**Нижегородский государственный
университет им. Н.И.Лобачевского**

Механико – математический факультет

Кафедра геометрии и высшей алгебры

Е.И.Гордон

ЛЕКЦИИ ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ И ТЕОРИИ АЛГОРИТМОВ

Часть I

Нижний Новгород 1998

Typeset by $\mathcal{AMS}$-TEX

С О Д Е Р Ж А Н И Е

Предисловие 3

ГЛАВА I. ВВЕДЕНИЕ В ЛОГИКУ 4

§1. Логика высказываний 4

§2. Предикаты и кванторы 15

ГЛАВА II. Язык исчисления предикатов и его интерпретации 29

§1. Основные определения 29

§2. Предваренная нормальная форма и исключение кванторов 41

§3. Арифметика Пресбургера 46

§4. Теория Тарского 52

ГЛАВА III. Исчисление предикатов и формальные теории 63

§1. Исчисление предикатов 63

§2. Формальные теории 73

§3. Теорема Геделя о полноте и ее следствия 76

§4. Полнота и категоричность теорий 83

Литература 86

Предисловие

Настоящее учебное пособие представляет собой почти точную запись лекций по первой части курса "Теория алгоритмов и математическая логика", который автор читает для студентов 3-его курса механико-математического факультета, обучающихся по специальности "Математика". Курс читается в 6-ом семестре (3 часа лекций и 1 час практических занятий в неделю). Пособие содержит следующие разделы.

1. *Введение в логику.* Здесь излагаются основные понятия логики высказываний и логики предикатов и разбираются различные примеры записи содержательных математических предложений на языке логики предикатов. Эта часть курса существенно опирается на курс "Элементы дискретной математики и математической логики", который читается для тех же студентов на 1-ом курсе, в первом семестре. На самом деле весь материл этого раздела целесообразней излагать на первом курсе.

2. *Язык логики предикатов и его интерпретации.* Здесь дается формальное определение формул языка логики предикатов и их интерпретации в алгебраических системах. Доказывается теорема о приведении к предваренной нормальной форме и рассматривается метод исключения кванторов, который применяется для доказательства разрешимости теории плотного линейного порядка и арифметики Пресбургера. Подробно обсуждается теория Тарского и дается краткое введение в теорию o-минимальных структур.

3. *Исчисление предикатов и формальные теории.* Здесь изложен стандартный материал о формальной выводимости в исчислении предикатов, включающий теорему Геделя о полноте и ее следствия – теорему компактности Мальцева, теорему Левенгейма – Сколема – Тарского, а также теорему Вота о категоричных теориях. Демонстрируется возможность применения теоремы компактности для доказательства локальных свойств алгебраических систем. В основу изложения в этом разделе положен подход, намеченный в известной книге П.Коэна "Теория множеств и континуум – гипотеза". При этом подходе исчисление высказываний не рассматривается, а в число аксиом исчисления предикатов включены все предложения, которые получаются подстановкой в тавтологии логики высказываний произвольных предложений языка логики предикатов. По мнению автора этот подход обладает рядом методических преимуществ, в частности он позволяет добиться существенных технических упрощений при изложении теоремы Геделя о полноте.

Остальные разделы данного курса содержат основные понятия теории алгоритмов, формальную арифметику, теоремы Геделя о неполноте, введение в аксиоматическую теорию множеств. Их предполагается изложить в следующем учебном пособии.

ЛЕКЦИЯ 1

Математика изучает мир посредством построения и исследования формальных моделей тех или иных объектов или явлений. Математическая логика это наука, основными объектами исследования которой являются такие фундаментальные понятия математики, как язык, на котором формулируются математические предложения, истинность и ложность высказываний языка, доказательство и алгоритм. Таким образом можно сказать, что объектом исследования математической логики является сама математика. Поэтому математическую логику иногда называют метаматематикой. Приставка "мета" означает "над", т.е. математическая логика – надматематика.

Из сказанного ясно значение изучения этой науки, особенно для будущих учителей математики, которые должны очень отчетливо понимать, что такое доказательство и почему тот или иной текст является доказательством, а какой-то очень похожий на него текст, отличающийся иногда только порядком предложений или даже порядком слов в предложении доказательством не является. Кроме того математическая логика позволяет представить структуру математики в целом, что совершенно необходимо для ее успешного преподавания.

На самом деле именно точные формальные модели алгоритма и математического языка, возникшие в математической логике сначала исходя из чисто теоретических вопросов, вызванных к жизни внутренними потребностями развития самой математики, привели к созданию современных компьютеров и языков программирования, совершенно преобразивших повседневную жизнь практически всех людей, даже далеких от какой-либо науки. В данном курсе можно будет получить представление о том, как происходил этот процесс.

ГЛАВА I. ВВЕДЕНИЕ В ЛОГИКУ

§1. Логика высказываний

Мы начнем с исследования формальной модели языка и прежде всего займемся формализацией построения сложных предложений из простых и исследованием того, как истинность или ложность сложных предложений зависит от истинности или ложности составляющих их простых предложений.

Под высказыванием понимается предложение русского (английского, французского, etc.) языка, о котором имеет смысл говорить является оно истинным или ложным. В частности, вопросительные и повелительные предложения не являются высказываниями в нашем понимании. Как и всякое предложение высказывание может быть простым или сложным. Последние в логике высказываний принято называть составными. Сложные высказывания получаются

соединением простых при помощи союзов и других вспомогательных слов. Все их будем называть связками.

В логике высказываний выделяются следующие основные связки:

"и" – $\wedge$ ($\&$, $\cdot$) – конъюнкция;

"или" – $\vee$ – дизъюнкция;

"если ..., то ... " – $\longrightarrow$ – импликация;

"не" ("неверно, что ...") – $\neg$ – отрицание.

В дальнейшем простые высказывания обозначаются буквами $p, q, r \ldots$, возможно, с индексами. Сложные высказывания получаются из простых при помощи указанных связок. На самом деле в любом реальном языке гораздо больше связок, но перечисленных выше на самом деле достаточно, чтобы выразить большинство высказываний. Например, союз "а" в большинстве случаев играет ту же роль, что и союз "и". Так предложение: "Число 2 – простое, а 6 – составное." формально может быть записано в виде $p \wedge q$, где буквой p обозначено простое высказывание "Число 2 – простое", а буквой q – простое высказывание "Число 6 – составное".

Высказывание "Ни Север, ни Юг не победили в гражданской войне может быть записано в виде $\neg p \wedge \neg q$, где p обозначает простое высказывание "Север победил в гражданской войне", а q – простое высказывание "Юг победил в гражданской войне".

При помощи введенных связок можно выразить и существенно более сложные предложения. Рассмотрим, например, известный афоризм Козьмы Пруткова "Бросая в воду камешки, смотри на круги ими образуемые, иначе такое бросание будет пустою забавою."

Заметим, что если оставить только ту часть предложения, которая предшествует слову "иначе", то полученное предложение вообще не является высказыванием, поскольку оно есть предложение в повелительном наклонении. В целом же исходное предложение может быть переформулировано в виде: "Если ты бросаешь в воду камешки и не смотришь на круги, ими образуемые, то такое бросание – пустая забава." Теперь оно может быть формально записано при помощи наших связок в виде $(p \wedge \neg q) \longrightarrow r$, где p – "ты бросаешь камешки", q – "ты смотришь на круги, ими образуемые", r – "такое бросание – пустая забава".

Остановимся более внимательно на импликации. Запись $p \longrightarrow q$ формализует любой из следующих равнозначных оборотов речи: "если p, то q", "p влечет q", "p является достаточным условием для q", q является необходимым условием для p." Напомним для иллюстрации формулировки известных теорем математического анализа.

"Если ряд сходится, то его общий член стремится к нулю". Равносильная формулировка: "Сходимость к нулю общего члена является необходимым (но, вообще говоря, не достаточным условием) сходимости ряда".

"Если функция дифференцируема в точке, то она непрерывна в данной точке". Равносильная формулировка: "Дифференцируемость функции в точке является достаточным (но, вообще говоря, не необходимым) условием ее непрерывности в точке".

Теперь уже ясно, как сформулировать утверждение о том, что p является необходимым и достаточным условием для q ("p тогда и только тогда, когда q", "p эквивалентно q", "p равносильно q" и т.д.). Ввиду особой важности этой связки в математике, для нее вводят специальное обозначение $\longleftrightarrow$ и название "эквивалентность", хотя она и выражается через другие связки:

$$p \longleftrightarrow q \;\rightleftharpoons\; (p \longrightarrow q) \wedge (q \longrightarrow p) \tag{1.1}$$

Теперь мы в состоянии дать точное математическое определение класса составных высказываний, которые получаются из некоторого фиксированного (конечного или бесконечного) набора простых высказываний при помощи перечисленных союзов. Мы будем называть их формулами логики высказываний (ФЛВ). Будем считать, что фиксирован некоторый счетный, т.е. занумерованный натуральными числами, список $P = \{p_1, p_2, \ldots, p_n, \ldots\}$ переменных для обозначения простых высказываний. Кроме того фиксированы два символа **И** и **Л** для обозначения констант "истина" и "ложь" соответственно.

Под ФЛВ будет пониматься некоторая конечная последовательность элементов множества $S = P \cup \{\mathbf{И}, \mathbf{Л}\} \cup \{\wedge, \vee, \neg, \longrightarrow, (,)\}$, построенная по определенным правилам. Напомним из курса дискретной математики, что когда говорят о конечных последовательностях элементов множества A, то обычно само A называют алфавитом, а конечные последовательности элементов A – словами в алфавите A. Таким образом ФЛВ являются словами определенного вида в алфавите S.

Определение 1.1.

(1) Каждая переменная p из списка P есть ФЛВ.
(2) Константы **И** и **Л** есть ФЛВ
(3) Если $\mathcal{A}$ и $\mathcal{B}$ – ФЛВ, то $\neg\mathcal{A}$, $(\mathcal{A} \wedge \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \longrightarrow \mathcal{B})$ – ФЛВ.
(4) Всякая ФЛВ может быть получена по правилам 1) – 3)

Последнее условие означает, что слово A в алфавите S есть ФЛВ тогда и только тогда, когда существует последовательность $A_1, A_2, \ldots, A_n$ слов в алфавите S, такая, что $A_n = A$ и каждое A_i либо удовлетворяет одному из условий 1 или 2 определения 1.1, либо получается из предшествующих по правилу 3. Последовательность $A_1, A_2, \ldots, A_n$ называется построением формулы A, число n – длиной этого построения. Ясно, что одна и та же формула может иметь разные построения. Приведенное определение ФЛВ позволяет доказывать разные утверждения про класс всех ФЛВ индукцией по длине (минимального) построения ФЛВ. Эта индукция принимает следующий

вид. Пусть требуется доказать, что некоторое предложение справедливо для всех ФЛВ. Для этого достаточно показать, что оно верно для всех переменных и констант, и если оно верно для ФЛВ $\mathcal{A}$ и $\mathcal{B}$, то оно верно и для ФЛВ $\neg\mathcal{A}$, $(\mathcal{A} \wedge \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \longrightarrow \mathcal{B})$.

Задача*. Под формулой ФЛВ A называется такое подслово A в алфавите S, которое само является ФЛВ. Доказать, что B – подформула A тогда и только тогда, когда $B = A_i$ для некоторого построения $A_1, \ldots, A_n$ формулы A. Вывести отсюда, что при замене в ФЛВ A подформулы B произвольной формулой снова получается ФЛВ.

Заметим, что слово, стоящее справа в (1.1), формулой не является (почему?). Однако при записи ФЛВ применяются следующие правила сокращения скобок:

(1) внешние скобки опускаются
(2) сначала применяется $\neg$, затем $\wedge$, затем $\{\vee, \longrightarrow\}$.

Таким образом в формальной записи приведенного выше афоризма Козьмы Пруткова расстановка скобок не обязательна – в соответствии с указанными правилами она определена однозначно. В выражении же $p \vee q \longrightarrow r$ расстановка скобок необходима поскольку эти правила не определяют о какой из двух формул $(p \vee q) \longrightarrow r$ или $p \vee (q \longrightarrow r)$ идет речь.

Теперь мы дадим определение истинности ФЛВ. Прежде, чем это сделать приведем некоторые мотивировки.

Заметим, что каждое высказывание само по себе, как правило, не является ни истинным, ни ложным. Это существенно зависит от обстоятельств. Например, высказывание "Сегодня идет снег" истинно в какие-то дни в каких-то местах, а в другие дни или в других местах – ложно. Однако ложность или истинность составного высказывания однозначно определяется в зависимости от ложности или истинности входящих в него простых высказываний.

Таким образом в логике на составные высказывания смотрят как на функции из $\{\mathbf{И}, \mathbf{Л}\}^n$ в $\{\mathbf{И}, \mathbf{Л}\}$, где n – число простых высказываний, входящих в данное составное. В дальнейшем множество $\{\mathbf{И}, \mathbf{Л}\}$ обозначается через $\mathbb{B}$. Отметим, что бывают высказывания, истинные или ложные независимо от обстоятельств. Например, высказывание $2 \times 2 = 4$ абсолютно истинно, а высказывание "Волга впадает в Балтийское море" абсолютно ложно. С точки зрения логики высказываний все абсолютно истинные (ложные) высказывания представляют собой одно постоянное высказывание, для обозначения которого и введена константа $\mathbf{И}(\mathbf{Л})$.

Прежде всего определим, какие функции соответствуют основным логическим связкам.

Определение 1.2. Логические связки $\vee, \wedge, \longrightarrow, \longleftrightarrow$ есть бинарные опера-

ции на $\mathbb{B}$, а $\neg$ - унарная операция на $\mathbb{B}$. Они задаются следующими таблицами:

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \longrightarrow q$
И	**И**	**Л**	**И**	**И**	**И**
И	**Л**	**Л**	**Л**	**И**	**Л**
Л	**И**	**И**	**Л**	**И**	**И**
Л	**Л**	**И**	**Л**	**Л**	**И**

То, что приведенная таблица адекватно отражает естественную интерпретацию логических связок $\wedge, \vee, \neg$, не вызывает сомнений. Из таблицы видно, что связка $\vee$ интерпретируется как неразделительное "или", т.е. высказывание $p \vee q$ истинно, когда по крайней мере одно из входящих в него простых высказываний. Иногда союз "или" понимают как разделительный, т.е. высказывание "А или Б" считается истинным, когда истинно в точности одно из высказываний А и Б. Как выразить разделительное "или" через введенные связки будет показано ниже.

В некоторых пояснениях нуждается только связка $\longrightarrow$. Смысл импликации $p \longrightarrow q$ состоит в том, что из утверждения p правильно рассуждая можно вывести утверждение q. С этим связано то, что в данной импликации p иногда называют посылкой, а q – заключением. Ясно, что из истинного утверждения, правильно рассуждая, можно вывести только истинное утверждение. Из ложного же утверждения, правильно рассуждая можно вывести все, что угодно, т.е. как истинное утверждение, так и ложное утверждение.

Проиллюстрируем сказанное следующими примерами. Ниже, как обычно, $a|b$ означает, что b делится на a без остатка.

1). Высказывание $6|n \longrightarrow 3|n$ очевидно истинно при любом n. Посмотрим какие возможности реализуются при различных n. При $n = 12$ имеем **И** $\longrightarrow$ **И**, при $n = 3$ – **Л** $\longrightarrow$ **И**, при $n = 5$ – **Л** $\longrightarrow$ **Л**. Единственная не реализуемая возможность **И** $\longrightarrow$ **Л**.

2). Высказывание $A \subseteq B$ означает, что при любом x истинна импликация $x \in A \longrightarrow x \in B$. Напомним, что по определению считается, что для любого множества B $\emptyset \subseteq B$. Такое определение согласуется с тем, что в импликации $x \in \emptyset \longrightarrow x \in B$ посылка всегда ложна.

3). "Если черти существуют, то они все зеленые" – истинное высказывание.

Ниже, если ФЛВ F содержит только переменные из списка $p_1, \ldots, p_n$, то будем писать $F = F(p_1, \ldots, p_n)$.

Определение 1.3. Пусть каждой переменной p_i из списка $\{p_1, \ldots, p_n\}$ поставлено в соответствие истинностное значение $\sigma_i \in \mathbb{B}$. Тогда каждой ФЛВ

$F(p_1, \ldots, p_n)$ ставится в соответствие истинностное значение $\sigma(F) \in \mathbb{B}$ по следующему правилу:

(1) если $F = p_i$, то $\sigma(F) = \sigma_i$;
(2) если $F = \mathbf{И}(\mathbf{Л})$, то $\sigma(F) = \mathbf{И}(\mathbf{Л})$;
(3) если $\sigma(\mathcal{A})$ и $\sigma(\mathcal{B})$ уже определены, то $\sigma(\neg\mathcal{A}) = \neg\sigma(\mathcal{A})$; $\sigma(\mathcal{A} \wedge \mathcal{B}) = \sigma(\mathcal{A}) \wedge \sigma(\mathcal{B})$; $\sigma(\mathcal{A} \vee \mathcal{B}) = \sigma(\mathcal{A}) \vee \sigma(\mathcal{B})$; $\sigma(\mathcal{A} \longrightarrow \mathcal{B}) = \sigma(\mathcal{A}) \longrightarrow \sigma(\mathcal{B})$.

Ниже вместо $\sigma(F)$ при $p_1 = \sigma_1$, $p_2 = \sigma_2, \ldots$, $p_n = \sigma_n$ будем писать $F(\sigma_1, \ldots, \sigma_n)$. Это определение показывает каким образом ФЛВ определяет высказывание, т.е. функцию из $\mathbb{B}^n$ в $\mathbb{B}$. Поскольку эта функция задана на конечном множестве, можно составить ее таблицу, которая в данном случае называется *таблицей истинности*. Таблица истинности содержит 2^n строк, где n – число переменных в ФЛВ. Составим таблицу истинности для эквивалентности, пользуясь определением 1.3.

p	q	$p \longrightarrow q$	$q \longrightarrow p$	$p \longleftrightarrow q$
И	**И**	**И**	**И**	**И**
И	**Л**	**Л**	**И**	**Л**
Л	**И**	**И**	**Л**	**Л**
Л	**Л**	**И**	**И**	**И**

Ясно, что эта таблица согласуется с содержательным пониманием эквивалентности. Из нее видно также, что высказывание $\neg(p \longleftrightarrow q)$ представляет собой как раз разделительное "или".

