathfrak{C}_j$ содержит каждую из этих переменных, так как $\mathfrak{B}_1$ содержит переменные $t_0, t_1, \ldots, t_m$, $\mathfrak{B}_2$ содержит переменные $t_{m+1}, \ldots, t_{2m}$ и т. д., наконец, $\mathfrak{B}_j$ содержит переменные $t_{(j-1)m+1}, \ldots, t_{jm}$. Таким образом, связывание формулы $\mathfrak{B}_1 \vee \mathfrak{B}_2 \vee \ldots \vee \mathfrak{B}_j$ всеми кванторами $\forall t_0, \ldots, \forall t_{jm}$ имеет смысл.

Лемма 1. *Формула*

$$\forall u_1 \ldots \forall u_n (A(u_1, \ldots, u_n) \vee B(u_1, \ldots, u_n)) \to \\ \to \forall u_1 \ldots \forall u_k \ldots \forall u_n (A(u_1, \ldots, u_n) \vee \\ \vee \exists x_1 \ldots \exists x_k B(x_1, \ldots, x_k, u_{k+1}, \ldots, u_n)) \quad (4)$$

является выводимой формулой исчисления предикатов.

Имеем

$$B(u_1, \ldots, u_n) \to \\ \to \exists x_1 \ldots \exists x_k B(x_1, \ldots, x_k, u_{k+1}, \ldots, u_n). \quad (5)$$

Рассмотрим выводимую формулу исчисления высказываний

$$(C \to D) \to (A \vee C \to A \vee D).$$

Посредством подстановок в эту формулу получим

$$\vdash (B(u_1, \ldots, u_n) \to \\ \to \exists x_1 \ldots \exists x_k B(x_1, \ldots, x_k, u_{k+1}, \ldots, u_n)) \to \\ \to (A(u_1, \ldots, u_n) \vee B(u_1, \ldots, u_n) \to A(u_1, \ldots, u_n) \vee \\ \vee \exists x_1 \ldots \exists x_k B(x_1, \ldots, x_k, u_{k+1}, \ldots, u_n)). \quad (6)$$

Применив правило заключения к формулам (5) и (6), находим

$$\vdash A(u_1, \ldots, u_n) \vee B(u_1, \ldots, u_n) \to A(u_1, \ldots, u_n) \vee \\ \vee \exists x_1 \ldots \exists x_k B(x_1, \ldots, x_k, u_{k+1}, \ldots, u_n). \quad (7)$$

Далее, применив к выводимой формуле

$$\forall v_1 \ldots \forall v_n (A(v_1, \ldots, v_n) \vee B(v_1, \ldots, v_n)) \to \\ \to A(u_1, \ldots, u_n) \vee B(u_1, \ldots, u_n)$$

и формуле (7) правило силлогизма, получим

$$\forall v_1 \ldots \forall v_n (A(v_1, \ldots, v_n) \vee B(v_1, \ldots, v_n)) \to \\ \to A(u_1, \ldots, u_n) \vee \exists x_1 \ldots \exists x_k B(x_1, \ldots, x_k, u_{k+1}, \ldots, u_n).$$

Применяя к этой формуле последовательно n раз первое правило связывания квантором и переименовывая связанные переменные, получим формулу (4).

Заметим, что если некоторые из переменных u_i совпадают между собой и число кванторов $\forall u_i$ тем самым меньше n, то доказанная формула остается выводимой. При этом можно считать, что переменные $x_1, \ldots, x_k$, связанные кванторами существования, между собой не совпадают.

Пример.

$$\forall u\,(A(u, u) \vee B(u, u)) \to \forall u\,(A(u, u) \vee \exists x_1 \exists x_2 B(x_1, x_2)\,.$$

Доказательство для этого случая остается тем же самым.

Лемма 2. *Для каждого j выводима формула*

$$\mathfrak{D}_j \to \mathfrak{A}, \tag{8}$$

где $\mathfrak{A}$ есть формула (1).

Мы докажем лемму индукцией по номеру j. Легко убедиться, что выводима формула

$$\forall t_0 \forall t_1 \ldots \forall t_m \mathfrak{M}(t_0, \ldots, t_0, t_1, \ldots, t_m) \to$$
$$\to \exists x_1 \ldots \exists x_k \forall t_1 \ldots \forall t_m \mathfrak{M}(x_1, \ldots, x_k, t_1, \ldots, t_m)$$

или, если изменить обозначения переменных,

$$\forall t_0 \forall t_1 \ldots \forall t_m \mathfrak{M}(t_0, \ldots, t_0, t_1, \ldots, t_m) \to$$
$$\to \exists x_1 \ldots \exists x_k \forall y_1 \ldots \forall y_m \mathfrak{M}(x_1, \ldots, x_k, y_1, \ldots, y_m).$$

Принимая во внимание (1) и (2), эту формулу можно записать так:

$$\mathfrak{D}_1 \to \mathfrak{A}.$$

Покажем, что если формула (8) выводима для $j-1$, то она выводима и для j. Пусть

$$\vdash \mathfrak{D}_{j-1} \to \mathfrak{A}.$$

В силу (2) формула $\mathfrak{D}_j$ имеет вид

$$\forall t_0 \ldots \forall t_{jm} [\mathfrak{C}_{j-1} \vee \mathfrak{B}_j]. \tag{9}$$

Мы видели, что переменные $t_{(j-1)m+1}, \ldots, t_{jm}$ не входят в формулу $\mathfrak{C}_{j-1}$. В силу этого

$$\forall t_{(j-1)m+1} \ldots \forall t_{jm} [\mathfrak{C}_{j-1} \vee \mathfrak{B}_j] \sim$$
$$\sim \mathfrak{C}_{j-1} \vee \forall t_{(j-1)m+1} \ldots \forall t_{jm} \mathfrak{B}_j, \tag{10}$$

так как $\mathfrak{C}_{j-1}$ можно вынести за кванторы $\forall t_{(j-1)m+1}, \ldots$ $\ldots, \forall t_{jm}$. Выпишем более подробно формулу (9), эквивалентную $\mathfrak{D}_j$, принимая во внимание (10):

$$\forall t_0 \forall t_1 \ldots \forall t_{(j-1)m} [\mathfrak{C}_{j-1}(t_0, \ldots, t_{(j-1)m}) \vee$$
$$\vee \forall t_{(j-1)m+1} \ldots \forall t_{jm} \mathfrak{B}_j(t_{i_1}, \ldots, t_{i_k}, t_{(j-1)m+1}, \ldots, t_{jm})],$$

где $t_{i_1}, \ldots, t_{i_k}$ — переменные j-й группы. Они также связаны кванторами, так как находятся в числе переменных $t_0, \ldots, t_{(j-1)m}$. Некоторые из этих переменных могут между собой совпадать. Применим формулу (4):

$$\forall u_1 \ldots \forall u_n (A(u_1, \ldots, u_n) \vee B(u_1, \ldots, u_n)) \to$$
$$\to \forall u_1 \ldots \forall u_k \ldots \forall u_n (A(u_1, \ldots, u_n) \vee$$
$$\vee \exists x_1 \ldots \exists x_k B(x_1, \ldots, x_k, u_{k+1}, \ldots, u_n)),$$

положив в ней $n = (j-1)m + 1$ и заменив переменные $u_1, \ldots, u_n$ переменными $t_{i_1}, \ldots, t_{i_k}, \ldots, t_{(j-1)m}$ (т. е. теми же переменными $t_0, t_1, \ldots, t_{(j-1)m}$, только записанными в таком порядке, чтобы переменные j-й группы шли первыми). Кроме того, заменим в (4)

$$A(u_1, \ldots, u_n) \text{ на } \mathfrak{C}_{j-1}(t_{i_1}, \ldots, t_{(j-1)m}),$$
$$B(u_1, \ldots, u_n) \text{ на}$$
$$\forall t_{(j-1)m+1} \ldots \forall t_{jm} \mathfrak{B}_j(t_{i_1}, \ldots, t_{i_k}, t_{(j-1)m+1}, \ldots, t_{jm}).$$

В результате получим выводимую формулу

$$\forall t_{i_1} \ldots \forall t_{(j-1)m} [\mathfrak{C}_{j-1}(t_{i_1} \ldots, t_{(j-1)m}) \vee$$
$$\vee \forall t_{(j-1)m+1} \ldots \forall t_{jm} \mathfrak{B}_j(t_{i_1}, \ldots, t_{i_k}, t_{(j-1)m+1}, \ldots, t_{jm})] \to$$
$$\to \forall t_{i_1} \ldots \forall t_{(j-1)m} [\mathfrak{C}_{j-1}(t_{i_1}, \ldots, t_{(j-1)m}) \vee$$
$$\vee \exists x_1 \ldots \exists x_k \forall t_{(j-1)m+1} \ldots$$
$$\ldots \forall t_{jm} \mathfrak{B}_j(x_1, \ldots, x_k, t_{(j-1)m+1}, \ldots, t_{jm})]. \quad (11)$$

То, что некоторые из переменных $t_{i_1}, \ldots, t_{i_k}$ могут совпадать между собой, как мы указывали, никакого значения не имеет.

Левая часть следования (11) эквивалентна $\mathfrak{D}_j$. В правой части второй член логической суммы имеет вид

$$\exists x_1 \ldots \exists x_k \forall t_{(j-1)m+1} \ldots$$
$$\ldots \forall t_{jm} \mathfrak{B}_j(x_1, \ldots, x_k, t_{(j-1)m+1}, \ldots, t_{jm}).$$

Заменив в этой формуле переменные $t_{(j-1)m+1}, \ldots, t_{jm}$ соответственно на $y_1, \ldots, y_m$, а $\mathfrak{B}_j$ — его значением из (2), получим эквивалентную формулу:

$$\exists x_1 \ldots \exists x_k \forall y_1 \ldots \forall y_m \mathfrak{M}(x_1, \ldots, x_k, y_1, \ldots, y_m).$$

А это не что иное, как формула $\mathfrak{A}$ [(см. (1)]. Отсюда следует, что правая часть следования (11) эквивалентна формуле

$$\forall t_0 \ldots \forall t_{(j-1)m} (\mathfrak{C}_{j-1} \vee \mathfrak{A}).$$

Так как $\mathfrak{A}$ не содержит переменных $t_0, \ldots, t_{(j-1)m}$, то его можно вынести за все кванторы. Тогда получится формула

$$\mathfrak{A} \vee \forall t_0, \ldots, \forall t_{(j-1)m} \mathfrak{C}_{j-1},$$

опять-таки эквивалентная правой части следования (11), или, если заменить второе слагаемое на основании (2):

$$\mathfrak{A} \vee \mathfrak{D}_{j-1}. \tag{12}$$

Заменив обе части следования (11) эквивалентными формулами $\mathfrak{D}_j$ и (12), мы придем к формуле

$$\mathfrak{D}_j \to \mathfrak{D}_{j-1} \vee \mathfrak{A}.$$

Но согласно предположению мы имеем

$$\vdash \mathfrak{D}_{j-1} \to \mathfrak{A}.$$

Подстановками в выводимую формулу

$$\vdash (A \to B \vee C) \to ((B \to C) \to (A \to C))$$

получим

$$\vdash (\mathfrak{D}_j \to \mathfrak{D}_{j-1} \vee \mathfrak{A}) \to ((\mathfrak{D}_{j-1} \to \mathfrak{A}) \to (\mathfrak{D}_j \to \mathfrak{A})).$$

Применив сложное правило заключения, имеем

$$\vdash \mathfrak{D}_j \to \mathfrak{A},$$

и лемма доказана.

Доказательство теоремы Гёделя. Как мы указывали, для доказательства теоремы Гёделя достаточно ограничиться рассмотрением нормальных формул Сколема. Пусть $\mathfrak{A}$ — нормальная формула Сколема, являющаяся тождественно истинной. Тогда $\mathfrak{A}$ имеет вид (1). Покажем, что в таком случае по крайней мере одна из формул $\mathfrak{C}_j$ выводима в исчислении высказываний.

Допустим противное, т. е. ни одна формула $\mathfrak{C}_j$ *не выводима в исчислении высказываний.* В таком случае формула $\overline{\mathfrak{C}}_j$, рассмотренная как формула алгебры высказываний, будет выполнимой (см. § 18). Точно так же будет выполнимой и формула, полученная из $\overline{\mathfrak{C}}_j$ любой заменой переменных объектами произвольной области, если при этом разные переменные заменены разными объектами.

Возьмем произвольную счетную область объектов, которые обозначим

$$t_1^0,\ t_2^0,\ \ldots,\ t_n^0,\ \ldots$$

Пусть $\mathfrak{C}_j^0$ — формула, получившаяся из $\mathfrak{C}_j$ заменой переменных $t_{i_1}, \ldots, t_{i_k}, \ t_{(j-1)m+1}, \ldots, t_{jm}$ соответственно объектами $t_{i_1}^0, \ldots, t_{i_k}^0, \ t_{(j-1)m+1}^0, \ldots, t_{jm}^0$. Формула $\overline{\mathfrak{C}}_j^0$ при любом j выполнима, а отсюда следует, что равносильная ей формула $\overline{\mathfrak{B}}_1^0 \,\&\, \ldots \,\&\, \overline{\mathfrak{B}}_j^0$ также выполнима как формула алгебры высказываний. В таком случае, по теореме Мальцева, выполнима и бесконечная формула $\prod_{j=1}^{\infty} \overline{\mathfrak{B}}_j^0$, рассмотренная как формула алгебры высказываний. Если эта формула выполнима, то входящим в нее переменным высказываниям можно дать такие значения, при которых вся эта формула получит значение *И*.

Выберем определенные значения всех входящих в $\prod_{j=1}^{\infty} \overline{\mathfrak{B}}_j^0$ переменных высказываний A, обращающие эту формулу в *И*, и дальше будем рассматривать только эти значения A. В таком случае все переменные высказывания, входящие в каждую из формул $\mathfrak{B}_j^0$, получат определенные значения.

Рассмотрим формулу $\mathfrak{B}_j^0$. Эта формула, согласно определению (2), связана с формулой $\mathfrak{A}$ следующим образом: $\mathfrak{B}_j^0$ представляет собой выражение

$$\mathfrak{M}\left(t_{i_1}^0, \ldots, t_{i_k}^0, \ t_{(j-1)m+1}^0, \ldots, t_{jm}^0\right),$$

где $\left(t_{i_1}^0, \ldots, t_{i_k}^0\right)$ — группа значений переменных $t_{i_1}, \ldots, t_{i_k}$, составляющих j-ю группу.

Так как каждому переменному высказыванию, входящему в формулу $\mathfrak{B}_j^0$, мы дали определенное значение, то каждый предикат, входящий в $\mathfrak{M}$, например $A(t_1, \ldots, t_s)$, получил определенное значение, по крайней мере для некоторых значений входящих в него предметных переменных из области

$$t_1^0, \ldots, t_n^0, \ldots$$

При этом распределении значений каждый предикат, входящий в $\mathfrak{M}$, для определенных значений входящих в него переменных может получить только одно значение: *И* или *Л*. Действительно, выражение

$$A\left(t_{p_1}^0, \ldots, t_{p_s}^0\right)$$

хотя и может входить в различные $\mathfrak{B}_i^0$, но в формуле

$$\prod_{j=1}^{\infty} \overline{\mathfrak{B}}_j^0$$

оно рассматривается как одно и то же переменное высказывание и поэтому заменяется значениями *И* или *Л* везде одинаковым образом.

Пусть в формулу $\mathfrak{A}$ входят следующие предикаты:

$$A_1, A_2, \ldots, A_r.$$

Поставим каждому из этих предикатов A_p в соответствие индивидуальный предикат, определенный на области

$$t_1^0, \ldots, t_n^0, \ldots,$$

который мы обозначим A_p^0 и который определяется следующим образом. Если для значений $t_{p_1}^0, \ldots, t_{p_s}^0$ переменных $t_{p_1}, \ldots, t_{p_s}$, входящих в A_p, высказывание $A_p\left(t_{p_1}^0, \ldots, t_{p_s}^0\right)$ входит в формулу $\prod_{j=1}^{\infty} \overline{\mathfrak{B}}_j$, то $A_p^0\left(t_{p_1}^0, \ldots, t_{p_s}^0\right)$ мы приписываем то значение, которое оно получило, когда было рассмотрено как переменное высказывание в формуле $\prod_{j=1}^{\infty} \overline{\mathfrak{B}}_j^0$. Если же $A_p^0\left(t_{p_1}^0, \ldots, t_{p_s}^0\right)$ не входит в формулу $\prod_{j=1}^{\infty} \overline{\mathfrak{B}}_j^0$, то приписываем ему какое угодно значение. (Напомним, что при этих заменах формула $\prod_{j=1}^{\infty} \overline{\mathfrak{B}}_j^0$ получает значение $И$.)

Нетрудно видеть, что формула $\overline{\mathfrak{A}}$ при замене входящих в нее предикатов $A_1, \ldots, A_r$ предикатами $A_1^0, \ldots$ $\ldots, A_r^0$ получит значение $И$, т. е. становится истинной в смысле логики предикатов, описанной в главе III. В самом деле, формула $\overline{\mathfrak{A}}$ равносильна следующей формуле:

$$\forall x_1 \ldots \forall x_k \exists y_1 \ldots \exists y_m \overline{\mathfrak{M}}(x_1, \ldots, x_k, y_1, \ldots, y_m).$$

Рассмотрим произвольную совокупность значений переменных $x_1, \ldots, x_k$ взятых из области $t_1^0, \ldots, t_i^0, \ldots$ Каждая такая совокупность значений представляет собой одну из групп

$$\left(t_{i_1}^0, \ldots, t_{i_k}^0\right).$$

Пусть номер этой группы равен j. Формула

$$\overline{\mathfrak{M}}\left(t_{i_1}^0, \ldots, t_{i_k}^0, t_{(j-1)m+1}^0, \ldots, t_{jm}^0\right)$$

совпадает с формулой

$$\overline{\mathfrak{B}}_j\left(t_{i_1}^0, \ldots, t_{i_k}^0, t_{(j-1)m+1}^0, \ldots, t_{jm}^0\right),$$

которая при замене входящих в нее предикатов $A_1, \ldots, A_r$ предикатами $A_1^0, \ldots, A_r^0$ получает значение $И$ (так как при такой замене вся формула $\prod_{j=1}^{\infty} \overline{\mathfrak{B}}_j^0$ принимает значение $И$). Это значит, что для произвольной группы значений переменных $x_1, \ldots, x_k$ на области $t_1^0, \ldots, t_p^0, \ldots$ существует такая группа значений переменных $y_1, \ldots, y_m$, именно $t_{(j-1)m+1}^0, \ldots, t_{jm}^0$, что формула

$$\overline{\mathfrak{M}}\left(t_{i_1}^0, \ldots, t_{i_k}^0, t_{(j-1)m+1}^0, \ldots, t_{jm}^0\right)$$

получает значение *И*. Но тогда сама формула

$$\forall x_1 \ldots \forall x_k \exists y_1 \ldots \exists y_m \overline{\mathfrak{M}}(x_1, \ldots, x_k, y_1, \ldots, y_m)$$

при замене предикатов $A_1, \ldots, A_r$ предикатами $A_1^0, \ldots, A_r^0$ получает значение *И* для области $t_1^0, \ldots, t_n^0, \ldots$ Следовательно, эта формула *выполнима* на области $t_1^0, \ldots, t_n^0, \ldots$ Однако она равносильна отрицанию формулы

$$\exists x_1 \ldots \exists x_k \forall y_1 \ldots \forall y_m \mathfrak{M}(x_1, \ldots, x_k, y_1, \ldots, y_m),$$

которая есть формула $\mathfrak{A}$ и является, по предположению, тождественно истинной. Мы пришли к противоречию, так как отрицание тождественно истинной формулы не может быть выполнимо ни на какой области. Из полученного противоречия вытекает, что формула $\prod\limits_{j=1}^{\infty} \overline{\mathfrak{B}}_j$ не может быть выполнимой.

В таком случае наше предположение, что никакая формула $\mathfrak{C}_j$ не выводима в исчислении высказываний, неверно, и, следовательно, существует формула

$$\mathfrak{C}_{j_0},$$

которая выводима в исчислении высказываний, а следовательно, и в исчислении предикатов. В таком случае и формула $\mathfrak{D}_{j_0}$, которая представляет собой

$$\forall t_0 \ldots \forall t_{j_0 m} \mathfrak{C}_{j_0},$$

также выводима в исчислении предикатов (это устанавливается путем последовательного применения производного правила связывания квантором). Но мы знаем, что каждая формула

$$\mathfrak{D}_j \to \mathfrak{A}$$

выводима в исчислении предикатов; поэтому формула $\mathfrak{A}$ также выводима в исчислении предикатов, что и требовалось доказать.

§ 20. Системы аксиом в исчислении предикатов

Содержательный смысл формул, выводимых в исчислении предикатов, достаточно полно установлен в главах III и IV. Эти формулы представляют собой тождественно истинные высказывания, иными словами, логические тавтологии. Обратно, каждая тождественно истинная формула является выводимой в исчислении предикатов (см. § 19).

Из сказанного ясно, что в исчислении предикатов нельзя вывести никакое сколько-нибудь содержательное по существу высказывание, в частности математическое. Однако если к аксиомам исчисления предикатов присоединить какие-либо невыводимые формулы в качестве новых аксиом (сохраняя те же правила вывода), то получится другое исчисление, в котором выводимы, помимо тождественно истинных формул, и другие формулы.

Добавление к системе аксиом исчисления предикатов новых аксиом такого вида, как мы до сих пор рассматривали, хотя и расширяет ее содержание, но не слишком значительно. Примером подобного расширения системы аксиом исчисления предикатов является добавление рассмотренной выше формулы

$$\exists x\, F(x) \to \forall x\, F(x),$$

не выводимой в исчислении предикатов. Содержательный смысл этой аксиомы состоит в утверждении, что все предметы тождественны.

При содержательном изложении логики предикатов мы также рассматривали различные системы аксиом. Но там мы рассматривали различные типы символов предметов и предикатов. Именно, как предметы, так и предикаты разделялись на переменные и индивидуальные. В исчислении предикатов мы до сих пор имели дело только с переменными предметами и предикатами. Чтобы расширить область применения исчисления предикатов и получить возможность посредством аксиом описывать настоящие математические дисциплины, необходимо и в исчислении предикатов ввести индивидуальные предметы и индивидуальные предикаты.

Для индивидуальных предметов мы не введем никаких специальных символов. Мы будем для них употреблять также малые латинские буквы, оговаривая каждый раз, какие буквы мы называем индивидуальными предметами. Если никакой оговорки не сделано, то мы будем считать, что имеем дело с переменными предметами. Чаще всего для обозначения индивидуальных предметов мы будем употреблять начальные буквы алфавита. В некоторых случаях индивидуальные предметы мы будем обозначать иными символами, например цифрами. Точно так же введем в формализм и индивидуальные предикаты. Мы будем употреблять для них те же символы, что и для переменных предикатов, с соответствующей оговоркой, или же будем их изображать посредством символов, имеющих общепринятый вид. Так, например, индивидуальный предикат от двух переменных, носящий название «предиката равенства», мы будем изображать символом $=$, а другой индивидуальный предикат, называемый «предикатом порядка», — символом $<$.

Понятие элементарной формулы также несколько расширяется. К элементарным формулам добавляются выражения вида

$$F(x_1, \ldots, x_n),$$

где F — переменный или индивидуальный предикат от n переменных, а буквы $x_1, \ldots, x_n$ могут быть как предметными переменными, так и индивидуальными предметами. Элементарные формулы вида $F(x_1, \ldots, x_n)$, если они содержат предметные переменные, мы также будем называть предикатами (переменными или индивидуальными, соответственно тому, чем является предикат F). Для индивидуальных предикатов мы будем иногда писать эти элементарные формулы иначе. Так, предикат равенства мы будем записывать в виде

$$x = y \quad (\text{а не } =(x, y)),$$

а предикат порядка — в виде

$$x < y.$$

В остальном определение формулы остается без изменений. Следует только заметить, что на индивидуальные предметы не распространяется операция связывания квантором.

Правило подстановки в переменный предикат требует некоторого уточнения.

Подстановка

$$R_F^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}),$$

где F — переменный предикат от n переменных, представляет собой замену каждого выражения вида

$$F(x_1, \ldots, x_n),$$

входящего в формулу $\mathfrak{A}$, формулой $\mathfrak{B}(x_1, \ldots, x_n)$, причем здесь буквы $x_1, \ldots, x_n$ могут быть как предметными переменными, так и индивидуальными предметами.

Выражения $\forall a\, \mathfrak{A}(a)$ и $\exists a\, \mathfrak{A}(a)$, где a — индивидуальный предмет, не являются формулами.

Все аксиомы исчисления предикатов и все правила вывода, кроме правила подстановки в свободные предметные переменные, остаются прежними. Правило подстановки в предметные переменные расширяется и формулируется следующим образом:

Если $\mathfrak{A}$ — выводимая формула, то формула $\mathfrak{A}'$, полученная из $\mathfrak{A}$ заменой любой свободной предметной переменной другой предметной переменной или индивидуальным предметом, всюду, где эта переменная входит в $\mathfrak{A}$, также является выводимой.

Сохраним за полученной системой название исчисления предикатов. Легко видеть, что внесенные в систему исчисления предикатов дополнения по существу ничего не меняют. Аксиомы исчисления предикатов не содержат индивидуальных предметов и предикатов. Если мы вывели формулу, в которой мы различаем индивидуальные и переменные предметы и предикаты, то этот вывод был бы правильным и в предположении, что все входящие в формулу предметы (кроме, конечно, связанных предметных переменных) и все предикаты переменные. Это утверждение справедливо потому, что всё изменение в правилах вывода состоит только в ограничении их применения к индивидуальным предметам и предикатам. Таким образом, введенные дополнения ничего не дают для самого исчисления предикатов. Однако они оказываются весьма существенными для построения абстрактных логических исчислений, предназначенных для описания не логических, а математических дисциплин. Пусть

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$$

— формулы исчисления предикатов, которые теперь могут содержать как переменные, так и индивидуальные предикаты и предметы. Присоединим эти формулы к аксиомам исчисления предикатов, сохранив прежние правила вывода. Тогда мы получим некоторую формальную систему, в которой выводимы все выводимые формулы исчисления предикатов, но вместе с ними выводимы и другие, не выводимые в исчислении предикатов формулы. Это всегда имеет место, если хотя бы одна из формул $\mathfrak{A}_i$ не выводима в исчислении предикатов.

Для примера рассмотрим уже встречавшуюся нам в главе III систему аксиом равенства. Положим, что к аксиомам исчисления предикатов присоединены следующие аксиомы:

1. $x = x$,
2. $x = y \to (A(x) \to A(y))$.

В этих аксиомах предикат $x = y$ индивидуальный, а предикат $A(x)$ переменный. Легко видеть, что ни одна из этих аксиом не может быть выведена в исчислении предикатов. В самом деле, формулы, выводимые в исчислении предикатов, не содержат индивидуальных предикатов. Поэтому, если бы формула $x = x$ была выведена в исчислении предикатов, то предикат $x = x$ можно было бы рассматривать как переменный предикат. Но доказуемость элементарного переменного предиката невозможна, так как она немедленно приводит к противоречию. Подставляя вместо $x = x$ формулу $\overline{x = x}$, мы также получили бы выводимую в исчислении предикатов формулу и тем самым получили бы противоречие в самом исчислении предикатов. Аналогичным образом можно показать и невыводимость второй формулы в исчислении предикатов. Мы покажем дальше, что из аксиом 1 и 2 можно формально вывести основные свойства равенства.

Посредством присоединения к аксиомам исчисления предикатов других аксиом мы можем описывать различные математические дисциплины. Таким образом могут быть описаны арифметика, теория двойственных чисел, геометрия и, наконец, теория множеств в очень широких пределах. Вообще, любая дедуктивная система может быть выражена указанными средствами. Так что, в сущности, нет никакой необходимости построения иных формализмов.

Вместе с тем рассмотрение любой системы аксиом вызывает необходимость решить вопрос о ее внутренней непротиворечивости. Этот вопрос, как мы видели, является очень существенным, так как всякая внутренне противоречивая система рассматриваемого типа отличается тем свойством, что в ней все формулы являются одновременно истинными и ложными. Поэтому она не пригодна ни для каких познавательных целей. Вопрос непротиворечивости, однако, связан с особыми, не вполне преодоленными трудностями. Дело в том, что если мы проведем какое-либо доказательство непротиворечивости определенного исчисления, то само это рассуждение уже должно основываться на таких предпосылках, которые сами не могут быть выведены из аксиом данной системы. (Всякое рассуждение, и в том числе любое рассуждение о непротиворечивости какой-нибудь системы, может быть формализовано и представлено в виде дедукции из аксиом, выражаемых формулами исчисления предикатов.)

Итак, чтобы доказать непротиворечивость какого-либо исчисления, необходимо употребить предпосылки, не выводимые из аксиом данного исчисления. Таким образом, для решения вопросов непротиворечивости оказывается необходимым иметь возможность черпать из какого-то источника все более и более сильные предпосылки такого рода, что в непротиворечивости их самих мы уже имеем полную уверенность. Можно было бы думать, что такого рода предпосылки представляет собой та финитная система рассуждений, в рамках которой мы определяем логические системы и ведем о них рассуждения. Но оказывается, что уже для доказательства непротиворечивости арифметики финитизма Гильберта не хватит. Практическим источником предпосылок, употребляемых в настоящее время для решения вопросов непротиворечивости достаточно сильных математических теорий, остается теория множеств, и доказательство непротиворечивости какой-либо системы выглядит следующим образом: мы доказываем, что если теория множеств в тех или других размерах является непротиворечивой, то и данная интересующая нас система также непротиворечива.

Такого рода рассуждения бывает возможно делать опять-таки в рамках финитизма Гильберта, так как и теорию множеств в той мере, в какой нам нужно, и исследуемую систему мы уже можем описать аксиоматически и даже средствами исчисления предикатов. Таким образом, вместо вопроса о непротиворечивости данной системы мы решаем более слабую задачу — сведение проблемы непротиворечивости рассматриваемой системы к проблеме непротиворечивости некоторой формальной теоретико-множественной системы.

Существует возможность высказать принципы, позволяющие создавать предпосылки для доказательства непротиворечивости мощных формальных систем и, может быть, даже теоретико-множественных систем. Вместе с тем эти принципы таковы, что непротиворечивость самих предпосылок принципиально гораздо более обоснована, чем это имеет место для теоретико-множественных систем. Однако это выходит за рамки настоящей книги, и здесь мы этих вопросов касаться не будем. В дальнейшем мы ограничимся доказательством непротиворечивости только в таких пределах, в каких это допускает финитизм Гильберта.

Помимо вопроса о непротиворечивости системы аксиом, всегда возникает вопрос о независимости аксиом, т. е. о невыводимости каждой аксиомы из остальных. В вопросе независимости аксиом никаких новых принципиальных трудностей нет. Вообще вопрос о независимости аксиом обычно ставится для непротиворечивых систем или для таких систем, непротиворечивость которых предполагается. В последнем случае в вопросе о независимости аксиом ограничиваются сведением этого вопроса к непротиворечивости данной системы.

Хотя, как мы сказали, у нас нет никакой принципиальной необходимости для описания математических дисциплин выводить какое-либо изменение в символах, формулах и правилах вывода исчисления предикатов, тем не менее ради удобства в некоторых случаях разумно прибегать к различным видоизменениям в указанном направлении.

В дальнейшем для описания арифметики мы расширим совокупность символов исчисления предикатов, введя еще новые символы. Введение новых символов повлечет за собой расширение понятия формулы и потребует соответствующего изменения формулировок правил вывода.

АКСИОМАТИЧЕСКАЯ АРИФМЕТИКА

§ 1. Термы. Расширенное исчисление предикатов

В этой главе мы дадим описание арифметики в форме аксиоматической системы. Как мы уже указывали в конце предыдущей главы, мы могли бы получить такое описание, присоединив к исчислению предикатов (содержащему индивидуальные предикаты и предметы) некоторые новые аксиомы. Однако такое изложение было бы громоздким и неудобным. Поэтому, прежде чем написать аксиомы арифметики, мы произведем дальнейшее расширение исчисления предикатов, введя в него новые символы. Эти символы представляют собой маленькие греческие буквы:

$$\alpha, \beta, \ldots, \varphi, \psi, \ldots$$

Вместе с предметными переменными и индивидуальными предметами они образуют слова, которые мы будем называть *предметными функциями* и *предметными константами*. К ним относятся слова следующего вида:

$$\alpha(x),\ \beta(x, y),\ \psi(x_1, x_2, \ldots, x_n),\ \eta(a),\ \xi(a, b), \ldots \qquad (1)$$

Эти выражения составляются так же, как и предикаты [например, $F(x, y, z)$], но с той разницей, что вместо большой латинской буквы (в нашем примере F) в слово входит маленькая греческая.

Полностью понятия предметной функции и предметной константы определяются следующим образом.

1. Выражения вида (1) являются предметными функциями. Мы будем называть эти выражения *элементарными предметными функциями*.

2. Результат замены предметных переменных в предметной функции предметными функциями является также предметной функцией.

3. Индивидуальные предметы являются предметными константами.

4. Результат замены некоторых, но не всех, предметных переменных в предметной функции индивидуальными предметами является предметной функцией.

5. Результат замены всех предметных переменных в предметной функции индивидуальными предметами является предметной константой.

Примеры предметных функций и предметных констант:

$$\alpha(\beta(x)); \quad \beta(\alpha(x), \gamma(a)); \quad \beta(a, \gamma(a)).$$

Предметные переменные, предметные функции и предметные константы будем называть *термами*. Введя в исчисление предикатов термы, мы расширим также и правила образования формул. Именно, к элементарным формулам присоединим слова, полученные заменой произвольной предметной переменной в элементарном предикате любым термом.

Так, например, слова

$$A(\psi(x)), \quad B(x, \varphi(y, x)), \quad F(a, x, \psi(a, y)),$$
$$G(a, \psi(a), \varphi(a, b))$$

являются элементарными формулами; в остальном правила образования формул не меняются.

Заметим, что *сами термы формулами не являются*. Это соответствует и содержательному смыслу этих понятий: терм представляет собой предмет, а формула — высказывание о предметах. Подобно тому как для формул мы употребляем металогические обозначения в виде больших готических букв, будем обозначать термы малыми готическими буквами, например: $\mathfrak{a}$, $\mathfrak{c}$, ..., или $\mathfrak{a}(x_1, \ldots, x_n)$, если мы хотим выразить, что терм содержит переменные $x_1, \ldots, x_n$.

Далее мы расширим *правила подстановки*. Мы будем теперь формулировать правило подстановки в предметную переменную следующим образом.

Если в выводимой формуле $\mathfrak{A}$ заменить произвольную свободную предметную переменную термом, не содержащим таких переменных, которые были бы связаны в формуле $\mathfrak{A}$, то полученная при этом формула $\mathfrak{A}'$ также будет выводима.

Правило подстановки в переменное высказывание остается тем же, что и в исчислении предикатов.

Правило подстановки в переменный предикат несколько изменяется.

Подстановка, выражаемая символом

$$R_F^{\mathfrak{B}(t_1, \ldots, t_n)}(\mathfrak{A}),$$

где F — предикат от n переменных, представляет собой замену каждого выражения вида $F(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ в формуле $\mathfrak{A}$, где $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ — какие-то термы, формулой $\mathfrak{B}(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$, полученной из $\mathfrak{B}(t_1, \ldots, t_n)$ заменой переменных $t_1, \ldots, t_n$ соответственно термами $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ (ср. с § 4 главы IV).

Всякое исчисление, полученное из исчисления предикатов присоединением некоторых предметных функций и аксиом равенства

VI. 1. $x = x$,

VI. 2. $x = y \to (A(x) \to A(y))$

и расширением правил подстановки в указанном выше смысле, будем называть *расширенным исчислением предикатов*. Очевидно, что все производные правила, выведенные нами для исчисления предикатов, распространяются как на расширенное исчисление предикатов, так и на любую систему, полученную присоединением к расширенному исчислению предикатов каких угодно аксиом и новых правил образования выводимых формул. Справедливость этого ясна, так как все аксиомы и правила вывода исчисления предикатов, на основании которых выведены производные правила, во всех случаях сохраняются.

Выражение $\vdash \mathfrak{A}$, которое означает, что формула $\mathfrak{A}$ выводима в исчислении предикатов, мы будем употреблять теперь и для формул, выводимых в расширенном исчислении предикатов, и в других формализмах. Смешения смысла в употреблении этого символа для разных формализмов не может произойти, так как из контекста всегда будет видно, в каком формализме выводится данная формула.

§ 2. Свойства предиката равенства и предметных функций

Выведем основные свойства предиката равенства

$$\vdash x = y \to y = x. \tag{1}$$

В аксиому VI. 2 сделаем подстановку, заменив $A(t)$ формулой $t = x$. Тогда мы получим

$$\vdash x = y \to (x = x \to y = x).$$

Применив правило перестановки посылок, получим

$$\vdash x = x \to (x = y \to y = x).$$

Применив затем правило заключения, получим требуемую формулу:

$$x = y \to y = x.$$

Второе свойство равенства называется *транзитивностью*:

$$\vdash x = y \to (y = z \to x = z). \tag{2}$$

Сначала выведем формулу

$$x = y \to (A(y) \to A(x)).$$

Переименовав переменные в аксиоме VI. 2, получим

$$\vdash y = x \to (A(y) \to A(x)). \tag{3}$$

Из этой формулы и выведенной нами формулы (1), применив правило силлогизма, получим требуемую формулу:

$$\vdash x = y \to (A(y) \to A(x)). \tag{4}$$

Подставив в последнюю формулу вместо предиката $A(t)$ формулу $t = z$, получим (2).

Следствие

$$\vdash x = y \to (A(x) \sim A(y)).$$

Из (4) и аксиомы VI. 2 следует

$$\vdash x = y \to (A(x) \to A(y)) \,\&\, (A(y) \to A(x)),$$

или

$$\vdash x = y \to (A(x) \sim A(y)),$$

что и требовалось доказать.

Будем называть термы $\mathfrak{a}$ и $\mathfrak{c}$ равными в исчислении, содержащем аксиомы равенства, если формула

$$\mathfrak{a} = \mathfrak{c}$$

выводима в этом исчислении. В таком случае имеет место следующее правило.

Если термы $\mathfrak{a}$ и $\mathfrak{c}$ равны в некотором исчислении, то в нем выводима формула

$$\mathfrak{A}(\mathfrak{a}) \sim \mathfrak{A}(\mathfrak{c}),$$

где $\mathfrak{A}(\mathfrak{a})$ и $\mathfrak{A}(\mathfrak{c})$ получены заменой любой переменной x, входящей в формулу $\mathfrak{A}$.

В самом деле, сделав подстановку в формулу

$$x = y \to (A(x) \sim A(y)),$$

имеем сначала

$$\vdash x = y \to (\mathfrak{A}(x) \sim \mathfrak{A}(y)),$$

затем

$$\vdash \mathfrak{a} = \mathfrak{c} \to (\mathfrak{A}(\mathfrak{a}) \sim \mathfrak{A}(\mathfrak{c}));$$

так как имеет место $\vdash \mathfrak{a} = \mathfrak{c}$, то, применив правило заключения, получим

$$\vdash \mathfrak{A}(\mathfrak{a}) \sim \mathfrak{A}(\mathfrak{c}).$$

Отсюда следует, что если формула $\mathfrak{A}(\mathfrak{a})$ выводима в исчислении, содержащем аксиомы равенства, то формула $\mathfrak{A}(\mathfrak{c})$, полученная из предыдущей заменой терма $\mathfrak{a}$ равным ему термом $\mathfrak{c}$, также выводима в этом исчислении.

Заметим, что при замене терма, входящего в формулу $\mathfrak{A}$, равным нет необходимости заменять его всюду, где он входит в формулу $\mathfrak{A}$. Пусть терм $\mathfrak{a}$ входит в разные части формулы $\mathfrak{A}$; представим формулу $\mathfrak{A}$ в виде $\mathfrak{A}(\mathfrak{a}, \mathfrak{a})$. Тогда, если $\mathfrak{c}$ равен $\mathfrak{a}$, то имеет место

$$\vdash \mathfrak{A}(\mathfrak{a}, \mathfrak{a}) \sim \mathfrak{A}(\mathfrak{a}, \mathfrak{c}).$$

В самом деле, возьмем переменные x и y, не входящие в термы $\mathfrak{a}$ и $\mathfrak{c}$; тогда, заменив в формуле

$$x = y \to (A(x) \sim A(y))$$

предикат $A(t)$ предикатом $\mathfrak{A}(\mathfrak{a}, t)$, будем иметь

$$\vdash x = y \to (\mathfrak{A}(\mathfrak{a}, x) \sim \mathfrak{A}(\mathfrak{a}, y)).$$

Подставив $\mathfrak{a}$ вместо x, а $\mathfrak{c}$ вместо y, получим

$$\vdash \mathfrak{a} = \mathfrak{c} \rightarrow (\mathfrak{A}(\mathfrak{a}, \mathfrak{a}) \sim \mathfrak{A}(\mathfrak{a}, \mathfrak{c})).$$

Отсюда и из равенства $\mathfrak{a} = \mathfrak{c}$ следует

$$\vdash \mathfrak{A}(\mathfrak{a}, \mathfrak{a}) \sim \mathfrak{A}(\mathfrak{a}, \mathfrak{c}),$$

так что, заменив $\mathfrak{a}$ только в одном месте на $\mathfrak{c}$, мы получаем эквивалентную формулу.

Выведем некоторые формулы, связывающие предикат равенства с предметными функциями.

$$\vdash \exists x [\mathfrak{a}(x) = \mathfrak{a}(y)]. \tag{5}$$

Из аксиомы $F(z) \rightarrow \exists x F(x)$ путем подстановки получим

$$\vdash \mathfrak{a}(z) = \mathfrak{a}(y) \rightarrow \exists x [\mathfrak{a}(x) = \mathfrak{a}(y)].$$

Заменив свободную переменную z на y, получим

$$\vdash \mathfrak{a}(y) = \mathfrak{a}(y) \rightarrow \exists x [\mathfrak{a}(x) = \mathfrak{a}(y)].$$

Применив правило заключения, получим (5).

$$\vdash \forall x A(x) \rightarrow \forall x \forall y A(\mathfrak{a}(x, y)). \tag{6}$$

Из аксиомы $\forall x A(x) \rightarrow A(z)$, заменив в ней свободную переменную z термом $\mathfrak{a}(u, v)$, получим

$$\vdash \forall x A(x) \rightarrow A(\mathfrak{a}(u, v)).$$

Применив дважды первое правило связывания квантором и переименовав связанные переменные, получим формулу (6). Очевидно, аналогичную выводимую формулу можно получить для функции $\mathfrak{a}$ с любым числом переменных.

$$\vdash x = y \rightarrow \mathfrak{a}(x) = \mathfrak{a}(y). \tag{7}$$

Заменив во второй аксиоме равенства $A(t)$ на $\mathfrak{a}(x) = \mathfrak{a}(t)$, получим

$$\vdash x = y \rightarrow [\mathfrak{a}(x) = \mathfrak{a}(x) \rightarrow \mathfrak{a}(x) = \mathfrak{a}(y)].$$

Переставив посылки, получим

$$\vdash \mathfrak{a}(x) = \mathfrak{a}(x) \rightarrow [x = y \rightarrow \mathfrak{a}(x) = \mathfrak{a}(y)].$$

Удалив, наконец, выводимую посылку, получим формулу (7).

Докажем теперь следующую формулу:

$$(x = u) \mathbin{\&} (y = v) \to [\mathfrak{g}(x, y) = \mathfrak{g}(u, v)]. \tag{8}$$

Аналогично предыдущему случаю мы выведем две формулы:

$$x = u \to [\mathfrak{g}(x, y) = \mathfrak{g}(u, y)], \tag{9}$$

$$y = v \to [\mathfrak{g}(u, y) = \mathfrak{g}(u, v)]. \tag{10}$$

Из выводимой формулы

$$x = u \to (u = y \to x = y)$$

путем замены свободных переменных термом получим

$$\mathfrak{g}(x, y) = \mathfrak{g}(u, y) \to \{\mathfrak{g}(u, y) = \mathfrak{g}(u, v) \to \mathfrak{g}(x, y) = \mathfrak{g}(u, v)\}.$$

Применив к формуле (9) и последней формуле правило силлогизма, получим

$$x = u \to \{\mathfrak{g}(u, y) = \mathfrak{g}(u, v) \to \mathfrak{g}(x, y) = \mathfrak{g}(u, v)\}.$$

Переставив в этой формуле посылки, получим формулу

$$\mathfrak{g}(u, y) = \mathfrak{g}(u, v) \to \{x = u \to \mathfrak{g}(x, y) = \mathfrak{g}(u, v)\}. \tag{11}$$

Применив правило силлогизма к формулам (10) и (11), получим

$$y = v \to \{x = u \to \mathfrak{g}(x, y) = \mathfrak{g}(u, v)\}.$$

Соединив посылки в произведение и переставив множители, получим формулу (8).

Содержательный смысл последних теорем состоит в том, что *введенные нами предметные функции однозначны*, т. е. равным значениям аргументов соответствуют равные значения функций.

То обстоятельство, что для всякой предметной функции $\mathfrak{r}(u_1, \ldots, u_n)$ имеет место равенство, выражаемое формулой

$$u_1 = v_1 \mathbin{\&} u_2 = v_2 \mathbin{\&} \ldots \mathbin{\&} u_n = v_n \to$$
$$\to (\mathfrak{r}(u_1, \ldots, u_n) = \mathfrak{r}(v_1, \ldots v_n)),$$

мы будем выражать словами: *«предметные функции однозначны»*.

§ 3. Отношение эквивалентности

В математике постоянно приходится иметь дело с отношениями, выражающими то или иное сходство между рассматриваемыми объектами. Таковы, например, равенство чисел, подобие геометрических фигур, логическая эквивалентность высказываний и другие. Назовем эти отношения *отношениями эквивалентности*, употребляя здесь термин «эквивалентность» в ином, более широком смысле, чем термин «эквивалентность формул», которым мы все время пользовались в определенном специально логическом смысле.

Можно охарактеризовать отношения эквивалентности следующими свойствами.

1) *Свойство рефлексивности*: каждый предмет эквивалентен самому себе.

2) *Свойство симметрии*: если x эквивалентно y, то и y эквивалентно x.

3) *Свойство транзитивности*: если x эквивалентно y, а y эквивалентно z, то и x эквивалентно z.

Если для какой-либо области объектов $\mathfrak{M}$ установлено отношение эквивалентности $S(x, y)$, то этим область $\mathfrak{M}$ разделяется на классы, состоящие из различных элементов, так что все элементы одного класса эквивалентны между собой и любые два эквивалентных элемента принадлежат одному и тому же классу.

Пример. Пусть $\mathfrak{M}$ — множество всех целых чисел, а $S(x, y)$ — сравнимость по модулю 3:

$$x \equiv y \pmod 3.$$

В таком случае $\mathfrak{M}$ разделяется на три класса. Первый класс состоит из чисел вида $3n$, делящихся на 3, второй — из чисел вида $3n + 1$, дающих 1 в остатке от деления на 3, а третий — из чисел вида $3n + 2$, дающих 2 в остатке от деления на 3.

Отношение эквивалентности может быть выражено формулами исчисления предикатов. Для этого надо записать в виде аксиом его свойства, т. е. рефлексивность, симметрию и транзитивность. Обозначим отношение эквивалентности знаком $\approx$. Тогда аксиомы эквивалентности запишутся так:

1. $x \approx x$.

2. $x \approx y \to y \approx x$.

3. $x \approx y \to [y \approx z \to x \approx z]$.

Отношение равенства обладает теми же свойствами, причем свойство рефлексивности совпадает с первой аксиомой равенства, а остальные два — симметрия и транзитивность, — как мы видели, в расширенном исчислении предикатов являются следствиями из аксиом равенства.

В содержательной математике и в наивной теории множеств существует один особый вид отношения эквивалентности, именно *тождественность*. Смысл этого понятия состоит в том, что если x и y тождественны, то они обозначают один и тот же объект. Ясно, что в этом случае каждый из классов, на которые разбивается $\mathfrak{M}$, состоит только из одного объекта. Если рассматривать исчисление предикатов с точки зрения наивной теории множеств, то равенство, которое определяется аксиомами VI. 1 и VI. 2, представляет собой именно теоретико-множественное тождество. Мы подчеркнем здесь еще раз, что вторая аксиома равенства имеет следующий содержательный смысл: «*если x тождественно y, то все, что можно высказать об x, можно высказать и об y*».

Можно формально доказать, что если два предмета тождественны, то они эквивалентны. Точнее говоря, можно вывести из аксиом равенства и эквивалентности формулу

$$x = y \to x \approx y.$$

В самом деле, подставив в аксиому равенства VI. 2 $x \approx t$ вместо $A(t)$, получим формулу

$$x = y \to [x \approx x \to x \approx y]$$

и, переставив посылки,

$$x \approx x \to [x = y \to x \approx y].$$

Удалив выводимую посылку $x \approx x$, получим требуемую формулу.

При содержательной трактовке системы аксиом исчисления предикатов мы считали, что имеющиеся в аксиомах переменные предикаты можно заменить любыми предикатами, определенными на данной области. Можно изменить характер интерпретации системы аксиом. Можно потребовать, чтобы данная система аксиом была истинна для данной области при заменах переменных предикатов не любыми предикатами, определенными на данной области, а только такими, которые принадлежат к некоторой определенной совокупности, составляющей часть множества всех предикатов. В таком случае для некоторого подмножества предикатов аксиомы VI. 1 и VI. 2 определят отношение эквивалентности, которое можно называть *относительным равенством* или равенством относительно данной системы предикатов.

§ 4. Теорема дедукции

Теорема дедукции, доказанная в предыдущей главе, распространяется и на расширенное исчисление предикатов. Для формулировки этой теоремы, как и раньше, сначала надо определить понятие выводимости формулы $\mathfrak{B}$ из формулы $\mathfrak{A}$.

1. Все выводимые формулы расширенного исчисления предикатов, не приводящие к коллизии переменных с $\mathfrak{A}$, выводимы из $\mathfrak{A}$.

2. Формула $\mathfrak{A}$ выводима из $\mathfrak{A}$.

3. Если $\mathfrak{B}_1$ и $\mathfrak{B}_1 \rightarrow \mathfrak{B}_2$ выводимы из $\mathfrak{A}$, то $\mathfrak{B}_2$ выводима из $\mathfrak{A}$.

4. Если $\mathfrak{B}_1 \rightarrow \mathfrak{B}_2(x)$ выводима из $\mathfrak{A}$ и переменная x не содержится ни в $\mathfrak{A}$, ни в $\mathfrak{B}_1$, то и формула $\mathfrak{B}_1 \rightarrow \forall x \mathfrak{B}_2(x)$ выводима из $\mathfrak{A}$.

5. Если формула $\mathfrak{B}_1(x) \rightarrow \mathfrak{B}_2$ выводима из $\mathfrak{A}$ и x не содержится ни в $\mathfrak{B}_2$, ни в $\mathfrak{A}$, то и формула $\exists x \mathfrak{B}_1(x) \rightarrow \mathfrak{B}_2$ выводима из $\mathfrak{A}$.

6. Если формула $\mathfrak{B}$ выводима из $\mathfrak{A}$, то всякая формула $\mathfrak{B}'$, полученная из $\mathfrak{B}$ подстановкой в переменное высказывание или переменный предикат, не входящие в формулу $\mathfrak{A}$, так что при этом $\mathfrak{B}'$ не приводит к коллизии переменных с $\mathfrak{A}$, также выводима из формулы $\mathfrak{A}$.

7. Если формула $\mathfrak{B}$ выводима из формулы $\mathfrak{A}$ и формула $\mathfrak{B}'$ получена из $\mathfrak{B}$ подстановкой в свободную переменную, не входящую в $\mathfrak{A}$, так что $\mathfrak{B}'$ не приводит

к коллизии переменных с $\mathfrak{A}$, то формула $\mathfrak{A}'$ выводима из $\mathfrak{A}$.

8. Если формула $\mathfrak{B}$ выводима из формулы $\mathfrak{A}$ и $\mathfrak{B}'$—формула, полученная из $\mathfrak{B}$ переименованием связанных переменных, так что $\mathfrak{B}'$ не приводит к коллизии переменных с $\mathfrak{A}$, то формула $\mathfrak{B}'$ выводима из $\mathfrak{A}$.

Таким образом, определение выводимости в расширенном исчислении предикатов в точности совпадает с соответствующим определением для исчисления предикатов. Содержание этого определения, однако, несколько иное, так как правила подстановок в расширенном исчислении предикатов отличаются от соответствующих правил в исчислении предикатов. Формулировка теоремы дедукции для расширенного исчисления предикатов остается той же, что и раньше, а доказательство ее проводится аналогично.

Теорема дедукции. *Если формула $\mathfrak{B}$ выводима из формулы $\mathfrak{A}$ в указанном смысле, то формула*

$$\mathfrak{A} \to \mathfrak{B}$$

выводима в расширенном исчислении предикатов.

§ 5. Аксиомы арифметики

Введем в нашу систему индивидуальный предмет 0 и предметную функцию $\lambda(x)$. В таком случае в нашу систему войдут еще следующие функции и постоянные термы:

$$\lambda(\lambda(x)),\ \lambda(\lambda(\lambda(x))),\ \ldots,\ \lambda(\lambda(\ldots\lambda(x)\ldots)) - n \text{ раз},\ \ldots,$$
$$\lambda(0),\ \lambda(\lambda(0)),\ \ldots,\ \lambda(\lambda(\ldots\lambda(0)\ldots)).$$

Для сокращения письма функцию $\lambda(x)$ мы будем писать в виде

$$x'.$$

Операцию замены аргумента, например

$$\lambda(\mathfrak{a}(x,\ y)),$$

в этой символике мы будем записывать так:

$$(\mathfrak{a}(x,\ y))'.$$

Тогда выражения

$$\lambda(x),\ \lambda(\lambda(x)),\ \ldots\ \lambda(\lambda(\ldots(\lambda(x)),\ \ldots)),\ \ldots$$

будут изображаться в виде

$$x',\ (x')',\ ((x')')',\ \ldots$$

Запись этих выражений мы еще упростим. Именно, $(x')'$ будем писать в виде x'', $((x')')'$ — в виде x''' и т. д.

Предметные постоянные

$$\lambda(0),\ \lambda(\lambda(0)),\ \ldots$$

теперь изобразятся в виде

$$0',\ 0'',\ \ldots,\ 0\overbrace{''\cdots'}^{n\ \text{раз}},\ \ldots$$

Эти постоянные вместе с предметом 0 *мы будем называть цифрами.* Цифры, представленные знаком 0 с n штрихами, мы будем обозначать $0^{(n)}$.

При содержательном изложении исчисления предикатов (глава III) мы уже рассматривали аксиомы арифметики или, точнее говоря, аксиомы порядковых отношений натурального ряда (аксиомы порядковых отношений арифметики) Выразим теперь те же свойства натурального ряда посредством формул некоторого исчисления. Для этого к расширенному исчислению предикатов (см. стр. 282), содержащему предмет 0 и функцию x', присоединим индивидуальный предикат $<$, который в содержательном понимании имеет смысл термина «меньше» и удовлетворяет следующим аксиомам:

VII. Аксиомы порядка

1. $\overline{x < x}$.
2. $x < y \rightarrow (y < z \rightarrow x < z)$.
3. $x < x'$.

VIII. Аксиома полной индукции

$$A(0)\ \&\ \forall x\,(A(x) \rightarrow A(x')) \rightarrow A(y).$$

Правила вывода в новом исчислении сохранены те же, что и в расширенном исчислении предикатов. Эта система аксиом по своему содержательному смыслу выражает то же самое, что и система аксиом натурального ряда, рассмотренная нами в § 8 главы III. Точнее говоря, если рассматривать нашу логическую систему с содержательной точки зрения, изложенной в главе III, то рассматриваемые нами понятия — предметы, предикаты и логические формулы — имеют смысл в отношении к заданному множеству или области. Предметная функция $\mathfrak{g}(x_1, \ldots, x_n)$ представляет собой функцию в обычном понимании — определенную на данной области и принимающую значения из данной области.

С этой точки зрения можно показать, что аксиомы VI, VII, VIII интерпретируются любым упорядоченным множеством, подобным натуральному ряду, в котором за предмет 0 принят элемент, предшествующий (в смысле отношения порядка данного упорядоченного множества) всем остальным, а значение функции x' представляет собой элемент, непосредственно следующий за элементом x. И обратно, только множество, подобное натуральному ряду, удовлетворяет написанной системе аксиом. Таким образом, если трактовать аксиомы содержательным образом, то система аксиом VI, VII, VIII равносильна той системе, которую мы уже рассматривали в § 8 главы III. Она, следовательно, интерпретируема и полна с точностью до изоморфизма. Однако теперь мы не рассматриваем систему аксиом VI, VII, VIII в духе главы III. Она совместно с аксиомами и правилами вывода исчисления предикатов представляет собой формализм, определенный на основе принципов финитизма. Поэтому приведенная выше содержательная трактовка этих аксиом может иметь только эвристическое значение для решения вопросов, возникающих при изучении данного формализма. Аксиомы VI, VII, VIII не исчерпывают формальной арифметики, они не содержат описания арифметических действий. В дальнейшем мы еще расширим это исчисление. Но предварительно мы рассмотрим систему аксиом VI, VII, VIII более детально.

§ 6. Примеры выводимых формул

Приведем в виде примеров формальные доказательства некоторых положений, выводимых из аксиом VI, VII, VIII.

Теорема 1.

$$\vdash 0 < x'.$$

Заменив в аксиоме полной индукции предикат $A(x)$ предикатом $0 < x'$, получим

$$\vdash 0 < 0' \,\&\, \forall x\,[0 < x' \to 0 < x''] \to 0 < y'. \qquad (1)$$

Посредством подстановки в аксиому VII. 3 получаем

$$\vdash 0 < 0'$$

и

$$\vdash x' < x''.$$

Сделав подстановки в аксиому VII. 2, получим

$$\vdash 0 < x' \to (x' < x'' \to 0 < x'').$$

Переставив посылки, получим

$$\vdash x' < x'' \to (0 < x' \to 0 < x'').$$

Так как $x' < x''$ — выводимая формула, то, применив правило заключения, будем иметь

$$\vdash 0 < x' \to 0 < x''.$$

И, наконец, применив производное правило связывания квантором, получим

$$\vdash \forall x\,(0 < x' \to 0 < x'').$$

Применив к формулам $0 < 0'$ и $\forall x\,(0 < x' \to 0 < x'')$ правило $\dfrac{\mathfrak{A},\ \mathfrak{B}}{\mathfrak{A} \,\&\, \mathfrak{B}}$, имеем

$$\vdash 0 < 0' \,\&\, \forall x\,(0 < x' \to 0 < x''). \qquad (2)$$

Применив к (2) и (1) правило заключения, получим

$$\vdash 0 < y'$$

и, следовательно,

$$\vdash 0 < x'.$$

Теорема 2.

$$\vdash \overline{x < 0} \to x = 0 \vee 0 < x.$$

Заменив предикат $A(x)$ в аксиоме VIII предикатом

$$\overline{x < 0} \to x = 0 \vee 0 < x,$$

получим

$$\vdash (\overline{0 < 0} \to 0 = 0 \vee 0 < 0) \mathbin{\&} \forall x\,[(\overline{x < 0} \to x = 0 \vee 0 < x) \to \\ \to (\overline{x' < 0} \to x' = 0 \vee 0 < x')] \to \\ \to (\overline{y < 0} \to y = 0 \vee 0 < y). \quad (3)$$

Посылка этого следования представляет собой логическое произведение двух множителей. Первый из них

$$\overline{0 < 0} \to 0 = 0 \vee 0 < 0$$

является выводимым. В самом деле, имеет место

$$\vdash 0 = 0,$$

откуда следует

$$\vdash 0 = 0 \vee 0 < 0;$$

и, наконец, поскольку из выводимости следствия вытекает выводимость импликации, мы получаем

$$\vdash \overline{0 < 0} \to 0 = 0 \vee 0 < 0. \quad (4)$$

Далее, на основании предыдущей теоремы имеем

$$\vdash 0 < x',$$

откуда следует

$$\vdash x' = 0 \vee 0 < x'.$$

И поэтому

$$\vdash \overline{x' < 0} \to x' = 0 \vee 0 < x'.$$

Отсюда заключаем, что

$$\vdash (\overline{x < 0} \to x = 0 \vee 0 < x) \to (\overline{x' < 0} \to x' = 0 \vee 0 < x').$$

Наконец, применив производное правило связывания квантором, получим

$$\vdash \forall x\,[(\overline{x < 0} \to x = 0 \vee 0 < x) \to \\ \to (\overline{x' < 0} \to x' = 0 \vee 0 < x')]. \quad (5)$$

Формулы (4) и (5) представляют собой множители посылки формулы (3), поэтому на основании правила $\dfrac{\mathfrak{A}, \mathfrak{B}}{\mathfrak{A} \mathbin{\&} \mathfrak{B}}$ эта посылка является выводимой формулой. В силу этого следствие в формуле (3) также выводимо и мы имеем

$$\vdash \overline{y < 0} \to y = 0 \vee 0 < y.$$

Заменив y на x, получим требуемую формулу.

Теорема 3.

$$\vdash \overline{x < 0}.$$

Подставив в аксиому полной индукции вместо предиката $A(x)$ предикат $\overline{x < 0}$, получим

$$\vdash \overline{0 < 0} \mathbin{\&} \forall x [\overline{x < 0} \to \overline{x' < 0}] \to \overline{y < 0}. \qquad 6)$$

Первый множитель выводится посредством подстановки в аксиому VII. 1. Выведем второй множитель. Подстановкой в аксиому VII. 2 получим

$$\vdash x < x' \to (x' < 0 \to x < 0).$$

Посылка этого следования есть аксиома VII. 3.

Применив правило заключения, имеем

$$\vdash x' < 0 \to x < 0.$$

Обратив эту импликацию, получим

$$\vdash \overline{x < 0} \to \overline{x' < 0}.$$

Применив производное правило связывания квантором, будем иметь

$$\vdash \forall x [\overline{x < 0} \to \overline{x' < 0}].$$

Итак, мы вывели и второй множитель посылки формулы (6). Отсюда следует, что и посылка и следствие — выводимые формулы, т. е.

$$\vdash \overline{y < 0}$$

и, следовательно,

$$\vdash \overline{x < 0}.$$

Сопоставляя теоремы 2 и 3 и применяя правило заключения, получим

$$\vdash x = 0 \vee 0 < x.$$

Итак, мы показали, что из аксиом арифметики формально вытекает, что 0 меньше любого другого предмета нашей системы.

Нетрудно также показать, что между цифрами 0 и 0′, 0′ и 0″ и т. д. (для каждой пары цифр в отдельности) не заключен ни один предмет нашей системы, т. е.

$$\vdash \overline{0 < x \,\&\, x < 0'},$$
$$\vdash \overline{0' < x \,\&\, x < 0''},$$
$$\cdots\cdots\cdots$$

Отсюда следует, что 0′ — наименьший из предметов, не равных 0, 0″ — наименьший из предметов, не равных 0 и 0′, и т. д. В этой системе выводимо и общее утверждение

$$\overline{t < x \,\&\, x < t'}.$$

Более того, можно доказать (но мы этого делать здесь не будем), что система аксиом I—VIII обладает внутренней полнотой, т. е. все формулы, истинные для любой интерпретации этой системы аксиом, в ней выводимы.

§ 7. Рекурсивные термы

Мы определим некоторую определенную категорию термов, которые будем называть *рекурсивными термами*. Определение это мы дадим индуктивным способом. Мы укажем исходные рекурсивные термы и дадим правила образования новых рекурсивных термов из ранее полученных. Одновременно с правилами образования рекурсивных термов мы определим правила образования равенств между ними и примем эти равенства за истинные или *выводимые по определению*.

1. 0 есть рекурсивный терм.

2. Всякая предметная переменная есть рекурсивный терм.

3. x' есть рекурсивный терм.

4. Если $\mathfrak{a}$ есть рекурсивный терм, содержащий предметную переменную x, то терм $\mathfrak{a}^*$, полученный из $\mathfrak{a}$ заменой этой предметной переменной любым рекурсивным термом, есть также рекурсивный терм.

5. Пусть $\mathfrak{a}(x_1, \ldots, x_{n-1})$ — любой рекурсивный терм, содержащий из предметных переменных только $x_1, \ldots, x_{n-1}$, но не обязательно все и, быть может, даже ни

одной, а $\mathfrak{b}(x_1, \ldots, x_{n+1})$ — любой рекурсивный терм, содержащий из предметных переменных только $x_1, \ldots$ $\ldots, x_{n+1}$, но также, может быть, не все. Для любых двух таких термов введем новый рекурсивный терм, представляющий собой предметную функцию, содержащую все переменные $x_1, x_2, \ldots, x_n$ и только их. При этом каждый раз вновь определяемая функция должна обозначаться символом, отличным от символов всех ранее определенных функций, т. е. двум различным парам термов должны ставиться в соответствие различные предметные функции. Допустим, что паре термов

$$\mathfrak{a}(x_1, \ldots, x_{n-1}) \quad \text{и} \quad \mathfrak{b}(x_1, \ldots, x_{n+1})$$

поставлена в соответствие функция $\xi(x_1, \ldots, x_n)$. Мы свяжем каждую такую функцию с соответствующими термами некоторыми равенствами, которые будем считать выводимыми или истинными и называть *рекурсивными равенствами*. Равенства эти имеют следующий вид:

$$\left.\begin{aligned} &\xi(x_1, \ldots, x_{n-1}, 0) = \mathfrak{a}(x_1, \ldots, x_{n-1}), \\ &\xi(x_1, \ldots, x_{n-1}, x_n') = \mathfrak{b}(x_1, \ldots, x_n, \xi(x_1, \ldots, x_n)). \end{aligned}\right\} \quad (1)$$

Если бы оказалось, что терм $\mathfrak{b}$ переменной x_{n+1} не содержит, то будем считать, что выражение

$$\mathfrak{b}(x_1, \ldots, x_n, \xi(x_1, \ldots, x_n))$$

представляет собой сам терм $\mathfrak{b}$ без всякого изменения. Например, если $\mathfrak{b}(x_1, x_2)$ представляет собой x_1', то выражение $\mathfrak{b}(x_1, \xi(x_1))$ представляет собой также x_1'. В рекурсивных равенствах фигурируют аргументы $x_1, \ldots, x_n$. Строго говоря, буквы $x_1, \ldots, x_n$ не обозначают произвольных предметных переменных, а представляют собой *определенные* предметные переменные, и, следуя определению, рекурсивные равенства надо писать именно с ними. Однако если мы вместо рекурсивных равенств (1) напишем равенства

$$\xi(x, y, \ldots, u, 0) = \mathfrak{a}(x, y, \ldots, u),$$
$$\xi(x, y, \ldots, u, v') = \mathfrak{b}(x, y, \ldots, u, \xi(x, y, \ldots, v)),$$

получающиеся из предыдущих подстановкой, то последние равенства будут выводимы в том же исчислении, что и первые. Мы сохраним за ними название рекурсивных равенств и в дальнейшем будем, когда это потребуется, писать их без всяких ссылок на основные рекурсивные равенства.

Правило образования рекурсивных термов и правило образования связывающих равенств, описанные в п. 5, распространяются и на случай $n = 1$. Только тогда терм $\mathfrak{a}$ не должен содержать никакой предметной переменной. Рекурсивные равенства для этого случая имеют следующий вид:

$$\mathfrak{f}(0) = \mathfrak{a},$$
$$\mathfrak{f}(x_1') = \mathfrak{b}(x_1, \mathfrak{f}(x_1)).$$

Таким образом, к системе аксиом VI, VII, VIII мы присоединяем неограниченное количество новых истинных формул, которые мы назвали рекурсивными равенствами. В результате мы получаем исчисление более сильное, чем исчисление с системой аксиом VI, VII, VIII, в том смысле, что расширенная система описывает свойства натурального ряда несравненно полнее, чем система аксиом VI, VII, VIII.

Полученное нами *исчисление, содержащее аксиомы* I—VIII, *рекурсивные термы и рекурсивные равенства, с правилами вывода расширенного исчисления предикатов мы будем называть аксиоматической арифметикой.*

§ 8. Ограниченная арифметика

Если из аксиом аксиоматической арифметики мы удалим аксиому полной индукции, то получим исчисление, которое будем называть ограниченной арифметикой. Рекурсивный терм, который не содержит предметных переменных, будем называть *рекурсивной константой* *).

Теорема. *Для всякой рекурсивной константы $\mathfrak{c}$ существует цифра $\mathfrak{z}$ такая, что равенство $\mathfrak{c} = \mathfrak{z}$ выводимо в ограниченной арифметике.*

Мы докажем наше утверждение в следующем виде. *Пусть $\mathfrak{c}$ — произвольный рекурсивный терм, а $\mathfrak{c}^*$ — терм, полученный из $\mathfrak{c}$ произвольной заменой всех вхо-*

*) Это определение вполне согласуется с определением предметной постоянной, данным в § 1.

дящих в него переменных цифрами. Тогда существует цифра $\mathfrak{z}$ такая, что равенство $\mathfrak{c}^* = \mathfrak{z}$ выводимо в ограниченной арифметике. Мы считаем при этом, что в случае, когда $\mathfrak{c}$ не имеет переменных, $\mathfrak{c}^*$ совпадает с $\mathfrak{c}$.

Это утверждение мы будем доказывать по индукции, соответственно правилам образования рекурсивных термов. Для исходных рекурсивных термов наше утверждение очевидно, так как 0 есть цифра; переменная после замены ее цифрой превращается в цифру; функция x' после замены x цифрой также превращается в цифру.

Пусть для рекурсивного терма $\mathfrak{a}(x)$, содержащего некоторую переменную, например x, и для рекурсивного терма $\mathfrak{t}$ наше утверждение справедливо. Покажем, что тогда оно справедливо и для терма

$$\mathfrak{a}(\mathfrak{t}).$$

Если мы заменим в этом терме все переменные цифрами, то получим терм, который можно представить в виде

$$\mathfrak{a}^*(\mathfrak{t}^*),$$

где $\mathfrak{t}^*$ есть результат замены переменных в $\mathfrak{t}$ цифрами, а $\mathfrak{a}^*$ есть результат замены всех переменных в $\mathfrak{a}(x)$, кроме x, цифрами. По условию для $\mathfrak{t}$ существует цифра $\mathfrak{z}^*$ такая, что равенство $\mathfrak{t}^* = \mathfrak{z}^*$ выводимо в ограниченной арифметике.

Но формула
$$\mathfrak{t}^* = \mathfrak{z}^* \to \mathfrak{a}^*(\mathfrak{t}^*) = \mathfrak{a}^*(\mathfrak{z}^*)$$

выводима из аксиом равенства, без применения аксиомы полной индукции (см. § 2); поэтому, применив правило заключения, мы получим, что равенство

$$\mathfrak{a}^*(\mathfrak{t}^*) = \mathfrak{a}^*(\mathfrak{z}^*)$$

также выводимо в ограниченной арифметике.

Так как $\mathfrak{a}^*(\mathfrak{z}^*)$ представляет собой результат замены всех переменных в $\mathfrak{a}(x)$ цифрами, то, по условию, существует цифра $\mathfrak{z}$ такая, что $\mathfrak{a}^*(\mathfrak{z}^*) = \mathfrak{z}$.

Из равенств

$$\mathfrak{a}^*(\mathfrak{t}^*) = \mathfrak{a}^*(\mathfrak{z}^*) \quad \text{и} \quad \mathfrak{a}^*(\mathfrak{z}^*) = \mathfrak{z}$$

и аксиом равенства выводимо равенство

$$\mathfrak{a}^*(\mathfrak{t}^*) = \mathfrak{z}.$$

Следовательно, последнее равенство выводимо в ограниченной арифметике. Так как терм $\mathfrak{a}^*(\mathfrak{t}^*)$ есть результат произвольной замены переменных, входящих в $\mathfrak{a}(\mathfrak{t})$, цифрами, то для терма $\mathfrak{a}(\mathfrak{t})$ наше утверждение доказано.

Допустим, далее, что для термов $\mathfrak{a}(x_1, \ldots, x_{n-1})$ и $\mathfrak{y}(x_1, \ldots, x_n, y)$ наше утверждение справедливо, и докажем, что тогда оно справедливо и для терма $\mathfrak{x}(x_1, \ldots, x_n)$, введенного на основании п. 5. Возьмем $n-1$ произвольных цифр $\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}$ и рассмотрим последовательность термов

$$\mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0),$$
$$\mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0'), \ldots, \mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k)}), \ldots$$

Докажем, что для каждого члена этой последовательности можно определить цифру $\mathfrak{z}_k^*$ такую, что выводимо равенство

$$\mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k)}) = \mathfrak{z}_k^*.$$

Докажем это индукцией по индексу k. Мы имеем выводимое в ограниченной арифметике равенство

$$\mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0) = \mathfrak{a}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}).$$

Но, по условию, для $\mathfrak{a}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1})$ существует цифра $\mathfrak{z}_0^*$ такая, что выводимо равенство

$$\mathfrak{a}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}) = \mathfrak{z}_0^*.$$

Следовательно, и равенство

$$\mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0) = \mathfrak{z}_0^*$$

также выводимо в ограниченной арифметике.

Допустим, что для $\mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k)})$ существует цифра $\mathfrak{z}_k^*$ такая, что в ограниченной арифметике выводимо равенство

$$\mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k)}) = \mathfrak{z}_k^*. \tag{1}$$

Вместе с тем на основании предположения, сделанного относительно функции $\mathfrak{y}$, существует цифра $\mathfrak{z}_{k+1}^*$ такая, что равенство

$$\mathfrak{y}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k)}, \mathfrak{z}_k^*) = \mathfrak{z}_{k+1}^*$$

выводимо в ограниченной арифметике.

Используя эти два равенства и равенство

$$\mathfrak{x}(x_1, \ldots, x_{n-1}, x_n') = \mathfrak{y}(x_1, \ldots, x_n, \mathfrak{x}(x_1, \ldots, x_n)),$$

получим

$$\mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k+1)}) =$$
$$= \mathfrak{y}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k)}, \mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k)})) =$$
$$= \mathfrak{y}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k)}, \mathfrak{z}_k^*) = \mathfrak{z}_{k+1}^*.$$

Следовательно, равенство

$$\mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k+1)}) = \mathfrak{z}_{k+1}^*$$

выводимо в ограниченной арифметике.

Итак, для каждого выражения $\mathfrak{x}(\mathfrak{z}_1, \ldots, \mathfrak{z}_{n-1}, 0^{(k)})$ мы можем определить цифру $\mathfrak{z}_k^*$ такую, что равенство (1) выводимо в ограниченной арифметике.

Таким образом, для всех правил образования рекурсивных термов наше утверждение доказано. Так как оно верно для исходных рекурсивных термов, то тем самым наше индуктивное доказательство закончено, и мы доказали, что для каждой рекурсивной константы можно определить цифру такую, что равенство данной константы и цифры выводимо в ограниченной арифметике.

Если допустить, что аксиоматическая арифметика непротиворечива, то для любой рекурсивной константы $\mathfrak{c}$ *существует единственная цифра* $\mathfrak{z}$, *для которой равенство* $\mathfrak{c} = \mathfrak{z}$ *выводимо в ограниченной арифметике.*

Действительно, если бы нашлись две различные цифры $\mathfrak{z}_1$ и $\mathfrak{z}_2$ такие, что и $\mathfrak{c} = \mathfrak{z}_1$ и $\mathfrak{c} = \mathfrak{z}_2$ выводимы в ограниченной арифметике, то в ней было бы выводимо также и равенство $\mathfrak{z}_1 = \mathfrak{z}_2$. Однако если $\mathfrak{z}_1$ и $\mathfrak{z}_2$ различны, то это равенство приводит к противоречию в ограниченной арифметике. В самом деле, пусть $\mathfrak{z}_1$ есть $0^{(m)}$, а $\mathfrak{z}_2$ есть $0^{(n)}$ и число штрихов m меньше числа штрихов n. Тогда подстановками в VII. 3 получим

$$0^{(m)} < 0^{(m+1)}, \; 0^{(m+1)} < 0^{(m+2)}, \; \ldots, \; 0^{(n-1)} < 0^{(n)}, \; \ldots,$$

откуда, применив аксиому VII. 2, найдем, что

$$0^{(m)} < 0^{(n)}$$

выводимо из одних только аксиом группы VII.

Следовательно, в ограниченной арифметике выводимо $0^{(m)} < 0^{(n)}$. Пользуясь еще аксиомами равенства, легко выводим

$$\overline{\mathfrak{z}_1 = \mathfrak{z}_2}$$

и, следовательно, получаем противоречие.

Следствие. *Если исчисление, содержащее ограниченную арифметику, непротиворечиво и в нем выводимо равенство*

$$\mathfrak{c}_1 = \mathfrak{c}_2,$$

где $\mathfrak{c}_1$ и $\mathfrak{c}_2$ — рекурсивные константы, то это равенство выводимо в ограниченной арифметике.

В самом деле, по доказанному существует цифра $\mathfrak{z}_1$ такая, что равенство $\mathfrak{c}_1 = \mathfrak{z}_1$ выводимо в ограниченной арифметике. Существует также цифра $\mathfrak{z}_2$ такая, что равенство $\mathfrak{c}_2 = \mathfrak{z}_2$ выводимо в ограниченной арифметике. Так как рассматриваемое исчисление содержит ограниченную арифметику, то последние равенства выводимы и в нем. Поэтому в нем также выводимо равенство $\mathfrak{z}_1 = \mathfrak{z}_2$. Но если исчисление непротиворечиво, то цифры $\mathfrak{z}_1$ и $\mathfrak{z}_2$ должны совпадать, иначе в ограниченной арифметике, а следовательно, и в данном исчислении была бы выводима формула $\overline{\mathfrak{z}_1 = \mathfrak{z}_2}$. Но если $\mathfrak{z}_1$ и $\mathfrak{z}_2$ представляют собой одну и ту же цифру $\mathfrak{z}$, а $\mathfrak{c}_1 = \mathfrak{z}$ и $\mathfrak{c}_2 = \mathfrak{z}$ выводимы в ограниченной арифметике, то и $\mathfrak{c}_1 = \mathfrak{c}_2$ также в ней выводимо. Из сказанного также следует, что в рассматриваемом исчислении для каждой рекурсивной константы $\mathfrak{c}$ существует единственная цифра $\mathfrak{z}$ такая, что равенство $\mathfrak{c} = \mathfrak{z}$ выводимо в этом исчислении.