Заметим, что функции со значениями в двухэлементном множестве изучались в курсе дискретной математики. Там это множество было $\{0, 1\}$. Установив соответствие $\mathbf{И} \longleftrightarrow 1$, $\mathbf{Л} \longleftrightarrow 0$, легко заметить, что определение операций $\neg, \wedge, \vee, \longrightarrow$ такое же, как в курсе дискретной математики. Поэтому здесь имеют место те же тождества, что и для функций алгебры логики.

Определение 1.4. ФЛВ $F(p_1, \ldots, p_n)$ и $G(p_1, \ldots, p_n)$ называются логически равносильными (обозначение $F \equiv G$), если для любых $\sigma_1, \ldots, \sigma_n \in \mathbb{B}$ имеет место равенство $F(\sigma_1, \ldots, \sigma_n) = G(\sigma_1, \ldots, \sigma_n)$. Если $F(p_1, \ldots, p_n) \equiv \mathbf{И}$, т.е. $\forall \sigma_1, \ldots, \sigma_n \in \mathbb{B} F(\sigma_1, \ldots, \sigma_n) = \mathbf{И}$, то F называется тавтологией (обозначение $\vdash F$).

Другими словами ФЛВ F и G логически равносильны, если они определяют одно и то же высказывание, т.е. если соответствующие им таблицы истинности совпадают.

Предложение 1.5. $F \equiv G \iff \vdash F \longleftrightarrow G$

Доказательство очевидно.

Теорема 1.6 (Основные тождества логики высказываний).

(1) $p \wedge q \equiv q \wedge p;\ p \vee q \equiv q \vee p$
(2) $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r;\ p \vee (q \vee r) \equiv (p \vee q) \wedge r$
(3) $p \wedge (q \vee r) \equiv p \wedge q \vee p \wedge r;\ p \vee q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
(4) $p \wedge p \equiv p;\ p \vee p \equiv p$
(5) $p \wedge \mathbf{И} \equiv p;\ p \wedge \mathbf{Л} \equiv \mathbf{Л};\ p \vee \mathbf{И} \equiv \mathbf{И};\ p \vee \mathbf{Л} \equiv p$
(6) $\neg\neg p \equiv p$
(7) $\vdash p \vee \neg p$
(8) $\neg(p \wedge q) \equiv \neg p \vee \neg q;\ \neg(p \vee q) \equiv \neg p \wedge \neg q$

Все эти тождества были доказаны в курсе дискретной математики. Доказательства очень простые – нужно составить таблицы истинности левых и правых частей и убедиться, что они совпадают.

Напомним, что тождества 8) называются законами де Моргана.

Определение 1.7. ФЛВ называется дизъюнктивной нормальной формой (ДНФ), если она является

(1) переменной, константой, или отрицанием переменной;
(2) конъюнкцией конечного числа формул типа 1;
(3) дизъюнкцией конечного числа формул типов 1 и 2.

Из курса дискретной математики известно, что любое высказывание может быть задано некоторой ДНФ. Наиболее важный для нас пример:

$$p \longrightarrow q \equiv \neg p \vee q$$

ЛЕКЦИЯ 2

Некоторые из тождеств теоремы 1.6 могут быть выведены из других посредством формальных преобразований. Кроме того, из этих основных тождеств можно выводить и другие тождества и тавтологии.

Примеры. 1). Выведем второй закон де Моргана из первого, пользуясь остальными равносильностями теоремы 1.6. В тождество

$$\neg(p \wedge q) \equiv \neg p \vee \neg q \tag{2.1}$$

подставим $\neg p$ вместо p и $\neg q$ вместо q. Получим тождество

$$\neg(\neg p \wedge \neg q) \equiv \neg\neg p \vee \neg\neg q. \tag{2.2}$$

Используя снятие двойного отрицания (тождество (6) теоремы 1.6), получим

$$\neg(\neg p \wedge \neg q) \equiv p \vee q. \tag{2.3}$$

Применив отрицание к обеим частям последней равносильности, и снова воспользовавшись снятием двойного отрицания, получи как раз второй закон де Моргана.

2). Докажем, что $\neg\mathbf{И} \equiv \mathbf{Л}$. Заменим в тождестве

$$p \wedge \mathbf{И} \equiv p \tag{2.4}$$

(тождество (4) теоремы 1.6) переменную p на $\neg q$. Получим тождество

$$\neg q \wedge \mathbf{И} \equiv \neg q. \tag{2.5}$$

Пользуясь тавтологией (7) теоремы 1.6, подставим в это тождество, $\neg p \vee p$ вместо **И**. Получим тождество

$$\neg q \wedge (\neg p \vee p) \equiv \neg q. \tag{2.6}$$

Применив теперь к обеим частям последнего тождества отрицание и воспользовавшись слева законами де Моргана, приходим к тождеству:

$$q \vee (\neg p \wedge p) \equiv q \tag{2.7}$$

Подставив в него вместо q – **Л** и воспользовавшись тождествами (4) теоремы 1.6, получим

$$p \wedge \neg p \equiv \mathbf{Л} \tag{2.8}$$

Далее в силу законов де Моргана

$$\mathbf{Л} \equiv p \wedge \neg p \equiv \neg(\neg p \vee p) \equiv \neg\mathbf{И},$$

что и требовалось. Заметим, что попутно мы доказали равносильность (2).

В процессе проведения формальных доказательств в рассмотренных примерах мы пользовались тем, что при подстановке в тождество произвольных формул вместо переменных снова получаются тождества (см., например, переход от (2.1) к (2.2)), а также тем, что при замене некоторой подформулы на эквивалентную ей формулу получается формула, равносильная исходной (см. переход от (2.2) к (2.3) или переход от (2.5) к (2.6)). Эти утверждения интуитивно совершенно очевидны. Они постоянно используются в математике, начиная со школьной алгебры, без каких-либо специальных обоснований. Однако при строго формальном подходе к математике, принятом в математической логике, они все-таки нуждаются в обосновании. По крайней мере один раз следует продемонстрировать, как подобные обоснования проводятся. Начнем с определения.

Определение 2.1. Пусть $F(p_1, \ldots, p_n)$ и $A_1, \ldots, A_n$ – ФЛВ. Тогда результатом подстановки в F формул $A_1, \ldots, A_n$ вместо переменных $p_1, \ldots, p_n$ соответственно, называется формула, обозначаемая $F(A_1, \ldots, A_n)$, которая определяется по следующим правилам:

(1) если $F(p_1, \ldots, p_n) = p_i$, то $F(A_1, \ldots, A_n) = A_i$;
(2) если $F(p_1, \ldots, p_n) = \mathbf{И}(\mathbf{Л})$, то $F(A_1, \ldots, A_n) = \mathbf{И}(\mathbf{Л})$;
(3) если $F(p_1, \ldots, p_n) = \neg G(p_1, \ldots, p_n)$ и $G(A_1, \ldots, A_n)$ определена, то $F(A_1, \ldots, A_n) = \neg G(A_1, \ldots, A_n)$;
(4) если $F(p_1, \ldots, p_n) = G(p_1, \ldots, p_n) * H(p_1, \ldots, p_n)$, где $*$ есть либо $\wedge$, либо $\vee$, либо $\longrightarrow$, а $G(A_1, \ldots, A_n)$ и $H(A_1, \ldots, A_n)$ уже определены, то $F(A_1, \ldots, A_n) = G(A_1, \ldots, A_n) * H(A_1, \ldots, A_n)$.

Предложение 2.2. *Пусть $q_1, \ldots, q_n$ – полный список переменных, входящих в формулы $A_1, \ldots, A_n$ а $\delta_1, \ldots, \delta_n \in \mathbb{B}$. Предположим, что $A_i(\delta_1, \ldots, \delta_n) = \sigma_i \in \mathbb{B}$. Тогда*

$$F(A_1(\delta_1, \ldots, \delta_n), \ldots, A_n(\delta_1, \ldots, \delta_n)) = F(\sigma_1, \ldots, \sigma_n).$$

Доказательство может быть легко выведено из определения 2.1 при помощи индукции по построению формулы.

Следствие 1. *Если $F(p_1, \ldots, p_n) \equiv G(p_1, \ldots, p_n)$, а $A_1, \ldots, A_n$ – ФЛВ, то $F(A_1, \ldots, A_n) \equiv G(A_1, \ldots, A_n)$.*

Следствие 2. *Если $A_1, \ldots, A_n$ и $B_1, \ldots, B_n$ – ФЛВ, причем $A_i \equiv B_i$, $i = 1, \ldots, n$, то $F(A_1, \ldots, A_n) \equiv F(B_1, \ldots, B_n)$.*

Следствие 1 было использовано в примере 1 при переходе от (2.1) к (2.2) и от (2.2) к (2.3), а также в примере 2 при переходе от (2.4) к (2.5) и от (2.7) к (2.8). Следствие 2 использовалось в примере 2 при переходе от (2.5) к (2.6).

Возникает вопрос, зачем нужны эти формальные доказательства, когда можно очень легко все проверить при помощи таблиц истинности, а тождество, доказанное в примере 2, есть непосредственное следствие определения отрицания. Дело в том, что выведенные формально из равносильностей теоремы 1.6 тождества верны и в более общей ситуации.

Определение 2.3. Множество $\mathcal{B}$, в котором определены две бинарные операции $\wedge$ и $\vee$, одна одноместная операция $\neg$ и выделены два элемента $\mathbf{И}, \mathbf{Л} \in \mathcal{B}$ так, что имеют место все тождества теоремы 1.6, называется алгеброй Буля или булевой алгеброй.

Таким образом множество $\mathbb{B}$ с операциями, определенными в определении 1.2, является булевой алгеброй. Кроме этой существуют и другие булевы алгебры, например, алгебра $\mathcal{P}(A)$ всех подмножеств множества A. В качестве

операции $\wedge(\vee)$ здесь берется $\cap(\cup)$, в качестве операции $\neg$ – дополнение, в качестве элемента **И** – само множество A, а в качестве элемента **Л** – $\emptyset$. Легко понять, что любая алгебра множеств есть булева алгебра. Ясно, что все тождества, формально выведенные из тождеств теоремы 1.6, истинны в любой булевой алгебре.

Тавтологии особенно важны с точки зрения оснований математики, поскольку они представляют собой формальные записи законов логики. Остановимся на некоторых из них.

1. $\vdash p \vee \neg p$. Этот закон известен в логике как закон исключенного третьего. На первый взгляд он не вызывает сомнений, однако в начале нашего века он стал подвергаться серьезной критике со стороны некоторых математиков, которых возглавил знаменитый голландский тополог Л.Э.Я.Брауэр. Критика их была связана с тем, что закон исключенного третьего позволяет доказывать существования объектов без их построения. Такие доказательства впервые появились в конце прошлого столетия и вызвали большие сомнения у многих работавших в то время математиков. Приведем один очень наглядный пример такого доказательства. Докажем следующее утверждение.

Существуют два иррациональных числа α и β, таких, что α^β рационально.

В силу закона исключенного третьего число $(\sqrt{2})^{\sqrt{2}}$ либо рационально, либо иррационально. Если оно рационально, то положив $\alpha = \beta = \sqrt{2}$, получим требуемое. Если же оно иррационально, то, положив $\alpha = (\sqrt{2})^{\sqrt{2}}$, $\beta = \sqrt{2}$, получим

$$\alpha^\beta = \left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2$$

И мы снова получили требуемое.

Приведенное доказательство совершенно корректно, однако не дает абсолютно никакой информации какие же именно числа α и β удовлетворяют требуемому условию. На самом деле иррациональным является число $(\sqrt{2})^{\sqrt{2}}$, т.е. реализуется второй вариант, но установление этого факта требует значительных усилий и ни в какой степени не использует описанное выше рассуждение.

Сомнение в корректности рассуждений подобного рода применительно к бесконечным объектам, привело Брауэра и его последователей к поиску других систем оснований математики, в которых истинность $p \vee \neg p$ признается лишь тогда, когда точно известно какой именно из членов данной дизъюнкции истинен. Это направление в основаниях математики получило название *интуиционизм*.

За закон исключенного третьего очень горячо и эмоционально вступился великий немецкий математик Д.Гильберт. Он писал: "Отнять у математика закон исключенного третьего это все равно, что отнять у боксера кулаки, у

шахтера – отбойный молоток...” В результате этой полемики Гильберт выдвинул программу обоснования математики. Это программа, как выяснилось позднее, не могла быть реализована в полной мере. Однако она сыграла исключительно важную роль в развитии математической логики и теории алгоритмов и, в конечном итоге, оказала существенное влияние на возникновение современных компьютеров. С этими вопросами мы на протяжении нашего курса познакомимся подробнее. Изучать интуиционизмом мы не будем. Отмечу только, что как программа нового обоснования математики он успехов не добился, но продолжает развиваться и сейчас как раздел оснований математики, занимающийся исследованием доказательств на конструктивность. На протяжении двух последних десятилетий обнаружились интересные связи интуиционизма с топологией и теорией пучков, которые представляются весьма перспективными. Кроме того работы интуициониста Крипке натолкнули Коэна на идеи, которые привели затем к его знаменитому результату – доказательству независимости гипотезы континуума.

2. Рассмотрим тавтологию $\vdash (p \longrightarrow q) \longleftrightarrow (\neg q \longrightarrow \neg p)$. (Формальный вывод ее из основных тождеств предлагается в качестве упражнения)

Эта тавтология представляет собой формальную запись закона логики, который называется *законом контрапозиции.* На этом законе основаны все доказательства ”от противного”.

3. Тавтология $(\neg p \longrightarrow q) \wedge (\neg p \longrightarrow \neg q) \longrightarrow p$ представляет собой формальную запись ”закона приведения к противоречию”. В доказательствах он используется следующим образом: чтобы доказать утверждение p, мы предполагаем, что оно неверно и выводим из этого предположения два взаимоисключающих утверждения. После этого утверждение p можно считать доказанным. Вспомните, например, известное доказательство иррациональности числа $\sqrt{2}$, в котором сначала предполагается, что это число рационально, после чего оно представляется в виде несократимой дроби, а затем доказывается, что эта дробь сократима. Здесь как раз используется закон приведения к противоречию.

Законы логики были впервые сформулированы знаменитым греческим философом Аристотелем (4 в. до н.э.). Операции над высказываниями, рассмотренные здесь и основные тождества для них были открыты в середине прошлого века английским математиком Джорджем Булем (отцом известной писательницы, автора романа ”Овод” – Э.Войнич). Буль построил алгебру высказываний (названную впоследствии его именем – см. определение 2.3), аналогичную алгебре чисел, что позволило получать законы логики и проверять правильность рассуждений посредством формальных вычислений. С открытия этой алгебры и начала развиваться математическая логика.

§2. Предикаты и кванторы.

Существуют такие логические рассуждения, которые не могут быть формализованы в рамках исчисления высказываний. Я ограничусь одним классическим примером такого рассуждения, входившим еще в гимназические учебники логики.

Все люди смертны. Сократ – человек. Следовательно Сократ смертен.

Корректность таких умозаключений основана не только на структуре их соединения из простых высказываний, но и на внутренней структуре самих простых предложений, в частности, на понимании таких выражений как "все", "всякий", "существует" и т.п. В подобных рассуждениях приходится иметь дело с выражениями вида $P(x)$ – "x обладает свойством P". При этом $\forall x P(x)$ означает, что свойство P выполнено для всякого предмета x, а $\exists x P(x)$ – "существует хотя бы один предмет x, обладающий свойством P. Если теперь буква s обозначает Сократа, $H(x)$ – высказывание "x – человек", $D(x)$ – "x смертен", то приведенное выше рассуждение может быть записано в виде:

$$\forall x(H(x) \longrightarrow D(x)) \wedge H(s) \longrightarrow D(s)$$

Наша задача состоит в том, чтобы научиться анализировать такие выражения.

Мы начнем, однако, не с формального, или, как еще говорят *синтаксического*, а с содержательного, или *семантического* подхода.

Выражение $P(x)$ – "предмет x обладает свойством P" – это переменное высказывание. В зависимости от того, какой предмет мы подставляем вместо x оно может быть либо истинным, либо ложным.

Например, если $P(x)$ – "x – простое число", то $P(2) = \mathbf{И}$, $P(6) = \mathbf{Л}$, $P(2^{2^4} + 1) = \mathbf{И}$, $P(2^{2^5} + 1) = \mathbf{Л}$ (это впервые установил Л. Эйлер).

Итак, если задана некоторая предметная область M, то переменное высказывание $P(x)$ можно рассматривать как функцию из M в множество $\mathbb{B} = \{\mathbf{И}, \mathbf{Л}\}$. Такие функции принято называть *предикатами*. Предикаты могут зависеть и от нескольких переменных.

Определение 2.4. n-местным предикатом на множестве M называется отображение $P : M^n \longrightarrow \mathbb{B}$. Множество M называется предметной областью, а переменные, принимающие значения в M, – предметными переменными. Множество

$$\sigma_P = \{< x_1, \ldots, x_n > \in M^n \mid P(x_1, \ldots, x_n) = \mathbf{И}\}$$

называется областью истинности предиката P.

Отметим , что для любого $C \subseteq M^n$ существует n-местный предикат P, такой, что $\sigma_P = C$, а именно,

$$P(x_1, \ldots, x_n) = \mathbf{И} \Longleftrightarrow < x_1, \ldots, x_n > \in C.$$

Иногда удобно рассматривать 0-местные предикаты, которые отождествляются с константами из $\mathbb{B}$. При этом, если 0-местный предикат $P = \mathbf{Л}$, то по определению считается, что его область истинности равна $\emptyset$, а если $P = \mathbf{И}$, то его область истинности равна $\{\emptyset\}$. Последнее соглашение связано с тем, что для любого непустого множества M по определению считается, что $M^0 = \{\emptyset\}$.