В дальнейшем мы для любых рекурсивных констант $\mathfrak{c}_1$ и $\mathfrak{c}_2$ выражение «$\mathfrak{c}_1 = \mathfrak{c}_2$ *выводимо в ограниченной арифметике*» будем заменять более кратким: «$\mathfrak{c}_1$ *равно* $\mathfrak{c}_2$». Опускание здесь термина «ограниченная арифметика» имеет то основание, что, как мы видели, в любом непротиворечивом и более сильном исчислении выводимость равенства рекурсивных констант равносильна выводимости этого равенства в ограниченной арифметике.

§ 9. Рекурсивные функции

Рассмотрим произвольный рекурсивный терм $\mathfrak{g}(x_1, \ldots, x_n)$. Мы отнесем некоторым образом каждому выражению $\mathfrak{g}(\mathfrak{z}_1, \ldots, \mathfrak{z}_n)$ определенную цифру $\mathfrak{h}_{\mathfrak{z}_1, \ldots, \mathfrak{z}_n}$. Таким образом, мы определим на области цифр некоторую функцию $\mathfrak{h} = \mathfrak{h}_{\mathfrak{z}_1, \ldots, \mathfrak{z}_n}$, принимающую в качестве значений также цифры. Эта функция, связанная с рекурсивным термом $\mathfrak{g}(x_1, \ldots, x_n)$, представляющим собой некоторый символ, сама имеет содержательный математический смысл, именно, она является функцией, которая каждой системе цифр $\mathfrak{z}_1, \ldots, \mathfrak{z}_n$ ставит в соответствие определенную цифру $\mathfrak{h}_{\mathfrak{z}_1, \ldots, \mathfrak{z}_n}$. Такие функции могут быть рассмотрены в рамках математики таким же образом, как любые другие математические понятия, уже нам знакомые, например выводимая формула, правила получения выводимых формул и те или иные соответствия, которые мы уже раньше рассматривали для символов исчислений.

Определенные таким образом через рекурсивные термы математические функции мы назовем *рекурсивными функциями*. (Точнее, их следовало бы называть *примитивно рекурсивными функциями*, так как термин «рекурсивные функции» обычно используется для более общего понятия.)

Сложение и умножение. Определим рекурсивный терм $\sigma(x, y)$ с помощью рекурсивных равенств:

$$\text{a. } \sigma(x, 0) = x.$$

$$\text{b. } \sigma(x, y') = (\sigma(x, y))'.$$

Этому терму соответствует рекурсивная функция, которая совпадает с обычно арифметической суммой в том смысле, что значение $\sigma(0^{(n)}, 0^{(m)})$ представляет собой $0^{(n+m)}$. Ввиду этого мы выражение $\sigma(x, y)$ будем записывать в более привычном виде, именно как $x + y$. Тогда рекурсивные равенства для сложения будут записаны так:

$$\text{a. } x + 0 = x.$$

$$\text{b. } x + y' = (x + y)'.$$

Введем рекурсивный терм $\pi(x, y)$, написав для него рекурсивные равенства:

$$\text{a. } \pi(x, 0) = 0.$$

$$\text{b. } \pi(x, y') = \pi(x, y) + x.$$

Рекурсивная функция, соответствующая терму $\pi(x, y)$, представляет собой обычное арифметическое произведение. Мы для нее также будем употреблять обычную запись: $x \cdot y$. Тогда рекурсивные равенства, ее определяющие, примут вид:

$$\text{a. } x \cdot 0 = 0.$$

$$\text{b. } x \cdot y' = x \cdot y + x.$$

Рекурсивные функции $\alpha(x)$ *и* $\beta(x)$:

$$\text{a. } \alpha(0) = 0. \qquad \text{a. } \beta(0) = 0'.$$

$$\text{b. } \alpha(x') = 0'. \qquad \text{b. } \beta(x') = 0.$$

Функция $\alpha(\mathfrak{z})$, как видно из определения, равна 0 при $\mathfrak{z} = 0$ и равна $0'$ при всех прочих значениях $\mathfrak{z}$. Функция $\beta(\mathfrak{z})$, наоборот, равна $0'$ при $\mathfrak{z} = 0$ и равна 0 при других значениях $\mathfrak{z}$.

Рекурсивные функции $\delta(x)$ *и* $\delta(x, y)$:

$$\text{a. } \delta(0) = 0.$$

$$\text{b. } \delta(x') = x.$$

Функция $\delta(\mathfrak{z})$, определенная этими формулами, очевидно, ставит 0 в соответствие 0, а каждой цифре, отличной от 0, ставит в соответствие предшествующую ей цифру. Таким образом, функции $\delta(\mathfrak{z})$ содержательно соответствует вычитание единицы из всех цифр, кроме 0.

$$\text{a. } \delta(x, 0) = x.$$

$$\text{b. } \delta(x, y') = \delta(\delta(x, y)).$$

Рассмотрим подробнее рекурсивную функцию, определенную этими равенствами:

$$\delta(x, 0') = \delta(\delta(x, 0)).$$

Следовательно,

$$\delta(x, 0') = \delta(x).$$

Далее,

$$\delta(x,\ 0'') = \delta(\delta(x,\ 0')),$$

т. е.

$$\delta(x,\ 0'') = \delta(\delta(x)).$$

Легко видеть, что вообще

$$\delta\left(x,\ 0^{(k)}\right) = \underbrace{\delta(\delta(\ldots\delta}_{k \text{ раз}}(x))\ldots).$$

Итак, $\delta(\mathfrak{z}_1,\ \mathfrak{z}_2)$ равно цифре, которая получается из $\mathfrak{z}_1$ применением операции δ от одной переменной столько раз, сколько штрихов содержит цифра $\mathfrak{z}_2$. Таким образом, если $\mathfrak{z}_1$ не меньше $\mathfrak{z}_2$, то $\delta(\mathfrak{z}_1,\ \mathfrak{z}_2)$ получится, если удалить из цифры $\mathfrak{z}_1$ столько штрихов, сколько их содержит цифра $\mathfrak{z}_2$. Если же $\mathfrak{z}_1 < \mathfrak{z}_2$, то $\delta(\mathfrak{z}_1,\ \mathfrak{z}_2) = 0$. Иначе говоря,

$$\delta\left(0^{(k_1)},\ 0^{(k_2)}\right) = 0^{(k_1 - k_2)},$$

если $k_2 \leqslant k_1$, и

$$\delta\left(0^{(k_1)},\ 0^{(k_2)}\right) = 0$$

в противном случае.

§ 10. Аксиоматическая и содержательная выводимость свойств арифметических функций

Как мы уже указывали выше, понятие рекурсивной функции, связанное с рекурсивным термом, является содержательным понятием. В частности, рекурсивным термам

$$x + y \quad \text{и} \quad x \cdot y$$

соответствуют рекурсивные функции, по существу являющиеся просто обычными арифметической суммой и арифметическим произведением. Точнее говоря, при каждой замене переменных x и y в терме $x + y$ цифрами $0^{(i)}$ и $0^{(j)}$ значение соответствующей рекурсивной функции представляет собой цифру $0^{(i+j)}$, где через $i + j$ здесь обозначена обыкновенная, содержательно понимаемая, арифметическая сумма чисел штрихов первой и второй цифр, а значение рекурсивной функции, отвечающей терму $x \cdot y$ при замене x цифрой $0^{(i)}$, а y цифрой $0^{(j)}$, является цифрой $0^{(i \cdot j)}$, где $i \cdot j$ представляет собой содержательно понимаемое арифметическое произведение чисел штрихов цифр $0^{(i)}$ и $0^{(j)}$. Содержательными рассуждениями можно вывести все арифметические свойства рекурсивных функций, отвечающих термам

$$x+y \quad \text{и} \quad x\cdot y.$$

Для этого надо просто повторить обычные рассуждения, употребляемые для этой цели в арифметике. Однако следует заметить, что *такие доказательства являются не формальными выводами в самой ограниченной арифметике, а содержательными рассуждениями об ограниченной арифметике.*

Рассмотрим для примера предложение: «Значение рекурсивной функции, соответствующей терму $x\cdot y$, есть 0, если переменная x или переменная y заменена цифрой 0».

Мы докажем это предложение по индукции, но не путем применения аксиомы полной индукции, записанной в виде формулы исчисления предикатов, которой в ограниченной арифметике нет, а посредством содержательной металогической индукции, проводимой над ограниченной арифметикой. Такая индукция является приемом рассуждения, входящим в круг финитизма. Таково, например, доказательство теоремы в § 8.

То, что при замене в терме $x\cdot y$ переменной y на 0 произведение $x\cdot y$ принимает также значение 0, следует прямо из определения рекурсивной функции $x\cdot y$ посредством рекурсивных равенств. Докажем, что при замене переменной x цифрой 0 рекурсивная функция также принимает значение 0. Это утверждение справедливо, если y также принимает значение 0. Допустим, что оно справедливо, если *y принимает значение* $\mathfrak{z}$, и покажем, что тогда оно справедливо и при замене y цифрой $\mathfrak{z}'$. В самом деле, по предположению $0\cdot\mathfrak{z}$ имеет значение 0. Но $0\cdot\mathfrak{z}'$, по определению, имеет то же значение, что и $0\cdot\mathfrak{z}+0$. Но $0\cdot\mathfrak{z}+0$ имеет, по определению суммы, то же значение, что и $0\cdot\mathfrak{z}$, т. е. 0.

Таким образом, мы доказали, что значение $0\cdot\mathfrak{z}$ равно 0 для всякой цифры $\mathfrak{z}$. Аналогичным образом можно доказать все элементарные теоремы арифметики. Но, повторяем, все эти теоремы не доказываются средствами ограниченной арифметики, а являются теоремами об ограниченной арифметике.

Однако в аксиоматической арифметике с аксиомой полной индукции можно доказывать уже внутренними средствами теоремы, соответствующие указанным содержательным теоремам об арифметике. Так, например, можно доказать средствами аксиоматической арифметики теорему

$$\vdash 0 \cdot y = 0 \,\&\, x \cdot 0 = 0,$$

соответствующую только что рассмотренной содержательной теореме об ограниченной арифметике. Приведем это доказательство.

Чтобы доказать выводимость в арифметике формулы

$$\vdash 0 \cdot y = 0 \,\&\, x \cdot 0 = 0,$$

достаточно вывести

$$\vdash 0 \cdot y = 0$$

и

$$\vdash x \cdot 0 = 0.$$

Вторая из этих формул представляет собой первое рекурсивное равенство, связанное с термом $x \cdot y$, и поэтому выводима в арифметике.

Докажем выводимость первой формулы. Сделав подстановку в аксиому полной индукции формулы $0 \cdot t = 0$ вместо $A(t)$, получим

$$\vdash 0 \cdot 0 = 0 \,\&\, \forall x\, (0 \cdot x = 0 \rightarrow 0 \cdot x' = 0) \rightarrow 0 \cdot y = 0. \qquad (1)$$

Из первого рекурсивного равенства для терма $x \cdot y$ вытекает

$$\vdash 0 \cdot 0 = 0. \qquad (2)$$

Затем имеет место

$$\vdash 0 \cdot x = 0 \rightarrow 0 \cdot x = 0,$$

$$\vdash 0 \cdot x' = 0 \cdot x + 0,$$

$$\vdash 0 \cdot x + 0 = 0 \cdot x.$$

Заменив в правой части первой из этих формул терм $0 \cdot x$ равным термом $0 \cdot x + 0$ и приняв во внимание второе равенство, получим

$$\vdash 0 \cdot x = 0 \rightarrow 0 \cdot x' = 0.$$

Применив правило связывания квантором, находим

$$\vdash \forall x\,(0 \cdot x = 0 \to 0 \cdot x' = 0). \qquad (3)$$

Из выводимости формул (1), (2) и (3) вытекает, что

$$\vdash 0 \cdot y = 0,$$

и, таким образом, доказано, что

$$\vdash x \cdot 0 = 0 \,\&\, 0 \cdot y = 0.$$

Отметим разницу между металогическими теоремами об ограниченной арифметике, в которых устанавливаются свойства рекурсивных функций, и соответствующими теоремами самой арифметики с аксиомой полной индукции. Содержание каждой металогической теоремы указанного типа состоит в том, что некоторая формула

$$\mathfrak{A}\,(x_1, \ldots, x_n)$$

превращается в выводимую в ограниченной арифметике формулу при любой замене переменных $x_1, \ldots, x_n$ цифрами. Содержание соответствующей теоремы аксиоматической арифметики состоит в том, что формула $\mathfrak{A}\,(x_1, \ldots, x_n)$ выводима в арифметике с аксиомой полной индукции.

Может на первый взгляд показаться, что эти предложения всегда равносильны. Однако это не так. Формальная теорема аксиоматической арифметики

$$\vdash \mathfrak{A}\,(x_1, \ldots, x_n)$$

является иногда более сильным утверждением, чем утверждение о том, что каждая формула вида

$$\mathfrak{A}\,(\mathfrak{z}_1, \ldots, \mathfrak{z}_n),$$

где $\mathfrak{z}_1, \ldots, \mathfrak{z}_n$ — произвольные цифры, выводима в ограниченной арифметике. Это имеет место, например, в случае, когда формула $\mathfrak{A}\,(x_1, \ldots, x_n)$ имеет вид

$$\mathfrak{r} = 0, \ \ \mathfrak{r}_1 = \mathfrak{r}_2 \quad \text{или} \quad \mathfrak{r}_1 < \mathfrak{r}_2, \qquad (4)$$

где $\mathfrak{r}$, $\mathfrak{r}_1$ и $\mathfrak{r}_2$ — произвольные рекурсивные термы. Из формальной выводимости в арифметике какой-нибудь из формул (4) вытекает выводимость в ограниченной арифметике соответствующей формулы:

$$\mathfrak{r}^0 = 0, \ \ \mathfrak{r}_1^0 = \mathfrak{r}_2^0 \quad \text{или} \quad \mathfrak{r}_1^0 < \mathfrak{r}_2^0,$$

полученной из соответствующей формулы (4) заменой всех переменных цифрами. Действительно, если формула $\mathfrak{r}_1 = \mathfrak{r}_2$ (соответственно $\mathfrak{r}_1 < \mathfrak{r}_2$, $\mathfrak{r} = 0$) формально выводима в арифметике, то каждая из формул $\mathfrak{r}_1^0 = \mathfrak{r}_2^0$ (соответственно $\mathfrak{r}_1^0 < \mathfrak{r}_2^0$, $\mathfrak{r}^0 = 0$), полученная из предыдущей заменой всех переменных цифрами, также формально выводима в арифметике. Но мы знаем, что для каждой рекурсивной константы можно найти цифру, которая равна этой константе в том смысле, что это равенство выводимо в ограниченной арифметике. Отсюда следует, что из двух формул

$$\mathfrak{r}_1^0 = \mathfrak{r}_2^0 \quad \text{и} \quad \overline{\mathfrak{r}_1^0 = \mathfrak{r}_2^0}$$

одна всегда выводима в ограниченной арифметике. Точно так же одна из формул

$$\mathfrak{r}_1^0 < \mathfrak{r}_0^2 \quad \text{и} \quad \overline{\mathfrak{r}_1^0 < \mathfrak{r}_2^0}$$

выводима в ограниченной арифметике.

Если же формула $\mathfrak{r}_1^0 = \mathfrak{r}_2^0$ выводима в арифметике и если арифметика непротиворечива, то тогда $\mathfrak{r}_1^0 = \mathfrak{r}_2^0$ должно быть выводимо и в ограниченной арифметике. То же самое можно сказать и о формулах $\mathfrak{r}_0^1 < \mathfrak{r}_2^0$ и $\mathfrak{r}^0 = 0$. Итак, если формула $\mathfrak{A}(x_1, \ldots, x_n)$ указанного типа выводима в арифметике, то каждая из формул

$$\mathfrak{A}(\mathfrak{z}_1, \ldots, \mathfrak{z}_n)$$

выводима в ограниченной арифметике.

Обратное положение, однако, неверно. Можно доказать, что существуют формулы вида

$$\mathfrak{r} = 0,$$

где $\mathfrak{r}$ — некоторый рекурсивный терм, такие, что каждая из формул вида

$$\mathfrak{r}^0 = 0,$$

полученная заменой в формуле $\mathfrak{r} = 0$ всех переменных цифрами, выводима в ограниченной арифметике, но в то же время формула

$$\mathfrak{r} = 0$$

не выводима в арифметике, несмотря на наличие в ней аксиомы полной индукции.

В дальнейшем мы часто будем пользоваться арифметическими свойствами рекурсивных функций в неформальном, металогическом смысле. Доказывать, однако, эти свойства мы не будем, так как эти доказательства были бы простым повторением соответствующих рассуждений в обычной арифметике.

§ 11. Рекурсивные предикаты

Термин «индивидуальный предикат» мы до сих пор употребляли только для элементарных выражений $P(x)$, $Q(x, y)$, $x = y, \ldots$ Расширим теперь его смысл и будем называть индивидуальным предикатом каждую формулу арифметики, которая содержит предметные переменные и не содержит переменных предикатов. *Индивидуальные предикаты, не представляющие собой элементарной формулы, мы будем называть сложными индивидуальными предикатами.* Мы будем говорить, что *два предиката $P(x_1, \ldots)$ и $Q(x_1, \ldots)$ эквивалентны, если формула, полученная из формулы*

$$P(x_1, \ldots) \sim Q(x_1, \ldots)$$

заменой свободных переменных любыми цифрами, выводима в ограниченной арифметике.

Предикаты вида

$$\mathfrak{g}(x_1, \ldots, x_n) = 0,$$

где $\mathfrak{g}$ — рекурсивный терм, и все им эквивалентные называются рекурсивными предикатами, соответствующими терму $\mathfrak{g}$.

Теорема 1. *Если все свободные переменные рекурсивного предиката $P(x_1, \ldots, x_n)$ заменить цифрами $\mathfrak{z}_1, \ldots, \mathfrak{z}_n$, то или $P(\mathfrak{z}_1, \ldots, \mathfrak{z}_n)$, или $\bar{P}(\mathfrak{z}_1, \ldots, \mathfrak{z}_n)$ выводимо в ограниченной арифметике.*

В самом деле, по условию существует рекурсивный терм $\mathfrak{p}(x_1, \ldots, x_n)$ такой, что

$$P(\mathfrak{z}_1, \ldots, \mathfrak{z}_n) \sim \mathfrak{p}(\mathfrak{z}_1, \ldots, \mathfrak{z}_n) = 0$$

выводимо в ограниченной арифметике. Но мы уже знаем, что можно определить такую цифру $\mathfrak{z}^*$, что равенство

$$\mathfrak{p}(\mathfrak{z}_1, \ldots, \mathfrak{z}_n) = \mathfrak{z}^*$$

выводимо в ограниченной арифметике. $\mathfrak{z}^* = 0$ или $\overline{\mathfrak{z}^*=0}$ также выводимо в ограниченной арифметике. Следовательно, $P(\mathfrak{z}_1, \ldots, \mathfrak{z}_n)$ или $\overline{P}(\mathfrak{z}_1, \ldots, \mathfrak{z}_n)$ выводимо в ограниченной арифметике, что и требовалось доказать.

Теорема 2. *Если два предиката $P(x, y, \ldots)$ и $Q(x, y, \ldots)$ рекурсивны, то предикаты $P(x, y, \ldots) \vee Q(x, y, \ldots)$ и $\overline{P}(x, y, \ldots)$ также рекурсивны.*

Если $P(x, y, \ldots)$ и $Q(x, y, \ldots)$ рекурсивны, то существуют рекурсивные термы $\mathfrak{p}$ и $\mathfrak{q}$ такие, что P эквивалентно $\mathfrak{p} = 0$, а Q эквивалентно $\mathfrak{q} = 0$. Рассмотрим терм $\mathfrak{p} \cdot \mathfrak{q}$. Это также рекурсивный терм. Покажем, что предикат $\mathfrak{p} = 0 \vee \mathfrak{q} = 0$ эквивалентен предикату $\mathfrak{p} \cdot \mathfrak{q} = 0$. В самом деле, ввиду того, что рекурсивная функция, соответствующая терму $\mathfrak{p} \cdot \mathfrak{q}$, имеет все свойства обычного арифметического произведения, мы можем заключить, что если $\mathfrak{p}$ или $\mathfrak{q}$ принимает значение 0, то и $\mathfrak{p} \cdot \mathfrak{q}$ также обращается в 0, и обратно, если $\mathfrak{p} \cdot \mathfrak{q}$ принимает значение 0, то или $\mathfrak{p}$, или $\mathfrak{q}$ принимает значение 0. В таком случае формула

$$\mathfrak{p} = 0 \vee \mathfrak{q} = 0 \sim \mathfrak{p} \cdot \mathfrak{q} = 0$$

при каждой замене цифрами выводима из аксиом ограниченной арифметики и, следовательно, предикаты

$$\mathfrak{p} = 0 \vee \mathfrak{q} = 0 \quad \text{и} \quad \mathfrak{p} \cdot \mathfrak{q} = 0$$

эквивалентны.

Очевидно, что $\mathfrak{p} = 0 \vee \mathfrak{q} = 0$ эквивалентно $P \vee Q$. Отсюда следует, что последний предикат эквивалентен $\mathfrak{p} \cdot \mathfrak{q} = 0$ и, следовательно, представляет собой рекурсивный предикат.

Для доказательства рекурсивности предиката $\overline{P}(x_1, \ldots)$ рассмотрим терм $\beta(\mathfrak{p})$, где β — введенный выше (см. § 9) рекурсивный терм. Из свойств этого терма вытекает, что $\beta(\mathfrak{p}) = 0$, если $\mathfrak{p}$ после замены свободных переменных цифрами не равен 0, и $\overline{\beta(\mathfrak{p}) = 0}$, если $\mathfrak{p} = 0$. Но в таком случае $\beta(\mathfrak{p}) = 0$ эквивалентно предикату $\overline{P}(x_1, \ldots)$, и, следовательно, этот предикат рекурсивен, что и требовалось доказать.

Пользуясь тем, что операции исчисления высказываний & и $\rightarrow$ выражаются через операции $\vee$ и —, легко показать, что *если предикаты P и Q рекурсивны, то рекурсивны и предикаты $P \& Q$ и $P \rightarrow Q$.*

Очевидно, что если предикат $P(x_1, \ldots, x_n)$ рекурсивен, то предикат $P(\mathfrak{g}_1, \ldots, \mathfrak{g}_n)$, полученный из него заменой переменных x_i произвольными рекурсивными термами $\mathfrak{g}_i$, также рекурсивен.

Рекурсивность элементарных предикатов арифметики. Докажем, что *предикаты* $x = y$ *и* $x < y$ *рекурсивны.* Именно, мы докажем, что предикат $x = y$ эквивалентен предикату

$$\delta(x, y) + \delta(y, x) = 0. \tag{1}$$

Подставим вместо x и y произвольные цифры $0^{(n)}$ и $0^{(m)}$. Если $n = m$, то $\delta(0^{(n)}, 0^{(m)}) = 0$ и $\delta(0^{(m)}, 0^{(n)}) = 0$, и предикаты $x = y$ и (1) оба истинны. Если же цифры не равны, то одно из слагаемых (1) равно 0, а другое нет. В таком случае и сумма отлична от 0. Следовательно, предикаты $x = y$ и (1) эквивалентны.

Так же можно показать, что предикат $x < y$ эквивалентен предикату

$$\overline{\delta(y, x) = 0}.$$

Но $\delta(y, x) = 0$ — рекурсивный предикат. Отрицание рекурсивного предиката — также рекурсивный предикат. Следовательно, и $x < y$ — рекурсивный предикат.

Исходя из элементарных предикатов, можно с помощью операций исчисления высказываний и подстановки образовать новые рекурсивные предикаты, соответствующие переменным рекурсивным термам.

§ 12. Другие способы образования рекурсивных предикатов. Ограниченные кванторы

Пусть $P(x)$ — некоторый рекурсивный предикат. Тогда, по определению, существует такой рекурсивный терм $\mathfrak{p}(x)$, что для каждой цифры $\mathfrak{z}$ формула

$$P(\mathfrak{z}) \sim \mathfrak{p}(\mathfrak{z}) = 0$$

выводима в ограниченной арифметике.

Введем в связи с предикатом $P(x)$ рекурсивный терм $\mathfrak{v}(x)$ с рекурсивными равенствами

$$\mathfrak{v}(0) = \mathfrak{p}(0),$$
$$\mathfrak{v}(x') = \mathfrak{v}(x) \cdot \mathfrak{p}(x').$$

Этот рекурсивный терм $\mathfrak{v}(h)$ мы еще выразим условно в виде

$$\bigcap_{x \leqslant h} \mathfrak{p}(x).$$

Такое изображение удобно потому, что (как легко доказать по индукции) $\mathfrak{v}(\mathfrak{z})$ равно арифметическому произведению

$$\mathfrak{p}(0) \cdot \mathfrak{p}(0') \ldots \mathfrak{p}(\mathfrak{z}).$$

Терму $\bigcap\limits_{x \leqslant h} \mathfrak{p}(x)$ соответствует рекурсивный предикат

$$\bigcap_{x \leqslant h} \mathfrak{p}(x) = 0,$$

который мы обозначим символом

$$\underset{\leqslant h}{\exists x}\, P(x).$$

Для каждой цифры $\mathfrak{z}$ предикат $\underset{\leqslant \mathfrak{z}}{\exists x}\, P(x)$ эквивалентен формуле

$$\mathfrak{p}(0) \cdot \mathfrak{p}(0') \ldots \mathfrak{p}(\mathfrak{z}) = 0$$

и, следовательно, формуле

$$P(0) \vee P(0') \vee \ldots \vee P(\mathfrak{z}).$$

Символ

$$\underset{\leqslant h}{\exists x}$$

мы назовем ограниченным квантором существования.

Введем также символ *ограниченного квантора всеобщности*

$$\underset{\leqslant h}{\forall x}.$$

Выражение

$$\underset{\leqslant h}{\forall x}\, P(x)$$

определим как эквивалентное выражению

$$\overline{\underset{\leqslant h}{\exists x}\, \overline{P(x)}}.$$

Предикат, представленный этим выражением, также является рекурсивным предикатом.

При этом формула

$$\underset{\leqslant \mathfrak{z}}{\forall x}\, P(x),$$

очевидно, эквивалентна формуле

$$P(0) \,\&\, P(0') \,\&\, \ldots \,\&\, P(\mathfrak{z}).$$

§ 13. Приемы образования новых рекурсивных термов

Мы введем некоторые вспомогательные приемы, позволяющие образовать рекурсивные термы, исходя из рекурсивных предикатов. Пусть $P(x)$ — любой рекурсивный предикат, содержащий переменную x (и, может быть, другие), и пусть $\mathfrak{p}(x)$ — соответствующий ему рекурсивный терм. Определим новый рекурсивный терм

$$\underset{0<x\leqslant h}{\mu x} \mid P(x),$$

который содержательно можно было бы трактовать как *минимальное из значений переменной x таких, что $P(x)$ истинно и $0 < x \leqslant h$*. Этот терм иначе можно записать в виде $\mathfrak{g}(x_1, \ldots, x_k, h)$, где $x_1, \ldots, x_k$ — отличные от x свободные переменные, входящие в $P(x)$. Напишем для терма $\underset{0<x\leqslant h}{\mu x} \mid P(x)$ определяющие равенства в обычной форме:

a. $\underset{0<x\leqslant 0}{\mu x} \mid P(x) = 0.$

b. $\underset{0<x\leqslant h'}{\mu x} \mid P(x) = \underset{0<x\leqslant h}{\mu x} \mid P(x) + h'\beta(\underset{0<x\leqslant h}{\mu x} \mid P(x) + \mathfrak{p}(h')).$

Очевидно, не существует никакого числа x, удовлетворяющего неравенству $0 < x \leqslant 0$. Запись $\underset{0<x\leqslant 0}{\mu x} \mid P(x)$, однако, имеет смысл и является обозначением введенного нами терма $\underset{0<x\leqslant \mathfrak{z}}{\mu x} \mid P(x)$ при $\mathfrak{z} = 0$. Покажем, что для каждой отличной от 0 цифры $\mathfrak{z}$ имеем

$$\underset{0<x\leqslant \mathfrak{z}}{\mu x} \mid P(x) = \mathfrak{h},$$

где $\mathfrak{h}$ — наименьшая цифра, отличная от 0 и не превышающая $\mathfrak{z}$, для которой $P(\mathfrak{h})$ истинно, и 0, если такой цифры не существует. Наше утверждение очевидно, если $\mathfrak{z} = 0$, так как цифр, отличных от 0 и не превышающих 0, не существует. Допустим, что наше утверждение справедливо для $\mathfrak{z} = 0^{(k)}$, и покажем, что в таком случае оно справедливо и для цифры $0^{(k+1)}$. На основании b имеем

$$\underset{0<x\leqslant 0^{(k+1)}}{\mu x} \mid P(x) =$$

$$= \underset{0<x\leqslant 0^{(k)}}{\mu x} \mid P(x) + 0^{(k+1)}\beta\left(\underset{0<x\leqslant 0^{(k)}}{\mu x} \mid P(x) + \mathfrak{p}\left(0^{(k+1)}\right)\right).$$

Допустим, что существует цифра $0^{(j)}$, отличная от 0 и не превышающая $0^{(k)}$ $(j \leqslant k)$, для которой $P(0^{(j)})$ истинно. Тогда среди таких цифр найдется наименьшая; пусть это будет $0^{(j)}$. Тогда

$$\underset{0<x\leqslant \mathfrak{z}}{\mu x} \mid P(x) = 0^{(j)}$$

и

$$\underset{0<x\leqslant 0^{(k+1)}}{\mu x} \mid P(x) = 0^{(j)} + 0^{(k+1)} \cdot \beta\left(0^{(j)} + \mathfrak{p}\left(0^{(k+1)}\right)\right).$$

Но $0^{(j)} + \mathfrak{p}\left(0^{(k+1)}\right)$ больше 0, поэтому

$$\beta\left(0^{(j)} + \mathfrak{p}\left(0^{(k+1)}\right)\right) = 0$$

и, следовательно,

$$\underset{0<x\leqslant 0^{(k+1)}}{\mu x} \mid P(x) = 0^{(j)},$$

и для этого случая наше утверждение доказано.

Допустим теперь, что среди цифр $0', 0'', \ldots, 0^{(k)}$ нет такой, для которой $P(x)$ истинно. Тогда, по условию,

$$\underset{0<x\leqslant 0^{(k)}}{\mu x} \mid P(x) = 0$$

и, следовательно,

$$\underset{0<x\leqslant 0^{(k+1)}}{\mu x} \mid P(x) = 0^{(k+1)}\beta\left(\mathfrak{p}\left(0^{(k+1)}\right)\right).$$

Если $P\left(0^{(k+1)}\right)$ истинно, то $\mathfrak{p}\left(0^{(k+1)}\right) = 0$ и $\beta(0) = 0'$. Тогда

$$\underset{0<x\leqslant 0^{(k+1)}}{\mu x} \mid P(x) = 0^{(k+1)} \cdot 0' = 0^{(k+1)},$$

что согласуется с нашим утверждением.

Если $P\left(0^{(k+1)}\right)$ ложно, то

$$\overline{\mathfrak{p}\left(0^{(k+1)}\right)=0}$$

истинно. В таком случае

$$\beta\left(\mathfrak{p}\left(0^{(k+1)}\right)\right)=0$$

и

$$\underset{0<x\leqslant 0^{(k+1)}}{\mu x} \mid P(x)=0.$$

И в этом случае наше утверждение справедливо.

Аналогично определяется функция

$$\underset{0<x\leqslant h}{\mathrm{M}x} \mid P(x),$$

где $P(x)$ — любой рекурсивный предикат:

a. $$\underset{0<x\leqslant 0}{\mathrm{M}x} \mid P(x)=0,$$

b. $$\underset{0<x\leqslant h'}{\mathrm{M}x} \mid P(x)=\underset{0<x\leqslant h}{\mathrm{M}x} \mid P(x)\cdot\alpha(\mathfrak{p}(h'))+h'\beta(\mathfrak{p}(h')),$$

где $\mathfrak{p}(x)$ — рекурсивный терм, соответствующий предикату $P(x)$. Покажем, что $\underset{0<x\leqslant \mathfrak{z}}{\mathrm{M}x} \mid P(x)$ *есть наибольшая из тех цифр* $\mathfrak{z}=0', 0'', \ldots, 0^{(k)}$, *для которых* $P(x)$ *истинно, и* $\underset{0<x\leqslant \mathfrak{z}}{\mathrm{M}x} \mid P(x)=0$, *если такой цифры не существует*.

Наше утверждение, очевидно, справедливо для $\mathfrak{z}=0$. Допустим, что оно справедливо для цифры $0^{(k)}$. Покажем, что тогда оно справедливо и для $0^{(k+1)}$. Пусть сначала среди цифр $0', \ldots, 0^{(k)}$ есть цифры, для которых $P(x)$ истинно, и $0^{(l)}$ — наибольшая из этих цифр. В таком случае

$$\underset{0<x\leqslant 0^{(k)}}{\mathrm{M}x} \mid P(x)=0^{(l)}$$

и

$$\underset{0<x\leqslant 0^{(k+1)}}{\mathrm{M}x} \mid P(x)=0^{(l)}\cdot\alpha\left(\mathfrak{p}\left(0^{(k+1)}\right)\right)+0^{(k+1)}\cdot\beta\left(\mathfrak{p}\left(0^{(k+1)}\right)\right).$$

Если $P\left(0^{(k+1)}\right)$ истинно, то

$$\mathfrak{p}\left(0^{(k+1)}\right)=0,$$

$$\alpha\left(\mathfrak{p}\left(0^{(k+1)}\right)\right)=0$$

и

$$\beta\left(\mathfrak{p}\left(0^{(k+1)}\right)\right)=0'.$$

Тогда

$$\underset{0<x\leqslant 0^{(k+1)}}{\mathrm{M}x} \mid P(x)=0^{(k+1)}.$$

Если же $P\left(0^{(k+1)}\right)$ ложно, то, наоборот,

$$\alpha\left(\mathfrak{p}\left(0^{(k+1)}\right)\right)=0',$$

$$\beta\left(\mathfrak{p}\left(0^{(k+1)}\right)\right)=0$$

и

$$\underset{0<x\leqslant 0^{(k+1)}}{\mathrm{M}x} \mid P(x)=0^{(l)}.$$

В обоих случаях наше утверждение справедливо.

Допустим теперь, что среди цифр $0', \ldots, 0^{(k)}$ нет цифры, для которой $P(x)$ истинно. В таком случае, по предположению,

$$\underset{0<x\leqslant 0^{(k)}}{\mathrm{M}x} \mid P(x)=0$$

и

$$\underset{0<x\leqslant 0^{(k+1)}}{\mathrm{M}x} \mid P(x)=0^{(k+1)}\cdot\beta\left(\mathfrak{p}\left(0^{(k+1)}\right)\right).$$

Если $P\left(0^{(k+1)}\right)$ истинно, то

$$\mathfrak{p}\left(0^{(k+1)}\right)=0$$

и

$$\beta\left(\mathfrak{p}\left(0^{(k+1)}\right)\right)=0'.$$

Тогда

$$\underset{0<x\leqslant 0^{(k+1)}}{\mathrm{M}x} \mid P(x)=0^{(k+1)}.$$

Если же $P\left(0^{(k+1)}\right)$ ложно, то

$$\beta\left(\mathfrak{p}\left(0^{(k+1)}\right)\right)=0$$

и

$$\underset{0<x\leqslant 0^{(k+1)}}{\mathrm{M}x} \mid P(x)=0.$$

Итак, наше утверждение доказано для всех случаев. Следовательно, оно справедливо для всех цифр.

§ 14. Некоторые теоретико-числовые предикаты и термы

1. *Предикат делимости* $D(x, y)$. Через $D(x, y)$ мы обозначим предикат, выражаемый формулой

$$\underset{\leqslant y}{\exists t}\,[t \cdot x = y].$$

Легко видеть, что если $D(\mathfrak{z}_1, \mathfrak{z}_2)$ истинно, то существует цифра $\mathfrak{h}$ такая, что

$$\mathfrak{h} \cdot \mathfrak{z}_1 = \mathfrak{z}_2,$$

т. е. $\mathfrak{z}_2$ *делится на* $\mathfrak{z}_1$. В самом деле, допустим, что $\mathfrak{z}_1 = 0^{(k_1)}$, а $\mathfrak{z}_2 = 0^{(k_2)}$. Формула

$$\underset{\leqslant \mathfrak{z}_2}{\exists t}\,[t\mathfrak{z}_1 = \mathfrak{z}_2]$$

эквивалентна формуле

$$0 \cdot \mathfrak{z}_1 = \mathfrak{z}_2 \vee 0' \cdot \mathfrak{z}_1 = \mathfrak{z}_2 \vee \ \ldots \ \vee \mathfrak{z}_2 \cdot \mathfrak{z}_1 = \mathfrak{z}_2.$$

По предположению эта формула истинна. Так как сумма истинна, то по крайней мере одно из входящих в нее равенств должно быть истинным, т. е. найдется цифра $\mathfrak{h}$ такая, что

$$\mathfrak{h} \cdot \mathfrak{z}_1 = \mathfrak{z}_2.$$

Допустим теперь, что $D(\mathfrak{z}_1, \mathfrak{z}_2)$ ложно. Тогда истинна формула

$$\underset{\leqslant \mathfrak{z}_2}{\forall t}\,\overline{[t \cdot \mathfrak{z}_1 = \mathfrak{z}_2]}$$

или, что то же, формула

$$\overline{0 \cdot \mathfrak{z}_1 = \mathfrak{z}_2} \,\&\, \overline{0' \cdot \mathfrak{z}_1 = \mathfrak{z}_2} \,\&\, \ldots \,\&\, \overline{\mathfrak{z}_2 \cdot \mathfrak{z}_1 = \mathfrak{z}_2}.$$

Тогда среди цифр $0, 0', \ldots, \mathfrak{z}_2$ не найдется такой цифры $\mathfrak{h}$, что $\mathfrak{h} \cdot \mathfrak{z}_1 = \mathfrak{z}_2$ — истинная формула. Но в таком случае и вообще нет цифры, удовлетворяющей этому равенству. В самом деле, в случае, когда $\mathfrak{z}_1 = 0$ и $\mathfrak{z}_2 = 0$, ясно, что не существует цифры $\mathfrak{h}$, для которой $\mathfrak{h} \cdot \mathfrak{z}_1 = \mathfrak{z}_2$. Если $\mathfrak{z}_1$ не 0, то $\mathfrak{z}_2 < \mathfrak{h}\mathfrak{z}_1$, если $\mathfrak{h}$ больше, чем $\mathfrak{z}_2$.

2. *Предикат «быть простым числом»* — $P(x)$. Обозначим через $P(x)$ предикат, выражаемый формулой

$$\underset{\leqslant x}{\forall t}\,[0' < x \,\&\, (0' < t < x \to \overline{D(t,\ x)})] \;{}^{*)}.$$

Из написанной формулы видно, что $P(x)$ — рекурсивный предикат. Легко установить (аналогично тому, как в примере 1), что для тех и только для тех цифр $\mathfrak{z}$, для которых $P(\mathfrak{z})$ — истинная формула, не существует цифры, отличной от $0'$ и от $\mathfrak{z}$, на которую $\mathfrak{z}$ делится; $\mathfrak{z}$ при этом больше $0'$.