Соединяя предикаты логическими связками, можно получать новые предикаты. При этом очевидно следующее

Предложение 2.5. *Если $P(x_1, \ldots, x_n)$ и $Q(x_1, \ldots, x_n)$ – n-местные предикаты на множестве M, то*

(1) $\sigma_{P \wedge Q} = \sigma_P \cap \sigma_Q$
(2) $\sigma_{P \vee Q} = \sigma_P \cup \sigma_Q$
(3) $\sigma_{\neg P} = M^n \setminus \sigma_P$

Некоторые сложности возникают, когда исходные предикаты зависят от разных переменных. При соединении их связками получается предикат, зависящий от всех переменных, входящих в исходные предикаты. Пусть полный набор переменных, входящих в составной предикат Q есть $x_1, \ldots, x_n, y_1, \ldots, y_k$, а один из предикатов, из которых Q составлен, есть $P(x_1, \ldots, x_n)$. По предикату P составим новый предикат $P'(x_1, \ldots, x_n, y_1, \ldots, y_k)$, такой, что $P'(x_1, \ldots, x_n, y_1, \ldots, y_k) = \mathbf{И} \Longleftrightarrow P(x_1, \ldots, x_n) = \mathbf{И}$. Говорят, что P' получен из P добавлением фиктивных переменных $y_1, \ldots, y_k$. Ясно, что $\sigma_{P'} = \sigma_P \times M^k$. Проделав такую операцию со всеми, входящими в Q предикатами, получим, что Q составлен из предикатов, зависящих от одних и тех же переменных, и для определения его области истинности можно использовать предложение 2.5.

Пример 1. Пусть $P(x) \rightleftharpoons 1 \leq x \wedge x \leq 3$, $Q(y) \rightleftharpoons 2 \leq y \wedge y \leq 3$ – предикаты, определенные на $\mathbb{R}_+$. Рассмотрим предикаты $R(x, y) = P(x) \vee Q(y)$ и $S(x, y) = P(x) \wedge Q(y)$. Если предикат P' получен из P добавлением фиктивной переменной y, а предикат Q' получен из Q добавлением фиктивной переменной x. Тогда $\sigma_{P'} = \sigma_P \times \mathbb{R}_+$ (рис.1), $\sigma_{Q'} = \mathbb{R}_+ \times \sigma_Q$ (рис.2). Теперь $\sigma_R = \sigma_{P'} \cup \sigma_{Q'}$ и $\sigma_S = \sigma_{P'} \cap \sigma_{Q'}$ изображены на рисунках 3 и 4 соответственно.

Определение 2.6. Пусть $P(x_0, x_1, \ldots, x_n)$ – $(n+1)$-местный предикат на множестве M. Говорят, что n-местный предикат $Q(x_1, \ldots, x_n)$ получен из P применением квантора существования (всеобщности) по переменной x_0 и пишут

$$Q(x_1, \ldots, x_n) = \exists x_0 P(x_0, x_1, \ldots, x_n)$$

$$(Q(x_1, \ldots, x_n) = \forall x_0 P(x_0, x_1, \ldots, x_n)),$$

если для любых $u_1, \ldots, u_n \in M$ $Q(u_1, \ldots, u_n) = \mathbf{И}$ тогда и только тогда, когда найдется такое (для любого) $u \in M$, что (выполнено) $P(u, u_1, \ldots, u_n) = \mathbf{И}$

Если $Q(x_1,\ldots,x_n) = \exists x_0 P(x_0,x_1,\ldots,x_n))$, то область истинности $\sigma_Q \subseteq M^n$ предиката Q называется *проекцией* области истинности предиката $\sigma_P \subseteq M^{n+1}$ предиката P. Это определение согласуется с обычным геометрическим определением проекции в случае, когда $M = \mathbb{R}$ – см. рис. 5.

Пример 2. Пусть $P(x,y) \rightleftharpoons y = x^2$, тогда $\sigma_P \subseteq \mathbb{R}^2$ есть обычная парабола на плоскости XOY. Ее проекция на ось OY есть положительная полуось (рис.6), т.е. $\exists x(y = x^2) = y \geq 0$, что можно увидеть и из других соображений – вещественное число y является квадратом некоторого вещественного числа x тогда и только тогда, когда оно неотрицательно. Проекция параболы на ось OX совпадает со всей осью. Отсюда следует, что $\exists y(y = x^2) \equiv \mathbf{И}$. Это тоже очевидно, поскольку любое число x можно возвести в квадрат.

Пример 3. Рассмотрим трехместный предикат $P(x,y,z) \rightleftharpoons x + z = y$ на $\mathbb{R}_+$. Его область истинности есть часть плоскости $x + z = y$, расположенная в положительном октанте пространства $OXYZ$ (рис.7). Проекция этой части плоскости на положительный квадрант плоскости XOY изображена на рис.8. Из него видно, что $\exists z(x+z = y) = y \geq x$, что понятно и из других соображений: $y \geq x$ тогда и только тогда, когда $y - x \geq 0$. Заметим, что здесь существенно используется тот факт, что предметная область состоит из неотрицательных чисел. Если тот же самый предикат рассмотреть на всем $\mathbb{R}$, то его область истинности представляет собой уже всю плоскость $x + z = y$, а ее проекция вдоль оси OZ совпадает со всей плоскостью XOY, т.е. $\exists z(x + z = y) \equiv \mathbf{И}$, что тоже очевидно, поскольку в этом случае в качестве z всегда можно взять $y - x$.

Квантор всеобщности не имеет такой наглядной геометрической интерпретации, но между кванторами всеобщности и существования имеется простая связь, позволяющая, в частности, легко строить области истинности предикатов, полученных применением квантора всеобщности.

Теорема 2.7. *Пусть $P(x)$ – предикат, зависящий от переменной x и, возможно, еще от каких-нибудь переменных. Тогда имеют место равенства*

$$\neg\forall x P(x) = \exists x \neg P(x); \quad \neg\exists x P(x) = \forall x \neg P(x) \tag{1}$$

Доказательство. Пусть левая часть первого равенства истинна. Тогда $\forall x P(x) = \mathbf{Л}$ и, по определению квантора всеобщности, найдется элемент $m \in M$, такой, что $P(m) = \mathbf{Л}$. Здесь M – предметная область предиката P. Тогда $\neg P(m) = \mathbf{И}$ и, по определению квантора существования, $\exists x \neg P(x) = \mathbf{И}$.

Если правая часть первого равенства истинна, то существует $m \in M$, такой, что $\neg P(m) = \mathbf{И}$. Это означает, что $P(m) = \mathbf{Л}$ и по определению квантора всеобщности $\forall x P(x) = \mathbf{Л}$, т.е. $\neg\forall x P(x) = \mathbf{И}$. Тем самым первое равенство

доказано. Второе равенство может быть выведено из первого формально. Заменим в первом равенстве предикат P на $\neg P$. Тогда после снятия двойного отрицания, получим

$$\neg\forall x\neg P(x) = \exists x P(x)$$

Теперь, применив отрицание к обеим частям последнего равенства и сняв двойное отрицание, получим как раз второе из требуемых равенств ■

Замечание. В этом доказательстве мы всюду предполагали, что значения остальных переменных, входящих в предикат P (кроме переменной x), фиксированы.

Равенства (1) показывают, что квантор всеобщности может быть выражен через квантор существования и наоборот.

Следствие.

$$\forall x P(x) = \neg\exists x\neg P(x); \quad \exists x P(x) = \neg\forall x\neg P(x)$$

В случае бесконечной предметной области равенства (1) можно рассматривать как бесконечные аналоги законов де Моргана. В самом деле, если предметная область конечна, т.е. $M = \{a_1, a_2, \ldots, a_n\}$, то

$$\forall x P(x) = P(a_1) \wedge P(a_2) \wedge \cdots \wedge P(a_n); \ \exists x P(x) = P(a_1) \vee P(a_2) \vee \cdots \vee P(a_n)$$

и равенства (1) переходят в равенства

$$\neg(P(a_1) \wedge P(a_2) \wedge \cdots \wedge P(a_n)) = \neg P(a_1) \vee \neg P(a_2) \vee \cdots \vee \neg P(a_n);$$
$$\neg(P(a_1) \vee P(a_2) \vee \cdots \vee P(a_n)) = \neg P(a_1) \wedge \neg P(a_2) \wedge \cdots \wedge \neg P(a_n),$$

которые представляют собой обычные законы де Моргана.

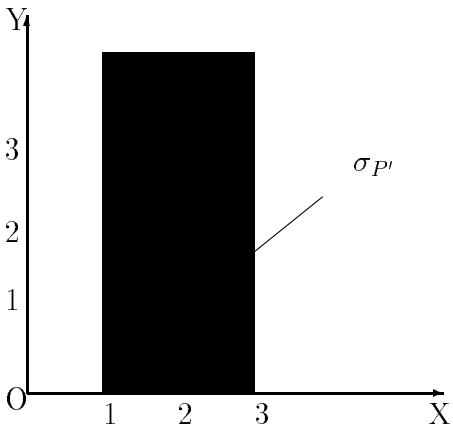
Пример 4. Найти область истинности предиката

$$\forall y(x^2 - y^2 \leq 1) \wedge \exists x(x^2 + y^2 \leq 1).$$

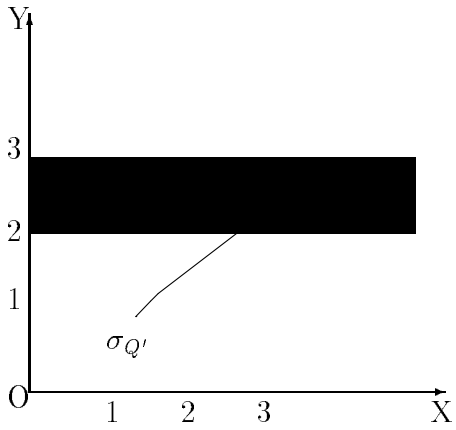
Первый из входящих в конъюнкцию предикатов зависит только от переменной x. Его область истинности есть дополнение до области истинности предиката

$$\neg\forall y(x^2 - y^2 \leq 1) = \exists y\neg(x^2 - y^2 \leq 1) = \exists y(x^2 - y^2 > 1).$$

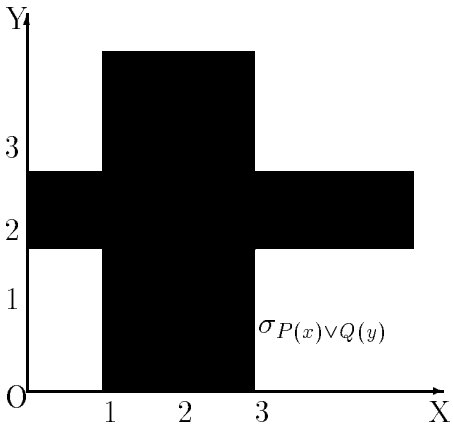
Область истинности предиката $x^2 - y^2 > 1$ заштрихована на рис.9. Дополнение до ее проекции на ось OX есть отрезок $-1 \leq x \leq 1$. Это и есть область истинности предиката $\forall y(x^2 - y^2 \leq 1)$. Область истинности предиката $\exists x(x^2 + y^2 \leq 1)$ есть проекция на ось OY круга $x^2 + y^2 \leq 1$ (рис.10), т.е. отрезок $-1 \leq y \leq 1$. Теперь, рассуждая также, как в примере 1, видим, что область истинности нашего предиката есть квадрат $[-1, 1] \times [-1, 1]$ (рис.11).



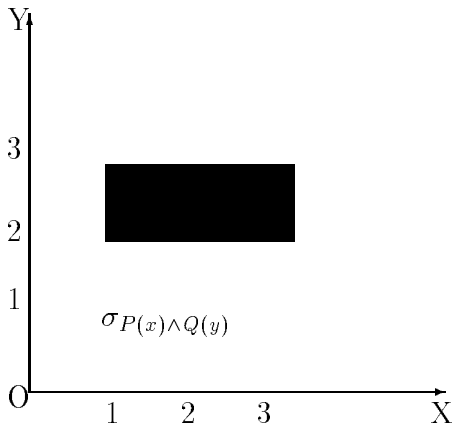
Puc.1.



Puc.2.



Puc.3.



Puc.4.

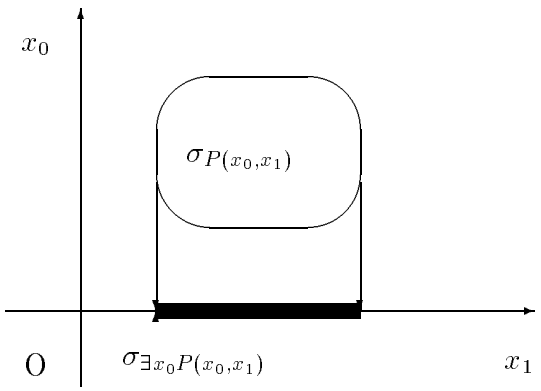


Рис.5.

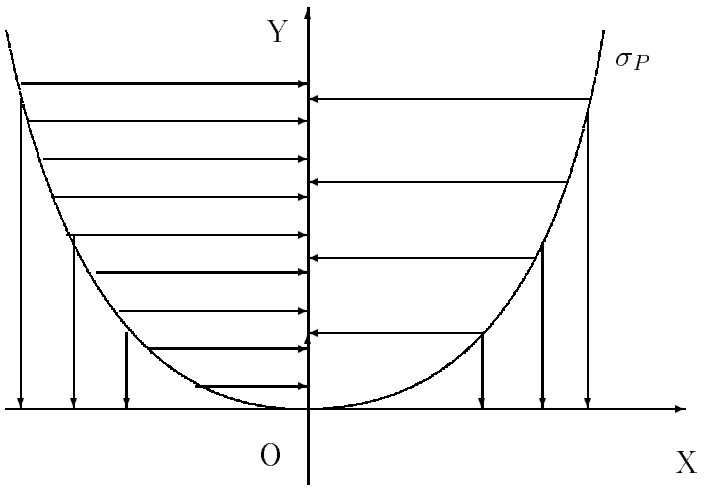
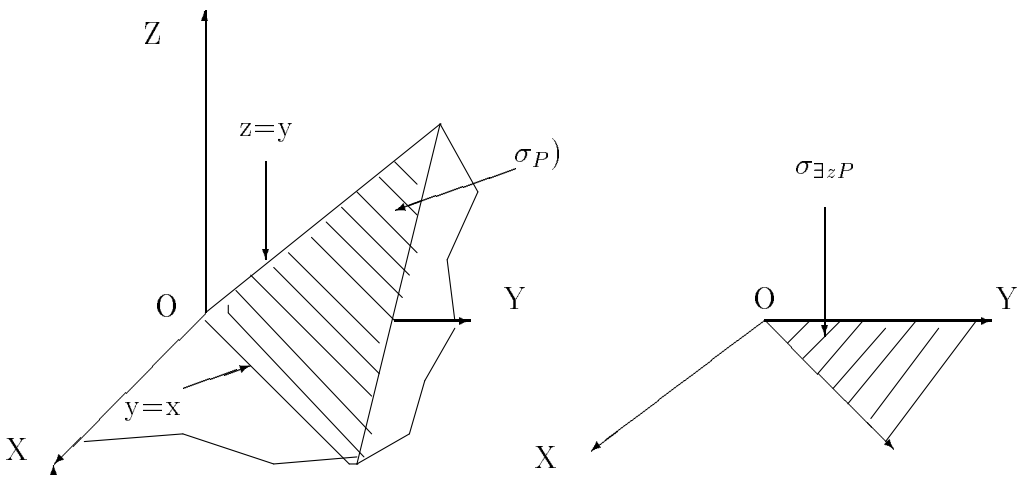
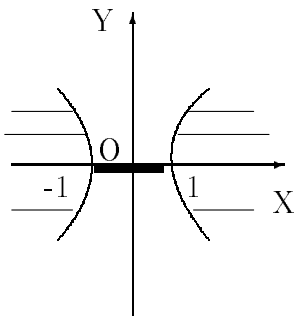


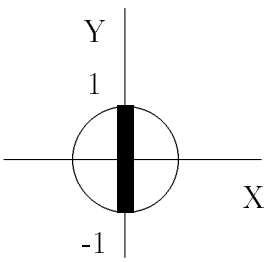
Рис.6.



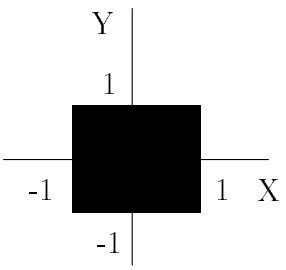
Puc.7.



Puc.7.



Puc.8.



Puc.9.

ЛЕКЦИЯ 3

Сформулируем теперь основные тождества логики предикатов, связывающие кванторы и логические связки. Для удобства ссылок включим сюда и тождества, доказанные в теореме 2.7. Как и в предыдущей лекции, предикаты, входящие в нижеследующие формулы, кроме тех переменных, по которым применяются кванторы, могут содержать и другие переменные. Ниже $\mathcal{Q}$ используется для обозначения как квантора $\forall$ так и квантора $\exists$.

Теорема 3.1 (Основные тождества логики предикатов).

(1) $\mathcal{Q}xP(x) = \mathcal{Q}tP(t)$, *если переменная* t *не входит в предикат* P;
(2) $\neg\forall xP(x) = \exists x\neg P(x)$; $\neg\exists xP(x) = \forall x\neg P(x)$;
(3) $\exists x(P(x) \vee Q(x)) = \exists xP(x) \vee \exists xP(x)$;
$\forall x(P(x) \wedge Q(x)) = \forall xP(x) \wedge \forall xQ(x)$;
(4) $\exists x(P(x) \wedge R) = \exists xP(x) \wedge R$;
$\forall x(P(x) \vee R) = \forall xP(x) \vee R$, *если* R *не зависит от* x;
(5) $\mathcal{Q}x\mathcal{Q}yP(x,y) = \mathcal{Q}y\mathcal{Q}xP(x,y)$

Доказательство. Равенства (1) и (5) непосредственно следуют из определения кванторов. Равенства (2) доказаны в теореме 2.6. Докажем первое из равенств (3). Если $\exists x(P(x) \vee Q(x)) = \mathbf{И}$, то существует $m \in M$, где M – предметная область, такое, что $P(m) \vee Q(m) = \mathbf{И}$, т. е. $P(m) = \mathbf{И}$ или $Q(m) = \mathbf{И}$ (как и выше считается, что значения остальных переменных, входящих в предикаты P и Q фиксированы). В первом случае $\exists xP(x) = \mathbf{И}$, а следовательно и $\exists xP(x) \vee \exists xP(x) = \mathbf{И}$. Второй случай рассматривается аналогично. Пусть, наоборот, $\exists xP(x) \vee \exists xP(x) = \mathbf{И}$. Это значит, что либо $\exists xP(x) = \mathbf{И}$, либо $\exists xQ(x) = \mathbf{И}$. В первом случае существует такое $m \in M$, которое удовлетворяет условию $P(m) = \mathbf{И}$, а следовательно и $P(m) \vee Q(m) = \mathbf{И}$, т.е. $\exists x(P(x) \vee Q(x)) = \mathbf{И}$. Второй случай рассматривается аналогично. Второе из равенств (3) мы выведем формально из первого, аналогично тому, как это было сделано в доказательстве теоремы 2.6.