Функция $h!$. Эта функция определяется следующими равенствами:

a. $0! = 0'$.

b. $h'! = h! \cdot h'$.

Легко установить, что для каждой цифры $\mathfrak{z}$ имеет место

$$\mathfrak{z}! = 0' \cdot 0'' \ldots \mathfrak{z}.$$

Ниже нам потребуется утверждение, что *«для всякой цифры* $\mathfrak{z}$, *отличной от* 0, *среди цифр* $\mathfrak{z}, \mathfrak{z}', \ldots, \mathfrak{z}! + 0'$ *существует такая цифра* $\mathfrak{r}$, *что* $P(\mathfrak{r})$ *истинно в ограниченной арифметике»*. Чтобы доказать этот факт, известный под названием «теорема Евклида», достаточно повторить обычное доказательство Евклида. Это доказательство не использует понятие актуальной бесконечности, так как рассуждения здесь относятся к конечной области цифр до $\mathfrak{z}! + 0'$. Кроме того, все используемые понятия представляются рекурсивными предикатами, которые конструктивно вычислимы для цифр.

3. *Рекурсивный предикат* $S(x, y, z)$, *имеющий смысл «x — простое число, заключенное между y' и z»*. Этот предикат определяется формулой

$$P(x) \,\&\, y < x \leqslant z.$$

---

*) $0' < t < x$ — сокращенная запись предиката $0' < t \,\&\, t < x$.

Из этой формулы следует, что $S(x, y, z)$ — рекурсивный предикат. Определим теперь рекурсивный терм $\varphi(x, y)$ следующей формулой

$$\varphi(x, y) = \underset{0<t\leqslant y}{\mu t} \mid S(t, x, y).$$

Рекурсивная функция, определенная этим термом, представляет собой наименьшее простое число, заключенное между числами x' и y, если оно существует, и 0 в противном случае.

4. *Рекурсивная функция* $\pi(x)$, *значения которой пробегают последовательно все простые числа.* Определим рекурсивный терм $\pi(x)$ следующими равенствами:

a. $\pi(0) = 0''$.

b. $\pi(x') = \varphi(\pi(x), \pi(x)! + 0')$.

Покажем, что значения рекурсивной функции $\pi(\mathfrak{z})$ пробегают последовательно все простые числа. В силу a значение $\pi(\mathfrak{z})$ для $\mathfrak{z} = 0$ равно наименьшему простому числу. Допустим, что $\pi(0)$, $\pi(0')$, ..., $\pi(\mathfrak{z})$ представляют собой последовательный (без пропусков) ряд простых чисел. Но

$$\pi(\mathfrak{z}') = \varphi(\pi(\mathfrak{z}), \pi(\mathfrak{z})! + 0'),$$

т. е. значение $\pi(\mathfrak{z}')$ есть наименьшее простое число, заключенное между $\pi(\mathfrak{z})$ и $\pi(\mathfrak{z})! + 0'$, или 0, если такого числа нет. Но, по теореме Евклида, такое число существует, следовательно, значение $\pi(\mathfrak{z}')$ есть непосредственно следующее за $\pi(\mathfrak{z})$ простое число. Итак, $\pi(\mathfrak{z})$ представляет собой искомую рекурсивную функцию.

5. *Предикат «быть показателем степени простого делителя числа y в разложении этого числа на простые множители»* — $R(x, y)$. Этот предикат выражается формулой

$$\underset{\leqslant y}{\exists t}\left[P(t)\,\&\,D(t^x, y)\,\&\,\overline{D(t^{x'}, y)}\right].$$

Из формулы видно, что предикат $R(x, y)$ рекурсивен.

6. *Предикат* $W(x)$ — *«быть числом вида*

$$\mathfrak{h}_1^{h_1} \cdot \mathfrak{h}_2^{h_2} \ldots \mathfrak{h}_k^{h_k}\text{»}, \qquad (1)$$

где $\mathfrak{h}$ представляет собой i-е по порядку простое число; h_i — степень этого простого множителя в произведении

(1) (в частности, h_i может быть равно 0), k — фиксированное число.

Этот предикат определяется формулой

$$\underset{\leqslant x}{\exists u_1} \ldots \underset{\leqslant x}{\exists u_k} \left[\mathfrak{h}_1^{u_1} \cdot \mathfrak{h}_2^{u_2} \ldots \mathfrak{h}_k^{u_k} = x \right].$$

Это, очевидно, рекурсивный предикат.

7. *Рекурсивная функция* $\sigma(x)$, *пробегающая все числа вида*

$$\mathfrak{h}_1^{u_1} \cdot \mathfrak{h}_2^{u_2} \ldots \mathfrak{h}_k^{u_k}$$

при фиксированном k. Построение этой функции аналогично построению функции, пробегающей все простые числа. Построим сначала рекурсивный предикат $M(x, y, z)$, соответствующий такой фразе: «*x есть число вида* $\mathfrak{h}_1^{u_1} \ldots \mathfrak{h}_k^{u_k}$, *заключенное между числами* y' *и* z». $M(x, y, z)$ выражается формулой

$$W(x) \,\&\, y < x \leqslant z$$

и является, очевидно, рекурсивным предикатом. Введем рекурсивный терм $\psi(x, y)$ следующим образом:

$$\psi(x, y) = \underset{0 < t \leqslant y}{\mu t} \mid M(t, x, y).$$

Напишем теперь формулу, определяющую требуемую рекурсивную функцию:

a. $\sigma(0) = \mathfrak{h}_1^0 \cdot \mathfrak{h}_2^0 \ldots \mathfrak{h}_k^0$.

b. $\sigma(x') = \psi(\sigma(x),\ 0'' \cdot \sigma(x))$.

Определенная таким образом функция пробегает последовательно все числа вида (1). Действительно, $\sigma(0)$ есть минимальное число вида (1). Далее, из b следует, что если $\sigma(\mathfrak{z})$ — число вида (1), то $\sigma(\mathfrak{z}')$ есть наименьшее число вида (1), заключенное между $(\sigma(\mathfrak{z}))'$ и $0'' \cdot \sigma(\mathfrak{z})$, если такое существует. Так как $0'' = \mathfrak{z}_1$, то $0'' \cdot \sigma(\mathfrak{z})$ есть число вида (1), поэтому между $(\sigma(\mathfrak{z}))'$ и $0'' \cdot \sigma(\mathfrak{z})$ число вида (1) существует; следовательно, $\sigma(\mathfrak{z}')$ есть число вида (1), непосредственно следующее за $\sigma(\mathfrak{z})$.

8. Построим k рекурсивных функций $\rho_1(x), \ldots, \rho_k(x)$ таких, что когда $\mathfrak{z}$ пробегает последовательно все цифры, то совокупность значений k функций $\rho_1(\mathfrak{z}), \ldots$

$\ldots, \rho_k(\mathfrak{z})$ пробегает всевозможные наборы по k цифр. Положим

$$\rho_1(\mathfrak{z}) = \underset{0<t\leqslant\mathfrak{z}}{\mathrm{M}t} \mid D(\mathfrak{h}_1^t, \sigma(\mathfrak{z})),$$

$$\rho_2(\mathfrak{z}) = \underset{0<t\leqslant\mathfrak{z}}{\mathrm{M}t} \mid D(\mathfrak{h}_2^t, \sigma(\mathfrak{z})),$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$\rho_k(\mathfrak{z}) = \underset{0<t\leqslant\mathfrak{z}}{\mathrm{M}t} \mid D(\mathfrak{h}_k^t, \sigma(\mathfrak{z})).$$

Первая из этих функций $\rho_1(\mathfrak{z})$ есть степень числа $\mathfrak{h}_1$, т. е. двойки, в разложении числа $\sigma(\mathfrak{z})$, вторая $\rho_2(\mathfrak{z})$ — степень $\mathfrak{h}_2$, т. е. тройки, в разложении $\sigma(\mathfrak{z})$ и т. д., наконец, $\rho_k(\mathfrak{z})$ есть степень k-го простого числа $\mathfrak{h}_k$ в разложении $\sigma(\mathfrak{z})$. Так как $\sigma(\mathfrak{z})$ пробегает все числа вида (1), когда $\mathfrak{z}$ пробегает последовательно все цифры, то совокупность значений определенных таким образом функций $\rho_1(\mathfrak{z}), \ldots, \rho_k(\mathfrak{z})$ пробегает всевозможные наборы по k цифр, когда $\mathfrak{z}$ пробегает последовательно все цифры.

§ 15. Вычислимые функции

Присоединение рекурсивных равенств к аксиомам VI, VII, VIII вводит арифметические действия над термами. Если мы ограничимся только рекурсивными равенствами, определяющими сложение, умножение и степень, то получится система аксиом, представляющая собой несущественное видоизменение системы аксиом Пеано. Присоединение всех рекурсивных равенств вводит в арифметику, помимо обычных арифметических действий, широкий класс других операций. Как мы видели, при помощи этих операций можно определять всевозможные теоретико-числовые понятия, связанные с делимостью чисел, простыми множителями, степенями простых множителей, и многие другие.

Связанные с рекурсивными термами рекурсивные функции представляют довольно широкий класс функций, определенных на натуральном ряде и принимающих целочисленные значения (в нашей терминологии цифровые).

Вместе с тем определение этих функций таково, что они являются эффективно вычислимыми, т. е. для каждой совокупности значений аргументов функции $\mathfrak{r}(x_1, \ldots, x_n)$ мы эффективным образом находим значение самой функции. Понятие *эффективно вычислимой* функции имеет очень большое значение. К нему сводится общее понятие алгоритма, по которому совершаются какие-либо операции, например решаются задачи определенного круга. Если какой-нибудь алгоритм производит регулярным образом определенные операции, то легко себе представить, что элементы этих операций и всевозможные комбинации их могут быть обозначены цифрами так, чтобы каждый акт операции и ее результат были при этом занумерованы определенной цифрой. Тогда то, что производит алгоритм, будет выглядеть как последовательная конструкция цифр $\mathfrak{z}_1, \mathfrak{z}_2, \ldots, \mathfrak{z}_n, \ldots$ Таким образом, алгоритму соответствует некоторая вычислимая функция, определенная на цифрах и принимающая в качестве значений также цифры. Утверждение, что всякий алгоритм может быть описан в виде вычислимой функции одной переменной, не должно казаться удивительным, так как в известном смысле вычислимую функцию любого числа переменных можно свести к вычислимой функции от одной переменной. Если мы имеем, например, вычислимую функцию от n переменных $\mathfrak{r}(x_1, \ldots, x_n)$, перенумеруем все наборы из n цифр посредством рекурсивных функций:

$$\mathfrak{z}_1 = \rho_1(\mathfrak{z}), \ \ldots, \ \mathfrak{z}_n = \rho_n(\mathfrak{z}),$$

так что каждому набору $\mathfrak{z}_1, \ldots, \mathfrak{z}_n$ мы ставим в соответствие номер $\mathfrak{z}$. Тогда функция

$$\mathfrak{r}(\rho_1(\mathfrak{z}), \ \ldots, \ \rho_n(\mathfrak{z}))$$

номеру набора $(\mathfrak{z}_1, \ldots, \mathfrak{z}_n)$ ставит в соответствие вычислимым образом значение функции $\mathfrak{r}$, которое она принимает для набора $\mathfrak{z}_1, \ldots, \mathfrak{z}_n$.

Понятие «алгоритма» давно существовало и употреблялось в математике. Однако его понимание имело чисто интуитивный характер, что, естественно, затрудняло пользование этим понятием. Рядом авторов (Чёрч, Тьюринг, Пост, Марков и др.) были даны определения понятия алгоритма. Все эти определения различны по форме, но они оказались эквивалентными между собой. Наиболее просто формулируется это определение в терминах вычислимых функций. Мы его здесь приведем. Рекурсивные функции, которые мы рассмотрели в предыдущих параграфах, являются вычислимыми. Можно было бы предположить, что интуитивное понятие вычислимой функции совпадает с понятием рекурсивной функции. Оказывается, однако, что это не так. Можно определить функцию двух переменных $\mathfrak{b}(x, y)$, обладающую следующими свойствами.

1. Для каждой пары цифр $\mathfrak{z}_1$, $\mathfrak{z}_2$ значение функции $\mathfrak{b}(\mathfrak{z}_1, \mathfrak{z}_2)$ представляет собой цифру, вычислимую способом, вполне соответствующим нашему представлению об алгоритме.

2. Для каждой рекурсивной функции $\mathfrak{r}(\mathfrak{z}_1)$ существует такая цифра $\mathfrak{z}_2^0$, что $\mathfrak{r}(\mathfrak{z}_1)$ равно $\mathfrak{b}(\mathfrak{z}_1, \mathfrak{z}_1^0)$ для каждого значения $\mathfrak{z}_1$.

В таком случае функция $\mathfrak{b}(\mathfrak{z}, \mathfrak{z}) + 0'$ является, очевидно, вычислимой функцией. Покажем, что она не совпадает ни с одной рекурсивной функцией. В самом деле, предположим, что $\mathfrak{b}(\mathfrak{z}, \mathfrak{z}) + 0'$ представляет собой рекурсивную функцию, Обозначим ее через $\mathfrak{c}(\mathfrak{z})$. В таком случае найдется цифра $\mathfrak{z}_2^*$ такая, что $\mathfrak{c}(\mathfrak{z}_1)$ равно $\mathfrak{b}(\mathfrak{z}_1, \mathfrak{z}_2^*)$ для каждого значения $\mathfrak{z}_1$. Для $\mathfrak{z}_1$, равного $\mathfrak{z}_2^*$, значение функции $\mathfrak{c}(\mathfrak{z}_2^*)$ равно $\mathfrak{b}(\mathfrak{z}_2^*, \mathfrak{z}_2^*)$. Но $\mathfrak{c}(\mathfrak{z}_2^*)$ представляет собой $\mathfrak{b}(\mathfrak{z}_2^*, \mathfrak{z}_2^*) + 0'$; следовательно, $\mathfrak{b}(\mathfrak{z}_2^*, \mathfrak{z}_2^*)$ равно $\mathfrak{b}(\mathfrak{z}_2^*, \mathfrak{z}_2^*) + 0'$, что невозможно. Таким образом, предположив, что $\mathfrak{b}(\mathfrak{z}, \mathfrak{z}) + 0'$ — рекурсивная функция, мы пришли к противоречию.

Итак, нельзя считать, что понятие рекурсивной функции совпадает с понятием вычислимой функции. Однако определение вычислимой функции тесно связано с понятием рекурсивной функции. Вводится понятие *общерекурсивной функции*. В отличие от общерекурсивных функций, введенные выше рекурсивные функции часто называют *примитивно рекурсивными функциями*. Мы не употребляли этот термин потому, что не вводили понятия общерекурсивной функции. Да и в дальнейшем мы не будем иметь с ним дело, так как ограничимся только определением общерекурсивной функции. Поэтому и в следующей главе мы будем примитивно рекурсивные функции называть по-прежнему рекурсивными функциями.

Определение общерекурсивной функции состоит в следующем. Пусть $\mathfrak{r}(\mathfrak{z}_1, \mathfrak{z}_2)$ — произвольная примитивно рекурсивная функция от двух переменных, а $\mathfrak{f}(\mathfrak{z}_2)$ — произвольная примитивно рекурсивная функция от одной переменной. Допустим, что для каждого значения $\mathfrak{z}_1$ существует единственная цифра $\mathfrak{z}_2$ такая, что имеет место

$$\vdash \mathfrak{r}(\mathfrak{z}_1, \mathfrak{z}_2) = 0.$$

Тогда тем самым определяется неявная функция $\mathfrak{g}(\mathfrak{z}_1)$ такая, что

$$\vdash \mathfrak{z}_2 = \mathfrak{g}(\mathfrak{z}_1) \sim \mathfrak{r}(\mathfrak{z}_1, \mathfrak{z}_2) = 0.$$

Вместе с тем можно определить еще функцию

$$\mathfrak{f}(\mathfrak{g}(\mathfrak{z}_1)).$$

Назовем функцию общерекурсивной, если она совпадает с функцией $\mathfrak{f}(\mathfrak{g}(\mathfrak{z}_1))$, *образованной из некоторой пары примитивно рекурсивных функций* $\mathfrak{r}(\mathfrak{z}_1, \mathfrak{z}_2)$ *и* $\mathfrak{f}(\mathfrak{z}_2)$ *указанным способом.*

Как мы указывали выше, под термином «вычислимая функция» подразумевается, что для этой функции задан алгоритм, позволяющий для каждого значения аргумента определить значение функции. Задача же состоит в уточнении понятия вычислимой функции, так как понятие алгоритма, на которое оно опирается, здесь пока употребляется лишь в интуитивном понимании, без всякого определения. Определение вычислимой функции формулируется следующим образом.

«*Вычислимая функция есть общерекурсивная функция*». При этом закон вычисления значений общерекурсивной функции состоит в том, что для каждой цифры $\mathfrak{z}$ мы вычисляем значения соответствующей примитивно рекурсивной функции $\mathfrak{r}(\mathfrak{z}, 0)$, $\mathfrak{r}(\mathfrak{z}, 0')$ и т. д., пока не дойдем до такой цифры $\mathfrak{z}^*$, что $\mathfrak{r}(\mathfrak{z}, \mathfrak{z}^*)$ примет значение 0. В силу предположения о функции $\mathfrak{r}$ это непременно случится, и, следовательно, через конечное число шагов мы получим требуемую цифру $\mathfrak{z}^*$. После этого мы вычислим значение второй рекурсивной функции $\mathfrak{f}(\mathfrak{z}^*)$, которое, по определению, и будет значением данной общерекурсивной функции. Может на первый взгляд показаться, что приведенное определение вычислимой функции имеет слишком частный характер и не соответствует нашему интуитивному представлению об алгоритме и вычислимой функции. Иными словами, можно подумать, что возможно указать алгоритм для вычисления значений некоторой функции, которая заведомо не является общерекурсивной. Однако оказывается, что все известные нам способы построения вычислимых функций, определенных на всем множестве натуральных чисел, приводят к общерекурсивным функциям. Более детальный анализ этого вопроса, на котором мы останавливаться не будем, убедительно показывает, что понятие общерекурсивной функции покрывает наше интуитивное представление о вычислимой функции и заключает в себе самое общее понятие алгоритма. Так как здесь дело касается сравнения точного определения общерекурсивной функции с интуитивным понятием вычислимой функции, то не может быть речи о каком бы то ни было строгом доказательстве. Вопрос заключается в достаточной убедительности обстоятельств, на которые опирается сравнение этих понятий. Утверждение о том, что эти два понятия совпадают, известно под названием *тезиса Чёрча.*

Определение понятия алгоритма было использовано для доказательства несуществования алгоритмов для решения того или иного класса задач. Так, например, Чёрч показал, что не существует алгоритма, решающего проблему разрешимости исчисления предикатов. Проблемы, заключающиеся в отыскании алгоритма, решающего ту или иную бесконечную серию однотипных задач, получили название алгоритмических проблем. Неразрешимость алгоритмической проблемы означает, что искомый алгоритм невозможен. В последнее время получен ряд результатов, относящихся к неразрешимости алгоритмических проблем в различных разделах математики. В частности, советские математики А. А. Марков, П. С. Новиков и их ученики установили неразрешимость ряда алгоритмических проблем, касающихся групп, полугрупп, матриц, полиэдров, диофантовых уравнений и т. п. Эти результаты являются приложением математической логики к вопросам, лежащим вне ее.

§ 16. Некоторые теоремы аксиоматической арифметики

В арифметике, представленной системой аксиом I—VIII с рекурсивными равенствами, формально выводимы все теоремы известной нам элементарной арифметики. По-видимому, в ней выводимы также и все теоремы существующей в настоящее время теории чисел. То обстоятельство, что теория чисел широко использует средства и идеи анализа, доказывает только, что в этих средствах заключаются богатые эвристические элементы, позволяющие отыскивать подходы и пути для решения трудных проблем теории чисел. Но вместе с тем вполне возможно, что формальное доказательство любой теоремы теории чисел может быть проведено средствами одной аксиоматической арифметики. Мы ограничимся здесь формальным выводом самых основных теорем элементарной арифметики, именно — мы выведем свойства сложения и умножения.

Теорема 1.

$$\vdash 0 + x = x.$$

Сделаем подстановку в аксиому полной индукции, заменив $A(t)$ на $0 + t = t$; получим

$$\vdash 0 + 0 = 0 \,\&\, \forall x [0 + x = x \to 0 + x' = x'] \to 0 + y = y. \quad (1)$$

Из рекурсивных равенств, определяющих сумму, следует

$$\vdash 0 + 0 = 0. \quad (2)$$

Далее, на основании общего свойства однозначности термов (см. § 2) имеем

$$\vdash 0 + x = x \to (0 + x)' = x'.$$

Из рекурсивных равенств, определяющих сумму, следует

$$\vdash (0 + x)' = 0 + x'.$$

Заменив в предыдущей формуле терм $(0 + x)'$ равным ему термом $0 + x'$, получим

$$\vdash 0 + x = x \to 0 + x' = x'.$$

Применив производное правило связывания квантором, имеем

$$\vdash \forall x \, (0 + x = x \to 0 + x' = x'). \quad (3)$$

Из выводимости формул (2) и (3) вытекает выводимость посылки в формуле (1). Поэтому, применив правило заключения, получим

$$\vdash 0 + y = y,$$

и теорема доказана.

Теорема 2.

$$\vdash z + x' = z' + x.$$

Подставим в аксиому полной индукции вместо $A(t)$ предикат $z + t' = z' + t$. Получим

$$\vdash z + 0' = z' + 0 \,\&\, \forall x\,[z + x' = z' + x \to z + x'' = z' + x'] \to$$
$$\to z + y' = z' + y. \qquad (4)$$

На основании рекурсивных равенств имеем

$$\vdash z + 0' = (z + 0)',$$
$$\vdash z + 0 = z,$$
$$\vdash z' + 0 = z'.$$

Следовательно,

$$z + 0' = (z + 0)' = z' = z' + 0,$$

т. е.

$$\vdash z + 0' = z' + 0. \qquad (5)$$

Возьмем выводимую в арифметике формулу

$$z + x' = z' + x \to (z + x')' = (z' + x)'. \qquad (6)$$

В силу рекурсивных равенств имеем

$$\vdash (z + x')' = z + x'',$$
$$\vdash (z' + x)' = z' + x'.$$

Заменив в формуле (6) некоторые термы равными, получим

$$\vdash z + x' = z' + x \to z + x'' = z' + x'. \qquad (7)$$

Из выводимости формул (5) и (7) вытекает выводимость посылки, а значит, и следствия формулы (4). Следовательно,

$$\vdash z + y' = z' + y.$$

Доказанная теорема может быть сформулирована следующим образом: *если в сумме штрих с одного тер-*

ма перенести на другой, то определенный суммой терм перейдет в равный.

Теорема 3.

$$\vdash z + x = x + z.$$

Подставив в аксиому полной индукции $z + t = t + z$ вместо $A(t)$, получим

$$\vdash z + 0 = 0 + z \,\&\, \forall x [z + x = x + z \to z + x' = x' + z] \to \\ \to z + y = y + z. \qquad (8)$$

Из рекурсивных равенств, определяющих сумму, следует

$$\vdash z + 0 = z.$$

На основании теоремы 1 имеем

$$\vdash 0 + z = z.$$

Из двух последних равенств получаем

$$\vdash z + 0 = 0 + z. \qquad (9)$$

Из свойства однозначности термов имеем

$$\vdash z + x = x + z \to (z + x)' = (x + z)', \qquad (10)$$

а из рекурсивных равенств

$$\vdash (z + x)' = z + x',$$
$$\vdash (x + z)' = x + z'$$

на основании теоремы 2 получаем

$$\vdash x + z' = x' + z$$

и, следовательно,

$$\vdash (x + z)' = x' + z.$$

Заменив в формуле (10) термы равными термами, получим

$$\vdash z + x = x + z \to z + x' = x' + z. \qquad (11)$$

Из выводимости формул (9) и (11) вытекает выводимость посылки, а значит, и следствия формулы (8), т. е.

$$\vdash z + y = y + z.$$

Таким образом, *мы доказали коммутативность сложения.*

Теорема 4.

$$(z+u)+x=z+(u+x).$$

Подставив в аксиому полной индукции $(z+u)+t=$ $=z+(u+t)$ вместо $A(t)$, получим

$$\vdash (z+u)+0=z+(u+0)\,\&\,\forall x\,((z+u)+x= \\ =z+(u+x)\to(z+u)+x'=z+(u+x'))\to \\ \to(z+u)+y=z+(u+y). \qquad (12)$$

Из рекурсивных равенств имеем

$$\vdash (z+u)+0=z+u,$$
$$\vdash u+0=u.$$

Из второго равенства следует

$$\vdash z+(u+0)=z+u.$$

Из этих равенств легко следует

$$\vdash (z+u)+0=z+(u+0). \qquad (13)$$

Из свойства однозначности термов следует

$$\vdash (z+u)+x=z+(u+x)\to \\ \to((z+u)+x)'=(z+(u+x))'. \qquad (14)$$

Из рекурсивных равенств выводим следующие формулы:

$$\vdash ((z+u)+x)'=(z+u)+x',$$
$$\vdash (z+(u+x))'=z+(u+x)',$$
$$\vdash (u+x)'=u+x'.$$

Из двух последних равенств вытекает

$$\vdash (z+(u+x))'=z+(u+x').$$

Заменив в формуле (14) термы равными термами, получим

$$\vdash (z+u)+x=z+(u+x)\to(z+u)+x'=z+(u+x').$$

Связывая последнюю формулу квантором, имеем

$$\vdash \forall x\,[(z+u)+x=z+(u+x)\to \\ \to(z+u)+x'=z+(u+x')]. \qquad (15)$$

Из выводимости формул (13) и (15) заключаем, что посылки, а значит, и следствие формулы (12) выводимы, т. е.

$$\vdash (z + u) + y = z + (u + y).$$

Таким образом, *мы доказали ассоциативность сложения.*

Для умножения также можно вывести законы ассоциативности, коммутативности и дистрибутивности по отношению к сложению. Формулы, выражающие эти законы, в нашем написании имеют обычный вид:

$$\vdash (x \cdot y) \cdot z = x \cdot (y \cdot z),$$

$$\vdash xy = yx,$$

$$\vdash (x + y)\, z = xz + yz.$$

Мы ограничимся доказательством последней формулы, считая две первые выведенными.

Теорема 5.

$$\vdash (x + y) \cdot z = x \cdot z + y \cdot z.$$

Заменив в аксиоме полной индукции $A(x)$ формулой $(u + v)x = ux + vx$, получим

$$\vdash (u + v) \cdot 0 = u \cdot 0 + v \cdot 0 \,\&\, \forall x\, [(u + v)\, x = ux + vx \to \\ \to (u + v)\, x' = ux' + vx'] \to (u + v) \cdot y = uy + vy. \qquad (16)$$

Из рекурсивных равенств, определяющих умножение, следует

$$\vdash (u + v) \cdot 0 = 0,$$

$$\vdash u \cdot 0 = 0,$$

$$\vdash v \cdot 0 = 0.$$

Кроме того, имеет место

$$\vdash 0 + 0 = 0.$$

Из четырех последних равенств вытекает

$$\vdash (u + v) \cdot 0 = u \cdot 0 + v \cdot 0. \qquad (17)$$

Заметим теперь, что если имеет место

$$\vdash s = t,$$

то имеет место и

$$\vdash s+w=t+w.$$

В самом деле, заменив в выводимой формуле

$$\vdash s+w=s+w$$

в правой части терм s равным термом t, получим

$$\vdash s+w=t+w.$$

Сделав подстановку в выводимую формулу

$$\vdash s=t \rightarrow s+w=t+w,$$

получим

$$\vdash (u+v)\cdot x=u\cdot x+v\cdot x \rightarrow (u+v)\cdot x+(u+v)= \\ =(ux+vx)+(u+v). \tag{18}$$

На основании законов ассоциативности и коммутативности сложения имеем

$$\vdash (ux+vx)+u+v=(ux+u)+(vx+v).$$

Заменив в формуле (18) последний терм равным, получим

$$\vdash (u+v)\cdot x=ux+vx \rightarrow (u+v)\,x+(u+v)= \\ =(ux+u)+(vx+v). \tag{19}$$

На основании рекурсивных равенств, определяющих умножение, имеем

$$\vdash (u+v)\,x'=(u+v)\,x+(u+v),$$
$$\vdash ux'=ux+u,$$
$$\vdash vx'=vx+v.$$

Заменив в формуле (19) некоторые термы равными, будем иметь

$$\vdash (u+v)\,x=ux+vx \rightarrow (u+v)\,x'=ux'+vx'.$$

Связывая последнюю формулу квантором, получим

$$\vdash \forall x\,((u+v)\,x=ux+vx \rightarrow (u+v)\,x'=ux'+vx'). \tag{20}$$

Из истинности формул (17) и (20) заключаем, что посылка, а значит, и следствие формулы (16) выводимы, т. е.

$$(u+v)\,y = u\cdot y + v\cdot y.$$

Таким образом, *закон дистрибутивности умножения относительно сложения доказан.*

Мы уже указывали, что система аксиом VI, VII, VIII без рекурсивных функций плохо выражает свойства натурального ряда, так как в ней не выводимы самые основные свойства натурального ряда, как, например,

$$x' = y' \to x = y.$$

Не выводимо также свойство упорядоченности

$$\overline{x = y} \to x < y \vee y < x$$

и многие другие. Введение рекурсивных равенств исправляет это положение, и в арифметике с рекурсивными функциями все основные свойства натурального ряда оказываются выводимыми.

Здесь мы ограничимся выводом первого из указанных выше положений, а для второго только вкратце наметим идею доказательства.

Теорема 6.

$$\vdash x' = y' \to x = y.$$

Напишем рекурсивные равенства для функции $\delta(x)$, определенной в § 9:

$$\vdash \delta(0) = 0,$$

$$\vdash \delta(x') = x.$$

На основании свойства однозначности термов имеем

$$\vdash x = y \to \delta(x) = \delta(y).$$

Совершив подстановки в эту формулу, получим

$$\vdash x' = y' \to \delta(x') = \delta(y'). \tag{21}$$

На основании рекурсивных равенств для функции $\delta(x)$ получим

$$\vdash \delta(x') = x,$$

$$\vdash \delta(y') = y.$$

Заменив в формуле (21) термы равными термами, будем иметь

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

Доказательство формулы

$$\overline{x = y} \rightarrow x < y \vee y < x \qquad (22$$

можно провести следующим образом. Сначала с помощью аксиомы полной индукции докажем, что

$$\vdash x < y \sim \exists t\,(y = x + t').$$

Если обозначить формулу $\exists t\,(y = x + t')$ через $\mathfrak{A}(x, y)$, то вопрос о выводимости формулы (22) сводится к вопросу о выводимости формулы

$$\overline{x = y} \rightarrow \mathfrak{A}(x, y) \vee \mathfrak{A}(y, x).$$

Эта формула без особого труда доказывается с помощью аксиомы полной индукции.

ЭЛЕМЕНТЫ ТЕОРИИ ДОКАЗАТЕЛЬСТВА

§ 1. Постановка вопроса о непротиворечивости и независимости аксиом

В главе II мы уже указывали метод, который применялся и применяется для доказательства непротиворечивости и независимости аксиом. Это метод интерпретаций системы аксиом на той или иной области объектов, построенной средствами теории множеств, принимаемой в качестве основы. Но неудовлетворительность теоретико-множественного обоснования как раз и является основной причиной обращения к аксиоматическому описанию математических систем. Поэтому возникла иная постановка вопроса о независимости и непротиворечивости. Обо всем этом мы уже неоднократно говорили. Здесь мы напомним только основной смысл постановки вопроса о непротиворечивости и независимости аксиом. Доказать внутреннюю непротиворечивость исчисления — это значит доказать, что в нем не существует такой формулы $\mathfrak{A}$, что и она и ее отрицание $\overline{\mathfrak{A}}$ выводимы в исчислении. Независимость аксиомы означает невыводимость ее из других аксиом с помощью правил вывода рассматриваемого исчисления. Для решения вопроса о непротиворечивости исчисления или независимости какой-либо из его аксиом в такой постановке нет необходимости прибегать к интерпретации Требуется металогическими средствами доказать невозможность формального вывода в нем тех или иных формул. Новая постановка вопроса о непротиворечивости и независимости аксиом вызвала и новые методы для решения этих вопросов. Эти методы составляют так называемую *теорию доказательства.* Мы познакомимся с ними в применении к вопросам аксиоматической арифметики. Поставим себе задачу найти метод, позволяющий решить следующие два вопроса:

1) *вопрос о непротиворечивости ограниченной арифметики* и

2) *вопрос о независимости аксиомы полной индукции в арифметике.*

Что касается вопроса о непротиворечивости арифметики с аксиомой полной индукции, то здесь возникают трудности принципиального характера, так что принятых нами средств металогики оказывается недостаточно для решения этой проблемы. Связанные с этим вопросы и в настоящее время занимают существенное место в математической логике. Мы остановимся на них несколько подробнее.

В главе IV, стр. 278, мы уже указывали, что невозможно доказать непротиворечивость какого-либо исчисления средствами, формализующимися в самом этом исчислении. Точный смысл этого утверждения состоит в следующем.

Если формализовать средства, при помощи которых доказана непротиворечивость некоторого исчисления, то полученная в результате этой формализации система будет содержать формулы, не выводимые в исчислении, непротиворечивость которого доказывается. Это положение имеет достаточно общий характер, и оно во всяком случае справедливо для аксиоматической арифметики.

Принятая нами финитная металогика может быть формализована так, что все высказывания, которые в ней делаются, являются формулами аксиоматической арифметики, а все рассуждения — формальной дедукцией в этой арифметике. Поэтому средствами финитной металогики оказывается невозможным доказать непротиворечивость аксиоматической арифметики. Таким образом, требуется изменение самой постановки вопроса о непротиворечивости аксиоматической арифметики. Если речь идет об обосновании идеи актуальной бесконечности, то вопрос о непротиворечивости арифметики может быть поставлен достаточно удовлетворительным образом. Анализ оснований математики, проведенный Брауэром, показал, что в арифметике единственным принципом, опирающимся на актуальную бесконечность, является закон исключенного третьего. Предполагая арифметику без закона исключенного третьего непротиворечивой, можно доказать ее непротиворечивость с законом исключенного третьего *).

В этой книге мы не будем касаться вопроса о непротиворечивости аксиоматической арифметики. Мы ограничимся решением таких вопросов непротиворечивости, для которых достаточно средств финитизма Гильберта.

В частности, мы докажем непротиворечивость ограниченной арифметики. Решение этого вопроса хотя и представляет собой очень неполный и ограниченный результат, все же имеет интерес, так как здесь мы доказываем с помощью содержательной системы рассуждений, не опираясь на понятие актуальной бесконечности, непротиворечивость системы, которая своим предметом имеет бесконечное множество объектов и допускает для них такие средства рассуждения, как закон исключенного третьего.

Таким образом, доказательство непротиворечивости ограниченной арифметики представляет собой обоснование возможности пользоваться в некоторой мере актуальной бесконечностью.

§ 2. Простые множители и простые слагаемые

Предположим, что формула $\mathfrak{A}$ представляет собой логическое произведение, т. е. имеет вид $\mathfrak{A}_1 \& \ldots \& \mathfrak{A}_n$. Может случиться, что некоторые множители (а может быть, и все) также являются произведениями. Пусть, например, $\mathfrak{A}_1$ имеет вид $\mathfrak{A}_{11} \& \ldots \& \mathfrak{A}_{1m}$. В силу закона ассоциативности формула $\mathfrak{A}$ эквивалентна формуле

$$\mathfrak{A}_{11} \& \ \ldots \ \& \mathfrak{A}_{1m} \& \mathfrak{A}_2 \& \ \ldots \ \& \mathfrak{A}_n.$$

Мы можем продолжать такие же преобразования и далее до тех пор, пока не придем к формуле, эквивалентной формуле $\mathfrak{A}$ и представляющей собой произведение, ни один множитель которого уже не является произведением. Будем называть множители такого логического произведения *простыми множителями*. Мы видим, что каждое логическое произведение можно

*) А. Н. Колмогоров, О принципе tertium non datur, Матем. сб. **32** (1925), 646—667; K. Gödel, Zur intuitionistischen Arithmetik und Zahlentheorie, Ergebnisse eines math. Koll., Heft 4 (за 1931—1932 г., вышла из печати в 1933 г.), 34—38.

преобразовать на основании закона ассоциативности в эквивалентное ему произведение, в котором все множители простые. Назовем указанное преобразование *разложением на простые множители.* Совершенно очевидно, что полученное в результате разложения произведение простых множителей совершенно не зависит от того, в каком порядке мы производим разложение. Таким образом, состав простых множителей однозначно определяется исходной формулой $\mathfrak{A}$. (Нетрудно видеть, что простые множители сами являются частями формулы $\mathfrak{A}$.) В силу этого мы можем говорить о простых множителях произведения, подразумевая под этим те простые множители, которые могут быть получены в результате разложения формулы $\mathfrak{A}$.

Аналогичным образом назовем *простым слагаемым* такое слагаемое логической суммы, которое само не является суммой. Рассуждая так же, как и в случае произведения, можно показать, что каждая логическая сумма может быть разложена на простые слагаемые. Разложение это также единственно, так что имеет смысл говорить о простых слагаемых любой формулы $\mathfrak{A}$, являющейся суммой.

Легко видеть, что каждый не простой множитель $\mathfrak{A}_i$ произведения $\mathfrak{A}$ сам разлагается на простые множители, которые входят в число простых множителей формулы $\mathfrak{A}$. И обратно, каждый простой множитель произведения $\mathfrak{A}_1 \& \ldots \& \mathfrak{A}_n$ либо совпадает с одним из множителей $\mathfrak{A}_i$, либо является простым множителем одного из этих множителей. Аналогично, каждое не простое слагаемое суммы разлагается на простые слагаемые, входящие в число простых слагаемых данной суммы. Во всех дальнейших рассуждениях любое произведение $\mathfrak{A}$ и произведение $\mathfrak{A}'$, представляющее собой разложение $\mathfrak{A}$ на простые множители, совершенно равноправны, так что $\mathfrak{A}$ всегда можно заменить через $\mathfrak{A}'$. Аналогично, любую сумму можно заменить ее разложением на простые слагаемые.

§ 3. Примитивно истинные формулы

В дальнейшем мы введем очень существенное понятие *регулярной формулы.* Для этого сначала нам придется дать некоторые предварительные определения.

Формула, не содержащая кванторов, называется примитивной формулой.

Рассмотрим все элементарные индивидуальные высказывания и предикаты, входящие в примитивную формулу. Каждое такое высказывание имеет вид

$$\mathfrak{r}_1 = \mathfrak{r}_2 \quad \text{или} \quad \mathfrak{r}_1 < \mathfrak{r}_2,$$

где $\mathfrak{r}_1$ и $\mathfrak{r}_2$ — некоторые константы.