Заменим в первом из равенств (3) предикат P на $\neg P$, а Q – на $\neg Q$ и применим к обеим частям полученного равенства отрицание. Получим равенство

$$\neg\exists x(\neg P(x) \vee \neg Q(x)) = \neg(\exists x\neg P(x) \vee \exists x\neg P(x))$$

К левой части полученного равенства применим второе из равенств (2), а к правой – закон де Моргана. Получим равенство

$$\forall x\neg(\neg P(x) \vee \neg Q(x)) = \neg\exists x\neg P(x) \wedge \neg\exists x\neg Q(x)$$

Применив к левой части полученного равенства закон де Моргана и снятие двойного отрицания, а к каждому из членов конъюнкции в правой части –

второе из равенств (2) и снятие двойного отрицания, получим требуемое равенство.

Докажем теперь первое из равенств (4). Пусть его левая часть истинна, тогда существует такое $m \in M$, что $P(m) \wedge R = \mathbf{И}$, т.е. $P(m) = \mathbf{И}$ и $R = \mathbf{И}$. Теперь видно, что $\exists x P(x) = \mathbf{И}$, т.е. истинна и правая часть равенства (4). Обратно, если истинна правая часть (4), то $\exists x P(x) = \mathbf{И}$ и $R = \mathbf{И}$. Следовательно, существует такое $m \in M$, что $P(m) = \mathbf{И}$, но тогда и $P(m) \wedge R = \mathbf{И}$, поскольку R не зависит от m. Отсюда следует, что истинна левая часть равенства (4). Второе из равенств (4) формально выводится из первого аналогично тому, как это было сделано для равенств (3) ■

Следствие. *Если предикат R не зависит от x, то $\mathcal{Q}xR = R$.*

Замечание. Равенство (1) показывает, что переменная x в выражении $\mathcal{Q}xP(x)$ играет такую же роль как индекс суммирования или переменная интегрирования. Оговорка о том, что x может быть заменена только на переменную, не входящую в P существенна. Например, $\exists x(y < x)$ равносильно $\exists t(y < t)$, но не равносильно $\exists y(y < y)$. Последний предикат ложен, если $<$ интерпретируется как отношение строгого порядка на непустом множестве, в то время как первый истинен, например, во всех упорядоченных множествах, не имеющих наибольшего элемента. Аналогичная оговорка должна быть сделана и относительно переменной интегрирования: $\int_1^2 f(x,t)dx$ есть функция, зависящая от x, в то время как $\int_1^2 f(t,t)dt$ есть постоянное число.

Легко видеть, что квантор существования не проносится через конъюнкцию, квантор всеобщности – через дизъюнкцию и разноименные кванторы нельзя менять местами. Тем не менее имеет место

Предложение 3.2. *Следующие импликации истинны:*

(1) $\exists x(P(x) \wedge Q(x)) \longrightarrow \exists x P(x) \wedge \exists x Q(x) \equiv \mathbf{И}$
(2) $(\forall x P(x) \vee \forall x Q(x)) \longrightarrow \forall x(P(x) \vee Q(x)) \equiv \mathbf{И}$
(3) $\exists x \forall y P(x,y) \longrightarrow \forall y \exists x P(x,y) = \mathbf{И}$

Доказательство. Если посылка импликации (1) истинна, то существует такое $m \in M$, что $P(m) \wedge Q(m) = \mathbf{И}$, т.е. $P(m) = \mathbf{И}$ и $Q(m) = \mathbf{И}$, т.е. $\exists x P(x) = \mathbf{И}$ и $\exists x Q(x) = \mathbf{И}$. Отсюда следует, что и заключение импликации (1) истинно. Импликацию (2) можно доказать аналогично, а можно вывести формально из импликации (1) (полезное упражнение!).

Если посылка импликации (3) истинна, то существует такое $m \in M$, что $\forall y P(m,y) = \mathbf{И}$. Тогда для произвольного $n \in M$ $P(m,n) = \mathbf{И}$, но тогда для произвольного $n \in M$ $\exists x P(x,n) = \mathbf{И}$, но это и означает, что $\forall y \exists x P(x,y) = \mathbf{И}$ ■

Обратные к (1) – (3) импликации не всегда истинны, а точнее, как правило, ложны. В самом деле, например, понятно, что посылка импликации (1) означает существование одного m, обращающего в истину как P, так и Q. В то время как ее заключение означает существование некоторого m, обращающего в истину P и некоторого n, возможно отличного от m, которое обращает в истину Q.

Пусть, например, $M = \mathbb{N}$, $P(x) \rightleftharpoons x = 2$, $Q(x) \rightleftharpoons x = 3$. Тогда очевидно, что

$$\exists x P(x) \wedge \exists x Q(x)) \longrightarrow \exists x (P(x) \wedge Q(x)) = \text{Л}$$

Чтобы доказать ложность импликации, обратной к (2) определим M и P также, как и выше, а $Q(x) \rightleftharpoons x \neq 2$. Тогда очевидно, что

$$(\forall x (P(x) \vee Q(x))) \longrightarrow (\forall x P(x) \vee \forall x Q(x)) = \text{Л}$$

Ясно, что здесь в качестве P можно взять любой не тождественно истинный предикат, а в качестве Q – его отрицание.

Для того, чтобы построить контрпример к импликации, обратной к (3), заметим, что посылка в (3) означает, что существует один элемент x, который обращает P в истину при любом y, а ее заключение – что для каждого y существует, вообще говоря, свой элемент x, обращающий P в истину.

Пусть снова $M = \mathbb{N}$, а $P(x, y) \rightleftharpoons y < x$. Тогда очевидно, что

$$\forall y \exists x P(x, y) \longrightarrow \exists x \forall y P(x, y) = \text{Л},$$

поскольку в $\mathbb{N}$ для каждого элемента имеется больший, но нет наибольшего элемента.

Тем не менее истинен некоторый вариант импликации, обратной к (3). Чтобы его рассмотреть введем сначала понятие ограниченного квантора.

Как отмечалось при определении предикатов, любой n-местный предикат можно отождествить с его областью истинности, представляющей собой подмножество M^n, где M – предметная область. В частности, одноместные предикаты отождествляются с произвольными подмножествами M. При этом вместо $A(x)$ пишут $x \in A$ и часто пользуются сокращениями:

$$(\exists x \in A)\, \mathcal{B} \rightleftharpoons \exists x (x \in A \wedge \mathcal{B})$$
$$(\forall x \in A)\, \mathcal{B} \rightleftharpoons \forall x (x \in A \longrightarrow \mathcal{B})$$

Конструкции такого вида принято называть кванторами,ограниченными множеством A, или, просто, ограниченными кванторами.

Предложение 3.3. *Все тождества теоремы 3.1 и предложения 3.1 останутся истинными, если заменить какие-либо входящие в них кванторы на одноименные ограниченные кванторы.*

Доказательство этого предложения можно провести формально, используя определение ограниченных кванторов, тождества теоремы 3.1 и предложения 3.2 (упражнение).

Предложение 3.4. *Пусть $P(x,y)$ – предикат, зависящий от x, y и, возможно, еще от каких-нибудь переменных. Тогда*

$$(\forall x \in A)(\exists y \in B)\, P(x,y) \;=\; (\exists f \in B^A)(\forall x \in A)\, P(x, f(x))$$

Доказательство. Требуется доказать истинность импликаций $\mathcal{A} \longrightarrow \mathcal{B}$ и $\mathcal{B} \longrightarrow \mathcal{A}$, где $\mathcal{A}$ и $\mathcal{B}$ – левая и правая части доказываемого равенства соответственно. Импликация $\longleftarrow$ очевидна: при каждом фиксированном x в качестве y следует взять $f(x)$. Для доказательства импликации $\longrightarrow$ заметим, что, если ее посылка истинна, то при каждом фиксированном $a \in A$ множество $B_a = \{b \in B \,|\, P(a,b) = \mathbf{И}\} \neq \emptyset$. Выберем из каждого множества B_a по элементу b_a и определим $f : A \longrightarrow B$, положив для любого $a \in A\, f(a) = b_a$. Тогда ясно, что при любом $a \in A\, P(a, f(a)) = \mathbf{И}$, т.е. $(\forall x \in A)\, P(x, f(x)) = \mathbf{И}$. Таким образом и заключение данной импликации истинно ■

Заметим, что при доказательстве предложения 3.4 использовалась *аксиома выбора*. Легко видеть, что на самом деле предложение 3.4 (точнее, импликация $\longrightarrow$) равносильна аксиоме выбора. Формулировку аксиомы выбора и ее подробное обсуждение можно найти в [6].

ЛЕКЦИЯ 4

Рассмотрим теперь несколько примеров записи математических предложений в языке логики предикатов и формализации рассуждений при помощи основных тождеств логики предикатов, рассмотренных в предыдущей лекции.

1°. Еще в самом начале вашего обучения, в курсе математического анализа вас учили применять кванторы при записи определений и говорили, что при формулировке отрицания любого предложения все кванторы нужно поменять на двойственные. Проделаем это теперь строго на примере определения предела функции. Ниже ограниченные кванторы вида $\mathcal{Q}x \in (0, +\infty)$ будем записывать в виде $\mathcal{Q}x > 0$. Итак, определение того, что $\lim\limits_{x \to a} f(x) = b$, записывается следующим образом.

$$\forall \varepsilon > 0\, \exists \delta > 0\, \forall x (|x - a| < \delta \;\longrightarrow\; |f(x) - b| < \varepsilon) \tag{4.1}$$

Если теперь мы хотим сформулировать предложение $\lim\limits_{x\to a} f(x) \neq b$, т.е. отрицание (4.1), то, в соответствии с тождествами (2) теоремы 3.1 и предложением 3.3, это отрицание запишется в виде

$$\exists\varepsilon > 0\,\forall\delta > 0\,\exists x\neg(|x-a| < \delta \;\longrightarrow\; |f(x)-b| < \varepsilon) \tag{4.2}$$

Теперь воспользовавшись тождеством логики высказываний

$$\neg(p \;\longrightarrow\; q) \;\equiv\; p \wedge \neg q$$

и тем, что $\neg\,(|f(x)-b| < \varepsilon) \;\equiv |f(x)-b| \geq \varepsilon$, получим окончательную формулировку утверждения $\lim\limits_{x\to a} f(x) \neq b$:

$$\exists\varepsilon > 0\,\forall\delta > 0\,\exists x\,(|x-a| < \delta \;\wedge\; |f(x)-b| \geq \varepsilon)$$

2°. Если подставить в (1) вместо a – y, а вместо b – $f(y)$, получим определение непрерывности функции f в точке y. Следовательно непрерывность функции f на всей области определения запишется так:

$$\forall y\forall\varepsilon > 0\,\exists\delta > 0\,\forall x(|x-y| < \delta \;\longrightarrow\; |f(x)-f(y)| < \varepsilon) \tag{4.3}$$

Напомним, что равномерная непрерывность f определяется следующим образом:

$$\forall\varepsilon > 0\,\exists\delta > 0\,\forall y\forall x(|x-a| < \delta \;\longrightarrow\; |f(x)-b| < \varepsilon) \tag{4.4}$$

Воспользовавшись импликацией (4) предложения 3.2, поменяем в (4.4) местами кванторы $\forall y$ и $\exists\delta > 0$. После этого можно поменять местами стоящие рядом одноименные кванторы $\forall y$ и $\forall\varepsilon > 0$ (тождество (5) теоремы 3.1). В результате мы придем к (4.3). Таким образом истинна импликация (4.4) $\longrightarrow$ (4.3), которая утверждает, что из равномерной непрерывности функции следует ее непрерывность в каждой точке. Такое же формальное доказательство обратной импликации не проходит потому, что импликация, обратная к импликации (4) предложения 3.2 не является тождественно истинной (см. лекцию 3). Действительно, известны примеры функций, непрерывных в каждой точке своей области определения, но не равномерно непрерывных (например, функция $y = x^2$ не является равномерно непрерывной на $\mathbb{R}$). Теорема Кантора о том, что функция, непрерывная в каждой точке замкнутого отрезка, равномерна непрерывна на этом отрезке существенно использует свойства замкнутого отрезка.

3°. Если $\mathcal{A}$ – некоторое семейство множеств, то объединением $\mathcal{A}$ называется множество, обозначаемое $\bigcup\mathcal{A}$ или $\bigcup\limits_{A\in\mathcal{A}} A$, которое определяется из условия

$$x \in \bigcup\mathcal{A} \iff \exists A \in \mathcal{A}\,(x \in A) \tag{4.5}$$

Пересечением семейства $\mathcal{A}$ называется множество $\bigcap \mathcal{A}$ или $\bigcap\limits_{A\in\mathcal{A}} A$, которое определяется из условия

$$x \in \bigcap \mathcal{A} \iff \forall A \in \mathcal{A}\,(x \in A)$$

Теперь из тождеств (2) теоремы 3.1 немедленно следуют законы де Моргана для бесконечных объединений и пересечений:

$$\overline{\bigcup_{A\in\mathcal{A}} A} = \bigcap_{A\in\mathcal{A}} \overline{A}, \quad \overline{\bigcap_{A\in\mathcal{A}} A} = \bigcup_{A\in\mathcal{A}} \overline{A},$$

а из тождеств (4) теоремы 3.1 – законы дистрибутивности для бесконечных объединений и пересечений:

$$\left(\bigcup_{A\in\mathcal{A}} A\right) \cap B = \bigcup_{A\in\mathcal{A}} (A \cap B), \quad \left(\bigcap_{A\in\mathcal{A}} A\right) \cup B = \bigcap_{A\in\mathcal{A}} (A \cup B).$$

Пусть $\mathcal{A} = \{A_i \,|\, i \in I\}$. Тогда $\bigcup \mathcal{A}$ ($\bigcap \mathcal{A}$) записывают еще в виде $\bigcup\limits_{i\in I} A_i$ ($\bigcap\limits_{i\in I} A_i$). Теперь из тождеств (3) теоремы 3.1 вытекают следующие теоретико-множественные равенства:

$$\bigcup_{i\in I}(A_i \cup B_i) = \left(\bigcup_{i\in I} A_i\right) \cup \left(\bigcup_{i\in I} B_i\right), \quad \bigcap_{i\in I}(A_i \cap B_i) = \left(\bigcap_{i\in I} A_i\right) \cap \left(\bigcap_{i\in I} B_i\right).$$

Провести соответствующие формальные выводы предлагается в качестве упражнения. Мы рассмотрим аналогичный пример формального вывода еще одного теоретико-множественного равенства.

Пусть $f : X \longrightarrow Y$ и $\mathcal{A}$ – семейство подмножеств X. Тогда имеет место равенство:

$$f\left(\bigcup_{A\in\mathcal{A}} A\right) = \bigcup_{A\in\mathcal{A}} f(A) \tag{4.6}$$

Для доказательства равенства (4.6) заметим, что по определению образа множества при отображении

$$y \in f\left(\bigcup_{A\in\mathcal{A}} A\right) \equiv \exists x(x \in \bigcup_{A\in\mathcal{A}} A \wedge y = f(x)$$

В силу (4.5), выражение справа в последней эквивалентности равносильно выражению

$$\exists x(\exists A \in \mathcal{A}(x \in A) \wedge y = f(x)) \tag{4.7}$$

Поскольку предикат $y = f(x)$ не содержит переменной A квантор $\exists A \in \mathcal{A}$ можно вынести за внешние скобки и поменять местами с одноименным квантором $\exists x$. Поскольку

$$\exists x(x \in A \wedge y = f(x) \equiv y \in f(A),$$

то (4.7) равносильно выражению

$$\exists A \in \mathcal{A}(y \in f(A)) \equiv y \in \bigcup_{A \in \mathcal{A}} f(A),$$

что и доказывает (4.6).

4°. Пусть снова $f : X \longrightarrow Y$. Тогда утверждение о том, что f – сюръективно запишется в виде $\forall y \in Y \exists x \in X\,(y = f(x))$. В силу предложения 3.4 последнее выражение равносильно следующему: $\exists g \in X^Y \forall x \in X\,(y = f(g(y)))$. Утверждение $\forall x \in X\,(y = f(g(y)))$ означает, что $f \circ g = \mathrm{id}_X$, т.е., что g – правое обратное к f отображение. Тем самым доказана известная теорема о том, что отображение сюръективно тогда и только тогда, когда оно имеет правое обратное.

5°. Запишем формально известную теорему о том, что каждое непустое подмножество $\mathbb{N}$ имеет наименьший элемент:

$$\forall A(A \neq \emptyset \longrightarrow \exists x(x \in A \wedge \forall y(y \in A \longrightarrow x \leq y))) \tag{4.8}$$

Поскольку (4.8) справедливо для любого множества A, то в нем можно заменить A на $\neg A$. Кроме того воспользуемся известным тождеством логики высказываний

$$p \longrightarrow q \equiv \neg q \longrightarrow \neg p \tag{4.9}$$

. В результате (4.8) равносильно следующему предложению:

$$\forall A(\neg\exists x(x \in \bar{A} \wedge \forall y(y \in \bar{A} \longrightarrow x \leq y)) \longrightarrow \neg\bar{A} \neq \emptyset) \tag{4.10}$$

Преобразуем посылку импликации (4.10), воспользовавшись следующим легко проверяемым тождеством логики высказываний:

$$\neg(p \wedge q) \equiv q \longrightarrow \neg p$$

Получим, что (4.10) равносильно

$$\forall A(\forall x(\forall y(y \in \bar{A} \longrightarrow x \leq y) \longrightarrow \neg x \in \bar{A}) \longrightarrow \neg\bar{A} \neq \emptyset) \tag{4.11}$$

Далее воспользуемся следующими очевидными эквивалентностями: $\neg\bar{A} \neq \emptyset \equiv A = \mathbb{N}$, $\neg x \in \bar{A} \equiv x \in A$ и $x \leq y \equiv y < x$, а также применим к импликации, стоящей под квантором $\forall y$ тождество (4.9). В результате получим, что (4.11) равносильно

$$\forall A(\forall x(\forall y(y < x \longrightarrow y \in A) \longrightarrow x \in A) \longrightarrow A = \mathbb{N}) \tag{4.12}$$

Понятно, что (4.12) есть ни что иное, как принцип математической индукции в следующей форме.

*Если для произвольного натурального числа x из того, что все числа, меньшие x, обладают свойством A следует, что x обладает свойством A, то все натуральные числа обладают свойством A.**

Поскольку мы доказали, что (4.8) равносильно (4.12), то тем самым доказано, что утверждение о том, что всякое непустое подмножество натурального ряда имеет наименьший элемент, равносильно принципу математической индукции.

Заметим, что в этих рассуждениях мы нигде не пользовались спецификой множества $\mathbb{N}$. Таким образом наши рассмотрения допускают следующее обобщение. Напомним, что линейно упорядоченное множество называется вполне упорядоченным, если каждое его непустое подмножество имеет наименьший элемент. Очевидно, что формальный вывод (4.12) из (4.8) не изменится, если заменить $\mathbb{N}$ на произвольное вполне упорядоченное множество. Тем самым в произвольном вполне упорядоченном множестве $\mathbf{M}$ справедливо следующее утверждение:

$$\forall A \subseteq \mathbf{M}(\forall x(\forall y(y < x \longrightarrow y \in A) \longrightarrow x \in A) \longrightarrow A = \mathbf{M})$$

Это утверждение называется принципом трансфинитной индукции. Согласно известной теореме Цермело, каждое множество может быть вполне упорядочено. Таким образом принцип индукции можно применять для доказательства различных утверждений не только относительно счетных множеств, но и относительно произвольных бесконечных множеств. Следует однако иметь в виду, что теорема Цермело крайне не эффективна – она равносильна аксиоме выбора. В частности, хотя из нее следует, что можно вполне упорядочить множество $\mathbb{R}$, однако описать однозначно хотя бы одно такое упорядочение не представляется возможным. Это существенно ограничивает возможности применения принципа трансфинитной индукции для несчетных множеств. Более подробное обсуждение теоремы Цермело и других утверждений равносильных аксиоме выбора можно найти в [6].

ЛЕКЦИЯ 5

ГЛАВА II. Язык исчисления предикатов и его интерпретации

§1. Основные определения.

Как мы уже видели, совершенно одинаковые по форме выражения, составленные из предикатов при помощи логических связок и кванторов, могут

*Мы отождествили свойство A с множеством элементов, обладающих этим свойством

быть при одних предикатах истинны, а при других ложны. С другой стороны имеются выражения, которые истинны (ложны) независимо от того, какие конкретно предикаты в них входят.

Чтобы проанализировать эту ситуацию математическими методами необходимо дать формальное определение класса предложений, которые получаются из предикатов при помощи логических связок и кванторов, а также – формальное определение истинности и ложности таких предложений. При этом ясно, что в формальном определении предложений должны присутствовать лишь обозначения для предикатов, а при определении истинности этим обозначениям должны быть поставлены в соответствие конкретные предикаты. Из предыдущего понятно, что при этом формализуется существенно более богатый класс предложений, чем те, которые соответствуют формулам логики высказываний.

Прежде, чем переходить к определениям, заметим, что помимо обозначений для предикатов полезно ввести еще обозначения для функций. Разумеется, каждой $n-$местной функции $f(x_1, \ldots, x_n)$ соответствует $n+1$-местный предикат $P(x_1, \ldots, x_n, x_{n+1}) \rightleftharpoons f(x_1, \ldots, x_n) = x_{n+1}$. Однако, если при этом все время оговаривать, что данный предикат обозначает функцию, то это приведет к существенным усложнениям формальных предложений. Например, тот факт, что предикат $P(x, y) = \mathbf{И} \Longleftrightarrow y = f(x)$ для некоторой функции f записывается так:

$$\forall x \left[\exists y P(x, y) \wedge \forall y \forall y' (P(x, y) \wedge P(x, y') \longrightarrow y = y')\right].$$

Выражение стоящее в квадратных скобках принято обозначать $\forall! y P(x, y)$ и читать "существует и при том единственное y, такое, что $P(x, y)$.

Особенно значительные сложности при использовании предикатных символов вместо функциональных возникают, когда имеют дело с выражениями, где одни функции подставляются в качестве аргументов в другие. Представим себе, например, что вместо функциональных символов $+$ и $\cdot$ используются трехместные предикатные символы $S(x, y, z)$ и $\Pi(x, y, z)$ соответственно. Тогда выражение $\exists x(x^2 + px + q = 0)$ должно быть записано следующим образом:

$$\exists x \forall u \forall v \forall w \forall t (\Pi(x, x, u) \wedge \Pi(p, x, v) \wedge S(u, v, w) \wedge S(w, q, t) \longrightarrow t = 0)$$

Следует иметь ввиду, что при строго формальном подходе функции записываются в виде $f(x, y)$, т.е. вместо $x + y$ и $x \cdot y$ следует писать $+(x, y)$ и $\cdot(x, y)$ соответственно, т.е рассмотренное выше выражение запишется в виде

$$\exists x \left[+(+(\cdot(x, x), \cdot(x, p)), q) = 0\right].$$

Ниже, однако, мы, допуская некоторую нестрогость, будем пользоваться общепринятой формой записи, поскольку, как правило, это не приводит к недоразумениям.

Переходим к описанию множества $\mathcal{S}$ основных символов языка исчисления предикатов.

Определение 5.1. Множество $\mathcal{S}$ основных символов языка исчисления предикатов включает в себя следующие объекты

(1) Счетный набор символов $x_1, \ldots, x_n, \ldots$ для обозначения переменных (иногда для записи переменных будут употребляться и другие буквы).
(2) Некоторое множество $\mathcal{C}$ символов для обозначения констант.
(3) Множество функциональных символов $\mathcal{F}$ с фиксированным отображением $\varphi : \mathcal{F} \longrightarrow \mathbb{N} \setminus \{0\}$. При этом $\varphi(f) = n$ означает, что f – символ функции от n переменных (n-местной функции).
(4) Множество логических констант $\mathbb{B} = \{\mathbf{И}, \mathbf{Л}\}$.
(5) Множество предикатных символов $\mathcal{P}$ с фиксированным отображением $\psi : \mathcal{P} \longrightarrow \mathbb{N}\setminus\{0\}$. При этом запись $\psi(p) = n$ означает, что p – n-местный предикатный символ.
(6) Логические символы, скобки и знаки препинания:

$$\wedge,\ \vee,\ \neg,\ \longrightarrow,\ \forall,\ \exists,\ =,\ (,\ ),\ ,$$

Тройка $\sigma =< \mathcal{C}, \mathcal{F}, \mathcal{P} >$ называется сигнатурой языка исчисления предикатов. Язык сигнатуры σ обозначается L_σ.

Мощностью сигнатуры σ – $|\sigma|$ называется мощность множества $\mathcal{C} \cup \mathcal{F} \cup \mathcal{P}$.

Замечания. 1. Константные символы (элементы множества $\mathcal{C}$) можно рассматривать как 0-местные функциональные символы. Точно также логические константы **И** и **Л** можно рассматривать как 0-местные предикатные символы.

2. Напомним, что если алфавит конечен, то множество слов в нем счетно, а если бесконечен, то множество слов в нем равномощно самому алфавиту. Поскольку определяемые ниже формулы языка L_σ представляют собой построенные по определенным правилам слова в алфавите $\mathcal{S}$, то мощность множества всех формул языка L_σ не превосходит $\max\{\aleph_0, |\sigma|\}$.

Определение 5.2 (Термы языка L_σ). Термами языка L_σ называются слова в алфавите $\mathcal{S}$, которые получаются по следующим правилам

(1) Каждый константный символ c – терм.
(2) Каждый символ переменной x_i – терм.
(3) Если f – n-местный функциональный символ, а $t_1, \ldots, t_n$ – термы, то $f(t_1, \ldots, t_n)$ – терм.
(4) Всякий терм может быть получен по правилам 1 – 3.

Термы представляют собой описания всевозможных функций, которые получаются из функций, имеющих обозначения в множестве $\mathcal{F}$, при помощи

суперпозиций, отождествления переменных и подстановки констант вместо переменных.

Определение 5.3 (Формулы языка L_σ). Формулами языка L_σ называются слова в алфавите $\mathcal{S}$, которые получаются по следующим правилам

(1) Если $t_1, \ldots, t_n$ – термы, а p – n-местный предикатный символ, то $p(t_1, \ldots, t_n)$, $t_i = t_j$ а также **И** и **Л** – формулы языка L_σ.
(2) Если $\mathcal{A}$ и $\mathcal{B}$ – формулы языка L_σ, то $\neg\mathcal{A}$, $(\mathcal{A} \wedge \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \longrightarrow \mathcal{B})$, $\forall x\mathcal{A}$, $\exists x\mathcal{A}$ – формулы языка L_σ
(3) Всякая формула языка L_σ может быть получен по правилам 1 – 2.

Формулы вида (1) называются элементарными или атомарными. Вхождение переменной x в формулу $\mathcal{A}$ называется связанным, если оно является вхождением в подформулу вида $\forall x\mathcal{B}$ или $\exists x\mathcal{B}$. В противном случае оно называется свободным. Формула, не имеющая свободных вхождений переменных, называется предложением.

Пример. $\forall x(x = y + z \longrightarrow \forall z(x < z \longrightarrow \forall y(\neg x \cdot y = z)))$.

Здесь все вхождения x связанные, первые вхождения y, z свободны, остальные связаны.

Определение 5.4. Пусть $\sigma =< \mathcal{C}, \mathcal{F}, \mathcal{P} >$ – некоторая сигнатура. Алгебраической системой $\mathcal{M}$ сигнатуры σ называется пара $< M, i >$, где M – некоторое множество, называемое носителем системы $\mathcal{M}$ а i – отображение, ставящее в соответствие каждому $c \in \mathcal{C}$ элемент $i(c) \in M$, каждому n-местному функциональному символу $f \in \mathcal{F}$ – отображение $i(f) : M^n \longrightarrow M$, каждому n-местному предикатному символу $p \in \mathcal{P}$ – n-местный предикат $i(p) : M^n \longrightarrow \mathbb{B}$.

Если $\mathcal{F} = \emptyset$, то $\mathcal{M}$ называется моделью, если $\mathcal{P} = \emptyset$, то $\mathcal{M}$ называется (универсальной) алгеброй.

Мощностью системы $\mathcal{M}$ называется мощность ее носителя.

Замечания. 1. В дальнейшем, если это не приводит к недоразумениям, то c и $i(c)$, f и $i(f)$, p и $i(p)$ отождествляется.

2. Разумеется, всякую алгебраическую систему можно превратить в модель, переходя от n-местных функций к соответствующим $n+1$-местным предикатам так, как было описано выше. При изучении конкретных алгебраических систем этим не пользуются из-за описанных выше сложностей. В общих же рассмотрениях этот переход будет иногда использоваться.

Примеры. 1. Группы можно рассматривать как алгебраические системы в сигнатуре $< \{e\}, \{\cdot, ^{-1}\}, \emptyset >$. Тогда аксиомы групп запишутся в виде

$$1).\forall x\forall y\forall z(x \cdot (y \cdot z) = (x \cdot y \cdot z)) \quad 2).\forall x(x \cdot e = x \wedge e \cdot x = x)$$

$$3).\forall x(x \cdot x^{-1} = e \wedge x^{-1} \cdot x = e).$$

Если убрать из сигнатуры $^{-1}$, то третья аксиома запишется в виде $\forall x \exists y(x \cdot y = e \wedge y \cdot x = e)$.

Наконец, можно убрать и константу e. Тогда вторая аксиома запишется в виде $\exists y \forall x(x \cdot y = x \wedge y \cdot x = x)$, а третья в виде
$\forall x \exists y \forall z(z \cdot (x \cdot y) = z \wedge z \cdot (y \cdot x) = z \wedge (x \cdot y) \cdot z = z \wedge (y \cdot x) \cdot z = z)$.

2. Упорядоченное множество есть модель в сигнатуре $\sigma =< \emptyset, \emptyset, \{\leq\} >$.

Аксиомы порядка записываются в виде предложений языка L_σ следующим образом:

$$1).\forall x \; x \leq x$$
$$2).\forall x \forall y(x \leq y \wedge y \leq x \longrightarrow x = y)$$
$$3).\forall x \forall y \forall z(x \leq y \wedge y \leq z \longrightarrow x \leq z)$$

Отношение линейного порядка – это отношение порядка, удовлетворяющее еще одной аксиоме:

$$4).\forall x \forall y(x \leq y \vee y \leq x).$$

Иногда упорядоченное множество рассматривают также как модель в сигнатуре $\sigma' =< \emptyset, \emptyset, \{<\} >$. Аксиомы порядка записываются в виде предложений языка $L_{\sigma'}$ следующим образом

$$1').\forall x \;\; \neg x < x$$
$$2').\forall x \forall y \forall z(x < y \wedge y < z \longrightarrow x < z)$$

Аксиома линейного порядка в этом случае имеет вид:

$$3').\forall x \forall y(x < y \vee y < x \vee x = y).$$

Аксиомы 1)-3) эквивалентны аксиомам 1')-2') в следующем смысле. Предикат $x < y$ может быть выражен в виде следующей формулы языка L_σ:

$$x < y \rightleftharpoons x \leq y \wedge \neg x = y.$$

Если теперь в аксиомы 1')-2') подставить эту формулу вместо предиката ¡, то, пользуясь основными тождествами логики предикатов, легко доказать, что предложения 1)-3) равносильны предложениям 1')-2'), а предложения 1)-4) равносильны предложениям 1')-3'). Наоборот, в языке $L_{\sigma'}$ предикат $x \leq y$ записывается формулой

$$x < y \vee x = y,$$

и снова требуемая равносильность может быть доказана теперь уже в языке $L_{\sigma'}$ (Упражнение!).

3. Поле можно рассматривать как универсальную алгебру в сигнатуре $< \{0,1\}, \{+, \cdot\}, \emptyset >$. При этом можно добавить операцию –, но нельзя $^{-1}$,

поскольку эта операция в поле не является всюду определенной. Напомним аксиомы поля:

$$1).\forall x\forall y(x+y=y+x\wedge x\cdot y=y\cdot x)$$
$$2).\forall x\forall y\forall z((x+y)+z=x+(y+z)\wedge(x\cdot y)\cdot z=x\cdot(y\cdot z)$$
$$3).\forall x\forall y\forall z(x\cdot(y+z)=x\cdot y+x\cdot z)$$
$$4).\forall x(x+0=x\wedge x\cdot 1=x)$$
$$5).\forall x\exists y(x+y=0)$$
$$6).\forall x(\neg(x=0)\longrightarrow\exists y(x\cdot y=1)$$

Поля характеристики p, где p – простое число – это поля, удовлетворяющие аксиоме

$$\mathrm{AChar}(p):\qquad \underbrace{1+\cdots+1}_{p\text{ раз}}=0.$$

А для того чтобы описать поля характеристики 0 требуется добавить счетное множество аксиом вида

$$\mathrm{AChar}(0)_n:\qquad \neg\underbrace{1+\cdots+1}_{n\text{ раз}}=0.$$

Здесь $n=2,3,\ldots$.

Точно также, для того, чтобы описать алгебраически замкнутые поля, требуется добавить счетное множество аксиом вида

$$\mathrm{ACl}_n.\qquad \forall a_0\forall a_1\ldots\forall a_{n-1}\exists x(x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0),$$

где $n=1,2,\ldots$

Замечание. Более строго, в последней аксиоме должен быть записан какой-либо терм, соответствующий данному многочлену.

4. Упорядоченное поле – это алгебраическая система общего вида в сигнатуре $<\{0,1\},\{+,\cdot\},\{\leq\}>$.

Аксиомы упорядоченного поля – это аксиомы поля (аксиомы 1 – 6 примера 3), аксиомы линейного порядка (аксиомы 1 – 4 примера 2 и еще одна аксиома, связывающая отношение порядка с линейными операциями:

$$\forall x\forall y\forall z\left((x\leq y\longrightarrow(x+z\leq y+z\wedge(0\leq z\longrightarrow x\cdot z\leq y\cdot z))\right).$$

Среди упорядоченных полей выделяются вещественно замкнутые поля. Вещественно замкнутым называется упорядоченное поле, в котором, каждый

многочлен *нечетной* степени имеет хотя бы один корень, а каждый положительный элемент является квадратом. Чтобы описать вещественно замкнутые поля нужно к аксиомам упорядоченного поля добавить аксиомы ACl_n для всех нечетных n и аксиому $\forall x(x > 0 \longrightarrow \exists y(y = x^2))$.

5. Линейное пространство над полем K – это универсальная алгебра в сигнатуре $< \{0\}, \{+\} \cup \{f_\alpha \mid \alpha \in K\}, \emptyset >$, где f_α – одноместная операция умножения на скаляр α. Аксиомы линейного пространства – это аксиомы аддитивной абелевой группы (см. те аксиомы поля, которые относятся к операции сложения) и бесконечное множество аксиом вида

$$\forall x \forall y(f_\alpha(f_\beta(x)) = f_{\alpha\cdot\beta}(x) \wedge f_\alpha(x + y) = f_\alpha(x) + f_\alpha(y))$$

для всевозможных $\alpha, \beta \in K$. Мощность этого множества аксиом равна мощности поля K.

Необходимость континуального множества аксиом для определения линейного пространства при нашем подходе связана с отсутствием переменных, пробегающих поле скаляров и, следовательно, невозможностью применять кванторы по скалярам. Имея ввиду такие неудобства, иногда допускают обобщение понятия языка и сигнатуры, допуская, что имеется несколько сортов переменных, каждая из которых принимает значения в своем множестве. Это приводит к некоторым усложнениям формулировок, однако по существу все результаты сохраняются. Поэтому здесь такие обобщения не рассматриваются (Сформулировать точные определения для этого случая – полезное упражнение).

ЛЕКЦИЯ 6

Определение 6.1. Пусть $\mathcal{M}_1 = (M_1, i_1)$, $\mathcal{M}_2 = (M_2, i_2)$ – две алгебраические системы сигнатуры σ. Биективное отображение $\varphi : M_1 \longrightarrow M_2$ называется изоморфизмом алгебраических систем, если

(1) для любого константного символа $c \in \mathcal{C}$ $\varphi(i_1(c)) = i_2(c)$;

(2) для любого n-местного символа $f \in \mathcal{F}$ и любых $m_1, \ldots, m_n \in M_1$ имеет место равенство

$$\varphi(i_1(f)(m_1, \ldots, m_n)) = i_2(f)(\varphi(m_1), \ldots, \varphi(m_n));$$

(3) для любого n-местного символа $p \in \mathcal{P}$ и любых $m_1, \ldots, m_n \in M_1$ имеет место равенство

$$i_1(p)(m_1, \ldots, m_n) = i_2(p)(\varphi(m_1), \ldots, \varphi(m_n)).$$

Очевидно, что определения изоморфизма для групп, колец, полей, а также отображения подобия для упорядоченных множеств являются частными случаями данного определения.