Каждый элементарный индивидуальный предикат имеет такой же вид, только $\mathfrak{r}_1$ и $\mathfrak{r}_2$ здесь — термы, из которых по крайней мере один содержит предметные переменные. Если мы в элементарном индивидуальном предикате заменим предметные переменные цифрами, то получим элементарное высказывание указанного типа. Если $\mathfrak{r}_1$ и $\mathfrak{r}_2$ — рекурсивные константы, то, как мы показали в главе V (§ 8), им могут быть однозначным и вполне финитным образом поставлены в соответствие цифры. Пусть это будет соответственно цифры $\mathfrak{z}_1$ и $\mathfrak{z}_2$. *Элементарное индивидуальное высказывание называется примитивно истинным, если число штрихов у цифр $\mathfrak{z}_1$ и $\mathfrak{z}_2$ совпадает для случая, когда высказывание имеет вид $\mathfrak{r}_1 = \mathfrak{r}_2$, и число штрихов $\mathfrak{z}_1$ меньше числа штрихов $\mathfrak{z}_2$ для случая, когда элементарное высказывание имеет вид $\mathfrak{r}_1 < \mathfrak{r}_2$.* В противном случае будем называть эти элементарные высказывания *примитивно ложными.*

Можно высказать следующее предложение.

Если элементарное высказывание указанного типа примитивно истинно, то оно выводимо в ограниченной арифметике. Справедливость этого утверждения следует из описания рекурсивных функций (см. главу V).

В примитивную формулу, помимо индивидуальных элементарных формул, могут входить еще переменные высказывания A, B, ... и переменные предикаты $P(x)$, $Q(x, y)$, $F(0, z)$, ... Заменим все нерекурсивные предикаты рекурсивными, затем все предметные переменные цифрами и, наконец, все получившиеся примитивно истинные элементарные высказывания символом *И*, а примитивно ложные — символом *Л*. Остальные элементарные формулы заменим символами *И* и *Л* произвольным образом, но так, чтобы одинаковые выражения заменялись одинаковым образом. После этого мы получим формулу, которую можно рассматривать как формулу алгебры высказываний, которой, по правилам алгебры высказываний, мы уже можем однозначно приписать значение *И* или *Л*. Какое именно из этих значений принимает формула, можно определить конечным числом шагов.

Примитивная формула называется примитивно истинной формулой, если

1° *она выводима в ограниченной арифметике;*

2° *после замены переменных предикатов произвольными рекурсивными предикатами, а предметных переменных произвольными цифрами и последующей замены элементарных формул символами И и Л указанным выше способом она превращается в формулу алгебры высказываний, принимающую значение И.*

В случае, если примитивная формула удовлетворяет только условию 2°, мы будем называть ее *примитивно истинной в слабом смысле.*

Заметим, что если предположить непротиворечивость ограниченной арифметики, то из условия 1° вытекает условие 2°. Мы, однако, не будем делать этого предположения, так как мы ставим себе задачу доказать непротиворечивость ограниченной арифметики. В дальнейшем мы будем существенно пользоваться свойством 2° примитивно истинной формулы. Поэтому в определении мы его высказали явным образом.

Примеры.

1. $A(x) \vee \bar{A}(x) \,\&\, 0 < x'$.

Если мы x заменим цифрой $0^{(k)}$, то получим формулу $A(0^{(k)}) \vee \bar{A}(0^{(k)}) \,\&\, 0 < 0^{(k)\prime}$. Но $0^{(k)\prime}$ есть цифра $0^{(k+1)}$. Индивидуальное высказывание $0 < 0^{(k+1)}$ примитивно истинно, поэтому мы должны заменить его символом *И*. Получим формулу $A(0^{(k)}) \vee \bar{A}(0^{(k)}) \,\&\, И$.

Рассматривая $A(0^{(k)})$ как переменное высказывание алгебры высказываний, мы получим тождественно истинную формулу. Следовательно, формула 1 примитивно истинна (ее выводимость в ограниченной арифметике легко следует из теоремы 5 § 7 главы II и теоремы 1 § 6 главы V).

2. Аксиомы арифметики VI и VII групп являются примитивно истинными формулами.

VI. Аксиомы равенства:

1. $x = x$.

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

VI. 1, очевидно, примитивно истинна. Заменив в VI. 2 x и y цифрами $\mathfrak{z}_1$ и $\mathfrak{z}_2$, получим формулу

$$\mathfrak{z}_1 = \mathfrak{z}_2 \rightarrow (A(\mathfrak{z}_1) \rightarrow A(\mathfrak{z}_2)).$$

Если цифры $\mathfrak{z}_1$ и $\mathfrak{z}_2$ различны, то выражению $\mathfrak{z}_1 = \mathfrak{z}_2$ мы должны приписать значение *Л*, поэтому вся формула принимает значение *И* при любых значениях $A(\mathfrak{z}_1)$ и $A(\mathfrak{z}_2)$. Если $\mathfrak{z}_1$ совпадает с $\mathfrak{z}_2$, мы получим формулу

$$\mathfrak{z} = \mathfrak{z} \rightarrow (A(\mathfrak{z}) \rightarrow A(\mathfrak{z})).$$

Второй член следования является тождественно истинной формулой в смысле алгебры высказываний; следовательно, формула опять-таки принимает значение *И*. Таким образом, аксиома VI. 2 также является примитивно истинной.

VII. Аксиомы порядка:

1. $\overline{x < x}$.

2. $x < y \rightarrow (y < z \rightarrow x < z)$.

3. $x < x'$.

Легко проверить, что при каждой замене x, y, z цифрами в этих аксиомах мы получим формулы, принимающие значение *И*. Это положение проверяется в конечное число шагов. Поэтому мы можем утверждать, что все аксиомы VII группы — примитивно истинные формулы.

Аксиома полной индукции не является примитивной формулой, следовательно, она не может быть и примитивно истинной.

3. Рассмотрим пример примитивной формулы, которая не является примитивно истинной:

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

Заменив x цифрой 0, а y цифрой $0'$, получим

$$(A(0) \rightarrow A(0')) \rightarrow 0 = 0'.$$

Заменим $A(0)$ символом *Л*, $A(0')$ символом *И*; $0 = 0'$ мы должны заменить символом *Л*. Тогда получим формулу

$$(Л \rightarrow И) \rightarrow Л.$$

Эта формула принимает значение *Л*. Следовательно, исходная примитивная формула не является примитивно истинной.

Заметим, что если над примитивно истинной формулой произвести тождественные преобразования алгебры высказываний, то получится также примитивно истинная формула.

§ 4. Операции 1, 2, 3

В логике предикатов мы ввели понятие приведенной формулы (см. главу III). Напомним это определение.

Приведенной формулой называется формула, не содержащая знака $\rightarrow$ и такая, что знаки отрицания в ней относятся только к элементарным частям. Это определение распространяется и на формулы арифметики. При этом распространяется и основное положение, что для каждой формулы существует эквивалентная ей приведенная формула. Доказательство этого в арифметике остается тем же, что и в исчислении предикатов. Приведенную формулу, эквивалентную данной формуле, мы будем называть ее приведенной формой. Все дальнейшие определения будут относиться к приведенным формулам.

Произвольную приведенную формулу можно представить себе в следующем виде:

$$\forall x_1 \ldots \forall x_n [(\mathfrak{A}_1 \vee \ldots \vee \mathfrak{A}_n) \& (\mathfrak{B}_1 \vee \ldots \vee \mathfrak{B}_m) \& \ldots \\ \ldots \& (\mathfrak{C}_1 \vee \ldots \vee \mathfrak{C}_p)]. \qquad (\alpha)$$

Можно считать, что вместо переменных $x_1, \ldots, x_n$ здесь могут стоять любые переменные, кванторов $\forall x_1, \ldots, \forall x_n$ может вовсе не быть, произведение, стоящее под знаком кванторов $\forall x_1, \ldots, \forall x_n$, может свестись к одному члену и, наконец, каждая сумма $\mathfrak{A}_1 \vee \ldots \vee \mathfrak{A}_n$, $\mathfrak{B}_1 \vee \ldots \vee \mathfrak{B}_m$ и т. д. может также свестись к одному члену. В этих случаях мы будем условно говорить, что имеем произведение, состоящее из одного множителя, или сумму, состоящую из одного слагаемого.

Кванторы $\forall x_1, \ldots, \forall x_n$ будем называть *внешними кванторами*. Простые множители произведения, стоящего под знаком кванторов $\forall x_1, \ldots, \forall x_n$, будем называть *внешними множителями*. Если произведение, стоящее под знаком кванторов, содержит не простые множители, то мы всегда можем разложить его на простые множители; подобная замена никак не отражается на всех дальнейших рассуждениях. В силу этого мы можем предполагать, что все множители в формуле (α) простые. Точно так же каждый из этих простых множителей, являющийся суммой, мы можем разложить на простые слагаемые и предполагать, что все слагаемые $\mathfrak{A}_i$, $\mathfrak{B}_j$, ..., $\mathfrak{C}_k$ простые. Простые слагаемые множителей формулы (α) называются *внешними слагаемыми* формулы (α). Заметим еще, что если произведение, стоящее под знаком кванторов $\forall x_1, \ldots, \forall x_n$, состоит из одного множителя, который в свою очередь состоит из одного слагаемого, то мы можем предполагать, что этот множитель не имеет вида $\forall x\, \mathfrak{A}(x)$, так как в противном случае мы квантор $\forall x$ можем отнести к внешним кванторам.

Введем операции, которые мы будем производить над формулами, представленными в форме (α).

1. Первая операция. Квантор всеобщности простого слагаемого внешнего множителя (например, $\mathfrak{A}_1$), если оно имеет вид $\forall z\, \mathfrak{A}_1'(z)$, выносится наружу и становится внешним квантором. При этом связанная этим квантором переменная переименовывается, если она совпадает с другими переменными в формуле. Назовем эту операцию *вынесением знака всеобщности*.

Если вынесен квантор $\forall z$ множителя $\mathfrak{A}_1$, то формула (α) примет вид

$$\forall x_1 \ldots \forall x_n \forall z\, [(\mathfrak{A}_1'(z) \vee \ldots \vee \mathfrak{A}_n) \,\&\, (\mathfrak{B}_1 \vee \ldots) \,\&\, \ldots].$$

При этом может оказаться, что слагаемое $\mathfrak{A}_1'(z)$ уже не является простым. Это обстоятельство ни на что не влияет, но для удобства можно сумму $\mathfrak{A}_1'(z) \vee \ldots \vee \mathfrak{A}_n$ тут же разложить на простые слагаемые.

2. Вторая операция. Эта операция связана со слагаемым, имеющим вид $\exists z\, \mathfrak{A}_1'(z)$. Пусть, например, $\mathfrak{A}_1$ имеет такой вид. Операция состоит в том, что к сумме $\mathfrak{A}_1 \vee \ldots \vee \mathfrak{A}_n$ добавляется слагаемое, имеющее вид $\mathfrak{A}_1'(\mathfrak{c})$, где $\mathfrak{c}$ — любой рекурсивный терм, содержащий любые предметные переменные, кроме переменных, связанных в формуле

$$(\mathfrak{A}_1 \vee \ldots \vee \mathfrak{A}_n) \,\&\, \ldots \,\&\, (\mathfrak{C}_1 \vee \ldots \vee \mathfrak{C}_p)$$

(таким образом, терм $\mathfrak{c}$ может содержать переменные $x_1, x_2, \ldots, x_n$).

Если эта операция проделывается со слагаемым $\mathfrak{A}_1$, то в результате мы получим формулу

$$\forall x_1 \ldots \forall x_n (\exists z \mathfrak{A}_1'(z) \vee \mathfrak{A}_1'(\mathfrak{c}) \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_n) \,\&\, \ldots$$
$$\ldots \,\&\, (\mathfrak{C}_1 \vee \ldots \vee \mathfrak{C}_p),$$

При этом новое слагаемое может оказаться не простым, и его опять можно разложить на простые слагаемые. Назовем эту операцию *отделением от квантора существования.*

3. Третья операция представляет собой преобразование дистрибутивности логического сложения по отношению к умножению. Эта операция применяется, когда одно из слагаемых в формуле (α) является произведением и вместе с тем *не является примитивной формулой.* Пусть, например, $\mathfrak{A}_1$ имеет вид произведения $\mathfrak{A}_{11} \,\&\, \ldots \,\&\, \mathfrak{A}_{1r}$ (причем можно предположить, что множители $\mathfrak{A}_{1i}$ простые). Третья операция состоит в том, что внешний множитель, содержащий это слагаемое, распадается на множители

$$(\mathfrak{A}_{11} \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_n) \,\&\, (\mathfrak{A}_{12} \vee \ldots \vee \mathfrak{A}_n) \,\&\, \ldots$$
$$\ldots \,\&\, (\mathfrak{A}_{1r} \vee \ldots \vee \mathfrak{A}_n)$$

и формула (α) переходит в формулу

$$\forall x_1 \ldots \forall x_n [(\mathfrak{A}_{11} \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_n) \,\&\, \ldots$$
$$\ldots \,\&\, (\mathfrak{A}_{1r} \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_n) \,\&\, (\mathfrak{B}_1 \vee \ldots \vee \mathfrak{B}_m) \,\&\, \ldots].$$

Опять, как и раньше, в новых множителях могут появиться не простые слагаемые $\mathfrak{A}_{1i}$, которые удобно разложить, чтобы иметь дальше дело только с суммами, у которых все слагаемые простые.

Отметим, что третья операция *не применяется к примитивным слагаемым.* Это значит, что в нашем случае слагаемое $\mathfrak{A}_1$ должно содержать хотя бы один квантор. Эта операция называется *дистрибутивной операцией.*

§ 5. Регулярные формулы

Дадим теперь определение регулярной формулы.

Формула называется элементарно регулярной, если она примитивно истинна или если она имеет вид дизъюнкции, один из членов которой примитивно истинен. (Заметим, что этот примитивно истинный член дизъюнкции сам может быть дизъюнкцией.)

Формула (α) *называется регулярной, если каждый ее внешний множитель элементарно регулярен или если посредством применения операций* 1, 2, 3 *ее можно привести к такому виду.*

Можно ввести несколько иное понятие, которое мы назовем *слабой регулярностью.*

Формула называется элементарно регулярной в слабом смысле, если она имеет вид $\mathfrak{A} \vee \mathfrak{B}$, *где* $\mathfrak{A}$ — *примитивно истинная в слабом смысле, а* $\mathfrak{B}$ — *произвольная формула.*

Формула называется слабо регулярной, если она операциями 1, 2, 3 *приводится к формуле, все внешние множители которой элементарно регулярны в слабом смысле.*

Все доказанные в последующих параграфах леммы остаются верными, если заменить в них термин «регулярная формула» термином «слабо регулярная формула». Доказательства при этом сохраняются, а в некоторых случаях упрощаются.

Примеры регулярных формул.

1. $\exists x\, A(x) \vee \bar{A}(y)$.

Здесь произведение в формуле (α) свелось к одному множителю, а внешние кванторы отсутствуют. Применив к формуле вторую операцию, получим формулу

$$A(y) \vee \exists x\, A(x) \vee \bar{A}(y),$$

которая является элементарно регулярной.

2. $\exists x\, (\forall y\, A(y) \vee \bar{A}(x))$.

В этой формуле также нет внешних кванторов. Произведение свелось к одному множителю, а этот множитель — к одному слагаемому. Произведем вторую операцию:

$$\forall y\, A(y) \vee \bar{A}(0) \vee \exists x\, (\forall y\, A(y) \vee \bar{A}(x)).$$

Далее произведем первую операцию, вынося первый квантор $\forall y$ и переименовывая связанную им переменную:

$$\forall z\,(A(z) \vee \bar{A}(0) \vee \exists x\,(\forall y\, A(y) \vee \bar{A}(x))).$$

Производим над этой формулой опять вторую операцию:

$$\forall z\,(A(z) \vee \bar{A}(0) \vee \forall y\, A(y) \vee \bar{A}(z) \vee \exists x\,(\forall y\, A(y) \vee \bar{A}(x))).$$

Единственный множитель этой формулы элементарно регулярен, так как содержит примитивно истинное слагаемое $A(z) \vee \bar{A}(z)$. Следовательно, формула 2 регулярна.

3. $\forall x\, \exists y\, (y = \varphi(x))$.

Произведем вторую операцию, заменив в отделенном члене переменную y термом $\varphi(x)$:

$$\forall x\,(\varphi(x) = \varphi(x) \vee \exists y\,(y = \varphi(x))).$$

Формула, стоящая под знаком квантора $\forall x$, элементарно регулярна. Следовательно, формула 3 регулярна.

4. $\forall x\, \forall y\, ((\bar{A}(x) \vee \exists z\, A(z))\, \&\, (A(y) \vee \bar{A}(y)\, \&\, x < x'))$.

Производим вторую операцию над квантором $\exists z$:

$$\forall x\, \forall y\, ((\bar{A}(x) \vee A(x) \vee \exists z\, A(z))\, \&\, (A(y) \vee \bar{A}(y)\, \&\, x < x')).$$

Производим третью операцию над вторым множителем:

$$\forall x\, \forall y\, ((\bar{A}(x) \vee A(x) \vee \exists z\, A(z))\, \&$$
$$\&\, (A(y) \vee \bar{A}(y))\, \&\, (A(y) \vee x < x')).$$

В этой формуле каждый множитель элементарно регулярен, следовательно, формула 4 регулярна.

Чтобы доказать регулярность какой-либо формулы $\mathfrak{A}$, мы применяем операции 1, 2, 3 и получаем при этом цепочку формул:

$$\mathfrak{A}_0,\ \mathfrak{A}_1,\ \ldots,\ \mathfrak{A}_n \equiv \mathfrak{A}.$$

Каждая формула $\mathfrak{A}_{i-1}$ получается из формулы $\mathfrak{A}_i$ применением одной из операций 1, 2, 3. Если в результате получится формула $\mathfrak{A}_0$, все внешние множители которой элементарно регулярны, то формула $\mathfrak{A}$ регулярна.

Цепочка $\mathfrak{A}_0, \mathfrak{A}_1, \ldots, \mathfrak{A}_n$, *в которой каждая формула* $\mathfrak{A}_{i-1}$ *получена из формулы* $\mathfrak{A}_i$ *применением одной из операций* 1, 2, 3, *а каждый внешний множитель формулы* $\mathfrak{A}_0$ *элементарно регулярен, называется цепочкой регулярности формулы* $\mathfrak{A}_n$.

Очевидно, что каждая формула цепочки регулярности является регулярной формулой. В дальнейшем мы будем доказывать некоторые утверждения, касающиеся регулярных формул, применяя индукцию по цепочке регулярности. Схема рассуждений при этом следующая. Утверждение доказывается для формулы $\mathfrak{A}_0$, все внешние множители которой элементарно регулярны. Затем для любой цепочки регулярности доказывается, что если утверждение верно для $\mathfrak{A}_{i-1}$, то оно верно и для $\mathfrak{A}_i$. Отсюда делается заключение, что утверждение справедливо для любой регулярной формулы. Мы ставим себе задачу доказать, что *каждая формула, выводимая в ограниченной арифметике, регулярна.* Но предварительно нам придется доказать ряд вспомогательных предложений.

Операции 1, 2, 3 обладают тем свойством, что изменения, которые они производят во внешних множителях любой формулы $\mathfrak{A}$, не зависят от того, какие были (и были ли) внешние кванторы у формулы $\mathfrak{A}$.

Допустим, что некоторая формула $\mathfrak{A}$ регулярна. Пусть

$$\mathfrak{R}_0, \mathfrak{R}_1, \ldots, \mathfrak{R}_n$$

— ее цепочка регулярности ($\mathfrak{R}_n$ совпадает с $\mathfrak{A}$). Рассмотрим формулу $\mathfrak{A}'$, которая отличается от $\mathfrak{A}$ только внешними кванторами, т. е. может быть получена из $\mathfrak{A}$ удалением внешних кванторов или приписыванием новых.

В таком случае, производя над $\mathfrak{A}'$ те же операции, что и над $\mathfrak{A}$, мы получим цепочку регулярности $\mathfrak{R}'_0, \ldots, \mathfrak{R}'_n$, где $\mathfrak{R}'_n$ совпадает с $\mathfrak{A}'$.

Внешние множители формул $\mathfrak{R}'_i$ и $\mathfrak{R}_i$ при этом одинаковы. Следовательно, одинаковы также и внешние множители формул $\mathfrak{R}'_0$ и $\mathfrak{R}_0$. Поэтому, так как по условию внешние множители $\mathfrak{R}_0$ элементарно регулярны, то внешние множители $\mathfrak{K}_0'$ также элементарно регулярны. Тогда, по определению регулярности, формула $\mathfrak{K}_n'$, т. е. $\mathfrak{A}'$, также регулярна. Отсюда вытекает:

1. *Если формула $\mathfrak{A}'$ регулярна и имеет вид $\forall x\, \mathfrak{A}(x)$, то формула $\mathfrak{A}(x)$ также регулярна*, и обратно:

2. *Если формула $\mathfrak{A}(x)$ регулярна, то формула $\forall x\, \mathfrak{A}(x)$ также регулярна.*

В самом деле, в формуле $\forall x\, \mathfrak{A}(x)$ квантор $\forall x$ является внешним, поэтому его удаление не нарушает регулярности; точно так же присоединение к регулярной формуле $\mathfrak{A}(x)$ внешнего квантора не нарушает регулярности.

Рассмотрим произвольную цепочку регулярности

$$\mathfrak{K}_0,\ \mathfrak{K}_1,\ \ldots,\ \mathfrak{K}_n.$$

Если мы удалим все внешние кванторы всех формул этой цепочки, то получим цепочку

$$\mathfrak{K}_0',\ \ldots,\ \mathfrak{K}_n',$$

формулы которой являются произведениями внешних множителей формул предшествующей цепочки. Однако о регулярности формул $\mathfrak{K}_i$ (так же как и $\mathfrak{K}_i'$) можно судить по второй цепочке так же хорошо, как и по первой, так как это свойство вполне определяется только внешними множителями.

Легко видеть, что формулы $\mathfrak{K}_n'$, $\mathfrak{K}_{n-1}'$, ..., $\mathfrak{K}_0'$ получаются одна из другой теми же операциями, что и формулы первой цепочки, за исключением операции вынесения квантора. Эта операция заменяется операцией уничтожения квантора, конечно, с соответствующим изменением переменной, которую он связывает.

Назовем эту операцию уничтожения квантора операцией 1′. Таким образом, цепочку регулярности

$$\mathfrak{K}_0,\ \mathfrak{K}_1,\ \ldots,\ \mathfrak{K}_n$$

мы можем переделать в цепочку

$$\mathfrak{K}_0',\ \mathfrak{K}_1',\ \ldots,\ \mathfrak{K}_n',$$

уничтожив все внешние кванторы формулы $\mathfrak{K}_n$ и применив далее те же операции, что и для первой цепочки, за исключением операции 1, которая заменяется операцией 1′. Так как формулы первой и второй цепочек различаются только наличием внешних кванторов всеобщности и, с другой стороны, $\mathfrak{K}'_0$ представляет произведение внешних множителей формулы $\mathfrak{K}_0$, то из сказанного следует, что регулярность первой цепочки влечет регулярность второй и обратно. Таким образом, мы можем в определении регулярности заменить операции 1, 2, 3 операциями 1′, 2, 3. Сохраним за цепочкой $\mathfrak{K}'_0, \ldots, \mathfrak{K}'_n$ название цепочки регулярности.

Докажем некоторые свойства регулярных формул.

1. *Каждый внешний множитель регулярной формулы сам есть регулярная формула.*

Пусть $\mathfrak{A}$ — регулярная формула. Применяя операции 1, 2, 3, мы получим для нее цепочку регулярности

$$\mathfrak{K}_0, \mathfrak{K}_1, \ldots, \mathfrak{K}_n,$$

где $\mathfrak{K}_n$ есть формула $\mathfrak{A}$.

Рассмотрим соответствующую цепочку регулярности

$$\mathfrak{K}'_0, \ldots, \mathfrak{K}'_n,$$

полученную из $\mathfrak{K}'_n$ операциями 1′, 2, 3.

Рассмотрим произвольный внешний множитель формулы $\mathfrak{A}$, например $\mathfrak{A}^{(1)}$. $\mathfrak{A}^{(1)}$ является внешним множителем и для формулы $\mathfrak{K}'_n$. Обозначим теперь его через $\mathfrak{A}^{(1)}_n$. Мы знаем, что операции 1, 2, 3 всегда производятся над одним из внешних множителей. То же, очевидно, справедливо и для операции 1′. Может случиться, что операция, произведенная над формулой $\mathfrak{K}'_n$, применяется не к множителю $\mathfrak{A}^{(1)}_n$. Тогда $\mathfrak{A}^{(1)}_n$ войдет в $\mathfrak{K}'_{n-1}$ без изменений. Может случиться, что операция применяется именно к этому множителю. Тогда он превратится в другой множитель или произведение множителей, которые войдут в формулу $\mathfrak{K}'_{n-1}$.

Обозначим через $\mathfrak{A}^{(1)}_{n-1}$ множитель или произведение множителей, в которые перешел множитель $\mathfrak{A}^{(1)}_n$.

При переходе от формулы $\mathfrak{K}'_{n-1}$ к $\mathfrak{K}'_{n-2}$ изменению может подвергнуться множитель, не входящий в состав $\mathfrak{A}^{(1)}_{n-1}$. Тогда $\mathfrak{A}^{(1)}_{n-1}$ перейдет без изменения в $\mathfrak{K}'_{n-2}$. В противном случае $\mathfrak{A}^{(1)}_{n-1}$ изменится и перейдет в формулу $\mathfrak{A}^{(1)}_{n-2}$, все множители которой будут внешними множителями формулы $\mathfrak{K}'_{n-2}$. Продолжая этот процесс далее, мы получим цепочку

$$\mathfrak{A}_n^{(1)},\ \mathfrak{A}_{n-1}^{(1)},\ \ldots,\ \mathfrak{A}_0^{(1)}.$$

В этой цепочке некоторые члены могут повторяться. Вычеркнув лишние, мы получим цепочку

$$\mathfrak{A}_n^{(1)},\ \mathfrak{A}_{n-s_1}^{(1)},\ \ldots,\ \mathfrak{A}_{n-s_k}^{(1)}.$$

Ясно, что множители последней формулы $\mathfrak{A}_{n-s_k}^{(1)}$ являются внешними множителями формулы $\mathfrak{K}_0'$ и, следовательно, формулы $\mathfrak{K}_0$. Так как, однако, все множители формулы $\mathfrak{K}_0$ элементарно регулярны, то и множители формулы $\mathfrak{A}_{n-s_k}^{(1)}$ также элементарно регулярны. Отсюда следует, что цепочка формул

$$\mathfrak{A}_{n-s_k}^{(1)},\ \ldots,\ \mathfrak{A}_n^{(1)}$$

является цепочкой регулярности. В силу этого формула $\mathfrak{A}_n^{(1)}$ или, что то же, $\mathfrak{A}^{(1)}$ — регулярная формула.

2. *Если все внешние множители формулы $\mathfrak{A}$ регулярны, то и формула $\mathfrak{A}$ регулярна.*

В самом деле, пусть $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ — внешние множители формулы $\mathfrak{A}$. Составим их произведение

$$\mathfrak{A}_1 \mathbin{\&} \mathfrak{A}_2 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_k.$$

Так как каждая формула $\mathfrak{A}_i$ регулярна, то применением операций 1, 2, 3 она приводится к формуле, все внешние множители которой элементарно регулярны. Обозначим $\mathfrak{A}_i^*$ произведение всех внешних множителей формулы $\mathfrak{A}_i$. Последовательностью операций 1, 2, 3, которые применяются к $\mathfrak{A}_i$, мы можем привести формулу $\mathfrak{A}$ к формуле, у которой произведение внешних множителей имеет вид

$$\mathfrak{A}_1^* \mathbin{\&} \mathfrak{A}_2 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_n.$$

Применяя далее к этой формуле последовательность операций 1, 2, 3, которые преобразуют формулу $\mathfrak{A}_2$, мы получим формулу, у которой произведение внешних множителей имеет вид

$$\mathfrak{A}_1^* \mathbin{\&} \mathfrak{A}_2^* \mathbin{\&} \mathfrak{A}_3 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_n.$$

Продолжая этот процесс, мы получим, наконец, формулу, у которой произведение внешних множителей имеет вид

$$\mathfrak{A}_1^* \mathbin{\&} \mathfrak{A}_2^* \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_n^*.$$

Каждый множитель этой формулы является произведением элементарно регулярных формул. Следовательно, формула $\mathfrak{A}$ регулярна. Из свойств 1 и 2 получаем:

3. *Если произведение регулярно, то и все множители регулярны, и, наоборот, произведение регулярных множителей регулярно.*

4. *Всякая регулярная формула выводима в ограниченной арифметике.*

В самом деле, легко видеть, что операции 1, 2, 3 преобразуют формулы исчисления предикатов в эквивалентные формулы. Это вытекает из выводимости следующих формул исчисления предикатов:

$$\mathfrak{A} \mathbin{\&} (\mathfrak{B} \vee \forall x\, \mathfrak{C}(x)) \sim \forall x\, (\mathfrak{A} \mathbin{\&} (\mathfrak{B} \vee \mathfrak{C}(x))),$$

$$\exists x\, \mathfrak{A}(x) \sim \mathfrak{A}(y) \vee \exists x\, \mathfrak{A}(x),$$

$$\mathfrak{A}_1 \mathbin{\&} \mathfrak{A}_2 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_n \vee \mathfrak{B} \sim (\mathfrak{A}_1 \vee \mathfrak{B}) \mathbin{\&} (\mathfrak{A}_2 \vee \mathfrak{B}) \mathbin{\&} \ldots \mathbin{\&} (\mathfrak{A}_n \vee \mathfrak{B}).$$

Эти формулы легко выводятся в исчислении предикатов. Первая следует из теорем 1, 2 § 12 главы IV. Третья представляет собой дистрибутивное преобразование. Вторая формула также легко выводится. В самом деле, имеем, очевидно,

$$\vdash \exists x\, \mathfrak{A}(x) \to \mathfrak{A}(y) \vee \exists x\, \mathfrak{A}(x).$$

Чтобы доказать обратное следование, сделаем подстановку в аксиому исчисления высказываний

$$(A \to C) \to ((B \to C) \to (A \vee B \to C)).$$

Получим

$$\vdash (\mathfrak{A}(y) \to \exists x\, \mathfrak{A}(x)) \to ((\exists x\, \mathfrak{A}(x) \to \exists x\, \mathfrak{A}(x)) \to$$
$$\to (\mathfrak{A}(y) \vee \exists x\, \mathfrak{A}(x) \to \exists x\, \mathfrak{A}(x))).$$

Обе посылки истинны (первая является аксиомой исчисления предикатов). Применив два раза правило заключения, получим

$$\vdash \mathfrak{A}(y) \vee \exists x\, \mathfrak{A}(x) \to \exists x\, \mathfrak{A}(x).$$

Таким образом, оба следования требуемой эквивалентности доказаны.

Из истинности первой и третьей формул вытекает, что операции 1 и 3 преобразуют формулы исчисления предикатов в эквивалентные формулы. Заменив во второй формуле переменную y произвольным рекурсивным термом $\mathfrak{c}$, получим истинную в ограниченной арифметике формулу

$$\exists x\,\mathfrak{A}(x) \sim \mathfrak{A}(\mathfrak{c}) \vee \exists x\,\mathfrak{A}(x).$$

Отсюда следует, что операция 2 также преобразует формулы исчисления предикатов в эквивалентные формулы.

Элементарно регулярная формула выводима в ограниченной арифметике, так как имеет вид $\mathfrak{A} \vee \mathfrak{B}$, где $\mathfrak{A}$ примитивно истинна и, следовательно, по определению, выводима в ограниченной арифметике. Тогда и произведение элементарно регулярных формул выводимо в ограниченной арифметике. Присоединение внешних кванторов также приводит к выводимой в ограниченной арифметике формуле. Поэтому $\mathfrak{K}_0$ — первая формула цепочки регулярности — выводима в ограниченной арифметике. Но тогда и все формулы $\mathfrak{K}_1, \ldots, \mathfrak{K}_n$ выводимы в ограниченной арифметике, так как получаются из $\mathfrak{K}_0$ последовательным применением эквивалентных преобразований. Следовательно, каждая регулярная формула выводима в ограниченной арифметике.

5. *Если регулярная формула* $\mathfrak{A}'$ *является результатом применения одной из операций* 1, 2, 3 *к формуле* $\mathfrak{A}$, *то и формула* $\mathfrak{A}$ *регулярна.* Это непосредственно следует из определения регулярной формулы.

Мы видели, что вычеркивание внешнего квантора всеобщности не нарушает регулярности.

6. *Удаление любого квантора всеобщности из регулярной формулы приводит к регулярной формуле.*

Пусть формула $\mathfrak{K}'_n$ получена удалением некоторого квантора всеобщности из регулярной формулы $\mathfrak{K}_n$. Рассмотрим цепочку регулярности формулы $\mathfrak{K}_n$:

$$\mathfrak{K}_0,\ \mathfrak{K}_1,\ \ldots,\ \mathfrak{K}_n.$$

Допустим, что рассматриваемый квантор подвергся операции 1 в формуле $\mathfrak{K}_p$. После этого в формуле $\mathfrak{K}_{p-1}$ он стал внешним квантором. Но, удалив его из всех формул $\mathfrak{K}_{p-1}$, $\mathfrak{K}_p$, ..., $\mathfrak{K}_n$, получим цепочку

$$\mathfrak{K}'_{p-1},\ \mathfrak{K}'_p,\ \ldots,\ \mathfrak{K}'_n.$$

Очевидно, что формулы $\mathfrak{K}'_{n-1}$, $\mathfrak{K}'_{n-2}$, ..., $\mathfrak{K}'_p$ получаются из $\mathfrak{K}'_n$ последовательным применением операций 1, 2, 3. Формула $\mathfrak{K}'_p$ совпадает с формулой $\mathfrak{K}'_{p-1}$, которая регулярна, так как она получена из регулярной формулы $\mathfrak{K}_{p-1}$ удалением внешнего квантора. В таком случае формула $\mathfrak{K}'_n$ операциями 1, 2, 3 приводится к регулярной формуле $\mathfrak{K}'_p$, которая приводится в свою очередь такими же операциями к формуле, у которой все внешние множители элементарно регулярны. Отсюда следует, что формула $\mathfrak{K}_n$ регулярна.

В случае, если удаляемый квантор не подвергался операции 1 ни в какой формуле цепочки

$$\mathfrak{K}_0,\ \ldots,\ \mathfrak{K}_n,$$

вычеркнем его во всех формулах цепочки. Получим цепочку

$$\mathfrak{K}'_0,\ \ldots,\ \mathfrak{K}'_n,$$

которая также будет цепочкой регулярности. В самом деле, $\mathfrak{K}'_n$ приводится к $\mathfrak{K}'_0$ теми же операциями, что и $\mathfrak{K}_n$ к $\mathfrak{K}_0$; кроме того, каждый внешний множитель $\mathfrak{K}'_0$ имеет ту же примитивно истинную сумму слагаемых, что и соответствующий множитель $\mathfrak{K}_0$, так как то слагаемое, куда входил вычеркиваемый квантор, не могло входить в эту примитивно истинную сумму, которая, по определению, не содержит кванторов.

§ 6. Некоторые леммы о регулярных формулах

Лемма 1. *Если в регулярной формуле некоторые слагаемые внешних множителей являются произведениями, то после вычеркивания любых (но не всех) множителей в каждом из этих произведений мы получим регулярную формулу.*

Пусть $\mathfrak{K}$ — регулярная формула, а

$$\mathfrak{K}_0,\ \mathfrak{K}_1,\ \ldots,\ \mathfrak{K}_n$$

— ее цепочка регулярности, где $\mathfrak{K}_n$ есть $\mathfrak{K}$. Докажем лемму, применяя индукцию по длине этой цепочки

Лемма справедлива для $\mathfrak{K}_0$. В самом деле, все внешние множители $\mathfrak{K}_0$ элементарно регулярны. Каждый множитель имеет вид $\mathfrak{A} \vee \mathfrak{B}$, где $\mathfrak{A}$ — примитивно истинная формула. Слагаемые этого множителя, являющиеся произведениями, входят либо в $\mathfrak{A}$, либо в $\mathfrak{B}$. Формула $\mathfrak{A}$ после вычеркивания некоторых множителей из ее слагаемых переходит в формулу $\mathfrak{A}'$, которая также примитивно истинна (это непосредственно вытекает из свойств формул алгебры высказываний). Слагаемые, входящие в $\mathfrak{B}$, можно вообще преобразовывать произвольным образом, так как состав $\mathfrak{B}$ не влияет на вопрос об элементарной регулярности формулы $\mathfrak{A} \vee \mathfrak{B}$. Следовательно, для $\mathfrak{K}_0$ наше утверждение справедливо. Предположим, что оно справедливо для $\mathfrak{K}_{i-1}$, и покажем, что тогда оно справедливо для $\mathfrak{K}_i$.

Формула $\mathfrak{K}_{i-1}$ получена из $\mathfrak{K}_i$ применением одной из операций 1, 2, 3 к одному из внешних множителей $\mathfrak{K}$. Если была применена одна из операций 1 или 2, то внешний множитель $\mathfrak{K}_i$ вида

$$\forall x\, \mathfrak{A}(x) \vee \mathfrak{B} \quad (\text{или } \exists x\, \mathfrak{A}(x) \vee \mathfrak{B})$$

перейдет в множитель $\mathfrak{K}_{i-1}$ вида

$$\mathfrak{A}(x) \vee \mathfrak{B} \quad (\text{или } \mathfrak{A}(\mathfrak{c}) \vee \exists x\, \mathfrak{A}(x) \vee \mathfrak{B}),$$

где $\mathfrak{c}$ — произвольный рекурсивный терм. Остальные множители $\mathfrak{K}_i$ не изменятся. Предположим, что мы вычеркнули какие-то множители из слагаемых внешних множителей $\mathfrak{K}_i$. Вычеркивание может произойти либо из слагаемых внешних множителей, не подвергшихся изменению при переходе к $\mathfrak{K}_{i-1}$, либо в множителе $\forall x\, \mathfrak{A}(x) \vee \mathfrak{B}$ (соответственно в $\exists x\, \mathfrak{A}(x) \vee \mathfrak{B}$) из слагаемых, входящих в $\mathfrak{B}$, так как $\forall x\, \mathfrak{A}(x)$ и $\exists x \mathfrak{A}(x)$ не являются произведениями. Слагаемые внешних множителей $\mathfrak{K}_i$, являющиеся произведениями, при переходе к $\mathfrak{K}_{i-1}$ не изменяются. Вычеркнув некоторые множители из слагаемых внешних множителей $\mathfrak{K}_i$ и те же множители из слагаемых внешних множителей $\mathfrak{K}_{i-1}$, получим формулы $\mathfrak{K}'_i$ и $\mathfrak{K}'_{i-1}$. Первая из них содержит внешний множитель $\forall x \mathfrak{A}(x) \vee \mathfrak{B}'$ (или соответственно $\exists x\, \mathfrak{A}(x) \vee \mathfrak{B}'$). Вторая имеет те же множители, как и первая, за исключением указанного, который переходит в множитель

$$\mathfrak{A}(x) \vee \mathfrak{B}' \quad (\text{или } \mathfrak{A}(c) \vee \exists x\, \mathfrak{A}(x) \vee \mathfrak{B}')$$

($\mathfrak{B}'$ есть результат вычеркивания множителей из слагаемых $\mathfrak{B}$). Поэтому формула $\mathfrak{K}'_{i-1}$ есть результат применения к формуле $\mathfrak{K}'_i$ той же операции, которая переводит $\mathfrak{K}_i$ в $\mathfrak{K}_{i-1}$. В силу индуктивного предположения формула $\mathfrak{K}'_{i-1}$ регулярна. А тогда (в силу 5 § 5) и $\mathfrak{K}_i$ регулярна. Таким образом, в случае, когда $\mathfrak{K}_{i-1}$ получается из $\mathfrak{K}_i$ операциями 1 или 2, из регулярности $\mathfrak{K}'_{i-1}$ следует регулярность $\mathfrak{K}'_i$.