Определение 6.2. Пусть $\mathcal{M} = (M, i)$ – алгебраическая система сигнатуры σ. Подмножество $M_1 \subseteq M$ назовем замкнутым, если оно содержит все элементы $i(c) \quad \forall c \in \mathcal{C}$ и замкнуто относительно всех операций вида $i(f) \quad \forall f \in \mathcal{F}$. Замкнутое подмножество $M_1 \subseteq M$ определяет алгебраическую систему $\mathcal{M}_1 = (M_1, i_1)$, где $\forall m_1, \ldots, m_n \in M_1 \quad \forall f \in \mathcal{F} \quad \forall p \in \mathcal{P}$

$$\begin{array}{l} i_1(f)(m_1, \ldots, m_n) = i(f)(m_1, \ldots, m_n) \\ i_1(p)(m_1, \ldots, m_n) = i(p)(m_1, \ldots, m_n) \end{array}.$$

Эта система называется подсистемой системы $\mathcal{M}$.

Если все переменные, входящие в терм t находятся среди $x_1, \ldots x_n$, то будем писать $t = t(x_1, \ldots x_n)$.

Определение 6.3 (Интерпретация термов). Пусть $\mathcal{M} = (M, i)$ – алгебраическая система сигнатуры σ. Каждому терму $t = t(x_1, \ldots x_n)$ ставится в соответствие отображение $i(t) : M^n \longrightarrow M$ по следующим правилам:

(1) если $t = c$, то $i(t) : M^n \longrightarrow M$ – постоянное отображение: $i(t)(m_1, \ldots, m_n) \equiv c$;
(2) если $t = x_i$, то $i(t) = \pi_i : M^n \longrightarrow M$, где $\pi_i(m_1, \ldots, m_n) = m_i$ – проектирование на i-ю компоненту;
(3) если $i(t_1), \ldots, i(t_n)$ определены, а $t = f(t_1, \ldots t_n)$, то $i(t) = f(i(t_1), \ldots i(t_n))$ – суперпозиция отображений.

Замечание. Если на самом деле в терме содержатся не все, а только часть переменных из списка $x_1, \ldots, x_n$, то полученная функция зависит от остальных переменных фиктивно. На самом деле в приведенном определении полученная функция зависит не только от самого терма, но и от некоторого множества переменных, содержащего все переменные, действительно входящие в терм. В частности, если терм не содержит переменных и, в качестве списка переменных, указано пустое множество, то интерпретацией такого терма является константа, а если в качестве списка переменных указано множество $x_1, \ldots, x_n$, то интерпретацией этого терма является функция от $x_1, \ldots, x_n$, тождественно равная некоторой константе.

Примеры. 1. Пусть K – некоторое ассоциативное и коммутативное кольцо $\mathcal{C} = \{c_\alpha \mid \alpha \in K\}$, $\mathcal{F} = \{+, \cdot\}$, причем $i(c_\alpha) = \alpha$, а операции $+$ и $\cdot$ интерпретируются как сложение и умножение в кольце K. Тогда интерпретациями термов являются всевозможные многочлены в этом кольце. При этом разные термы могут интерпретироваться как один и тот же многочлен. Например,

$$i\left(\cdot(+(x, y), +(x, y))\right) = i\left(+(+(\cdot(x, x), \cdot(2, \cdot(x, y))), \cdot(y, y))\right)$$

(Какая формула здесь записана?).

На самом деле многочлен в кольце K можно определить как функцию, которая является интерпретацией некоторого терма в указанной сигнатуре.

2. Сигнатура $< \{\mathbf{И}, \mathbf{Л}\}, \{\neg, \wedge, \vee, \longrightarrow\}, \emptyset >$. Термы в указанной сигнатуре – это всевозможные ФЛВ, а их интерпретации – это соответствующие им высказывания, т.е. функции из $\{\mathbf{И}, \mathbf{Л}\}^n$ в $\{\mathbf{И}, \mathbf{Л}\}$ (см. определения 1.1 – 1.3).

3. Рассмотрим сигнатуру

$$< \{c_\alpha \mid \alpha \in \mathbb{R}\}, \{\pm, \cdot, /, \exp, \ln, \sin, \arcsin\}, \emptyset > .$$

Если $i(c_\alpha) = \alpha$, а перечисленные функциональные символы интерпретируются как соответствующие функции, то функции, которые являются интерпретациями всевозможных термов в этой сигнатуре, называются элементарными функциями. Строго говоря, этот пример не подходит под определение интерпретации, поскольку здесь рассматриваются и не всюду определенные функции. Чтобы включить в определение интерпретации терма не всюду определенные функции, нужно приписать области определения всем исходным функциям и указать как находится область определения $i(t)$, где $t = f(t_1, \ldots t_n)$ и области определения функции $i(f)$ и термов $i(t_1), \ldots, i(t_n)$ уже известны (Задача!)

Как и выше, если формула $\mathcal{A}$ имеет свободные вхождения только переменных из списка $x_1, \ldots, x_n$, то будем писать $\mathcal{A}(x_1, \ldots, x_n)$.

Определение 6.4 (Интерпретация формул). Пусть $\mathcal{M} = (M, i)$ – алгебраическая система сигнатуры σ. Каждой формуле $\mathcal{A}(x_1, \ldots, x_n)$ $(n \geq 0)$ языка L_σ можно поставить в соответствие предикат $i(\mathcal{A}) : M^n \longrightarrow \{\mathbf{И}, \mathbf{Л}\}$ по следующим правилам.

(1) Если $\mathcal{A}$ имеет вид $t_1 = t_2$ или $p(t_1, \ldots, t_k)$, то $\forall m_1, \ldots, m_n \in M$

$$\begin{aligned}
&i(t_1 = t_2)(m_1, \ldots, m_n) = \mathbf{И} \Longleftrightarrow \\
&\Longleftrightarrow i(t_1)(m_1, \ldots, m_n) = i(t_2)(m_1, \ldots, m_n) \\
&i(p(t_1, \ldots, t_k))(m_1, \ldots, m_n) = \mathbf{И} \Longleftrightarrow \\
&\Longleftrightarrow i(p)(i(t_1)(m_1, \ldots, m_n), \ldots, i(t_k)(m_1, \ldots, m_n)) = \mathbf{И}.
\end{aligned}$$

(2) $i(\mathbf{И}) = \mathbf{И}$; $i(\mathbf{Л}) = \mathbf{Л}$.

(3) Если $i(\mathcal{A})$ и $i(\mathcal{B})$ уже определены, то

$$\begin{aligned}
&i(\neg\mathcal{A}) = \neg i(\mathcal{A}); \; i(\mathcal{A} \wedge \mathcal{B}) = i(\mathcal{A}) \wedge i(\mathcal{B}); \\
&i(\mathcal{A} \vee \mathcal{B}) = i(\mathcal{A}) \vee i(\mathcal{B}); i(\mathcal{A} \longrightarrow \mathcal{B}) = i(\mathcal{A}) \longrightarrow i(\mathcal{B}); \\
&i(\exists x \mathcal{A}) = \exists x \; i(\mathcal{A}); \; i(\forall x \mathcal{A}) = \forall x \; i(\mathcal{A}).
\end{aligned}$$

Если при некоторых $m_1, \ldots, m_n \in M$ выполняется равенство $i(\mathcal{A})(m_1, \ldots, m_n) = \mathbf{И}$, то будем писать $\mathcal{M} \models \mathcal{A}(m_1, \ldots, m_n)$.

Предложение истинно или ложно в $\mathcal{M}$ независимо от значений каких-либо переменных.

Определение 6.5. Формулы $\mathcal{A}(x_1, \ldots, x_n)$ и $\mathcal{B}(x_1, \ldots, x_n)$ равносильны в модели $\mathcal{M}$, если они определяют один и тот же предикат, т.е. если $\forall m_1, \ldots, m_n \in M$

$$i(\mathcal{A})(m_1, \ldots, m_n) = i(\mathcal{B})(m_1, \ldots, m_n).$$

Обозначение: $\mathcal{A} \equiv_{\mathcal{M}} \mathcal{B}$.

Формулы $\mathcal{A}(x_1, \ldots, x_n)$ и $\mathcal{B}(x_1, \ldots, x_n)$ равносильны в классе алгебраических систем $\mathcal{K}$, если $\forall \mathcal{M} \in \mathcal{K}$ $\mathcal{A} \equiv_{\mathcal{M}} \mathcal{B}$ ($\mathcal{A} \equiv_{\mathcal{K}} \mathcal{B}$).

Наконец, формулы $\mathcal{A}$ и $\mathcal{B}$ логически равносильны ($\mathcal{A} \equiv \mathcal{B}$), если они равносильны в классе всех алгебраических систем сигнатуры σ.

Формула $\mathcal{A}$ называется логически общезначимой ($\vdash \mathcal{A}$), если $\mathcal{A} \equiv \mathbf{И}$.

Предложение 6.6. $\mathcal{A} \equiv \mathcal{B} \Longleftrightarrow \vdash \mathcal{A} \longleftrightarrow \mathcal{B}$■

Предложение 6.7. *Следующие формулы логически равносильны (в п.п. 1 и 2 $Q = \forall, \exists$):*

(1) $Qx\mathcal{A}(x, x_1, \ldots, x_n) \equiv Qy\mathcal{A}(y, x_1, \ldots, x_n)$, *если y не входит в* $\mathcal{A}(x, x_1, \ldots, x_n)$, *а* $\mathcal{A}(y, x_1, \ldots, x_n)$ *получается заменой всех свободных вхождений x в* $\mathcal{A}(x, x_1, \ldots, x_n)$ *на y.*

(2) $Qx\mathcal{A} \equiv \mathcal{A}$, *если x не имеет свободных вхождений в $\mathcal{A}$.*

(3) $\neg\forall x\mathcal{A} \equiv \exists x\neg\mathcal{A}$; $\neg\exists x\mathcal{A} \equiv \forall x\neg\mathcal{A}$.

(4) $\forall x(\mathcal{A} \wedge \mathcal{B}) \equiv \forall x\mathcal{A} \wedge \forall x\mathcal{B}$.

(5) $\forall x(\mathcal{A} \vee \mathcal{B}) \equiv \forall x\mathcal{A} \vee \mathcal{B}$, *если x не имеет свободных вхождений в $\mathcal{B}$.*

(6) $\exists x(\mathcal{A} \vee \mathcal{B}) \equiv \exists x\mathcal{A} \vee \exists x\mathcal{B}$.

(7) $\exists x(\mathcal{A} \wedge \mathcal{B}) \equiv \exists x\mathcal{A} \wedge \mathcal{B}$, *если x не имеет свободных вхождений в $\mathcal{B}$.*

Это предложение вытекает из равенства соответствующих предикатов в любой системе (см. теорему 3.1).

Определение 6.8. Алгебраические системы $\mathcal{M}_1$ и $\mathcal{M}_2$ сигнатуры σ называются элементарно эквивалентными, если для любого предложения $\mathcal{A}$ сигнатуры σ выполняется условие

$$\mathcal{M}_1 \models \mathcal{A} \Longleftrightarrow \mathcal{M}_2 \models \mathcal{A}$$

Примеры. 1. Поля $\mathbb{Q}$ и $\mathbb{R}$ не являются элементарно эквивалентными поскольку, например, предложение $\forall y \exists x (y = x^3)$ истинно в $\mathbb{R}$, но ложно в $\mathbb{Q}$.

2. Поля $\mathbb{R}$ и $\mathbb{C}$ также не являются элементарно эквивалентными – предложение $\forall y \exists x (y = x^2)$ истинно в $\mathbb{C}$, но ложно в $\mathbb{R}$.

3. Абелевы группы $< \mathbb{Z}, + >$ и $< \mathbb{Q}, + >$ не являются элементарно эквивалентными (приведите пример соответствующего предложения).

4. Можно показать, что абелевы группы $< \mathbb{R}, + >$ и $< \mathbb{Q}, + >$ элементарно эквивалентны.

Предложение 6.9. *Любые две изоморфные алгебраические системы* $\mathcal{M}_1 = (M_1, i_1)$, *и* $\mathcal{M}_2 = (M_2, i_2)$ *элементарно эквивалентны.*

Доказательство. Ниже любой упорядоченный набор $< a_1, \ldots, a_n >$ обозначается $\bar{a}$. Если $m_1, \ldots, m_n \in M_1$, а $\varphi : M_1 \longrightarrow M_2$, то набор
$< \varphi(m_1), \ldots, \varphi(m_n) >$ обозначается $\varphi(\bar{m})$.

Пусть $\varphi : M_1 \longrightarrow M_2$ – изоморфизм. Мы докажем даже более общее, чем требуется, следующее утверждение. Для любой формулы $F(\bar{x})$ языка L_σ и любого набора $\bar{m} \in M_1^n$

$$\mathcal{M}_1 \models F(\bar{m}) \Longleftrightarrow \mathcal{M}_2 \models F(\varphi(\bar{m})). \tag{6.1}$$

Для этого сначала докажем аналогичное утверждение для термов. Пусть $t(\bar{x})$ – терм, а $\bar{m} \in M_1^n$. Тогда

$$\varphi(i_1(t)(\bar{m})) = i_2(t)(\varphi(\bar{m})). \tag{6.2}$$

Это утверждение непосредственно следует из определения изоморфизма в случае, когда терм представляет собой константный символ, поскольку в этом случае значение терма в любой системе есть соответствующая константа, независимо от набора значений переменных.

Пусть $t = x_j$. Тогда $i_1(t)(\bar{m}) = m_i$, $i_2(t)(\varphi(\bar{(m)}) = \varphi(m_i)$ и мы видим, что в этом случае утверждение также справедливо.

Пусть для термов $t_1, \ldots, t_k$ утверждение доказано, а $t = f(t_1, \ldots, t_k)$, где f –k-местный функциональный символ. Тогда

$$i_1(t)(\bar{m}) = i_1(f)(i_1(t_1)(\bar{m}), \ldots, i_1(t_k)(\bar{m})).$$

По определению изоморфизма

$$\varphi(i_1(t)(\bar{m})) = i_2(f)(\varphi(i_1(t_1)(\bar{m})), \ldots, \varphi(i_1(t_k)(\bar{m}))).$$

По предположению индукции последнее выражение равно

$$i_2(f)(i_2(t_1)(\varphi(\bar{m})), \ldots, i_2(t_k)(\varphi(\bar{m}))) = i_2(t)(\varphi(\bar{m})),$$

что и доказывает (6.2)

Докажем сначала (6.1) для атомарных формул. Если $F(\bar{x})$ имеет вид $t_1(\bar{x}) = t_2(\bar{x})$, а $\bar{m} \in M_1^n$, то $\mathcal{M}_1 \models F(\bar{m})$ означает, что $i_1(t_1)(\bar{m}) = i_1(t_2)(\bar{m})$, $\mathcal{M}_2 \models F(\varphi(\bar{m}))$ означает, что $i_2(t_1)(\varphi(\bar{m})) = i_2(t_2)(\varphi(\bar{m}))$. Из (6.2) теперь следует, что (6.1) в этом случае равносильно утверждению

$$i_1(t_1)(\bar{m}) = i_1(t_2)(\bar{m}) \Longleftrightarrow \varphi(i_1(t_1)(\bar{m})) = \varphi(i_1(t_2)(\bar{m})),$$

которое вытекает из инъективности φ.

Пусть теперь $F(\bar{x})$ имеет вид $p(\bar{t}(\bar{x}))$, где $\bar{t}$ – набор термов, а p – предикатный символ. Тогда $\mathcal{M}_1 \models F(\bar{m})$ означает, что $i_1(p)(i_1(\bar{t})(\bar{m})) = \mathbf{И}$, а $\mathcal{M}_2 \models F(\varphi(\bar{m}))$ означает, что $i_2(p)(i_2(\bar{t})(\varphi(\bar{m}))) = \mathbf{И}$. В силу (6.1) последнее равенство равносильно тому, что $i_2(p)(\varphi(i_1(\bar{t})(\bar{m}))) = \mathbf{И}$, т.е. (6.1) в этом случае равносильно утверждению

$$i_1(p)(i_1(\bar{t})(\bar{m})) = \mathbf{И} \Longleftrightarrow i_2(p)(\varphi(i_1(\bar{t})(\bar{m}))) = \mathbf{И},$$

которое вытекает из определения того, что φ – изоморфизм.

Пусть для формул F и G утверждение (6.1) доказано. Тогда

$$\begin{aligned}
&\mathcal{M}_1 \models F(\bar{m}) \wedge G(\bar{m}) \Longleftrightarrow \\
&\mathcal{M}_1 \models F(\bar{m}) \ \text{ и } \ \mathcal{M}_2 \models G(\bar{m}) \Longleftrightarrow \\
&\mathcal{M}_2 \models F(\varphi(\bar{m})) \ \text{ и } \ \mathcal{M}_2 \models G(\varphi(\bar{m})) \Longleftrightarrow \\
&\mathcal{M}_2 \models F(\varphi(\bar{m})) \wedge G(\varphi(\bar{m})).
\end{aligned}$$

Аналогично для отрицания:

$$\begin{aligned}
&\mathcal{M}_1 \models \neg F(\bar{m}) \Longleftrightarrow \ \text{ неверно что } \ \mathcal{M}_1 \models F(\bar{m}) \Longleftrightarrow \\
&\text{неверно что } \ \mathcal{M}_2 \models F(\varphi(\bar{m})) \Longleftrightarrow \mathcal{M}_2 \models \neg F(\varphi(\bar{m})).
\end{aligned}$$

Для остальных логических связок доказательство можно не проводить поскольку они выражаются через рассмотренные связки.