Предположим теперь, что $\mathfrak{K}_{i-1}$ получена из $\mathfrak{K}_i$ применением операции 3. В таком случае один из внешних множителей $\mathfrak{K}_i$,

$$\mathfrak{A}_1 \,\&\, \mathfrak{A}_2 \,\&\, \ldots \,\&\, \mathfrak{A}_k \vee \mathfrak{B},$$

переходит в произведение внешних множителей $\mathfrak{K}_{i-1}$:

$$(\mathfrak{A}_1 \vee \mathfrak{B}) \,\&\, (\mathfrak{A}_2 \vee \mathfrak{B}) \,\&\, \ldots \,\&\, (\mathfrak{A}_k \vee \mathfrak{B}),$$

где $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k$ — простые множители. Остальные множители $\mathfrak{K}_i$ при переходе к $\mathfrak{K}_{i-1}$ не изменяются. Предположим, что мы вычеркнули какие-то множители из некоторых внешних слагаемых $\mathfrak{K}_i$, являющихся произведениями. При этом мы могли вычеркнуть некоторые множители и из произведения $\mathfrak{A}_1 \,\&\ldots\&\, \mathfrak{A}_k$. Пусть это множители

$$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_p, \qquad p < k.$$

Полученную таким образом формулу обозначим $\mathfrak{K}'_i$. Вычеркнем в $\mathfrak{K}_{i-1}$ из всех тех внешних слагаемых, которые не изменяются при переходе от $\mathfrak{K}_i$ к $\mathfrak{K}_{i-1}$, те же множители, которые вычеркнуты в формуле $\mathfrak{K}_i$. Кроме того, удалим из $\mathfrak{K}_{i-1}$ внешние множители:

$$\mathfrak{A}_1 \vee \mathfrak{B}', \; \mathfrak{A}_2 \vee \mathfrak{B}', \; \ldots, \; \mathfrak{A}_p \vee \mathfrak{B}',$$

где $\mathfrak{B}'$ — результат вычеркивания из $\mathfrak{B}$. В силу 3 § 5 удаление внешних множителей не нарушает регулярности формулы. Полученную формулу обозначим $\mathfrak{K}'_{i-1}$. В силу индуктивного предположения формула $\mathfrak{K}'_{i-1}$, полученная из $\mathfrak{K}_{i-1}$ вычеркиванием некоторых множителей внешних слагаемых и удалением нескольких внешних множителей, остается регулярной. Но $\mathfrak{K}'_{i-1}$ получается из $\mathfrak{K}_i'$ применением операции 3, следовательно, и $\mathfrak{K}_i'$ регулярна. Итак, наше утверждение справедливо для $\mathfrak{K}_0$, и из справедливости его для $\mathfrak{K}_{i-1}$ следует его справедливость для $\mathfrak{K}_i$. Следовательно, оно справедливо для любой регулярной формулы, что и требовалось доказать.

Лемма 2. *Если к слагаемым внешних множителей регулярной формулы присоединить любые слагаемые, то формула останется регулярной.*

Лемма 3. *Если свободную предметную переменную регулярной формулы заменить произвольным термом, то формула останется регулярной.*

Доказательство этих двух лемм легко провести по индукции точно так же, как доказательство леммы 1.

Замечание 1. *Если произвести одну из операций* 1, 2, 3 *над регулярной формулой, то получится опять регулярная формула.* Это утверждение не является непосредственно очевидным, так как такая операция может не быть той, которая данную нам формулу приводит к формуле из цепочки регулярности. Чтобы доказать наше утверждение, достаточно показать, что тот внешний множитель, над которым производится эта операция, остается регулярным. Но если эта операция есть операция 1, то рассматриваемый внешний множитель перейдет в такой, у которого вычеркнут некоторый квантор всеобщности. На основании замечания 6 § 5 этот множитель остается регулярным. Если над ним производится операция 2, то он перейдет в множитель, в котором прибавится еще одно слагаемое (т. е. множитель вида $\exists x\, \mathfrak{A}(x) \vee \mathfrak{B}$ перейдет в множитель вида $\mathfrak{A}(c) \vee \vee \exists x\, \mathfrak{A}(x) \vee \mathfrak{B}$). В силу леммы 2 при этом регулярность не нарушится. Наконец, если произведена операция 3, то множитель вида

$$\mathfrak{A}_1 \& \mathfrak{A}_2 \& \ldots \& \mathfrak{A}_k \vee \mathfrak{B}$$

перейдет в произведение множителей

$$(\mathfrak{A}_1 \vee \mathfrak{B}) \& (\mathfrak{A}_2 \vee \mathfrak{B}) \& \ldots \& (\mathfrak{A}_k \vee \mathfrak{B}).$$

Но каждый из множителей этого произведения может быть получен из предыдущего вычеркиванием всех множителей в произведении $\mathfrak{A}_1 \& \ldots \& \mathfrak{A}_k$, кроме одного. Поэтому в силу леммы 1 все формулы $\mathfrak{A}_i \vee \mathfrak{B}$ регулярны, и, следовательно, их произведение также регулярно.

Лемма 4. *Если формулы $\mathfrak{A} \vee \mathfrak{K}$ и $\mathfrak{B} \vee \mathfrak{K}$ регулярны, то формула $\mathfrak{A} \,\&\, \mathfrak{B} \vee \mathfrak{K}$ также регулярна.*

Рассмотрим сначала случай, когда $\mathfrak{A}$ и $\mathfrak{B}$ — примитивные формулы. В силу регулярности формулы $\mathfrak{A} \vee \mathfrak{B}$ она применением операций 1, 2, 3 приводится к формуле $\mathfrak{K}_0$, у которой все внешние множители элементарно регулярны. Вместе с тем так как $\mathfrak{A}$ — примитивная формула, то производимые операции никогда не затрагивают слагаемого $\mathfrak{A}$ (см. стр. 344). Поэтому все внешние множители формулы $\mathfrak{A} \vee \mathfrak{K}$ имеют вид

$$\mathfrak{A} \vee \mathfrak{C}' \vee \mathfrak{K}',$$

где $\mathfrak{A} \vee \mathfrak{C}'$ — примитивно истинные формулы.

Если мы рассмотрим формулу, в которой $\mathfrak{A}$ заменено произвольной формулой $\mathfrak{X}$, т. е. $\mathfrak{X} \vee \mathfrak{K}$, то, производя над ней те же операции, которые мы производили над $\mathfrak{A} \vee \mathfrak{K}$, мы получим формулу, внешние множители которой имеют вид

$$\mathfrak{X} \vee \mathfrak{C}' \vee \mathfrak{K}'.$$

Только эти множители уже, вообще говоря, не элементарно регулярны. Если мы в качестве $\mathfrak{X}$ возьмем формулу $\mathfrak{B}$, то формулы

$$\mathfrak{B} \vee \mathfrak{C}' \vee \mathfrak{K}'$$

будут регулярны, так как они являются внешними множителями формулы, полученной применением операций 1, 2, 3 к формуле $\mathfrak{B} \vee \mathfrak{K}$, которая, по условию, регулярна. В таком случае из каждой формулы $\mathfrak{B} \vee \mathfrak{C}' \vee \mathfrak{K}'$ можно с помощью операций 1, 2, 3 получить вновь формулу, внешние множители которой — элементарно регулярные формулы, имеющие вид

$$\mathfrak{B} \vee \mathfrak{C}' \vee \mathfrak{C}'' \vee \mathfrak{K}'',$$

где формулы $\mathfrak{B} \vee \mathfrak{C}' \vee \mathfrak{C}''$ примитивно истинны. Тогда и из формулы $\mathfrak{X} \vee \mathfrak{C}' \vee \mathfrak{K}'$ теми же операциями получается формула

$$\mathfrak{X} \vee \mathfrak{C}' \vee \mathfrak{C}'' \vee \mathfrak{K}''.$$

Заменим теперь $\mathfrak{X}$ формулой $\mathfrak{A} \,\&\, \mathfrak{B}$. В таком случае нашими операциями мы сначала получим семейство формул

$$\mathfrak{A} \,\&\, \mathfrak{B} \vee \mathfrak{C}' \vee \mathfrak{K}',$$

а затем семейство формул

$$\mathfrak{A} \mathbin{\&} \mathfrak{B} \vee \mathfrak{C}' \vee \mathfrak{C}'' \vee \mathfrak{K}''. \tag{1}$$

Покажем, что каждая формула $\mathfrak{A} \mathbin{\&} \mathfrak{B} \vee \mathfrak{C}' \vee \mathfrak{C}''$ примитивно истинна. В самом деле, тождественными преобразованиями алгебры высказываний она может быть переведена в формулу

$$(\mathfrak{A} \vee \mathfrak{C}' \vee \mathfrak{C}'') \mathbin{\&} (\mathfrak{B} \vee \mathfrak{C}' \vee \mathfrak{C}'').$$

Каждый множитель этой формулы является примитивно истинной формулой. Поэтому и произведение, а следовательно, и формула

$$\mathfrak{A} \mathbin{\&} \mathfrak{B} \vee \mathfrak{C}' \vee \mathfrak{C}''$$

примитивно истинны. Следовательно, все формулы (1) элементарно регулярны, а значит, формула $\mathfrak{A} \mathbin{\&} \mathfrak{B} \vee \mathfrak{K}$ регулярна.

Если хотя бы одна из формул $\mathfrak{A}$ или $\mathfrak{B}$ не является примитивной формулой, доказательство проводится проще. Представим $\mathfrak{A}$ и $\mathfrak{B}$ в виде произведений:

$$\mathfrak{A} = \mathfrak{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_p, \qquad \mathfrak{B} = \mathfrak{B}_1 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{B}_q$$

(в частности, p и q могут оказаться равными 1).

Формулы $\mathfrak{A} \vee \mathfrak{K}$, $\mathfrak{B} \vee \mathfrak{K}$ и $\mathfrak{A} \mathbin{\&} \mathfrak{B} \vee \mathfrak{K}$ примут тогда соответственно вид

$$\mathfrak{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_p \vee \mathfrak{K}, \qquad \mathfrak{B}_1 \mathbin{\&} \ldots \mathfrak{B}_q \vee \mathfrak{K},$$

$$\mathfrak{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_p \mathbin{\&} \mathfrak{B}_1 \mathbin{\&} \ldots \mathfrak{B}_q \vee \mathfrak{K}.$$

Первые две формулы регулярны. Поэтому в силу леммы 1 каждая формула $\mathfrak{A}_i \vee \mathfrak{K}$ и $\mathfrak{B}_j \vee \mathfrak{K}$ регулярна. Так как произведение $\mathfrak{A} \mathbin{\&} \mathfrak{B}$ не является примитивной формулой, то к формуле $\mathfrak{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{B}_q \vee \mathfrak{K}$ можно применить операцию 3. После этого она перейдет в формулу

$$(\mathfrak{A}_1 \vee \mathfrak{K}) \mathbin{\&} \ldots \mathbin{\&} (\mathfrak{A}_p \vee \mathfrak{K}) \mathbin{\&} (\mathfrak{B}_1 \vee \mathfrak{K}) \mathbin{\&} \ldots \mathbin{\&} (\mathfrak{B}_q \vee \mathfrak{K}).$$

Эта формула является произведением регулярных множителей, следовательно, регулярна. А тогда и формула $\mathfrak{A} \mathbin{\&} \mathfrak{B} \vee \mathfrak{K}$ также регулярна.

Следствие. *Пусть формула* $\mathfrak{A}$ *регулярна и ее внешние множители имеют вид* $\mathfrak{A}' \vee \mathfrak{B}' \vee \mathfrak{B}''$, *причем* $\mathfrak{C} \vee \mathfrak{B}'$ — *регулярная формула. Тогда, заменив в формуле* $\mathfrak{A}$ *все или некоторые внешние множители формулами* $\mathfrak{A}' \& \mathfrak{C} \vee \mathfrak{B}' \vee \mathfrak{B}''$ *и переименовав, если это нужно, переменные, получим регулярную формулу.*

Замечание 2. Из доказанных лемм вытекает, что *применение дистрибутивных преобразований к регулярным формулам также приводит к регулярным формулам.* В частности, для второго дистрибутивного закона это утверждение можно формулировать следующим образом.

Если $\mathfrak{A}_1 \& \ldots \& \mathfrak{A}_n \vee \mathfrak{B}$ — *регулярная формула, то* $(\mathfrak{A}_1 \vee \mathfrak{B}) \& \ldots \& (\mathfrak{A}_n \vee \mathfrak{B})$ — *также регулярная формула, и обратно.* Доказательство этого утверждения получается немедленно из лемм 1, 4 и свойства 3 регулярных формул (стр. 351). Из этого следует, что указанные преобразования мы можем применять и к отдельным множителям формулы, являющейся произведением, сохраняя неизменными остальные множители. Применение первого дистрибутивного закона также возможно. Однако мы не будем его касаться, так как он нам не понадобится.

Лемма 5. *Если формулы* $\exists x\, \mathfrak{A}(x) \vee \mathfrak{L}$ *и* $\mathfrak{B} \vee \mathfrak{L}$ *регулярны, то и формула* $\exists x\, (\mathfrak{A}(x) \& \mathfrak{B}) \vee \mathfrak{L}$ *регулярна.*

Пусть

$$\mathfrak{K}_0,\ \mathfrak{K}_1,\ \ldots,\ \mathfrak{K}_n$$

—цепочка регулярности формулы $\exists x\, \mathfrak{A}(x) \vee \mathfrak{L}$. Так как при всех операциях слагаемое $\exists x\, \mathfrak{A}(x)$ не исчезает из формулы, то каждый внешний множитель формулы $\mathfrak{K}_i$ имеет вид

$$\exists x\, \mathfrak{A}(x) \vee \mathfrak{L}^{(i)}.$$

Для всех внешних множителей формулы $\mathfrak{K}_0$ утверждение леммы справедливо. В самом деле, если формула $\exists x\, \mathfrak{A}(x) \vee \mathfrak{L}'$ элементарно регулярна, то $\mathfrak{L}'$ содержит примитивно истинные слагаемые. Поэтому, какова бы ни была формула $\mathfrak{X}$, формула $\mathfrak{X} \vee \mathfrak{L}'$ элементарно регулярна. Следовательно, и формула

$$\exists x\, (\mathfrak{A}(x) \& \mathfrak{B}) \vee \mathfrak{L}'$$

в этом случае элементарно регулярна.

Допустим, что наше утверждение справедливо для всех внешних множителей формулы $\mathfrak{K}_{i-1}$, и покажем, что тогда оно справедливо для всех внешних множителей $\mathfrak{K}_i$.

В самом деле, пусть

$$\exists x\, \mathfrak{A}(x) \vee \mathfrak{L}^{(i)}$$

— внешний множитель формулы $\mathfrak{K}_i$, а формула $\mathfrak{B} \vee \mathfrak{L}^{(i)}$ регулярна. Среди внешних множителей $\mathfrak{K}_{i-1}$

1) либо найдется множитель

$$\mathfrak{A}(\mathfrak{c}) \vee \exists x\, \mathfrak{A}(x) \vee \mathfrak{L}^{(i)},$$

2) либо найдется множитель

$$\exists x\, \mathfrak{A}(x) \vee \mathfrak{L}^{(i-1)},$$

получившийся вследствие применения одной из операций 1, 2, 3 к формуле $\mathfrak{L}^{(i)}$.

3) либо, наконец, среди внешних множителей $\mathfrak{K}_{i-1}$ содержится сам множитель

$$\exists x\, \mathfrak{A}(x) \vee \mathfrak{L}^{(i)}.$$

В случае 1) в силу индуктивного предположения и леммы 2, если $\mathfrak{B} \vee \mathfrak{L}^{(i)}$ регулярна, то и формула

$$\mathfrak{A}(\mathfrak{c}) \vee \exists x\, (\mathfrak{A}(x) \,\&\, \mathfrak{B}) \vee \mathfrak{L}^{(i)}$$

регулярна. В силу следствия леммы 4 тогда регулярна формула

$$\mathfrak{A}(\mathfrak{c}) \,\&\, \mathfrak{B} \vee \exists x\, (\mathfrak{A}(x) \,\&\, \mathfrak{B}) \vee \mathfrak{L}^{(i)}.$$

В таком случае формула

$$\exists x\, (\mathfrak{A}(x) \,\&\, \mathfrak{B}) \vee \mathfrak{L}^{(i)} \qquad (2)$$

регулярна, так как предыдущая формула получается из нее применением операции 2.

В случае 2) операция, производимая над формулой, не относится к слагаемому $\exists x\, \mathfrak{A}(x)$. Она производится над каким-то членом, входящим в состав $\mathfrak{L}^{(i)}$. Поэтому та же операция над формулой $\mathfrak{X} \vee \mathfrak{L}^{(i)}$, где $\mathfrak{X}$ — произвольная формула, приводит к формуле $\mathfrak{X} \vee \mathfrak{L}^{(i-1)}$. Эта формула регулярна, если $\mathfrak{X} \vee \mathfrak{L}^{(i)}$ регулярна, и обратно. Поэтому, если формула $\mathfrak{B} \vee \mathfrak{L}^{(i)}$ регулярна, то и $\mathfrak{B} \vee \mathfrak{L}^{(i-1)}$ регулярна. Тогда в силу индуктивного предположения формула

$$\exists x\,(\mathfrak{A}(x)\,\&\,\mathfrak{B}) \vee \mathfrak{L}^{(i-1)}$$

регулярна, а значит, и формула (2), из которой последняя получена одной из операций 1, 2, 3, регулярна.

Для случая 3) индукция очевидна. Таким образом, мы показали, что если лемма верна для внешних множителей $\mathfrak{K}_{i-1}$, то она верна и для внешних множителей $\mathfrak{K}_i$. Следовательно, она верна для формулы $\exists x \mathfrak{A}(x) \vee \mathfrak{L}$, состоящей из одного внешнего множителя.

Отметим еще одно очень простое, но полезное для дальнейшего обстоятельство.

Замечание 3. *Если формула $\exists x\,\mathfrak{A}(x) \vee \mathfrak{L}' \vee \mathfrak{L}''$ регулярна, то после включения слагаемого $\mathfrak{L}'$ под знак квантора $\exists x$ она остается регулярной.*

Рассмотрим формулу

$$\exists x\,(\mathfrak{A}(x) \vee \mathfrak{L}') \vee \mathfrak{L}''.$$

Произведем над ней операцию 2, заменив в отделенном члене x термом 0:

$$\mathfrak{A}(0) \vee \mathfrak{L}' \vee \exists x\,(\mathfrak{A}(x) \vee \mathfrak{L}') \vee \mathfrak{L}''. \tag{3}$$

Эта формула содержит в числе своих слагаемых все слагаемые формулы

$$\exists x\,\mathfrak{A}(x) \vee \mathfrak{L}' \vee \mathfrak{L}'', \tag{4}$$

за исключением $\exists x\,\mathfrak{A}(x)$, которое заменяется слагаемым

$$\exists x\,(\mathfrak{A}(x) \vee \mathfrak{L}').$$

Если мы, исходя из формулы (4), с помощью операций 1, 2, 3 получим ряд формул, то, исходя из формулы (3), мы с помощью тех же операций получим другой ряд формул, отличающихся от первых тем, что вместо слагаемого $\exists x\,\mathfrak{A}(x)$ в них содержится слагаемое $\exists x(\mathfrak{A}(x) \vee \mathfrak{L}')$ и, кроме того, в некоторых внешних множителях могут появиться лишние слагаемые, которых не было в формулах первого ряда. Но если мы таким образом приведем формулу (4) к формуле, у которой все внешние множители элементарно регулярны, то очевидно, что и формулу (3) те же операции приведут к формуле, все внешние множители которой элементарно регулярны. Отсюда следует, что если формула (4) регулярна, то и формула (3) регулярна. А тогда и формула $\exists x(\mathfrak{A}(x) \vee \mathfrak{L}') \vee \mathfrak{L}''$, из которой (3) получается операцией 2, также регулярна.

Приведенную форму формулы $\overline{\mathfrak{A}}$ будем обозначать в виде $\mathfrak{A}^-$.

Лемма 6. *Формула*

$$\mathfrak{A}(x_1, \ldots, x_n) \vee \mathfrak{A}^-(y_1, \ldots, y_n) \vee \overline{x_1 = y_1} \vee \ldots \vee \overline{x_n = y_n}$$

регулярна, какова бы ни была формула $\mathfrak{A}$.

Доказательство этого утверждения мы проведем только для $n = 1$, так как оно остается по существу тем же и в общем случае.

Доказательство мы будем вести по индукции, связанной с конструкцией приведенной формулы. Докажем, что утверждение выполняется, если $\mathfrak{A}(x)$ — элементарная формула. В таком случае формула

$$\mathfrak{A}(x) \vee \mathfrak{A}^-(y) \vee \overline{x = y}$$

является примитивно истинной.

В самом деле, если мы заменим x и y цифрами $\mathfrak{z}_1$ и $\mathfrak{z}_2$, то получим формулу

$$\mathfrak{A}(\mathfrak{z}_1) \vee \mathfrak{A}^-(\mathfrak{z}_2) \vee \overline{\mathfrak{z}_1 = \mathfrak{z}_2}.$$

Если цифры различны, то слагаемое $\overline{\mathfrak{z}_1 = \mathfrak{z}_2}$ имеет значение *И*, значит, и вся формула также имеет значение *И*. Если цифры совпадают, то слагаемое

$$\mathfrak{A}(\mathfrak{z}) \vee \mathfrak{A}^-(\mathfrak{z})$$

всегда имеет значение *И*.

Допустим, что наше утверждение справедливо для формул $\mathfrak{A}_1$ и $\mathfrak{A}_2$; покажем, что тогда оно справедливо и для формул

$$\mathfrak{A}_1 \,\&\, \mathfrak{A}_2 \quad \text{и} \quad \mathfrak{A}_1 \vee \mathfrak{A}_2.$$

В самом деле, по условию формулы

$$\mathfrak{A}_1(x) \vee \mathfrak{A}_1^-(y) \vee \overline{x = y} \quad \text{и} \quad \mathfrak{A}_2(x) \vee \mathfrak{A}_2^-(y) \vee \overline{x = y}$$

регулярны; поэтому на основании леммы 2 формулы

$$\mathfrak{A}_1(x) \vee \mathfrak{A}_1^-(y) \vee \mathfrak{A}_2^-(y) \vee \overline{x = y}$$

и

$$\mathfrak{A}_2(x) \vee \mathfrak{A}_2^-(y) \vee \mathfrak{A}_1^-(y) \vee \overline{x=y}$$

также регулярны.

Тогда в силу леммы 4 формула

$$\mathfrak{A}_1(x) \& \mathfrak{A}_2(x) \vee \mathfrak{A}_1^-(y) \vee \mathfrak{A}_2^-(y) \vee \overline{x=y}$$

также регулярна. Так как формула

$$\mathfrak{A}_1^-(y) \vee \mathfrak{A}_2^-(y)$$

является приведенной формой формулы $\overline{\mathfrak{A}_1(y) \& \mathfrak{A}_2(y)}$, то наше утверждение для формулы $\mathfrak{A}_1 \& \mathfrak{A}_2$ доказано. Формула $\mathfrak{A}_1 \vee \mathfrak{A}_2$ рассматривается аналогично. Если лемма имеет место для формулы $\mathfrak{A}$, то она справедлива и для $\overline{\mathfrak{A}}$, так как выражение

$$\mathfrak{A}(x) \vee \mathfrak{A}^-(y) \vee \overline{x=y}$$

для обеих формул одинаково.

Допустим, что лемма справедлива для $\mathfrak{A}(t, x)$; покажем, что она справедлива и для формул

$$\forall t\, \mathfrak{A}(t, x), \qquad \exists t\, \mathfrak{A}(t, x).$$

По предположению формула

$$\mathfrak{A}(t, x) \vee \mathfrak{A}^-(t, y) \vee \overline{x=y}$$

регулярна. Очевидно, что $\mathfrak{A}(s, x) \vee \mathfrak{A}^-(s, y) \vee \overline{x=y}$ также регулярна, какова бы ни была предметная переменная s.

Формулу

$$\forall t\, \mathfrak{A}(t, x) \vee (\forall t\, \mathfrak{A}(t, y))^- \vee \overline{x=y}$$

можно представить в виде

$$\forall t\, \mathfrak{A}(t, x) \vee \exists t\, \mathfrak{A}^-(t, y) \vee \overline{x=y}. \tag{5}$$

Произведем над этой формулой сначала операцию 1:

$$\forall u \left(\mathfrak{A}(u, x) \vee \exists t\, \mathfrak{A}^-(t, y) \vee \overline{x=y}\right),$$

затем операцию 2:

$$\forall u \left(\mathfrak{A}(u, x) \vee \mathfrak{A}^-(u, y) \vee \exists t\, \mathfrak{A}^-(t, y) \vee \overline{x=y}\right).$$

Из регулярности формулы

$$\mathfrak{A}(u, x) \vee \mathfrak{A}^{-}(u, y) \vee \overline{x = y}$$

следует, что предыдущая формула регулярна и, следовательно, формула (5) также регулярна.

Доказательство для формулы $\exists t\, \mathfrak{A}(t, x)$ аналогично. Таким образом, мы доказали нашу лемму для всех приведенных формул.

Замечание 4. *Формула* $\mathfrak{A}(x_1, x_2, \ldots, x_n) \vee \vee\, \mathfrak{A}^{-}(x_1, x_2, \ldots, x_n)$ *всегда регулярна.*

Мы не будем доказывать это утверждение, так как его доказательство проводится по образцу предыдущей леммы.

Лемма 7. *Если совершить подстановку в регулярную формулу* $\mathfrak{A}$, *заменив переменное высказывание* A *или переменный предикат* $A(x, \ldots, u)$ *соответственно формулой* $\mathfrak{B}$ *или* $\mathfrak{B}(x, \ldots, u)$, *то получится формула, приведенная форма которой регулярна.*

Мы проведем доказательство для случая подстановки в предикат. То же рассуждение с некоторыми упрощениями годится для случая подстановки в переменное высказывание.

Кроме того, мы будем рассматривать только подстановку в предикат от одной переменной, так как доказательство для предиката от произвольного числа переменных по существу не отличается от случая $n = 1$, только пришлось бы выписывать более громоздкие выражения.

Пусть регулярная формула $\mathfrak{A}$ содержит предикат от одной переменной $A(t)$. Покажем, что формула $\mathfrak{R}$, полученная из $\mathfrak{A}$ заменой $A(t)$ формулой $\mathfrak{B}(t)$, регулярна.

Рассмотрим сначала случай, когда $\mathfrak{A}$ — примитивно истинная формула. Применив к ней дистрибутивные преобразования в соответствии со вторым дистрибутивным законом, мы можем привести ее к конъюнктивной нормальной форме $\mathfrak{A}'$, которая также является примитивно истинной формулой. Возьмем произвольный множитель этой формулы и отделим в нем члены, содержащие предикат $A(\ )$. Тогда множитель может быть представлен в виде

$$A(x_1) \vee \ldots \vee A(x_p) \vee \bar{A}(y_1) \vee \ldots \vee \bar{A}(y_q) \vee L. \qquad (6)$$

Этот множитель, очевидно, также является примитивно истинной формулой. Докажем, что формула

$$\sum (x_i = y_j) \vee L, \tag{7}$$

где знак $\sum$ обозначает логическую сумму слагаемых для всех пар (i, j) при $1 \leqslant i \leqslant p$ и $1 \leqslant j \leqslant q$, является примитивно истинной. Формула (6) примитивно истинна; поэтому, если мы в ней заменим переменный предикат $A(\ )$ любым рекурсивным предикатом, то получим формулу, также примитивно истинную. Введем переменные $s_1, s_2, \ldots, s_p$, не входящие в формулу (6), и сделаем подстановку, заменив предикат $A(t)$ формулой

$$\prod_i \overline{(s_i = t)}$$

($\prod$ обозначает логическое произведение множителей при $i = 1, 2, \ldots, p$).

Получим примитивно истинную формулу

$$\prod_i \overline{(s_i = x_1)} \vee \prod_i \overline{(s_i = x_2)} \vee \ldots$$
$$\ldots \vee \prod_i \overline{(s_i = x_p)} \vee \overline{\prod_i \overline{(s_i = y_1)}} \vee \ldots \vee \overline{\prod_i \overline{(s_i = y_q)}} \vee L.$$

L при этом не изменится, так как не содержит предиката A; преобразовав эту формулу по правилам алгебры высказываний, получим

$$\prod_i \overline{(s_i = x_1)} \vee \ldots \vee \prod_i \overline{(s_i = x_p)} \vee$$
$$\vee \sum_i (s_i = y_1) \vee \ldots \vee \sum_i (s_i = y_q) \vee L.$$

Заменив каждую переменную s_i переменной x_i, получим примитивно истинную формулу

$$\prod_i \overline{(x_i = x_1)} \vee \ldots \vee \prod_i \overline{(x_i = x_q)} \vee$$
$$\vee \sum_i (x_i = y_1) \vee \ldots \vee \sum_i (x_i = y_q) \vee L.$$

Каждое из слагаемых $\prod_i \overline{(x_i = x_1)}, \ldots, \prod_i \overline{(x_i = x_p)}$ содержит примитивно ложный множитель: первое — множитель $\overline{x_1 = x_1}$, второе — множитель $\overline{x_2 = x_2}$ и т. д.

Поэтому каждое из этих слагаемых примитивно ложно. По законам алгебры высказываний после удаления этих слагаемых формула останется примитивно истинной. Оставшаяся формула совпадает с формулой (7). Преобразовав эту формулу по правилам алгебры высказываний, получим примитивно истинную формулу

$$\prod_{i,\,j} \overline{(x_i = y_j)} \to L.$$

С другой стороны, подстановка в формулы

$$A(x_1) \vee \ldots \vee A(x_p) \vee \bar{A}(y_1) \vee \ldots \vee \bar{A}(y_q) \vee \overline{x_i = y_j},$$
$$i = 1, 2, \ldots, p; \quad j = 1, 2, \ldots, q,$$

при которой предикат $A(t)$ заменяется формулой $\mathfrak{B}(t)$, приводит к формулам

$$\mathfrak{B}(x_1) \vee \ldots \vee \mathfrak{B}(x_p) \vee \overline{\mathfrak{B}}(y_1) \vee \ldots \vee \overline{\mathfrak{B}}(y_q) \vee \overline{x_i = y_j}.$$

Привсденная форма каждой из этих формул имеет вид

$$\mathfrak{B}(x_1) \vee \ldots \vee \mathfrak{B}(x_p) \vee \mathfrak{B}^-(y_1) \vee \ldots \vee \mathfrak{B}^-(y_q) \vee \overline{x_i = y_j}. \tag{8}$$

Она содержит слагаемое

$$\mathfrak{B}(x_i) \vee \mathfrak{B}^-(y_j) \vee \overline{x_i = y_j}.$$

В силу леммы 6 эта формула является регулярной. На основании леммы 2 формула (8) также регулярна; наконец, применив лемму 4, получим, что формула

$$\mathfrak{B}(x_1) \vee \ldots \vee \mathfrak{B}(x_p) \vee \mathfrak{B}^-(y_1) \vee \ldots \vee \mathfrak{B}^-(y_q) \vee \prod_{i,\,j} \overline{(x_i = y_j)} \tag{9}$$

регулярна. Но тогда формула

$$\mathfrak{B}(x_1) \vee \ldots \vee \mathfrak{B}(x_p) \vee \mathfrak{B}^-(y_1) \vee \ldots \vee \mathfrak{B}^-(y_q) \vee L \tag{10}$$

также является регулярной. В самом деле, рассмотрим цепочку регулярности формулы (9)

$$\mathfrak{K}_0, \mathfrak{K}_1, \ldots, \mathfrak{K}_m.$$

Слагаемое $\prod\limits_{i,\,j} \overline{(x_i = y_j)}$ примитивно, поэтому оно не подвергается действию операций 1, 2, 3 и входит без изменения во внешние множители формулы $\mathfrak{K}_0$, где его можно считать включенным в примитивно истинную часть. Представим примитивно истинную часть из произвольного внешнего множителя $\mathfrak{K}_0$ в виде

$$\mathfrak{H} \vee \prod_{i,\, j} \overline{(x_i = y_j)}.$$

Если мы во всех формулах $\mathfrak{K}_i$ заменим $\prod\limits_{i,\, j} \overline{(x_i = y_j)}$ формулой L, то примитивно истинная часть каждого внешнего множителя формулы $\mathfrak{K}_0$ примет вид

$$\mathfrak{H} \vee L.$$

Но так как формула

$$\prod_{i,\, j} \overline{(x_i = y_j)} \rightarrow L$$

примитивно истинна, то при любых заменах всякий раз, когда $\prod\limits_{i,\, j} \overline{(x_i = y_j)}$ примет значение $И$, L также примет значение $И$; отсюда следует, что каждая формула $\mathfrak{H} \vee L$ также является примитивно истинной. Из сказанного вытекает, что, заменив в формуле (9) слагаемое $\prod\limits_{i,\, j} \overline{(x_i = y_j)}$ символом L, мы получим опять регулярную формулу.

С другой стороны, эта формула является приведенной формой результата рассматриваемой подстановки $\mathfrak{B}(t)$ на место $A(t)$ в произвольном множителе нормальной формулы $\mathfrak{A}'$. Следовательно, эта подстановка переводит формулу $\mathfrak{A}'$ в регулярную формулу, которую мы обозначим через $\mathfrak{N}'$. Если через $\mathfrak{N}$ обозначить формулу, получающуюся той же подстановкой из формулы $\mathfrak{A}$, то очевидно, что $\mathfrak{N}'$ из $\mathfrak{N}$ и, обратно, $\mathfrak{N}$ из $\mathfrak{N}'$ получается посредством тех же дистрибутивных операций, что и формула $\mathfrak{A}'$ из $\mathfrak{A}$ и, наоборот, $\mathfrak{A}$ из $\mathfrak{A}'$. Так как эти дистрибутивные операции представляют собой применение второго дистрибутивного закона, то из регулярности $\mathfrak{N}'$ следует регулярность формулы $\mathfrak{N}$. Итак, *подстановка в переменный предикат, входящий в примитивно истинную формулу, не нарушает регулярности.*

Для случая подстановки в переменное высказывание в примитивно истинной формуле доказательство проводится аналогично, с некоторыми упрощениями. Роль леммы 6 играет замечание 4, Перейдем теперь к рассмотрению общего случая. Пусть формула $\mathfrak{A}$ регулярна и содержит переменный предикат $A(\ )$. (Ради краткости мы опять ограничиваемся рассмотрением предиката от одной переменной.) Пусть

$$\mathfrak{K}_0, \ldots, \mathfrak{K}_n$$

— цепочка регулярности формулы $\mathfrak{A}$. Каждый внешний множитель формулы $\mathfrak{K}_0$ элементарно регулярен и поэтому может быть представлен в виде

$$\mathfrak{H} \vee L,$$

где $\mathfrak{H}$ — примитивно истинная формула. Заменив в $\mathfrak{H} \vee L$ предикат $A(t)$ произвольной формулой $\mathfrak{B}(t)$, мы получим формулу $\mathfrak{H}' \vee L'$. На основании доказанного формула $\mathfrak{H}'$, полученная при рассматриваемой подстановке из $\mathfrak{H}$, является примитивно истинной формулой. В силу этого каждый внешний множитель формулы $\mathfrak{H}_0$ после замены предиката $A(t)$ формулой $\mathfrak{B}(t)$ перейдет в элементарно регулярную формулу.

Если мы обозначим через $\mathfrak{K}'_0$ формулу, являющуюся результатом рассматриваемой подстановки в формулу $\mathfrak{K}_0$, то все внешние множители $\mathfrak{K}'_0$ будут элементарно регулярны. Заменим теперь $A(t)$ формулой $\mathfrak{B}(t)$ во всех формулах цепочки регулярности. Мы получим цепочку

$$\mathfrak{K}'_0, \ldots, \mathfrak{K}'_m.$$

Легко видеть, что $\mathfrak{K}'_{i-1}$ получается из $\mathfrak{K}'_i$ теми же операциями 1, 2, 3, что и формула $\mathfrak{K}_{i-1}$ из $\mathfrak{K}_i$. Так как формула $\mathfrak{K}'_0$ регулярна, то и все формулы данной цепочки также регулярны. Но последняя формула $\mathfrak{K}'_m$ есть результат подстановки формулы $\mathfrak{B}(t)$ вместо предиката $A(t)$ в формуле $\mathfrak{K}_m$, которая есть в то же время формула $\mathfrak{A}$. Таким образом, подстановка в переменный предикат не нарушает регулярности формулы. Справедливость этого утверждения для подстановки в переменное высказывание доказывается аналогично.

§ 7. Операции, двойственные операциям 1, 2, 3

Подобно тому как прежде мы рассматривали произвольную формулу в форме (α) (см. стр. 342), мы можем произвольную формулу представить в двойственной форме:

$$\exists x_1 \ldots \exists x_n (\mathfrak{A}_{11} \& \ldots \& \mathfrak{A}_{1p_1} \vee \ldots \vee \mathfrak{A}_{k1} \& \ldots \& \mathfrak{A}_{kp_k}). \quad (\beta)$$

Описание формулы (β) аналогично описанию формулы (α), только оно производится в двойственных терминах. Сумма $\mathfrak{A}_{11} \& \ldots \& \mathfrak{A}_{1p_1} \vee \ldots \vee \mathfrak{A}_{k1} \& \ldots \& \mathfrak{A}_{kp_k}$ состоит из простых слагаемых, которые мы будем называть *внешними*, а каждое произведение $\mathfrak{A}_{i1} \& \ldots \& \mathfrak{A}_{ip_i}$ состоит из простых множителей, которые мы также будем называть *внешними*. Кванторы $\exists x_i$ также называются *внешними*. В частном случае внешних кванторов может и не быть. Может оказаться, что в формуле (β) только одно внешнее слагаемое или что внешнее слагаемое содержит только один множитель. В таких условиях формула (β) может представлять любую формулу.

Для формул, заданных в форме (β), можно определить операции, двойственные операциям 1, 2, 3, которые мы обозначим соответственно 1*, 2*, 3*.

Операция 1* *представляет собой вынесение квантора существования из внешнего множителя вида* $\exists x\, \mathfrak{B}(x)$ и, если это нужно, переименование связанной этим квантором переменной.

Пример.

$$\exists x (\forall y\, A(y) \& \mathfrak{B} \vee \exists y\, \overline{A}(y) \& \mathfrak{C}).$$

Применив операцию 1* и переименовав соответствующую переменную, мы получим формулу

$$\exists x \exists z (\forall y A(y) \& \mathfrak{B} \vee \overline{A}(z) \& \mathfrak{C}).$$

Операция 2*, *двойственная операция* 2, *называется отделением от квантора всеобщности.* Мы не будем ее подробно описывать, а только ограничимся примером.

Пример.

$$\forall x \forall y (\forall z A(z, t) \& A(x, t) \vee \overline{A}(x, x) \& \overline{A}(y, y)).$$

Применив к этой формуле операцию 2* и заменив в отделенном члене z рекурсивным термом $x+y$, получим

$$\forall x \forall y (A(x+y, t) \& \forall z A(z, t) \& A(x, t) \vee \overline{A}(x, x) \& \overline{A}(y, y)).$$

Операция 3*, двойственная операции 3, имеет уже свой термин в алгебре высказываний. Она называлась там *первой дистрибутивной операцией.* Сохраним за ней это название и здесь. В случае, когда ее нельзя будет спутать со второй дистрибутивной операцией, мы будем ее называть просто дистрибутивной операцией. Она, подобно операции 3, *применяется только к непримитивным слагаемым.* Эту операцию можно применить, если в формулу входит внешнее слагаемое, один из множителей которого представляет собой сумму:

$$(\mathfrak{A}_1 \vee \ldots \vee \mathfrak{A}_n) \mathbin{\&} \mathfrak{B},$$

где $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ — простые слагаемые. В таком случае операция 3* состоит в замене этого слагаемого суммой

$$\mathfrak{A}_1 \mathbin{\&} \mathfrak{B} \vee \mathfrak{A}_2 \mathbin{\&} \mathfrak{B} \vee \ldots \vee \mathfrak{A}_n \mathbin{\&} \mathfrak{B}.$$

Пример. Применяя операцию 3* к формуле

$$\exists z\,(F(z) \mathbin{\&} (A \vee G(z)) \vee \overline{F}(z) \mathbin{\&} \overline{G}(z)),$$

получим формулу

$$\exists z\,(F(z) \mathbin{\&} A \vee F(z) \mathbin{\&} G(z) \vee \overline{F}(z) \mathbin{\&} \overline{G}(z)).$$

Каждая из операций 1*, 2*, 3* всегда связана с каким-то внешним слагаемым. Иногда для того, чтобы точнее указать операцию, мы будем говорить, что она применяется к данному внешнему слагаемому.

§ 8. Свойства операций 1*, 2*, 3*

Мы ставим своей ближайшей задачей показать, что если применить одну из операций 1*, 2*, 3* к регулярной формуле, то формула останется регулярной. Именно, мы покажем, что если применить одну из операций 1*, 2*, 3* к формуле $\mathfrak{A}$, являющейся частью регулярной формулы $\mathfrak{A} \vee \mathfrak{H}$, то полученная формула $\mathfrak{A}' \vee \mathfrak{H}$ останется регулярной.

Лемма 1. *Если $\mathfrak{A} \vee \mathfrak{H}$ — регулярная формула, а $\mathfrak{A}'$ — результат применения операции* 1* *к формуле $\mathfrak{A}$, то $\mathfrak{A}' \vee \mathfrak{H}$ — также регулярная формула.*

Напишем $\mathfrak{A}$ в форме (β):

$$\exists x_1 \ldots \exists x_n (\exists y\, \mathfrak{A}_0(y) \mathbin{\&} \mathfrak{B} \vee \mathfrak{C}), \tag{1}$$

где $\exists y$ — тот квантор, который выносится при осуществлении операции 1*. Тогда в этих обозначениях содержание леммы состоит в следующем: если формула

$$\exists x_1 \ldots \exists x_n (\exists y \mathfrak{A}_0(y) \& \mathfrak{B} \vee \mathfrak{C}) \vee \mathfrak{H} \tag{2}$$

регулярна, то формула

$$\exists x_1 \ldots \exists x_n \exists y (\mathfrak{A}_0(y) \& \mathfrak{B} \vee \mathfrak{C}) \vee \mathfrak{H} \tag{3}$$

также регулярна.

Рассмотрим сначала два частных случая.

1. В формуле (2) $n = 0$, т. е. кванторы отсутствуют.
2. Формула (2) элементарно регулярна.

В случае 1 формула (2) имеет вид

$$\exists y \mathfrak{A}_0(y) \& \mathfrak{B} \vee \mathfrak{C} \vee \mathfrak{H}.$$

По условию эта формула регулярна; тогда на основании леммы 1 § 6 формулы

$$\exists y \mathfrak{A}_0(y) \vee \mathfrak{C} \vee \mathfrak{H} \quad \text{и} \quad \mathfrak{B} \vee \mathfrak{C} \vee \mathfrak{H}$$

также регулярны. В силу леммы 5 и замечания 3 § 6 формула

$$\exists y (\mathfrak{A}_0(y) \& \mathfrak{B} \vee \mathfrak{C}) \vee \mathfrak{H}$$

регулярна, что и требовалось доказать.

Рассмотрим случай 2. Формула (2) элементарно регулярна. Эта формула, рассмотренная в форме (α), состоит из единственного внешнего множителя. По определению элементарной регулярности она должна иметь примитивно истинное слагаемое. Случай $n = 0$ мы уже можем не рассматривать. В случае, когда n не равно нулю, слагаемое (1) не входит в примитивно истинную часть формулы (2), так как оно не примитивно. В таком случае, как бы мы его ни изменили, регулярность формулы не нарушится.

Докажем теперь нашу лемму посредством двойной индукции. Сначала будем вести индукцию по числу кванторов $\exists x_i$ формулы (2). Для исходного случая, когда это число равно нулю, наша лемма доказана. Допустим, что она справедлива, когда это число равно $n - 1$. Будем доказывать ее справедливость, когда число кванторов равно n. Допустим, что формула (2) регулярна. Чтобы составить ее цепочку регулярности, надо рассмотреть ее в форме (α); тогда формула (2) сводится к единственному внешнему множителю. Пусть

$$\mathfrak{K}_0, \ldots, \mathfrak{K}_m$$

— цепочка регулярности формулы (2). Мы докажем утверждение леммы, если установим его справедливость для каждого внешнего множителя любой формулы $\mathfrak{K}_i$, имеющего вид (2) с числом кванторов $\exists x_j$, равным n.

Доказательство это мы проведем по второй индукции, проходящей по цепочке регулярности. Наше утверждение справедливо для любого внешнего множителя формулы $\mathfrak{K}_0$, так как эти внешние множители элементарно регулярны, а этот случай уже был нами рассмотрен выше. Предположим, что наше утверждение справедливо для каждого внешнего множителя вида (2) формулы $\mathfrak{K}_{i-1}$. Покажем, что тогда оно имеет место и для каждого внешнего множителя вида (2) формулы $\mathfrak{K}_i$. Рассмотрим произвольный внешний множитель $\mathfrak{L}_i$ формулы $\mathfrak{K}_i$, имеющий вид (2):

$$\exists x_1 \ldots \exists x_n (\exists y \mathfrak{A}_1(y) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1) \vee \mathfrak{H}_1$$

(по условию $n > 0$).

Очевидно, множитель $\mathfrak{L}_i$ регулярен. Нам достаточно доказать, что формула $\mathfrak{L}'_i$, полученная из $\mathfrak{L}_i$ применением операции 1* к слагаемому

$$\exists x_1 \ldots \exists x_n (\exists y \mathfrak{A}_1(y) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1), \tag{s}$$

также регулярна.

Рассмотрим сначала случай, когда операция, переводящая $\mathfrak{K}_i$ в $\mathfrak{K}_{i-1}$, не относится к слагаемому (s). Если эта операция производится не над множителем $\mathfrak{L}_i$, то все очевидно. Следовательно, мы можем считать, что она производится над множителем $\mathfrak{L}_i$ и переводит его в множитель $\mathfrak{L}_{i-1}$ формулы $\mathfrak{K}_{i-1}$. Если это операция 3, то она переводит $\mathfrak{L}_i$ не в один множитель $\mathfrak{L}_{i-1}$, а в произведение нескольких таких множителей. Во всяком случае каждый множитель $\mathfrak{L}_{i-1}$ формулы $\mathfrak{K}_{i-1}$, полученный из $\mathfrak{L}_i$ при переходе от $\mathfrak{K}_i$ к $\mathfrak{K}_{i-1}$, регулярен и содержит слагаемое (s). Тогда, по индуктивному предположению, формула $\mathfrak{L}'_{i-1}$, полученная из $\mathfrak{L}_{i-1}$ применением операции 1* к ее слагаемому (s), будет также регулярна. Так как формула $\mathfrak{L}'_{i-1}$ (в случае операции 3 — произведение соответствующих $\mathfrak{L}'_{i-1}$) получается из $\mathfrak{L}'_i$ той же операцией 1, 2 или 3, что и $\mathfrak{L}_{i-1}$ (в случае операции 3 — произведение соответствующих множителей $\mathfrak{L}_{i-1}$) из $\mathfrak{L}_i$, то из регулярности $\mathfrak{L}'_{i-1}$ в силу свойства 5 регулярных формул (см. § 5) следует регулярность $\mathfrak{L}'_i$.

Перейдем к случаю, когда операция 1, 2 или 3 применяется к слагаемому (s) рассматриваемого внешнего множителя. Тогда, очевидно, это может быть только операция 2, и внешний множитель перейдет во внешний множитель формулы $\mathfrak{K}_{i-1}$ следующего вида:

$$\exists x_2 \ldots \exists x_n (\exists y\, \mathfrak{A}_1(y, c) \,\&\, \mathfrak{B}_1(c) \vee \mathfrak{C}_1(c)) \vee \\ \vee \exists x_1 \ldots \exists x_n (\exists y \mathfrak{A}_1(y) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1) \vee \mathfrak{H}_1.$$

В силу второго индуктивного предположения мы можем без нарушения регулярности применить операцию 1* к любому внешнему множителю формулы $\mathfrak{K}_{i-1}$ соответствующего вида. Поэтому формула

$$\exists x_2 \ldots \exists x_n (\exists y\, \mathfrak{A}_1(y, c) \,\&\, \mathfrak{B}_1(c) \vee \mathfrak{C}_1(c)) \vee \\ \vee \exists x_1 \ldots \exists x_n \exists y (\mathfrak{A}_1(y) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1) \vee \mathfrak{H}_1$$

регулярна. В силу первого индуктивного предположения наша лемма справедлива для случая, когда число кванторов формулы (2) равно $n-1$. Мы можем применить вторично операцию 1* к полученной формуле, только по отношению к ее первому слагаемому. Получим регулярную формулу

$$\exists x_2 \ldots \exists x_n \exists y (\mathfrak{A}_1(y, c) \,\&\, \mathfrak{B}_1(c) \vee \mathfrak{C}_1(c)) \vee \\ \vee \exists x_1 \ldots \exists y (\mathfrak{A}_1(y) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1) \vee \mathfrak{H}_1.$$

Рассмотрим формулу

$$\exists x_1 \ldots \exists x_n \exists y (\mathfrak{A}_1(y) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1) \vee \mathfrak{H}_1.$$

Предыдущая регулярная формула получается из нее операцией 2. Поэтому эта формула также регулярна. С другой стороны, она получается из внешнего множителя $\mathfrak{L}_i$ формулы $\mathfrak{K}_i$ применением операции 1* к слагаемому (s). Таким образом, если лемма верна для внешних множителей вида (2) формулы $\mathfrak{K}_{i-1}$, то она верна и для внешних множителей вида (2) формулы $\mathfrak{K}_i$. Следовательно, она верна и для формулы (2).

Л е м м а 2. *Если формула* $\mathfrak{A} \vee \mathfrak{H}$ *регулярна и* $\mathfrak{A}'$ *есть результат применения операции* 2* *к формуле* $\mathfrak{A}$, *то формула* $\mathfrak{A}' \vee \mathfrak{H}$ *также регулярна.*

Формулу $\mathfrak{A}$ мы предположим заданной в форме (β). Тогда лемму 2 можно формулировать так. Пусть формула $\mathfrak{A} \vee \mathfrak{H}$ регулярна и некоторое внешнее слагаемое формулы $\mathfrak{A}$ имеет вид $\forall z\, \mathfrak{A}_0(z)\ \&\ \mathfrak{B}$. Тогда, заменив его в этой формуле слагаемым $\mathfrak{A}_0(\mathfrak{c})\,\&\,\forall z \mathfrak{A}_0(z)\,\&\,\mathfrak{B}$, где $\mathfrak{c}$ — любой рекурсивный терм, не приводящий к коллизии переменных, мы получим формулу $\mathfrak{A}'$ такую, что формула $\mathfrak{A}' \vee \mathfrak{H}$ регулярна.

Формула $\mathfrak{A}$ в форме (β) имеет вид

$$\exists x_1 \ldots \exists x_n (\forall z\, \mathfrak{A}_0(z)\,\&\,\mathfrak{B} \vee \mathfrak{C}). \tag{4}$$

Мы рассмотрим сначала два случая.

1. В формуле (4) $n = 0$.
2. Формула $\mathfrak{A} \vee \mathfrak{H}$ элементарно регулярна.

В первом случае формула $\mathfrak{A} \vee \mathfrak{H}$ имеет вид

$$\forall z\, \mathfrak{A}_0(z)\,\&\,\mathfrak{B} \vee \mathfrak{C} \vee \mathfrak{H}. \tag{5}$$

Если она регулярна, то на основании леммы I § 6 регулярны и формулы

$$\forall z\, \mathfrak{A}_0(z) \vee \mathfrak{C} \vee \mathfrak{H} \quad \text{и} \quad \mathfrak{B} \vee \mathfrak{C} \vee \mathfrak{H}.$$

Тогда формула $\mathfrak{A}_0(z) \vee \mathfrak{B} \vee \mathfrak{H}$ регулярна (см. стр. 352). Далее, на основании леммы 3 § 6 формула

$$\mathfrak{A}_0(\mathfrak{c}) \vee \mathfrak{C} \vee \mathfrak{H}$$

регулярна. На основании леммы 4 § 6 формула

$$\mathfrak{A}_0(\mathfrak{c})\,\&\,\forall z\, \mathfrak{A}_0(z)\,\&\,\mathfrak{B} \vee \mathfrak{C} \vee \mathfrak{H}$$

также регулярна. Но эта формула есть $\mathfrak{A}'$, полученная операцией 2* из $\mathfrak{A}$.

В случае 2 в силу элементарной регулярности формула $\mathfrak{A} \vee \mathfrak{H}$ содержит примитивно истинную часть, в которую слагаемое $\forall z\, \mathfrak{A}_0(z)\ \&\ \mathfrak{B}$ не может входить. Поэтому это слагаемое можно заменить любым другим, не нарушая регулярности.

После этого мы проведем доказательство нашей леммы путем двойной индукции. Первую индукцию ведем по числу кванторов $\exists x_i$ формулы (4), т. е. по числу n. Для $n = 0$ справедливость леммы уже установлена. Предположим, что лемма справедлива для числа кванторов $n - 1$, и будем доказывать, что тогда она справедлива для n.

Формула $\mathfrak{A} \vee \mathfrak{H}$ в этом случае имеет вид

$$\exists x_1 \ldots \exists x_n (\forall z\, \mathfrak{A}_0(z) \,\&\, \mathfrak{B} \vee \mathfrak{C}) \vee \mathfrak{H}. \tag{6}$$

Эта формула, по предположению, регулярна. Пусть

$$\mathfrak{K}_0, \ldots, \mathfrak{K}_m$$

— ее цепочка регулярности. Докажем, что для каждого внешнего множителя любой формулы $\mathfrak{K}_i$, имеющего вид (6), наша лемма справедлива. Тем самым она будет доказана и для самой формулы (6), состоящей из единственного внешнего множителя. Доказательство высказанного утверждения мы проведем по второй индукции (от $\mathfrak{K}_{i-1}$ к $\mathfrak{K}_i$).

Для формулы $\mathfrak{K}_0$ наше утверждение, как мы видели, справедливо (см. случай 2). Предположим, что оно справедливо для $\mathfrak{K}_{i-1}$.

Рассмотрим произвольный внешний множитель формулы $\mathfrak{K}_i$, имеющий вид (6):

$$\exists x_1 \ldots \exists x_n (\forall z\, \mathfrak{A}_1(z) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1) \vee \mathfrak{H}_1. \tag{7}$$

Если $\mathfrak{K}_{i-1}$ получена из $\mathfrak{K}_i$ операцией, произведенной не над слагаемым

$$\exists x_1 \ldots \exists x_n (\forall z\, \mathfrak{A}_1(z) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1), \tag{8}$$

то это слагаемое перейдет в $\mathfrak{K}_{i-1}$ без изменений. Произведя над ним в формулах $\mathfrak{K}_i$ и $\mathfrak{K}_{i-1}$ операцию 2* получим формулы $\mathfrak{K}'_i$ и $\mathfrak{K}'_{i-1}$. По индуктивному предположению $\mathfrak{K}'_{i-1}$ — регулярная формула. Но она получена из $\mathfrak{K}'_i$ такой же операцией 1, 2 или 3, как и формула $\mathfrak{K}_{i-1}$ из $\mathfrak{K}_i$. Следовательно, $\mathfrak{K}'_i$ регулярна.

Допустим, что $\mathfrak{K}_{i-1}$ получена из $\mathfrak{K}_i$ операцией, производимой над слагаемым (8). Тогда это может быть только операция 2. В этом случае внешний множитель $\mathfrak{K}_i$, содержащий слагаемое (8), перейдет во внешний множитель $\mathfrak{K}_{i-1}$ следующего вида:

$$\exists x_2 \ldots \exists x_n (\forall z\, \mathfrak{A}_1(z, \mathfrak{c}) \,\&\, \mathfrak{B}_1(\mathfrak{c}) \vee \mathfrak{C}_1(\mathfrak{c})) \vee \\ \vee \exists x_1 \ldots \exists x_n (\forall z\, \mathfrak{A}_1(z) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1) \vee \mathfrak{H}_1.$$

По индуктивному предположению, касающемуся формулы $\mathfrak{K}_{i-1}$, ко второму слагаемому можно применить операцию 2*, не нарушая регулярности последней формулы.

Тогда формула

$$\exists x_2 \ldots \exists x_n (\forall z \mathfrak{A}_1 (z, \mathfrak{c}) \,\&\, \mathfrak{B}_1 (\mathfrak{c}) \vee \mathfrak{C}_1 (\mathfrak{c})) \vee \\ \vee \exists x_1 \ldots \exists x_n (\mathfrak{A}_1 (\mathfrak{g}) \,\&\, \forall z \mathfrak{A}_1 (z) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1) \vee \mathfrak{H}_1$$

регулярна. По первому индуктивному предположению, касающемуся числа кванторов $\exists x_i$, мы можем применить операцию 2* и к первому слагаемому, так как в нем число кванторов равно $n-1$. После этого мы получим регулярную формулу

$$\exists x_2 \ldots \exists x_n (\mathfrak{A}_1 (\mathfrak{g}, \mathfrak{c}) \,\&\, \forall z \mathfrak{A}_1 (z, \mathfrak{c}) \,\&\, \mathfrak{B}_1 (\mathfrak{c}) \vee \mathfrak{C}_1 (\mathfrak{c})) \vee \\ \vee \exists x_1 \ldots \exists x_n (\mathfrak{A}_1 (\mathfrak{g}) \,\&\, \forall z \mathfrak{A}_1 (z) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1) \vee \mathfrak{H}_1.$$

Эта формула представляет собой результат применения операции 2 к формуле

$$\exists x_1 \ldots \exists x_n (\forall z \mathfrak{A}_1 (z) \,\&\, \mathfrak{A}_1 (\mathfrak{g}) \,\&\, \mathfrak{B}_1 \vee \mathfrak{C}_1) \vee \mathfrak{H}_1.$$

Следовательно, последняя формула также регулярна. Итак, мы доказали по индукции от $\mathfrak{K}_{i-1}$ к $\mathfrak{K}_i$, что формула (6) регулярна. Таким образом, мы завершили индукцию от $n-1$ к n, и лемма полностью доказана.

Лемма 3. *Пусть $\mathfrak{A}'$ есть результат операции 3*, примененной к формуле $\mathfrak{A}$. Тогда, если формула $\mathfrak{A} \vee \mathfrak{H}$ регулярна, то формула $\mathfrak{A}' \vee \mathfrak{H}$ также регулярна.*

Доказательство этой леммы проводится по тому же образцу, что и доказательство двух предыдущих лемм. Поэтому мы ограничимся тем, что только наметим его. Представим $\mathfrak{A}$ в форме (β), т. е. в виде

$$\exists x_1 \ldots \exists x_n ((\mathfrak{A}_1 \vee \ldots \vee \mathfrak{A}_p) \,\&\, \mathfrak{B} \vee \mathfrak{C}),$$

где $(\mathfrak{A}_1 \vee \ldots \vee \mathfrak{A}_p) \,\&\, \mathfrak{B}$ — член, к которому применяется операция 3. В этом случае лемму можно сформулировать так.

Если формула

$$\exists x_1 \ldots \exists x_n ((\mathfrak{A}_1 \vee \ldots \vee \mathfrak{A}_p) \,\&\, \mathfrak{B} \vee \mathfrak{C}) \vee \mathfrak{H} \tag{9}$$

регулярна, то и формула

$$\exists x_1 \ldots \exists x_n (\mathfrak{A}_1 \,\&\, \mathfrak{B} \vee \ldots \vee \mathfrak{A}_p \,\&\, \mathfrak{B} \vee \mathfrak{C}) \vee \mathfrak{H}$$

также регулярна.

Сначала следует доказать, что лемма справедлива, если в формуле (9) $n=0$ или если эта формула элементарно регулярна. Далее надо провести двойную индукцию, предположив, что наша лемма справедлива для числа кванторов, равного n, и доказав ее справедливость для $n+1$, прибегая ко второй индукции, следующей по цепочке регулярности.

Лемма 4. *Если формула*

$$\exists x_1 \ldots \exists x_n (\mathfrak{A}_1 \,\&\, \mathfrak{B}_1 \vee \ldots \vee \mathfrak{A}_p \,\&\, \mathfrak{B}_p) \vee \mathfrak{H} \qquad (10)$$

регулярна, а каждая формула $\mathfrak{A}_i$ *примитивно ложна, то формула* $\mathfrak{H}$ *регулярна.*

В содержание этой леммы мы включаем также и случай, когда $n = 0$. Но случай, когда $\mathfrak{H}$ отсутствует, здесь уже не возможен. Точнее говоря, мы предполагаем, что в содержание леммы входит и утверждение, что $\mathfrak{H}$ не может отсутствовать или, что то же, формула

$$\exists x_1 \ldots \exists x_n (\mathfrak{A}_1 \,\&\, \mathfrak{B}_1 \vee \ldots \vee \mathfrak{A}_p \,\&\, \mathfrak{B}_p) \qquad (11)$$

регулярна быть не может. Мы допускаем еще, что в слагаемом $\mathfrak{A}_i \,\&\, \mathfrak{B}_i$ множителя $\mathfrak{B}_i$ может не быть.

Докажем сначала, что из любой регулярной суммы можно, не нарушая регулярности, удалить любое примитивно ложное слагаемое.

Рассмотрим цепочку регулярности данной формулы

$$\mathfrak{K}_0, \ldots, \mathfrak{K}_m$$

и докажем это утверждение для всех внешних множителей формул $\mathfrak{K}_i$. Для внешних множителей формулы $\mathfrak{K}_0$ оно справедливо. В самом деле, пусть $\mathfrak{A}^0$ — примитивно ложное слагаемое некоторого внешнего множителя формулы $\mathfrak{K}_0$. Если слагаемое $\mathfrak{A}^0$ не входит в примитивно истинную часть этого множителя, то оно может быть удалено. Если же оно входит в примитивно истинную часть, то эта часть может быть представлена в виде

$$\mathfrak{A}^0 \vee \mathfrak{G}.$$

Но из алгебры высказываний следует, что $\mathfrak{G}$ при всех возможных заменах в этой формуле должно получать всегда значение *И*, так как $\mathfrak{A}^0$ всегда получает значение *Л*. Таким образом, $\mathfrak{G}$ само примитивно истинно и $\mathfrak{A}^0$ может быть удалено без нарушения регулярности рассматриваемого внешнего множителя. Допустим, что наше утверждение справедливо для формулы $\mathfrak{K}_{i-1}$, и покажем, что оно имеет место и для $\mathfrak{K}_i$. Но примитивно ложное слагаемое любого внешнего множителя $\mathfrak{K}_i$ не подвергается действию никакой из операций 1, 2, 3, как всякая примитивная формула. Поэтому оно сохраняется и в формуле $\mathfrak{K}_{i-1}$. Если мы его вычеркнем из формул $\mathfrak{K}_i$ и $\mathfrak{K}_{i-1}$, то получим формулы $\mathfrak{K}'_i$ и $\mathfrak{K}'_{i-1}$, причем $\mathfrak{K}'_{i-1}$ получается из $\mathfrak{K}'_i$ той же из операций 1, 2, 3, что и $\mathfrak{K}_{i-1}$ из $\mathfrak{K}_i$; но по предположению $\mathfrak{K}'_{i-1}$ регулярно, следовательно, $\mathfrak{K}'_i$ также регулярно. Из доказанного немедленно вытекает, что наша лемма справедлива, когда кванторов $\exists x_i$ в слагаемом (10) нет, т. е. когда $n = 0$. В этом случае формула (9) имеет вид

$$\mathfrak{A}_1 \& \mathfrak{B}_1 \vee \ldots \vee \mathfrak{A}_p \& \mathfrak{B}_p \vee \mathfrak{H}.$$

Из регулярности этой формулы на основании леммы 1 § 6 вытекает регулярность формулы

$$\mathfrak{A}_1 \vee \mathfrak{A}_2 \vee \ldots \vee \mathfrak{A}_p \vee \mathfrak{H}.$$

Но в силу доказанного все примитивно ложные слагаемые $\mathfrak{A}_i$ можно последовательно удалить, не нарушая регулярности формулы. Тогда формула $\mathfrak{H}$ также будет регулярна.

Итак, для $n = 0$ наша лемма справедлива. После этого ее легко доказать при помощи двойной индукции так же, как доказаны предыдущие леммы. Мы не будем проводить этого рассуждения, заметим только, что в нем при рассмотрении операции 2 приходится пользоваться утверждением, что если формула $\mathfrak{A}(x)$ примитивно ложна, то формула $\mathfrak{A}(\mathfrak{c})$, где $\mathfrak{c}$ — произвольный рекурсивный терм, также примитивно ложна. Справедливость этого утверждения прямо вытекает из определения примитивной ложности.

§ 9. Регулярность формул, выводимых в арифметике

В дальнейшем мы будем называть *регулярной* всякую формулу арифметики, приведенная форма которой регулярна.

Теорема 1. *Всякая формула арифметики, выводимая из регулярных формул посредством правил вывода арифметики, регулярна.*

Напомним, что правила вывода арифметики, по определению, совпадают с правилами вывода расширенного исчисления предикатов, которые в свою очередь отличаются от правил исчисления предикатов только тем, что в связи с введением термов расширены правила подстановки. Следовательно, нам достаточно доказать утверждение теоремы для всех правил вывода расширенного исчисления предикатов.

1. *Правило подстановки в переменное высказывание или предикат.* Справедливость теоремы для этого правила непосредственно следует из леммы 7 § 6.

2. *Правило подстановки в предметную переменную* очевидно, так как при такой подстановке структура формулы не меняется.

3. *Первое правило связывания квантором.*

Надо показать, что если формула

$$\mathfrak{B} \to \mathfrak{A}(x), \tag{1}$$

где $\mathfrak{B}$ не содержит переменной x, регулярна, то и формула

$$\mathfrak{B} \to \forall x\, \mathfrak{A}(x) \tag{2}$$

также регулярна. Рассмотрим приведенную форму формулы (1). Она имеет вид (см. стр. 362)

$$\mathfrak{B}^- \vee \mathfrak{A}(x). \tag{3}$$

По условию эта формула регулярна. Приведенная форма формулы (2) имеет вид

$$\mathfrak{B}^- \vee \forall x\, \mathfrak{A}(x). \tag{4}$$

Произведя над ней операцию 1 (операцию выноса квантора всеобщности), получим формулу

$$\forall x (\mathfrak{B}^- \vee \mathfrak{A}(x)).$$

Так как формула, стоящая под знаком квантора, регулярна, то и вся формула регулярна. Но тогда формула (4), а следовательно, и формула (2) регулярны.

4. *Второе правило связывания квантором* рассматривается аналогичным образом.

5. *Правило заключения.* Пусть формулы $\mathfrak{A}$ и $\mathfrak{A} \to \mathfrak{B}$ регулярны. Требуется показать, что и формула $\mathfrak{B}$ регулярна. Запишем формулу $\mathfrak{A}$ (точнее, ее приведенную

форму) в виде (α):

$$\forall x_1 \ldots \forall x_n ((\mathfrak{A}_{11} \vee \ldots \vee \mathfrak{A}_{1p_1}) \& \ldots \& (\mathfrak{A}_{m1} \vee \ldots \vee \mathfrak{A}_{mp_m})). \quad (5)$$

Эта формула, по условию, регулярна. Следовательно, посредством операций 1, 2, 3 ее можно привести к виду

$$\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_q ((\mathfrak{A}_0^{(1)} \vee \mathfrak{H}_0^{(1)}) \& \ldots \& (\mathfrak{A}_0^{(q)} \vee \mathfrak{H}_0^{(q)})), \quad (6)$$

где все $\mathfrak{A}_0^{(i)}$ — примитивно истинные формулы. Приведенная форма формулы $\mathfrak{A} \to \mathfrak{B}$ имеет вид

$$\mathfrak{A}^- \vee \mathfrak{B}',$$

где $\mathfrak{A}^-$ — приведенная форма $\overline{\mathfrak{A}}$, а $\mathfrak{B}'$ — приведенная форма $\mathfrak{B}$. Формула $\mathfrak{A}^-$ имеет вид

$$\exists x_1 \ldots \exists x_n (\mathfrak{A}_{11}^- \& \ldots \& \mathfrak{A}_{1p_1}^- \vee \ldots \vee \mathfrak{A}_{m1}^- \& \ldots \& \mathfrak{A}_{mp_m}^-). \quad (7)$$

Таким образом, $\mathfrak{A}^-$ записана в форме (β), двойственной форме (α). Если мы к этой формуле будем применять операции 1*, 2*, 3*, двойственные тем, которые применялись к формуле (5), то, очевидно, получим формулу

$$\exists x_1 \ldots \exists x_n (\mathfrak{A}_0^{(1)-} \& \mathfrak{H}_0^{(1)-} \vee \ldots \vee \mathfrak{A}_0^{(q)-} \& \mathfrak{H}_0^{(q)-}).$$

В силу доказанных в § 8 лемм 1—3 применение операций 1*, 2*, 3* к слагаемому $\mathfrak{A}^-$ в формуле $\mathfrak{A}^- \vee \mathfrak{B}'$ не нарушает регулярности этой формулы. Отсюда следует, что формула

$$\exists x_1 \ldots \exists x_n (\mathfrak{A}_0^{(1)-} \& \mathfrak{H}_0^{(1)-} \vee \ldots \vee \mathfrak{A}_0^{(q)-} \& \mathfrak{H}_0^{(q)-}) \vee \mathfrak{B}'$$

регулярна. Все формулы $\mathfrak{A}_0^{(i)-}$ в этой формуле примитивно ложны, так как $\mathfrak{A}_0^{(i)}$ примитивно истинны. Но тогда в силу леммы IV § 8 формула $\mathfrak{B}'$, а следовательно, и $\mathfrak{B}$ регулярны.

Таким образом, мы показали, что применение всех правил вывода расширенного исчисления предикатов к регулярным формулам приводит к регулярным формулам, что и требовалось доказать.

Теорема 2. *Формулы, выводимые в ограниченной арифметике, регулярны.*

Чтобы доказать эту теорему, нам теперь достаточно установить, что все аксиомы ограниченной арифметики регулярны. Однако из теоремы 1 легко следует, что все выводимые в ограниченной арифметике формулы регулярны. Рассмотрим сперва общелогические аксиомы. Они состоят из аксиом исчисления высказываний и двух аксиом исчисления предикатов.

Аксиомы исчисления высказываний и, следовательно, их приведенные формы являются тождественно истинными формулами алгебры высказываний. Поэтому все они примитивно истинны и, следовательно, регулярны.

Приведенная форма первой аксиомы исчисления предикатов имеет вид

$$\exists x\, \overline{A}(x) \vee A(y).$$

Произведя над этой формулой операцию 2, получим

$$\overline{A}(y) \vee \exists x\, \overline{A}(x) \vee A(y).$$

Эта формула элементарно регулярна; следовательно, аксиома $\forall x\, A(x) \to A(y)$ — регулярная формула.

Регулярность второй аксиомы исчисления предикатов устанавливается таким же способом.

В § 3 мы показали, что все аксиомы ограниченной арифметики VI и VII являются примитивно истинными формулами. Следовательно, они также регулярны.

Наконец, в ограниченную арифметику входят исходные истинные формулы вида

$$\mathfrak{f}(x_1, \ldots, x_{n-1}, 0) = \mathfrak{t}(x_1, \ldots, x_{n-1}),$$

$$\mathfrak{f}(x_1, \ldots, x_{n-1}, x_n') = \xi(x_1, \ldots, x_n, \mathfrak{f}(x_1, \ldots, x_n)),$$

где $\mathfrak{f}(x_1, \ldots, x_{n-1}, 0)$, $\mathfrak{t}(x_1, \ldots, x_{n-1})$ и $\xi(x_1, \ldots, x_n, x_{n+1})$ — рекурсивные термы. Числовая интерпретация этих равенств заключается в том, что мы приписываем формуле $\mathfrak{f}(0^{(k_1)}, \ldots, 0^{(k_{n-1})}, 0)$ [соответственно формуле $\mathfrak{f}(0^{(k_1)}, \ldots, 0^{(k_{n-1})}, 0^{(k_{n+1})})$] ту же цифру, которая приписана формуле $\mathfrak{t}(0^{(k_1)}, \ldots, 0^{(k_{n-1})})$ [соответственно формуле $\xi(0^{(k_1)}, \ldots, 0^{(k_n)}, \mathfrak{f}(0^{(k_1)}, \ldots, 0^{(k_n)}))$]. Поэтому все формулы этого вида примитивно истинны и, следовательно, регулярны. Таким образом, все аксиомы ограниченной арифметики регулярны. Следовательно, в силу теоремы 1 все формулы, выводимые в ограниченной арифметике, регулярны, что и требовалось доказать.

Заметим, что из регулярности формулы следует ее слабая регулярность. Таким образом, все выводимые в ограниченной арифметике формулы являются также слабо регулярными.

§ 10. Непротиворечивость ограниченной арифметики

Теорема. *Ограниченная арифметика непротиворечива.*

Как мы уже неоднократно указывали, вопрос о непротиворечивости любого из рассматриваемых нами исчислений равносилен вопросу о существовании в нем невыводимой формулы. Для доказательства непротиворечивости достаточно в таком случае доказать существование в рассматриваемом исчислении невыводимой формулы. Мы докажем, что в ограниченной арифметике формула $\overline{0 = 0}$ невыводима. В самом деле, если бы эта формула была выводима в ограниченной арифметике, то в силу замечания, сделанного нами в конце § 9, она была бы слабо регулярной. Но так как эта формула примитивна, то она тогда должна быть примитивно истинной в слабом смысле. Она, однако, таковой не является, так как высказывание $0 = 0$ мы, по условию, должны заменить символом *И* и, следовательно, высказывание $\overline{0 = 0}$ имеет значение *Л*. Итак, формула $\overline{0 = 0}$, не будучи слабо регулярной, не может быть выводима в ограниченной арифметике.

Смысл полученного результата состоит в том, что доказана содержательными и финитными средствами непротиворечивость употребления бесконечности в пределах ограниченной арифметики. Заметим, что все исчисления, непротиворечивость которых мы доказывали до сих пор, не могли служить определением бесконечности, так как интерпретировались на конечных областях. Ограниченная арифметика не может быть интерпретирована никакой конечной областью объектов. Описанный нами в этой главе метод позволяет, как мы увидим, устанавливать другие факты, которые сами по себе никак не очевидны.

§ 11. Независимость аксиомы полной индукции в арифметике

В следующем параграфе мы докажем более сильную теорему о независимости аксиомы полной индукции, которая содержит как частный случай теорему о независимости аксиомы полной индукции от остальных аксиом арифметики. Мы все же докажем сперва отдельно теорему о независимости аксиомы полной индукции в арифметике, так как хотя она и слабее той теоремы, которая будет доказана дальше, но зато и доказательство ее значительно проще.

Теорема. *Аксиома полной индукции не выводима из остальных аксиом арифметики.*

Если бы аксиома полной индукции была выводима из остальных аксиом, то она была бы слабо регулярной. Покажем, что она не может быть слабо регулярной. Аксиома полной индукции имеет вид

$$A(0) \mathbin{\&} \forall x\, (A(x) \to A(x')) \to A(y),$$

а ее приведенная форма —

$$\overline{A}(0) \vee \exists x\, (A(x) \mathbin{\&} \overline{A}(x')) \vee A(y). \qquad (1)$$

Допустим, что она слабо регулярна. В таком случае с помощью операций 1, 2, 3 ее можно привести к формуле, все внешние множители которой элементарно регулярны в слабом смысле. Однако единственная операция, которую можно применить к формуле (1), — это операция отделения от квантора $\exists x$. Формулы, полученные из (1) с помощью этой операции, опять-таки допускают применение только той же операции и т. д. Всякая формула, полученная из (1) применением n раз операции 2, имеет вид

$$\overline{A}(0) \vee A(c_1) \mathbin{\&} \overline{A}(c_1') \vee \ldots$$
$$\ldots \vee A(c_n) \mathbin{\&} \overline{A}(c_n') \vee \exists x\, (A(x) \mathbin{\&} \overline{A}(x')) \vee A(y). \qquad (2)$$

Как формула (1), так и формула (2) совпадают со своим единственным внешним множителем. Поэтому, если формула (1) слабо регулярна, то для некоторого n формула (2) элементарно регулярна в слабом смысле.

Поэтому формула

$$\overline{A}(0) \vee A(\mathfrak{c}_1) \& \overline{A}(\mathfrak{c}_1') \vee \ldots \vee A(\mathfrak{c}_n) \& \overline{A}(\mathfrak{c}_n') \vee A(y) \tag{3}$$

должна быть примитивно истинной в слабом смысле. Заменим в формуле (3) переменную y цифрой $0^{(n+1)}$, а переменные, входящие в $\mathfrak{c}_i$ (если они есть), — произвольными цифрами. В таком случае все термы получат определенные числовые значения. Пусть терм $\mathfrak{c}_i$ получил значение $\mathfrak{z}_i$. После замены всех термов цифрами формула (3) примет вид

$$\overline{A}(0) \vee A(\mathfrak{z}_1) \& \overline{A}(\mathfrak{z}_1') \vee \ldots \vee A(\mathfrak{z}_n) \& \overline{A}(\mathfrak{z}_n') \vee A(0^{(n+1)}). \tag{4}$$

Можно предположить, что все цифры $\mathfrak{z}_i$ различны между собой. Если бы две цифры $\mathfrak{z}_p$ и $\mathfrak{z}_q$ оказались равными, то в формуле (4) нашлись бы два одинаковых слагаемых $A(\mathfrak{z}_p) \& \overline{A}(\mathfrak{z}_p')$ и $A(\mathfrak{z}_q) \& \overline{A}(\mathfrak{z}_q')$. Но после зачеркивания в формуле алгебры высказываний одного из двух одинаковых слагаемых получается формула, эквивалентная прежней.