Пусть для формулы $F(y, \bar{x})$ утверждение (6.1) доказано. Рассмотрим формулу $\exists y F(y, \bar{x})$. Предположим, что $\mathcal{M}_1 \models \exists y F(y, \bar{m})$. Это означает, что существует такое $m_0 \in M_1$, что $\mathcal{M}_1 \models F(m_0, \bar{m})$. Тогда по предположению индукции $\mathcal{M}_2 \models F(\varphi(m_0), \varphi(\bar{m}))$ и, следовательно,

$$\mathcal{M}_2 \models \exists y F(y, \varphi(\bar{m})) \tag{6.3}$$

. Пусть, наоборот, выполнено (6.3). Тогда существует $n_0 \in M_2$, такое, что $\mathcal{M}_2 \models F(n_0, \varphi(\bar{m}))$. Поскольку отображение φ сюръективно существует такое

$m_0 \in M_1$, что $n_0 = \varphi(m_0)$, т.е. $\mathcal{M}_2 \models F(\varphi(m_0), \varphi(\bar{m}))$. Теперь в силу того, что (6.1) выполнено для F имеем $\mathcal{M}_1 \models F(m_0, \bar{m})$, т.е. $\mathcal{M}_1 \models \exists y F(y, \bar{m})$. Тем самым (6.1) доказано и для формулы $\exists y F$. Для квантора всеобщности доказательство можно не проводить, поскольку он выражается через квантор существования и отрицание.■

Замечания. 1. Доказанное предложение подводит базу под утверждения типа "С точки зрения теории групп изоморфные группы не различаются".

2. Мы провели во всех подробностях тривиальное доказательство предложения 6.9, чтобы продемонстрировать технику работы с определениями термов и формул.

Определение 6.10. Множество всех предложений, истинных в алгебраической системе $\mathcal{M}$ называется теорией системы $\mathcal{M}$ и обозначается $\mathrm{Th}(\mathcal{M})$. Множество предложений, истинных во всех системах некоторого класса $\mathcal{K}$ алгебраических систем сигнатуры σ, называется теорией класса $\mathcal{K}$ и обозначается $\mathrm{Th}(\mathcal{K})$.

Из предложения 6.9. следует, что теория системы $\mathcal{M}$ является теорией класса всех систем, изоморфных $\mathcal{M}$.

ЛЕКЦИЯ 7

§2. Предваренная нормальная форма и исключение кванторов.

Определение 7.1. Говорят что формула имеет предваренную (префиксную) нормальную форму (п.н.ф.), если она имеет вид

$$Q_1 x_1 \dots Q_s x_s F(x_1, \dots, x_s, y_1, \dots, y_t),$$

где $Q_i = \forall$ или $\exists$, а F – бескванторная формула ($s \geq 0$).

Теорема 7.2. *Для любой формулы $A(x_1, \dots, x_n)$ языка L_σ существует логически равносильная ей формула B в предваренной нормальной форме.*

Доказательство. Ниже формула в п.н.ф. B, логически равносильная формуле A называется предваренной нормальной формой формулы A.

Если A – элементарная формула, то она бескванторная и, следовательно, сама является своей п.н.ф.. Если формула B – п.н.ф. формулы A, то QxB – п.н.ф. формулы QxA, где $Q = \forall, \exists$.

Ниже, если $Q = \forall$, то $Q' = \exists$ и наоборот.

Если $Q_1 x_1 \dots Q_s x_s F$ – п.н.ф. для A, то $Q'_1 x_1 \dots Q'_s x_s \neg F$ – п.н.ф. для $\neg A$.

Пусть $R_1 y_1 \dots R_1 y_t G$, где каждое R_i есть либо $\forall$, либо $\exists$, есть п.н.ф. для B. Отметим, что списки переменных x_i и y_i могут, вообще говоря, пересекаться. Для того, чтобы избежать этого выберем переменные $z_1, \dots, z_t$, которые не

входят ни в F, ни в G и обозначим через $G(z)$ формулу, которая получается заменой каждого вхождения y_i в G на z_i соответственно. Тогда в силу предложения 6.7(1) $R_1y_1 \ldots R_1y_tG \equiv R_1z_1 \ldots R_1z_tG(z)$. Теперь, используя несколько раз предложение 6.7(5,7), получаем

$$\begin{aligned}\mathcal{A} \vee \mathcal{B} &\equiv Q_1x_1 \ldots Q_sx_sF \vee R_1z_1, \ldots, R_1z_tG(z) \equiv \\ &\equiv R_1z_1, \ldots, R_1z_tQ_1x_1 \ldots Q_sx_s(F \vee G(z)).\end{aligned}$$

Тем самым построена п.н.ф. для $\mathcal{A} \vee \mathcal{B}$ ■

Замечание. Приведенное доказательство эффективно – по существу, мы описали алгоритм, который по любой формуле строит логически равносильную ей формулу в п.н.ф. за конечное число шагов.

Примеры.

1. $$\begin{aligned}&\forall xP(x) \vee \forall xQ(x) \equiv \forall xP(x) \vee \forall yQ(y) \equiv \\ &\forall x(P(x) \vee \forall yQ(y)) \equiv \forall x\forall y(P(x) \vee Q(y))\end{aligned}$$

2. $$\begin{aligned}&\exists x\,(P(x,y) \longrightarrow \forall yQ(y,z)) \equiv \exists x\,(\neg P(x,y) \vee \forall yQ(y,z)) \equiv \\ &\equiv \exists x\,(\neg P(x,y) \vee \forall uQ(u,z)) \equiv \exists x\forall u\,(P(x,y) \longrightarrow Q(u,z))\end{aligned}$$

Определение 7.3. Будем говорить, что теория $\mathrm{Th}(\mathcal{M})$ системы $\mathcal{M} =< M, i >$ сигнатуры σ допускает исключение кванторов, если для любой формулы $A(x_1, \ldots, x_n)$ языка L_σ существует бескванторная формула $B(x_1, \ldots, x_n)$ языка L_σ, такая, что

$$A(x_1, \ldots, x_n) \equiv_{\mathcal{M}} B(x_1, \ldots, x_n). \tag{7.1}$$

Если (7.1) имеет место для любой системы $\mathcal{M}$ из некоторого класса $\mathcal{K}$, то говорят, что теория класса $\mathcal{K}$ допускает исключение кванторов.

Если существует алгоритм, который по любой формуле $A(x_1, \ldots, x_n)$ строит за конечное число шагов бескванторную формулу $B(x_1, \ldots, x_n)$, удовлетворяющую (7.1) для любой системы $\mathcal{M}$ из класса $\mathcal{K}$, то говорят, что теория класса $\mathcal{K}$ допускает эффективное исключение кванторов.

Замечание. Второй абзац последнего определения пока нельзя считать вполне строгим, поскольку мы не формулировали точного определения алгоритма. Однако интуитивно понятие эффективного исключения кванторов вполне ясно. После того, как точное определение алгоритма будет сформулировано, определение 7.3 станет полностью строгим.

Предложение 7.4. *Теория системы $\mathcal{M}$ (класса $\mathcal{K}$) допускает исключение кванторов, если каждая формула вида $\exists x B(x, x_1, \ldots, x_n)$, где B – конъюнкция конечного числа атомарных формул или их отрицаний, равносильна в $\mathcal{M}$ (в $\mathcal{K}$) некоторой бескванторной формуле.*

Доказательство. В силу теоремы 7.2 достаточно доказывать данное предложение только для формул в п.н.ф. Доказательство проведем индукцией по числу n кванторов в п.н.ф. A. При $n = 0$ формула A – бескванторная и утверждение доказано. Предположим, что любая п.н.ф., содержащая менее n кванторов, равносильна бескванторной формуле. Пусть

$$A = Q_n x_n \ldots Q_2 x_2 Q_1 x_1 C(x_1, \ldots, x_n, y_1, \ldots, y_m).$$

Предположим сначала, что $Q_1 = \exists$ и рассмотрим формулу
$\exists x_1 C(x_1, \ldots, x_n, y_1, \ldots, y_m)$. По теореме о приведении к ДНФ бескванторная формула C логически равносильна формуле вида

$$\bigvee_{j=1}^{k} D_{1j} \wedge \cdots \wedge D_{s_j j}, \tag{7.2}$$

где D_{ij} есть либо бескванторная формула, либо ее отрицание. Следовательно

$$\exists x_1 C \equiv \exists x_1 \left(\bigvee_{j=1}^{k} D_{1j} \wedge \cdots \wedge D_{s_j j} \right) \equiv$$
$$\equiv \bigvee_{j=1}^{k} \exists x_1 (D_{1j} \wedge \cdots \wedge D_{s_j j}).$$

По условию предложения формула $\bigvee_{j=1}^{k} \exists x_1 (D_{1j} \wedge \cdots \wedge D_{s_j j})$ равносильна в $\mathcal{K}$ некоторой бескванторной формуле $E(x_2, \ldots, y_m)$. Теперь

$$A \equiv_{\mathcal{K}} Q_n x_n \ldots Q_2 x_2 E(x_2, \ldots, y_m),$$

а стоящая справа формула допускает исключение кванторов по предположению индукции.

Если $Q_1 = \forall$, то заменим $\forall x_1 C$ на $\neg\exists x_1 \neg C$. После этого приведем $\neg C$ к виду (7.2) и точно также, как выше исключим квантор $\exists x_1$. После этого A снова окажется равносильной п.н.ф., содержащей только $n - 1$ квантор и опять можно применить предположение индукции. ■

В качестве первого примера рассмотрим теорию $\mathrm{Th}(\mathbb{Q})$ модели $\mathbb{Q}$ в сигнатуре линейного порядка $< \emptyset, \emptyset, \{<\} >$ с естественной интерпретацией предикатного символа $<$.

Теорема 7.5. *Теория $Th(\mathbb{Q})$ допускает эффективное исключение кванторов*

Доказательство. Ниже вместо $\neg x < y$ будем писать $y \leq x$ (см. пример 2 в лекции 5). Из предыдущего предложения следует, что нам достаточно исключить квантор из формулы вида

$$\begin{aligned}\exists y(x_1 < y \wedge \cdots \wedge x_k < y \wedge u_1 \leq y \wedge \cdots \wedge u_l \leq y \wedge y < v_1 \wedge \cdots \wedge y < v_s \wedge \\ \wedge y \leq w_1 \wedge \cdots \wedge y \leq w_t) \quad k \geq 0, l \geq 0, \sigma \geq 0, t \geq 0\end{aligned} \tag{7.3}$$

Среди переменных x_i, u_i, v_i, w_i могут быть и совпадающие. Покажем, что можно ограничиться случаем, когда все свободные переменные, входящие в формулу (7.3), различны. Прежде всего, если x_i совпадает с x_j, то $x_i < y \wedge x_j < y \equiv x_i < y$. Аналогично для u, v, w. Если $x_i(u_i)$ совпадает с некоторым v_j, то формула (7.3) ложна, поскольку в этом случае она влечет формулу $\exists y(v < y \wedge y < v)$ (или же формулу $\exists y(v \leq y \wedge y < v)$ соответственно). В обоих случая формула (7.3) равносильна бесквантворной формуле **Л**.

Аналогично рассматривается случай, когда x_i совпадает с некоторым w_j.

Пусть u_α совпадает с некоторым w_β. Тогда формула (7.3) содержит подформулу вида $u \leq y \wedge y \leq u$, которая равносильна формуле $y = u$. В этом случае все вхождения y можно заменить на u, и снова (7.3) оказывается равносильной бесквантворной формуле.

Если x_i совпадает с некоторым u_j, то подформулу $y \leq u_j$ можно убрать из (7.3) поскольку конъюнкция $x_i < y \wedge x_i \leq y$ равносильна формуле $x_i < y$. Аналогично, если v_i совпадает с некоторым w_j.

Итак, осталось рассмотреть случай, когда среди свободных переменных формулы (7.3) нет совпадающих.

В случае, когда y встречается в (7.3) только с одной стороны (т.е. когда $k = l = 0$, либо $s = t = 0$) формула (7.3) равносильна бесквантворной формуле **И**, поскольку в упорядоченном множестве $\mathbb{Q}$ нет ни наибольшего, ни наименьшего элемента.

Если же все переменные различны и y встречается с обеих сторон, то формула (7.3) равносильна формуле

$$\begin{aligned}\bigwedge_{\alpha=1}^{k}\bigwedge_{\beta=1}^{s}(x_\alpha < v_\beta) \wedge \bigwedge_{\alpha=1}^{k}\bigwedge_{\beta=1}^{t}(x_\alpha < w_\beta) \wedge \\ \wedge \bigwedge_{\alpha=1}^{l}\bigwedge_{\beta=1}^{s}(u_\alpha < w_\beta) \wedge \bigwedge_{\alpha=1}^{l}\bigwedge_{\beta=1}^{t}(u_\alpha \leq w_\beta)\end{aligned} \tag{7.4}$$

В самом деле, истинность (7.4) вытекает из истинности (7.3) и транзитивности отношений $<$ и $\leq$.

Пусть, наоборот, формула (7.4) истинна. Это равносильно истинности следующей системы неравенств

$$\begin{aligned} \max\{x_\alpha\} &< \min\{v_\beta\} \\ \max\{x_\alpha\} &< \min\{w_\beta\} \\ \max\{u_\alpha\} &< \min\{v_\beta\} \\ \max\{u_\alpha\} &\leq \min\{w_\beta\} \end{aligned} \tag{7.5}$$

Здесь возможны два случая.

1. Последнее неравенство в системе (7.5) тоже строгое. В этом случае очевидно, что $\max\{x_\alpha, u_\beta\} < \min\{v_\gamma, u_\delta\}$ и любое y, удовлетворяющее неравенству

$$\max\{x_\alpha, u_\beta\} < y < \min\{v_\gamma, u_\delta\},$$

обращает в истину формулу (7.3). Такое y существует, поскольку упорядоченное множество $\mathbb{Q}$ плотно, т.е. между любыми его двумя различными элементами можно вставить третий.

2. Последнее неравенство в системе (7.5) есть, на самом деле равенство. В этом случае легко видеть, что $y = \max\{u_\alpha\} = \min\{w_\beta\}$ обращает формулу (7.3) в истину. ■

Замечание. Отметим, что приведенное доказательство эффективно, т.е. предъявлен алгоритм, строящий по любой формуле, равносильную ей в $\mathbb{Q}$ бескванторную формулу. Следовательно теория $\mathrm{Th}(\mathbb{Q})$ допускает эффективное исключение кванторов (см. замечание к определению 7.3).

При доказательстве теоремы 7.5 мы пользовались лишь тем, что в линейно упорядоченном множестве $\mathbb{Q}$ истинны следующие предложения:

1). $\forall x(\exists y(x < y) \wedge \exists y(y < x))$;

2). $\forall x \forall y(x < y \longrightarrow \exists z(x < z \wedge z < y))$.

Линейно упорядоченное множество, в котором истинны предложения 1) и 2), назовем плотным неограниченным. Обозначим класс плотных неограниченных линейно упорядоченных множеств через DL. Таким образом DL есть класс моделей в сигнатуре σ, в которых истинны предложения 1') – 3') примера 2 лекции 5 и предложения 1) – 2) предыдущего абзаца. Таким образом нами доказано

Предложение 7.6. *Теория класса DL допускает эффективное исключение кванторов.*

Если множество констант некоторой сигнатуры пусто, то любое бескванторное предложение этой сигнатуры есть формула логики высказываний, не

содержащая переменных. Любая такая формула равносильна либо **И**, либо **Л**. Таким образом, если некоторая теория класса $\mathcal{K}$ этой сигнатуры допускает исключение кванторов, то каждое предложение равносильно в $\mathcal{K}$ либо **И**, либо **Л**. Это доказывает следующее

Предложение 7.7. *Если сигнатура σ не содержит констант, а теория некоторого класса $\mathcal{K}$ систем этой сигнатуры допускает исключение кванторов, то все системы из $\mathcal{K}$ элементарно эквивалентны*

Сопоставляя предложения 7.6 и 7.7, получаем такое

Следствие. *Любые два плотных неограниченных линейно упорядоченных множества элементарно эквивалентны. В частности, элементарно эквивалентны $\mathbb{Q}$ и $\mathbb{R}$.*

Теория системы или класса систем называется *разрешимой*, если существует алгоритм, который по любому предложению отвечает на вопрос о том, принадлежит оно этой теории или нет. Поскольку существует алгоритм, который по любой формуле логики высказываний отвечает на вопрос истинна она при заданных значениях переменных или ложна, то очевидно следующее

Предложение 7.8. *Если теория T некоторого класса систем допускает эффективное исключение кванторов и существует алгоритм, который по любому бескванторному атомарному предложению отвечает на вопрос о том, принадлежит оно этой теории или нет, то теория T разрешима.*

В условиях предложения 7.7 каждое бескванторное предложение есть просто **И** или **Л**, т.е. алгоритм, распознающий по любому бескванторному предложению принадлежит оно данной теории или нет, заведомо существует. Следовательно, если в условиях предложения 7.7 теория $\mathrm{Th}(\mathcal{K})$ допускает эффективное исключение кванторов, то она разрешима.

Следствие. *Теория $Th(DL)$ разрешима.*

ЛЕКЦИЯ 8

§3. Арифметика Пресбургера.

Рассмотрим сигнатуру $\sigma =< \{0, +1, -1\}, \{+\}, \{<\} >$ и систему $\mathbb{Z}^+ =< \mathbb{Z}, i >$ сигнатуры σ, где $\mathbb{Z}$, как всегда, множество целых чисел, а i – естественная интерпретация константных, функциональных и предикатного символов. В соответствии с этим, ниже символ i всюду опускается, в частности термы отождествляются с определяемыми ими функциями или константами. Так, вместо

$$\underbrace{1 + \cdots + 1}_{k \text{ раз}}, \quad \underbrace{(-1) + \cdots + (-1)}_{k \text{ раз}}, \quad \underbrace{x + \cdots + x}_{k \text{ раз}},$$

будем писать k, $-k$, $k \cdot x$ соответственно.