Формула (4), как формула алгебры высказываний, должна принимать значение *И* при всех значениях входящих логических переменных

$$A(0),\ A(\mathfrak{z}_1),\ A(\mathfrak{z}_1'),\ \ldots,\ A(\mathfrak{z}_n),\ A(\mathfrak{z}_n'),\ A(0^{(n+1)}).$$

Иначе говоря, эта формула, рассмотренная как формула алгебры высказываний, должна быть тождественно истинной. Если бы это было так, то формула

$$\overline{A}(0) \vee A(\mathfrak{z}_1) \vee \ldots \vee A(\mathfrak{z}_n) \vee A(0^{(n+1)}),$$

которая является множителем конъюнктивной нормальной формы формулы (4), также была бы тождественно истинной. Но, как известно, это может быть только в том случае, если в формулу в качестве слагаемых входят какая-то логическая переменная и ее отрицание. А это может случиться только если одна из цифр $\mathfrak{z}_i$ равна 0. Пусть, например, $\mathfrak{z}_1 = 0$. Рассмотрим другой множитель конъюнктивной нормальной формы формулы (4):

$$\overline{A}(0) \vee \overline{A}(0') \vee A(\mathfrak{z}_2) \vee \ldots \vee A(\mathfrak{z}_n) \vee A(0^{(n+1)}).$$

Эта формула также должна быть тождественно истинной. Поэтому одна из цифр $\mathfrak{z}_2, \ldots, \mathfrak{z}_n$ должна быть $0'$. Пусть это $\mathfrak{z}_2$. Рассуждая таким же образом далее, мы получим, что цифры $\mathfrak{z}_1, \ldots, \mathfrak{z}_n$ должны быть соответственно $0, 0', \ldots, 0^{(n-1)}$. Рассмотрим, наконец, следующий множитель конъюнктивной нормальной формы формулы (4):

$$\bar{A}(0) \vee \bar{A}(0') \vee \ldots \vee \bar{A}(0^{(n-1)}) \vee A(0^{(n+1)}).$$

Этот множитель уже никак не может быть тождественно истинной формулой. Следовательно, формула (4), а значит, и формула (3) не могут быть примитивно истинными в слабом смысле. Следовательно, формула (1), т. е. аксиома полной индукции, не является слабо регулярной. Но тогда в силу теоремы 2 § 9 аксиома полной индукции не выводима из остальных аксиом арифметики, что и требовалось доказать.

Из приведенного нами доказательства независимости аксиомы полной индукции от других аксиом арифметики можно усмотреть, что утверждение о независимости этой аксиомы может быть усилено и распространено на тот случай, когда, кроме рекурсивных термов, в исчислении содержатся и другие термы. Все наши рассуждения, во всяком случае, останутся в силе, если мы включим в арифметику любые термы, связав их как угодно отношениями $=$ и $<$, т. е. введя для них дополнительные аксиомы вида $\mathfrak{c} = \mathfrak{g}$ и $\mathfrak{c} < \mathfrak{g}$. При этом мы предполагаем, что каждому терму при произвольной замене его переменных цифрами можно поставить в соответствие определенную цифру так, чтобы все вновь введенные аксиомы удовлетворялись. В этом случае новые аксиомы примитивно истинны в слабом смысле, и, следовательно, все формулы, выводимые в новом исчислении, слабо регулярны. Доказательство же того, что аксиома полной индукции не может быть слабо регулярной, никак не связано с природой термов и потому сохраняется для нового исчисления.

§ 12. Усиленная теорема о независимости аксиомы полной индукции

З а м е ч а н и е. Теорема дедукции, которую мы формулировали в § 4 главы V для расширенного исчисления предикатов, остается справедливой и для ограниченной арифметики. Мы дальше используем эту теорему в следующей форме.

Если формула $\mathfrak{B}$ выводима из формулы $\mathfrak{A}$ в ограниченной арифметике и при этом выводе не производится подстановка в свободные предметные переменные и переменные предикаты, входящие в формулу $\mathfrak{A}$, и не производится связывания квантором таких переменных, то формула $\mathfrak{A} \to \mathfrak{B}$ выводима в ограниченной арифметике.

В самом деле, если формула $\mathfrak{B}$ выводима из $\mathfrak{A}$ в ограниченной арифметике, то это значит, что она выводима из аксиом расширенного исчисления предикатов, аксиом собственно арифметики, к которым мы причисляем рекурсивные равенства, и формулы $\mathfrak{A}$. При этом аксиомы собственно арифметики можно заменить формулами, в которых все предметные переменные связаны. Для этого достаточно связать в них все предметные переменные кванторами всеобщности. Сохраним за полученными формулами название аксиом собственно арифметики (переменных высказываний и предикатов эти формулы также не содержат, так как их не содержали сами арифметические аксиомы, из которых они преобразованы). Пусть

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_p$$

— аксиомы собственно арифметики, которые потребовались для вывода формулы $\mathfrak{B}$. В таком случае формула $\mathfrak{B}$ выводима из формулы

$$\mathfrak{A} \,\&\, \mathfrak{A}_1 \,\&\, \ldots \,\&\, \mathfrak{A}_p$$

средствами расширенного исчисления предикатов. При выводе формулы $\mathfrak{B}$ подстановки в свободные переменные последней формулы и связывания квантором предметных переменных можно избежать, так как с переменными формулы $\mathfrak{A}$ они не производились, а формулы $\mathfrak{A}_1, \ldots, \mathfrak{A}_p$ свободных переменных не содержат. Таким образом, условия теоремы дедукции выполнены, и мы можем заключить, что формула

$$\mathfrak{A} \,\&\, \mathfrak{A}_1 \,\&\, \ldots \,\&\, \mathfrak{A}_p \to \mathfrak{B}$$

выводима в расширенном исчислении предикатов. В таком случае в расширенном исчислении предикатов выводима эквивалентная формула

$$\mathfrak{A}_1 \,\&\, \ldots \,\&\, \mathfrak{A}_p \to (\mathfrak{A} \to \mathfrak{B}).$$

Но формула $\mathfrak{A}_1 \& \ldots \& \mathfrak{A}_p$, очевидно, выводима в ограниченной арифметике. Поэтому формула

$$\mathfrak{A} \to \mathfrak{B}$$

также выводима в ограниченной арифметике.

Теорема *Если к аксиомам ограниченной арифметики присоединим в качестве аксиом любые формулы арифметики* $\mathfrak{A}_1, \ldots, \mathfrak{A}_m$, *не содержащие переменных предикатов, то либо полученное исчисление противоречиво, либо аксиома полной индукции в нем невыводима.*

Заметим, что формулы $\mathfrak{A}_1, \ldots, \mathfrak{A}_m$ можно предполагать не содержащими переменных высказываний. В самом деле, пусть формула $\mathfrak{A}_i$ содержит переменное высказывание A. Запишем ее в виде $\mathfrak{A}_i(A)$. Можно показать, что формула $\mathfrak{A}_i(A)$ дедуктивно эквивалентна формуле $\mathfrak{A}_i(\mathfrak{R}) \& \mathfrak{A}_i(\mathfrak{F})$, где $\mathfrak{R}$ — произвольная истинная, а $\mathfrak{F}$ — произвольная ложная формула. Утверждение это в одну сторону очевидно [из $\mathfrak{A}_i(A)$ выводима $\mathfrak{A}_i(\mathfrak{R}) \& \mathfrak{A}_i(\mathfrak{F})$]. Обратное утверждение легко доказать, начиная от элементарных формул, индукцией по конструкции формул *).

Итак, можно предполагать, что аксиомы $\mathfrak{A}_1, \ldots, \mathfrak{A}_m$ не содержат переменных высказываний. Точно так же можно предполагать, что в этих аксиомах нет свободных предметных переменных, так как формулы $\mathfrak{A}(x)$ и $\forall x\, \mathfrak{A}(x)$ в ограниченной арифметике дедуктивно эквивалентны. Допустим, что из аксиом ограниченной арифметики и аксиом $\mathfrak{A}_1, \ldots, \mathfrak{A}_m$ выведена аксиома полной индукции. Тогда на основании теоремы дедукции в ограниченной арифметике выводима формула

$$\mathfrak{A}_1 \& \mathfrak{A}_2 \& \ldots \& \mathfrak{A}_m \to \mathfrak{B},$$

где $\mathfrak{B}$ — аксиома полной индукции. Запишем эту формулу в приведенной форме, заменив формулы $\mathfrak{A}_i$ и $\mathfrak{B}$ их приведенными формами; при этом мы оставим за

---

*) Пусть $\mathfrak{A}(A)$ есть A. Так как $\mathfrak{R} \& \mathfrak{F}$ — ложная формула, то из нее выводима любая формула, в частности A. Далее доказывается, что если утверждение верно для формул $\mathfrak{A}$, $\mathfrak{A}_1$, $\mathfrak{A}_2$, то оно верно для $\overline{\mathfrak{A}}$, $\mathfrak{A}_1 \& \mathfrak{A}_2$, $\mathfrak{A}_1 \vee \mathfrak{A}_2$, $\forall x\, \mathfrak{A}(x)$, $\exists x\, \mathfrak{A}(x)$.

приведенными формами этих формул прежние обозначения. Тогда наша формула примет следующий вид:

$$\mathfrak{A}_1^- \vee \mathfrak{A}_2^- \vee \ldots \vee \mathfrak{A}_m^- \vee \mathfrak{B}. \tag{1}$$

На основании теоремы 2 § 9 формула (1) регулярна. Докажем, что *в таком случае формула*

$$\mathfrak{A}_1^- \vee \ldots \vee \mathfrak{A}_m^- \tag{2}$$

также регулярна.

Пусть $\mathfrak{K}_0, \ldots, \mathfrak{K}_q$ — цепочка регулярности формулы (1), так что $\mathfrak{K}_q$ совпадает с формулой (1). Формула $\mathfrak{B}$, как мы выше видели, имеет вид

$$\overline{A}(0) \vee \exists x\,(A(x) \,\&\, \overline{A}(x')) \vee A(y).$$

Можно предположить, что переменная y не входит в формулу (2). Поэтому, если мы в каждой формуле $\mathfrak{K}_i$ заменим y цифрой $0^{(n+1)}$, то получим цепочку регулярности

$$\mathfrak{H}_0,\ \mathfrak{H}_1,\ \ldots,\ \mathfrak{H}_q,$$

где $\mathfrak{H}_q$ есть формула

$$\mathfrak{A}_1^- \vee \ldots \vee \mathfrak{A}_m^- \vee \overline{A}(0) \vee \exists x\,(A(x) \,\&\, \overline{A}(x')) \vee A\left(0^{(n+1)}\right).$$

Чтобы доказать регулярность (2), мы покажем, что из всех внешних множителей любой формулы $\mathfrak{H}_i$ можно, без потери регулярности, удалить все слагаемые, которые либо входят в $\mathfrak{B}$, либо произошли от $\mathfrak{B}$ в результате применения операций 1, 2, 3. Сначала докажем, что это утверждение справедливо для $\mathfrak{H}_0$. Все внешние множители $\mathfrak{H}_0$ элементарно регулярны и могут быть представлены в виде

$$\mathfrak{B}_0' \vee \mathfrak{B}_0'' \vee \mathfrak{A}_0 \vee \mathfrak{A}_0',$$

где $\mathfrak{B}_0'$ — сумма примитивных слагаемых, происшедших от $\mathfrak{B}$; $\mathfrak{B}_0''$ — сумма остальных слагаемых, происшедших от $\mathfrak{B}$; $\mathfrak{A}_0$ — сумма примитивных слагаемых, не вошедших в $\mathfrak{B}_0'$; $\mathfrak{A}_0'$ — сумма всех остальных слагаемых. Тогда формула $\mathfrak{B}_0' \vee \mathfrak{A}_0$ примитивно истинна в сильном смысле. Рассмотрим подробнее формулу $\mathfrak{B}_0'$. Эта формула содержит слагаемые, происшедшие от $\mathfrak{B}$. Но, как мы видели выше (§ 11), к $\mathfrak{B}$ и ко всем происшедшим от него членам возможно применение только операции 2, всегда производимой над слагаемым

$$\exists x\,(A(x)\,\&\,\overline{A}(x')).$$

Все отделенные члены при этих операциях имеют вид

$$A(\mathfrak{c})\,\&\,\overline{A}(\mathfrak{c}'),$$

где $\mathfrak{c}$ — произвольный терм. В таком случае формула $\mathfrak{B}'_0$ имеет вид

$$\overline{A}(0) \vee A(\mathfrak{c}_1)\,\&\,\overline{A}(\mathfrak{c}'_1) \vee \ldots \vee A(\mathfrak{c}_k)\,\&\,\overline{A}(\mathfrak{c}'_k) \vee A(0^{\prime(n+1)}).$$

Так как цифру $0^{(n+1)}$ мы выбирали произвольно, то можно предположить, что для всех внешних множителей формулы $\mathfrak{H}_0$ имеет место $k \leqslant n$. Но если бы для некоторых слагаемых k оказалось меньше, чем n, то можно было бы к полученному слагаемому $\mathfrak{B}'_0 \vee \mathfrak{B}''_0$ еще несколько раз применить операцию 2 так, чтобы число слагаемых $A(\mathfrak{c}_i)\,\&\,\overline{A}(\mathfrak{c}'_i)$ в отделенных членах было в точности равно n. Тогда формула $\mathfrak{B}'_0$ окончательно примет вид

$$\overline{A}(0) \vee A(\mathfrak{c}_1)\,\&\,\overline{A}(\mathfrak{c}'_1) \vee \ldots \vee A(\mathfrak{c}_n)\,\&\,\overline{A}(\mathfrak{c}'_n) \vee A(0^{(n+1)}).$$

Так как каждая формула $\mathfrak{B}'_0 \vee \mathfrak{A}_0$ примитивно истинна в сильном смысле, то она выводима в ограниченной арифметике. *Покажем, что в таком случае формула $\mathfrak{A}_0$ выводима в ограниченной арифметике.* Если произвести подстановку в формулу $\mathfrak{B}'_0 \vee \mathfrak{A}_0$, заменив предикат $A(t)$ произвольной формулой $\mathfrak{X}(t)$, то слагаемое $\mathfrak{A}_0$ не изменится. В самом деле, члены этого слагаемого являются слагаемыми внешнего множителя $\mathfrak{H}_0$ и происходят от слагаемого $\mathfrak{A}_1^- \vee \ldots \vee \mathfrak{A}_m^-$ формулы (1) в результате применения операций 1, 2, 3. Но формула $\mathfrak{A}_1^- \vee \ldots \vee \mathfrak{A}_m^-$, по условию, не содержит переменных предикатов. Поэтому и происшедшие из нее слагаемые внешних множителей всех формул $\mathfrak{H}_i$ не содержат никаких переменных предикатов, в частности предиката $A(\ )$. Таким образом, после указанной подстановки формула $\mathfrak{B}'_0 \vee \mathfrak{A}_0$ перейдет в формулу

$$\overline{\mathfrak{X}}(0) \vee \mathfrak{X}(\mathfrak{c}_1)\,\&\,\overline{\mathfrak{X}}(\mathfrak{c}'_1) \vee \ldots \vee \mathfrak{X}(\mathfrak{c}_n)\,\&\,\overline{\mathfrak{X}}(\mathfrak{c}'_n) \vee \mathfrak{X}(0^{(n+1)}) \vee \mathfrak{A}_0. \tag{3}$$

Выберем теперь в качестве $\mathfrak{X}(t)$ формулу

$$t=0 \vee \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0)\right) \& t=0' \vee$$
$$\vee \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0)\right) \& \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0')\right) \& t=0'' \vee \ldots$$
$$\ldots \vee \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0)\right) \& \ldots \& \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0^{(n-1)})\right) \& t=0^{(n)},$$

где знак $\sum$ обозначает логическую сумму.

Нетрудно видеть, что формулы $\mathfrak{X}(0)$ и $\overline{\mathfrak{X}}(0^{(n+1)})$ выводимы в ограниченной арифметике. Покажем, что все формулы

$$\overline{\mathfrak{X}(\mathfrak{c}_j) \& \overline{\mathfrak{X}}(\mathfrak{c}_j')}, \qquad j=1,\ 2,\ \ldots,\ n,$$

также выводимы в ограниченной арифметике.

Рассмотрим формулу $\mathfrak{X}(\mathfrak{c}_j)$, т. е.

$$\mathfrak{c}_j=0 \vee \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0)\right) \& \mathfrak{c}_j=0' \vee \ldots$$
$$\ldots \vee \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0)\right) \& \ldots \& \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0^{(n-1)})\right) \& \mathfrak{c}_j=0^{(n)}. \qquad (4)$$

Формула $\overline{\mathfrak{X}}(\mathfrak{c}_j')$, очевидно, эквивалентна формуле

$$\overline{\mathfrak{c}_j'=0} \& \left(\prod_{i=1}^{n}\overline{(\mathfrak{c}_i=0)} \vee \overline{\mathfrak{c}_j'=0'}\right) \& \ldots$$
$$\ldots \& \left(\prod_{i=1}^{n}\overline{(\mathfrak{c}_i=0)} \vee \ldots \vee \prod_{i=1}^{n}\overline{(\mathfrak{c}_i=0^{(n-1)})} \vee \overline{(\mathfrak{c}_j'=0^{(n)})}\right), \qquad (5)$$

где знак $\prod$ обозначает логическое произведение.

Выведем некоторые формальные следствия из формул (4) и (5), которые мы получим с помощью всех выводимых формул и правил ограниченной арифметики. Из формулы (4) таким способом выводима формула

$$\sum_{i=1}^{n}(\mathfrak{c}_i=0) \vee \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0)\right) \& \mathfrak{c}_j=0' \vee \ldots$$
$$\ldots \vee \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0)\right) \& \ldots \& \left(\sum_{i=1}^{n}(\mathfrak{c}_i=0^{(n-1)})\right) \& \mathfrak{c}_j=0^{(n)}. \qquad (6)$$

Формула (6) получается из формулы (4) присоединением к ней новых слагаемых $\mathfrak{c}_i = 0$, $i \neq j$. Из формулы (6) выводима формула

$$\sum_{i=1}^{n} (\mathfrak{c}_i = 0).$$

Действительно, рассмотрим выводимую формулу исчисления высказываний

$$A_1 \vee A_1 \,\&\, B_1 \vee \ldots \vee A_1 \,\&\, B_{n-1} \rightarrow A_1.$$

Заменив A_1 на $\sum_{i=1}^{n} (\mathfrak{c}_i = 0)$, а B_l соответствующим выражением, с тем чтобы в посылке получить формулу (6), мы получаем выводимую формулу:

$$\sum_{i=1}^{n} (\mathfrak{c}_i = 0) \vee \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0)\right) \& \, \mathfrak{c}_j = 0' \vee \ldots$$
$$\ldots \vee \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0)\right) \& \ldots \& \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0^{(n-1)})\right) \&$$
$$\& \, \mathfrak{c}_j = 0^{(n)} \rightarrow \sum_{i=1}^{n} (\mathfrak{c}_i = 0).$$

Применив правило заключения, находим, что формула $\sum_{i=1}^{n} (\mathfrak{c}_i = 0)$ выводима из формулы (6), следовательно, и из формулы (4). Из формулы (5) выводима формула

$$\prod_{i=1}^{n} \overline{(\mathfrak{c}_i = 0)} \vee \overline{(\mathfrak{c}'_j = 0')}.$$

Первое слагаемое этой формулы эквивалентно формуле

$$\overline{\sum_{i=1}^{n} (\mathfrak{c}_i = 0)}.$$

В таком случае выводима формула

$$\sum_{i=1}^{n} (\mathfrak{c}_i = 0) \rightarrow \overline{\mathfrak{c}'_j = 0'}.$$

Применив правило заключения, находим, что из формул (4) и (5) выводима формула

$$\overline{\mathfrak{c}_j' = 0'}.$$

Формула

$$\overline{(\mathfrak{c}_j' = 0')} \to \overline{(\mathfrak{c}_j = 0)}$$

выводима в ограниченной арифметике. Поэтому формула

$$\overline{\mathfrak{c}_j = 0}$$

также выводима из формул (4) и (5). Из нее и из формулы (4) можно вывести формулу

$$\left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0)\right) \& \ \mathfrak{c}_j = 0' \vee \ldots$$
$$\ldots \vee \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0)\right) \& \ldots \& \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0^{(n-1)})\right) \& \ \mathfrak{c}_i = 0^{(n)}.$$

Для вывода достаточно отбросить у формулы (4) ложное слагаемое $\mathfrak{c}_j = 0$. Далее, вынося в полученной формуле за скобку множитель $\sum_{i=1}^{n} (\mathfrak{c}_i = 0)$, получим формулу

$$\left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0)\right) \& \left(\mathfrak{c}_j = 0' \vee \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0')\right) \& \ \mathfrak{c}_j = 0'' \vee \ldots\right.$$
$$\left.\ldots \vee \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0')\right) \& \ldots \& \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0^{(n-1)})\right) \& \ \mathfrak{c}_j = 0^{(n)}\right)$$

и, отбрасывая первый множитель,

$$(\mathfrak{c}_j = 0') \vee \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0')\right) \& \ \mathfrak{c}_j = 0'' \vee \ldots$$
$$\ldots \vee \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0')\right) \& \ldots \& \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0^{(n-1)})\right) \& \ \mathfrak{c}_j = 0^{(n)}. \quad (7)$$

Из формулы (7) можно, далее, вывести формулу

$$\sum_{i=1}^{n} (\mathfrak{c}_i = 0')$$

совершенно тем же приемом, как выше из (6) была выведена формула $\sum_{i=1}^{n}(\mathfrak{c}_i = 0)$. Из формулы (5) можно вывести формулу

$$\prod_{i=1}^{n} \overline{(\mathfrak{c}_i = 0')} \vee \overline{\mathfrak{c}_j' = 0''}.$$

Действительно, из (5) непосредственно выводима формула

$$\prod_{i=1}^{n} \overline{(\mathfrak{c}_i = 0)} \vee \prod_{i=1}^{n} \overline{(\mathfrak{c}_i = 0')} \vee \overline{\mathfrak{c}_j' = 0''}.$$

Первое слагаемое можно отбросить, так как оно ложно. В самом деле, $\prod_{i=1}^{n} \overline{(\mathfrak{c}_i = 0)}$ совпадает с $\overline{\sum_{i=1}^{n} (\mathfrak{c}_i = 0)}$, а формула $\sum_{i=1}^{n}(\mathfrak{c}_i = 0)$, как мы видели, выводима из (4) и (5). Далее так же, как мы выше вывели формулу $\overline{\mathfrak{c}_j = 0}$, выведем формулу

$$\overline{\mathfrak{c}_j = 0'}.$$

После этого, отбросив от формулы (7) первое ложное слагаемое, получим формулу

$$\left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0')\right) \& \; \mathfrak{c}_j = 0'' \vee \ldots$$

$$\ldots \vee \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0')\right) \& \ldots \& \left(\sum_{i=1}^{n} (\mathfrak{c}_i = 0^{(n-1)})\right) \& \; \mathfrak{c}_j = 0^{(n)}. \quad (8)$$

Продолжая далее те же рассуждения, мы получим следующие выводимые из формул (4) и (5) формулы:

$$\sum_{i=1}^{n} (\mathfrak{c}_i = 0), \quad \overline{\mathfrak{c}_j = 0}; \quad \sum_{i=1}^{n} (\mathfrak{c}_i = 0'), \quad \overline{\mathfrak{c}_j = 0'}; \ldots$$

$$\ldots; \quad \sum_{i=1}^{n} (\mathfrak{c}_i = 0^{(n-1)}), \quad \overline{\mathfrak{c}_j = 0^{(n-1)}}.$$

Из них, очевидно, выводимы формулы

$$\sum_{i \neq j} (\mathfrak{c}_i = 0); \quad \sum_{i \neq j} (\mathfrak{c}_i = 0'); \ldots; \sum_{i \neq j} (\mathfrak{c}_i = 0^{(n-1)}). \quad (9)$$

Произведение всех формул (9) также выводимо из (4) и (5):

$$\left(\sum_{i\neq j}(\mathfrak{c}_i=0)\right)\&\left(\sum_{i\neq j}(\mathfrak{c}_i=0')\right)\&\ldots\&\left(\sum_{i\neq j}(\mathfrak{c}_i=0^{(n-1)})\right). \quad (10)$$

Рассмотрим дизъюнктивную нормальную форму формулы (10). Она также выводима из (4) и (5) и имеет вид

$$\sum_{i_1\neq j,\ \ldots,\ i_n\neq j}\left(\mathfrak{c}_{i_1}=0\right)\&\left(\mathfrak{c}_{i_2}=0'\right)\&\ldots\&\left(\mathfrak{c}_{i_n}=0^{(n-1)}\right). \quad (11)$$

Однако каждое слагаемое этой суммы является ложным в ограниченной арифметике. В самом деле, каждый индекс $i_1, \ldots, i_n$ может принять только $n-1$ значений:

$$1,\ 2,\ \ldots,\ j-1,\ j+1,\ \ldots,\ n.$$

Поэтому в каждом слагаемом формулы (11) по крайней мере два из индексов $i_1, i_2, \ldots, i_n$ принимают одинаковое значение. Пусть индексы i_r и i_s некоторого слагаемого приняли значение $\mathfrak{r}$. В таком случае в это слагаемое входят два множителя:

$$\mathfrak{c}_\mathfrak{r}=0^{(p-1)} \quad \text{и} \quad \mathfrak{c}_\mathfrak{r}=0^{(q-1)}, \quad p\neq q.$$

Формула

$$\left(\mathfrak{c}_\mathfrak{r}=0^{(p-1)}\right)\&\left(\mathfrak{c}_\mathfrak{r}=0^{(q-1)}\right)\to 0^{(p-1)}=0^{(q-1)}$$

выводима в ограниченной арифметике. Но формула $0^{(p-1)}=0^{(q-1)}$ ложна, так как $p\neq q$, следовательно, и формула

$$\left(\mathfrak{c}_\mathfrak{r}=0^{(p-1)}\right)\&\left(\mathfrak{c}_\mathfrak{r}=0^{(q-1)}\right)$$

ложна. Но тогда и все произведение

$$\left(\mathfrak{c}_{i_1}=0\right)\&\left(\mathfrak{c}_{i_2}=0'\right)\&\ldots\&\left(\mathfrak{c}_{i_n}=0^{(n-1)}\right)$$

ложно. Если обозначить формулу (11) буквой $\mathfrak{C}$, то формула $\overline{\mathfrak{C}}$ выводима в ограниченной арифметике. Так как $\mathfrak{C}$ выводима из выводимых формул ограниченной арифметики и формул (4) и (5), то она, следовательно, выводима из эквивалентных (4) и (5) формул $\mathfrak{X}(\mathfrak{c}_j)$ и $\mathfrak{X}(\mathfrak{c}_j')$. При этом выводе $\mathfrak{C}$ мы не прибегали к правилу подстановки в переменные исходной формулы и не связывали их кванторами. В таком случае, применив теорему дедукции, получаем, что в расширенном исчислении предикатов выводима формула

$$\mathfrak{X}(\mathfrak{c}_j) \,\&\, \overline{\mathfrak{X}}(\mathfrak{c}'_j) \to \mathfrak{C},$$

а следовательно, и формула

$$\overline{\mathfrak{C}} \to \overline{\mathfrak{X}(\mathfrak{c}_j) \,\&\, \overline{\mathfrak{X}}(\mathfrak{c}'_j)}.$$

Но так как формула $\overline{\mathfrak{C}}$ выводима в ограниченной арифметике, то и формула

$$\overline{\mathfrak{X}(\mathfrak{c}_j) \,\&\, \overline{\mathfrak{X}}(\mathfrak{c}'_j)}$$

также в ней выводима. Итак, для каждого индекса j от 1 до n слагаемое

$$\mathfrak{X}(\mathfrak{c}_j) \,\&\, \overline{\mathfrak{X}}(\mathfrak{c}'_j)$$

формулы (3) ложно в ограниченной арифметике. Так как, по доказанному выше, формулы $\overline{\mathfrak{X}}(0)$ и $\mathfrak{X}(0^{(n+1)})$ также ложны в ограниченной арифметике, то все слагаемые формулы (3), за исключением $\mathfrak{A}_0$, ложны, следовательно, формула $\mathfrak{B}'_0$ не выводима в нашем исчислении. Но так как формула (3) выводима в ограниченной арифметике, то, следовательно, $\mathfrak{A}_0$ в ней также выводима.

Итак, если в каждом внешнем множителе формулы $\mathfrak{H}_0$ удалить слагаемые $\mathfrak{B}'_0$ и $\mathfrak{B}''_0$, то оставшиеся слагаемые образуют выводимые в ограниченной арифметике формулы. Таким образом, мы показали, что, удалив из внешних множителей $\mathfrak{H}_0$ слагаемые, происшедшие из $\mathfrak{B}$, мы получим выводимые в ограниченной арифметике, следовательно, регулярные формулы.

Допустим, что это утверждение верно для формулы $\mathfrak{H}_{i-1}$, и покажем, что тогда оно верно для $\mathfrak{H}_i$. Пусть $\mathfrak{G}_i$ — произвольный внешний множитель $\mathfrak{H}_i$, а $\mathfrak{G}'_i$ — формула, полученная из $\mathfrak{G}_i$ после удаления слагаемых, происшедших из $\mathfrak{B}$. Если операция, посредством которой $\mathfrak{H}_{i-1}$ получено из $\mathfrak{H}_i$, производится над слагаемым, происшедшим из $\mathfrak{B}$, то множитель $\mathfrak{G}'_i$ может быть также получен удалением из некоторого происшедшего из $\mathfrak{G}_i$ внешнего множителя $\mathfrak{G}_{i-1}$ формулы $\mathfrak{H}_{i-1}$ слагаемых, происшедших из $\mathfrak{B}$. Поэтому, по индуктивному предположению, $\mathfrak{G}'_i$ представляет собой регулярную формулу. Пусть теперь операция, переводящая $\mathfrak{H}_i$ в $\mathfrak{H}_{i-1}$, производится над слагаемым, происшедшим не из $\mathfrak{B}$. Удалим из $\mathfrak{G}_i$ и $\mathfrak{G}_{i-1}$ слагаемые, происшедшие из $\mathfrak{B}$, и полученные формулы обозначим $\mathfrak{G}'_i$ и $\mathfrak{G}'_{i-1}$ (в случае, когда к множителю $\mathfrak{G}_i$ применяется операция 3, под $\mathfrak{G}_{i-1}$ будем подразумевать произведение всех внешних множителей формулы $\mathfrak{H}_{i-1}$, происшедших из $\mathfrak{G}_i$). Очевидно, что формула $\mathfrak{G}'_{i-1}$ получается из $\mathfrak{G}'_i$ той же операцией, что и формула $\mathfrak{G}_{i-1}$ из $\mathfrak{G}_i$. В силу индуктивного предположения формула $\mathfrak{G}'_{i-1}$ регулярна. Но тогда и $\mathfrak{G}'_i$ регулярна. Итак, мы показали, что формулы, полученные в результате удаления из внешних множителей $\mathfrak{H}_i$ слагаемых, происшедших из $\mathfrak{B}$, остаются регулярными. В таком случае это утверждение верно и для формулы $\mathfrak{H}_q$, состоящей из единственного внешнего множителя

$$\mathfrak{A}_1^- \vee \mathfrak{A}_2^- \vee \ldots \vee \mathfrak{A}_m^- \vee \mathfrak{B},$$

т. е. мы доказали, что формула $\mathfrak{A}_1^- \vee \ldots \vee \mathfrak{A}_m^-$ *регулярна.* Но тогда в силу свойства 4 § 5 эта формула выводима в ограниченной арифметике. Так как $\mathfrak{A}_i^-$ эквивалентна $\overline{\mathfrak{A}_i}$, то и формула

$$\overline{\mathfrak{A}_1} \vee \ldots \vee \overline{\mathfrak{A}_m}$$

выводима в ограниченной арифметике. Но эта формула эквивалентна формуле

$$\overline{\mathfrak{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_m}.$$

Тем самым мы получили противоречие, так как в нашем исчислении оказались выводимыми формулы

$$\mathfrak{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_m \quad \text{и} \quad \overline{\mathfrak{A}_1 \mathbin{\&} \ldots \mathbin{\&} \mathfrak{A}_m}.$$

Итак, предположив, что в исчислении, полученном после присоединения к аксиомам ограниченной арифметики формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_m$, выводима аксиома полной индукции, мы показали, что это исчисление противоречиво. Тем самым теорема доказана.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Аксиом система 139
— — для натурального ряда 150
— — интерпретируемая (содержательно непротиворечивая) 139
— — неинтерпретируемая (содержательно противоречивая) 139
— — непротиворечивая 140
Аксиома 10, 72
Алгебра Буля 45
— высказываний 36
Арифметика ограниченная 298
Ассоциативность сложения 331

Бесконечность актуальная 15
— потенциальная 19

Вывод формальный 27
Вынесение квантора всеобщности 343
— — существования 369
Высказывание переменное 67, 126, 184
— примитивно истинное 339
— — ложное 339
— элементарное 127

Гёделя теорема 264

Дедукции теорема 82, 218, 290
Дизъюнкция 67
Дополнение 133

Зависимость аксиомы от других аксиом системы 141
Заключения правило 73, 77, 193
— — сложное 79
Закон двойственности 48, 237
— дистрибутивности умножения относительно сложения 333
Законы дистрибутивные алгебры высказываний 44
Замены свободной предметной переменной правило 198

Изоморфизм областей 145
— —, сохраняющий предикаты 146
Импликация 38, 67
Интерпретация 12
— системы аксиом 139
Исключенного третьего закон 15
Исчисление 27
— высказываний 67
— предикатов расширенное 282

Квантор всеобщности 128, 185
— — ограниченный 163, 313
— существования 129, 185
— — ограниченный 163, 313
Кванторы внешние 342, 369
— двойственные 129
Коллизия переменных 190
Коммутативность сложения 329
Константа предметная 280
— рекурсивная 298
Конъюнкция 67

Лёвенгейма теорема 172, 179

Мальцева теорема 254
Металогика 28
Множества равномощные 172
Множество вполне упорядоченное 138
— несчетное 172
— счетное 172
— упорядоченное 138
Множители внешние 343, 369
Множитель простой 337
Монотонность 87

Независимость аксиом 112, 141
— — внутренняя 141
Непротиворечивость 18
— внутренняя 140
— исчисления высказываний 108
— — предикатов 209

Область 126, 132
— действия квантора 188
— предметная 126
Операции двойственные 47
— дистрибутивные алгебры высказываний 44
Операция дистрибутивная в теории доказательств 344, 370
Отделение от квантора всеобщности 369
— — — существования 344
Отношение 125
— порядка 138
Отрицание 38, 67

Переименования связанных предметных переменных правило 198
Переменная предметная 126
— свободная 129, 184
— связанная 129, 184, 185
Перестановки посылок правило 84
Подобие упорядоченных множеств 151
Подстановка в формулу 78
— — — сложная 78
— формулы в переменную 194, 196, 197
Подстановки операция 24, 75
— правило 73, 76, 77, 193, 281
Полной индукции аксиома (принцип) 25, 26, 150, 291
Полнота в узком смысле 111, 209
— — широком смысле 110, 261
— системы аксиом 148
— — — для натурального ряда 153
— — — содержательная (с точностью до изоморфизма) 149
Порядка аксиомы 291
Постоянная предметная 126
Посылка 38
Правило вывода 27, 72
Предикат 125
— индивидуальный сложный 310
Предикат переменный 184
— рекурсивный 310
Предмет индивидуальный 126
— переменный 183
Представление двухзначной функции посредством формулы алгебры высказываний 57
Преобразование двойственное 49
Произведение теоретико-множественное 132
— элементарное 50
Противоречивость формализма (исчисления) 27, 202
Противоречия закон 25

Равенства аксиомы 282
Равенство рекурсивное 297
Разложение на простые множители 338
Разрешения проблема 18, 50, 159
Разъединения посылок правило 86
Рассуждение металогическое 29
Рефлексивности свойство 287

Свойство 125
Связывания квантором правила 200
— — производное правило 216
Силлогизма правило 84
Символ индивидуального (постоянного) предиката 139
— металогический 28
— переменного предиката 139
Симметрии свойство 287
Скобки 67
Сколема теорема 245
Слагаемое внешнее 343, 369
Слагаемое простое 338
Следование 38, 67
Следствие 38
Сложение логическое 67
Соединения посылок правило 86
Сумма теоретико-множественная 132
— элементарная 50
Существование 16

Теорема формальная 27
Теория доказательства 335
— множеств 12
Терм 29, 281
— рекурсивный 296

Тождественность 288
Транзитивности свойство 287

Умножение логическое 67
Уничтожение квантора 348

Финитизм Гильберта 26
Форма нормальная дизъюнктивная 51
— — — совершенная 60
— — для формулы исчисления предикатов 243
— — — — логики предикатов 159
— — конъюнктивная 52
— — — совершенная 62
— — Сколема 253
— приведенная 131, 234
Формализм 27
— пустой 31
Формула 27, 68, 185
— выводимая 72
— — из формул 80, 81, 217
— выполнимая 49, 159
— — на области 179
— невыполнимая 49, 159
— нормальная 155, 240
— — Сколема 244
— приведенная 131, 233
— примитивная 339
— примитивно истинная 340
— — — в слабом смысле 340
— регулярная 338, 345, 378
Формула слабо регулярная 345
— тождественно истинная 49, 159
— — ложная 49, 159
— указующая 78
— элементарная 68, 127, 184
— элементарно регурярная 345
— — — в слабом смысле 345
Формулы двойственные 47, 235
— равносильные 41, 129
— — на области 129
Функции разрешающие (функции Сколема) 174
Функция логическая 125
— общерекурсивная 325
— предметная 280
— — элементарная 280
— примитивно рекурсивная 303, 324
— эффективно вычислимая 323

Цепочка регулярности 347
Цермело теорема 138

Часть формулы 69, 70, 187
Чёрча тезис 327

Эквивалентности знак 90, 221
— отношение 287
— теорема 92
Эквивалентность 39, 90, 221, 230
— дедуктивная 243
— предикатов 310

Петр Сергеевич Новиков

Элементы математической логики

(Серия: «Математическая логика
и основания математики»)

М., 1973 г., 400 стр. с илл.

Редактор *В. В. Донченко*

Техн. редактор *К. Ф. Брудно*

Корректоры *Т. С. Плетнева, Е. Я. Строева*

Сдано в набор 30/V 1973 г.
Подписано к печати 22/XI 1973 г.
Бумага $84\times108^1/_{32}$, тип. № 1. Физ. печ. л. 12,5.
Условн. печ. л. 21. Уч.-изд. л. 18,56.
Тираж 30 000 экз. Т-17669.
Цена книги 1 р. 43 к. Заказ 662.

Издательство «Наука»
Главная редакция
физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15

Ордена Трудового Красного Знамени
Ленинградская типография № 2
имени Евгении Соколовой
Союзполиграфпрома при Государственном комитете
Совета Министров СССР по делам издательств,
полиграфии и книжной торговли
198052, Ленинград, Л-52, Измайловский проспект, 29