Выясним сначала, что из себя представляют области истинности предикатов, определяемых бескванторными формулами сигнатуры σ. Пользуясь ассоциативностью и коммутативностью сложения в $\mathbb{Z}$, легко видеть, что каждая функция, определяемая некоторым термом сигнатуры σ, имеет вид

$$k_1 \cdot x_1 + \cdots + k_n \cdot x_n + b, \quad k_i, b \in \mathbb{Z}. \tag{8.1}$$

Собирая все члены равенства или неравенства с одной стороны, можно каждую атомарную формулу вида $t_1 = t_2$ привести к виду

$$k_1 \cdot x_1 + \cdots + k_n \cdot x_n + b = 0, \tag{8.2}$$

а каждую атомарную формулу вида $t_1 > t_2$ – к виду

$$k_1 \cdot x_1 + \ldots k_n \cdot x_n + b > 0. \tag{8.3}$$

Обозначим левую часть формул (8.2) и (8.3) через t. Тогда отрицание формулы (8.2) равносильно формуле $t > 0 \vee t < 0$, а отрицание формулы (8.3) – формуле $t \leq 0$. Эквивалентности

$$t > 0 \equiv t - 1 \geq 0$$
$$t < 0 \equiv t + 1 \leq 0$$
$$t = 0 \equiv t \leq 0 \wedge t \geq 0$$

показывают, что всякую атомарную формулу можно заменить конъюнкцией нестрогих неравенств, а ее отрицание – дизъюнкцией нестрогих неравенств. Если теперь привести бескванторную формулу к ДНФ, выполнить эти замены, а затем раскрыть скобки, пользуясь дистрибутивностью конъюнкции относительно дизъюнкции, то эта формула окажется равносильной в $\mathbb{Z}^+$ формуле вида

$$\bigvee_{j=1}^{n} \bigwedge_{i=1}^{m_n} k_1^{(ji)} \cdot x_1 + \cdots + k_t^{(ji)} \cdot x_t + b^{(ji)} \geq 0$$

Таким образом нами доказано следующее

Предложение 8.1. *Область истинности предиката, определяемого бескванторной формулы сигнатуры σ представляет собой конечное объединение множеств, каждое из которых есть множество целочисленных решений системы нестрогих линейных неравенств с целыми коэффициентами.*

Предложение 8.2. *Теория $Th(\mathbb{Z}^+)$ не допускает исключения кванторов.*

Доказательство. Рассмотрим формулу $\exists y(x = 2 \cdot y)$, которая истинна тогда и только тогда, когда x – четно, и покажем, что она не равносильна никакой бескванторной формуле. В самом деле, если бы эта формула была равносильна бескванторной, то из предложения 8.1 следовало бы, что область ее истинности представляет собой конечное объединение множеств, каждое из которых есть множество целых решений системы неравенств вида

$$k_1 \cdot x + b_1 \geq 0$$
$$\ldots\ldots\ldots\ldots$$
$$k_s \cdot x + b_s \geq 0.$$

Очевидно, что такое множество, либо конечно, либо содержит все целые положительные (отрицательные) числа, начиная с некоторого. Ясно, что этим же свойством обладает и конечное объединение таких множеств, но не обладает множество четных чисел ■

Аналогичные рассмотрения проходят и для любой формулы вида $\exists y(x = m \cdot y)$, где $m \geq 2$. Эта формула определяет предикат $x \equiv 0(\mod m)$. Расширим теперь сигнатуру σ до сигнатуры σ', добавив к ней счетное множество одноместных предикатных символов $D_m(x)$, $m \geq 2$, которые будем интерпретировать в нашей системе $\mathbb{Z}^+$ следующим образом:

$$i(D_m)(x) = \mathbf{И} \Longleftrightarrow x \equiv 0(\mathrm{mod}\ m).$$

Для удобства изложения считаем также, что в сигнатуре присутствует одноместный предикат $D_1(x)$, которой интерпретируется как тождественно истинный. Теория системы $\mathbb{Z}^+$ с указанной интерпретацией предикатных символов D_m называется Арифметикой Пресбургера и обозначается APr. Имеет место

Теорема 8.3. *Арифметика Пресбургера допускает эффективное исключение кванторов*

Для доказательства теоремы нам понадобятся некоторые утверждения из теории чисел, которые мы сформулируем как леммы.

Лемма 1. *Сравнение $ax \equiv b(mod\ m)$ имеет решение в том и только в том случае, когда b делится на $d = (a, m)$. В этом случае можно эффективно найти такое c, что решение данного сравнения имеет вид:*

$$x \equiv c(mod\ m)\ \textit{или}\ x \equiv c + \frac{m}{d}(mod\ m)\ \textit{или}\ldots\textit{или}\ x \equiv c + \frac{(d-1)m}{d}(mod\ m).$$

Лемма 2 (Китайская теорема об остатках). *Пусть натуральные числа* $m_1, \ldots, m_k$ *попарно взаимно просты. Тогда система сравнений*

$$x \equiv c_1 (mod\, m_1)$$
$$\ldots\ldots\ldots\ldots$$
$$x \equiv c_k (mod\, m_k)$$

имеет единственное решение по $mod\ m_1 \cdot \ldots \cdot m_k$. *При этом по* $m_1, \ldots, m_k$ *эффективно находятся такие целые числа* $d_1, \ldots, d_k$, *что для любых* $c_1, \ldots, c_k$ *решение данной системы сравнений имеет вид*

$$x \equiv d_1 c_1 + \ldots d_k c_k (mod\, m_1 \cdot \ldots \cdot m_k)$$

Эти два утверждения были доказаны в курсе "Алгебра и теория чисел". Следующее утверждение является несложным обобщением Китайской теоремы об остатках на случай, когда модули $m_1, \ldots, m_k$ не являются попарно взаимно простыми. Оно сравнительно несложно выводится из последней, что предлагается сделать читателю в качестве задачи.

Лемма 3. *Система сравнений*

$$x \equiv c_1 (mod\, m_1)$$
$$\ldots\ldots\ldots\ldots$$
$$x \equiv c_k (mod\, m_k)$$

имеет решение в том и только в том случае, когда $\forall i < j \leq k$
$c_i \equiv c_j (mod\, (m_i, m_j))$. *В этом случае решение единственно по* $mod\, [m_1, \ldots, m_k]$. *При этом по* $m_1, \ldots, m_k$ *эффективно находятся такие целые числа* $d_1, \ldots, d_k$, *что для любых* $c_1, \ldots, c_k$ *решение данной системы сравнений имеет вид*

$$x \equiv d_1 c_1 + \ldots d_k c_k (mod\, ([m_1, \ldots, m_k]))$$

Доказательство теоремы 8.3. Из предыдущих рассмотрений следует, что достаточно научиться исключать квантор из формул вида:

$$\begin{aligned} &\exists x\ (k_1 x + t_1 \wedge \ldots k_s x + t_s \wedge D_{m_1}(l_1 x + u_1) \wedge \ldots \\ &\wedge D_{m_t}(l_t x + u_t) \wedge \neg D_{n_1}(h_1 x + v_1) \wedge \cdots \wedge \neg D_{n_r}(h_r x + v_r), \end{aligned} \tag{8.4}$$

где $k_i, l_i, m_i, n_i, h_i \in \mathbb{Z}$, а t_i, u_i, v_i – термы, не содержащие переменной x. Учитывая соглашение, о предикате $D_1(x)$ можно считать, что $t > 0$, т.е. по крайней мере одно сравнение в формуле (8.5) присутствует.

Заменяя каждую формулу вида $\neg D_n(t)$ на равносильную ей формулу $D_n(t-1) \vee \cdots \vee D_n(t-n+1)$ $(\neg t \equiv 0(n) \Longleftrightarrow t \equiv 1(n) \vee \cdots \vee t \equiv n-1(n))$, раскрывая скобки и пронося квантор $\exists$ через дизъюнкцию, приходим к тому, что достаточно научиться исключать квантор только из формул вида (8.4) с $r = 0$, т.е. не содержащих формул вида $\neg D_n(t)$. Кроме этого, применяя лемму 1, можно считать, что $l_1 = \cdots = l_t = 1$. После этого, применив лемму 2 или лемму 3, т.е. заменив систему сравнений на одно сравнение, эквивалентной ей, приходим к тому, что достаточно научиться исключать квантор только из формул вида

$$\exists x \ (k_1 x + t_1 \wedge \ldots k_s x + t_s \wedge D_m(x+u) \qquad (8.5.)$$

Если в формуле (8.5) все k_i одного знака, то эта формула истинна, поскольку при любых значениях свободных переменных, содержащейся в ней системе неравенств, удовлетворяют все достаточно большие по абсолютной величине положительные или отрицательные x, а тогда среди них найдется и такое x, которое удовлетворяет входящему в эту формулу сравнению. В противном случае формула (8.5) приводится к виду

$$\exists x(a_1 x \geq p \wedge \cdots \wedge a_f x \geq p_f \wedge q_1 \geq b_1 x \wedge \cdots \wedge q_q \geq b_g x \wedge D_m(x+u)). \qquad (8.6)$$

Формула (8.6) приводится к виду

$$\bigvee_{i_0=1}^{f} \bigvee_{j_0=1}^{g} \frac{p_{i_0}}{a_{i_0}} = \max_i\{\frac{p_i}{a_i}\} \wedge \frac{q_{j_0}}{b_{j_0}} = \min_i\{\frac{q_j}{b_j}\} \wedge$$
$$\wedge \exists x(p_{i_0} \leq a_{i_0} x \wedge b_{j_0} x \leq q_{j_0} \wedge D_m(x_{i_0} + u))$$

Здесь $\frac{p_{i_0}}{a_{i_0}} = \max_i\{\frac{p_i}{a_i}\}$ есть сокращение для формулы

$$\bigwedge_{i=1}^{f} a_i p_{i_0} \geq a_{i_0} p_i$$

Аналогично для формулы $\frac{q_{j_0}}{b_{j_0}} = \min_i\{\frac{q_j}{b_j}\}$.

Итак, осталось рассмотреть случай формулы

$$\exists x(p \leq ax \wedge bx \leq q_{j_0} \wedge D_m(x_{i_0} + u)) \qquad (8.7)$$

Легко видеть, что эта формула равносильна бескванторной формуле

$$bp = aq \wedge p \equiv 0(a) \wedge q \equiv 0(b) \wedge p + au \equiv 0(ma) \vee \neg bp = aq \wedge aq \geq bp + abm \quad (8.8)$$

В самом деле, пусть формула (8.7) истинна, то $bp \leq abx \leq bq$. Возможны два случая: а) $bp = abx = aq$ и б) $\neq bp = aq$. В случае а) $bp + abu \equiv 0(mab)$, т.е. $p + au \equiv 0(ma)$ и формула (8.8) истинна. В случае б) $\frac{p}{a} \leq x \leq \frac{q}{b}$, т.е. $\frac{p}{a} + u \leq x + u \leq \frac{q}{b} + u$, а т.к. $x + u = mt$, то $\frac{p}{ma} + \frac{u}{m} \leq t \leq \frac{q}{mb} + \frac{u}{m}$. Между двумя вещественными числами α и β можно вставить целое число в том и только в том случае $\beta - \alpha \geq 1$. В данном случае это и есть последнее неравенство в формуле (8.8). В обратную сторону рассмотрение проводится аналогично ■

Из предыдущих рассмотрений видно, что каждое бесквантворное атомарное предложение сигнатуры σ' равносильно одному из предложений вида $k > 0$, $k = 0$, $k \equiv 0(\mod m)$, где $k \in \mathbb{Z}$, и очевидно, что существует алгоритм, распознающий по любому бесквантворному атомарному предложению, является оно истинным или ложным. Теперь, используя предложение 7.8, немедленно выводим из теоремы 8.3

Следствие. *Арифметика Пресбургера разрешима*

На самом деле Пресбургер доказал в 1929 году разрешимость теории сложения натуральных чисел, т.е. теории алгебры $\mathbb{N}^+ =< \mathbb{N}, i >$ в сигнатуре $\sigma'' =< \{1\}, \{+\}, \emptyset >$ с естественной интерпретацией константного и функционального символов. Легко видеть, что эта теория сводится к APr в следующем смысле.

Определение 8.4. Пусть $\mathcal{M}_1 =< M_1, i_1 >$ и $\mathcal{M}_2 =< M_2, i_2 >$ – алгебраические системы сигнатур δ_1 и δ_2 соответственно. Будем говорить, что теория $\mathrm{Th}(\mathcal{M}_2)$ интерпретируется в теории $\mathrm{Th}(\mathcal{M}_1)$, если по любому предложению A языка сигнатуры δ_2 можно построить такое предложение A' сигнатуры δ_1, что

$$\mathcal{M}_2 \models A \Longleftrightarrow \mathcal{M}_1 \models A'.$$

Если существует алгоритм, который по произвольному предложению A строит требуемое предложение A', то говорят, что $\mathrm{Th}(\mathcal{M}_2)$ интерпретируется в $\mathrm{Th}(\mathcal{M}_1)$ эффективно.

Теперь очевидно следующее

Предложение 8.5. *Если теория $Th(\mathcal{M}_2)$ эффективно интерпретируется в теории $Th(\mathcal{M}_1)$ и $Th(\mathcal{M}_1)$ разрешима, то разрешима и $Th(\mathcal{M}_2)$. Наоборот, если при этих условиях $Th(\mathcal{M}_2)$ неразрешима, то неразрешима и $Th(\mathcal{M}_1)$.*

Предложение 8.6. *Теория $Th(\mathbb{N}^+)$ эффективно интерпретируется в теории APr.*

Доказательство. Очевидно, чтобы построить A' по A нужно только заменить вхождение каждого квантора Qx в A на вхождение соответствующего ограниченного квантора $Qx \geq 0$ (см. лекцию 3).

В действительности справедливо и обратное, т.е. APr интерпретируется в $\mathrm{Th}(\mathbb{N}^+)$ в смысле Определения 8.4 (Задача*).

Результат Пресбургера был, по-видимому, первым результатом о разрешимости достаточно содержательного формализованного фрагмента математики и, тем самым, был первым существенным шагом к реализации программы Гильберта формализации математики (см. лекцию 2). Как мы увидим ниже, эта программа не реализуема в полном объеме. В частности, уже арифметика со сложением и умножением, т.е. теория алгебры $\mathbb{N}$ в сигнатуре $< \{1\}, \{+, \cdot\}, \emptyset >$, не является разрешимой.

Поскольку предикаты $D_m(x)$ в системе $\mathbb{Z}^+$ определимы формулами сигнатуры σ, то класс всех предикатов, определимых формулами сигнатуры σ в $\mathbb{Z}^+$, совпадает с классом предикатов, определимых формулами сигнатуры σ' в $\mathbb{Z}^+$. Этот класс допускает следующее описание.

Подмножество $L \subseteq \mathbb{Z}^n$ назовем *линейным*, если существуют такие векторы $\bar{a}_1, \ldots, \bar{a}_k, \bar{b} \in \mathbb{Z}^n$, что

$$L = \{t_1 \cdot \bar{a}_1 + \cdots + t_1 \cdot \bar{a}_1 + \bar{b} \mid t_i \in \mathbb{N}, i = 1 \ldots k\}$$

Конечное объединение линейных подмножеств $\mathbb{Z}$ назовем *полулинейным* множеством.

Имеет место следующая

Теорема 8.7. *Подмножество $M \subseteq \mathbb{Z}^n$ определимо некоторой формулой $F(x_1, \ldots, x_n)$ сигнатуры σ, т.е.*

$$M = \{< m_1, \ldots, m_n > \mid \mathbb{Z}^+ \models F(m_1, \ldots, m_n)\},$$

в том и только в том случае, когда M полулинейно.

ЛЕКЦИЯ 9

§4. Теория Тарского.

В этом разделе мы рассмотрим теорию упорядоченного поля вещественных чисел. Это теория поля $\mathbb{R}$ в сигнатуре $\sigma =< \{0, +1, -1\}, \{+, \cdot\}, \{<\} >$. Напомним, что в примере 4 лекции 5 сигнатура упорядоченных полей не включала константного символа -1. Здесь он включен в сигнатуру исключительно из соображений удобства. Эта теория называется теорией Тарского ввиду следующей теоремы, принадлежащей А.Тарскому.

Теорема 9.1 (Тарский). *Теория $Th(\mathbb{R})$ упорядоченного поля вещественных чисел допускает эффективное исключение кванторов.*

Не имея, возможности доказывать здесь эту теорему в полном объеме, ограничимся рассмотрением одного частного случая. Прежде всего заметим,

что каждая функция на $\mathbb{R}^n$, определяемая термом сигнатуры σ, есть некоторый многочлен $p(x_1, \ldots, x_n)$ с целыми коэффициентами (см. пример 1 к определению 6.3). Значит атомарные формулы сигнатуры σ могут быть записаны в виде $p(x_1, \ldots, x_n) = 0$ или $p(x_1, \ldots, x_n) > 0$. В соответствии с предложением 7.4 достаточно научиться исключать квантор из формул вида $\exists x B(x)$, где B – конъюнкция атомарных формул или их отрицаний. Имеем $\neg p = 0 \equiv p > 0 \vee p < 0$, $\neg p > 0 \equiv p \leq 0 \equiv -p > 0 \vee p = 0$. Заменяя при помощи этих эквивалентностей все отрицания атомарных формул, раскрывая скобки и пронося квантор $\exists$ через дизъюнкцию, приходим к тому, что достаточно научиться исключать квантор из формул вида

$$\exists x(p_1(x) = 0 \wedge \cdots \wedge p_n(x) = 0 \wedge q_1(x) > 0 \wedge \cdots \wedge q_m(x) > 0), \tag{9.1}$$

где p_i и q_j есть многочлены от переменной x, коэффициенты которых сами являются многочленами с целыми коэффициентами от других переменных, либо целыми числами. Поскольку в $\mathbb{R}$

$$p_1(x) = 0 \wedge \cdots \wedge p_n(x) = 0 \equiv p_1^2(x) + \cdots + p_n^2(x) = 0,$$

достаточно ограничиться рассмотрением формул вида (9.1), содержащих только одно уравнение и, возможно, несколько неравенств. Мы здесь рассмотрим только формулы вида

$$\exists x(p(x) = 0). \tag{9.2}$$

В случае, когда степень многочлена p по переменной x не превосходит 2, исключение кванторов из формулы (9.2) осуществляется следующим образом:

$$\begin{aligned} &\exists x(ax^2 + bx + c = 0) \equiv_{\mathbb{R}} \ a = 0 \wedge b = 0 \wedge c = 0 \vee \\ &\vee a = 0 \wedge b \neq 0 \vee a \neq 0 \wedge b^2 - 4ac \geq 0. \end{aligned}$$

Здесь a, b, c – многочлены с целыми коэффициентами от других переменных, либо целые числа.

В общем случае исключение кванторов из формулы вида (9.2) осуществляется при помощи теоремы Штурма. Чтобы продемонстрировать как это делается, но избежать слишком громоздких вычислений, рассмотрим формулу

$$\exists x(x^4 + bx + c = 0), \tag{9.3}$$

где, как и выше, b, c – многочлены с целыми коэффициентами от других переменных, либо целые числа. При этом можно считать, что $b \neq 0$, т.к. в противном случае формула (9.3) равносильна формуле $c \leq 0$.

Рассмотрим многочлен $f(x) = x^4 + bx + c$. Его дискриминант $D(f) = 256c^3 - 27b^4$. Если $D(f) \neq 0$, то $(f, f') = 1$. В этом случае система Штурма для f имеет вид:

$$f_0(x) = f(x),\ f_1(x) = f'(x) = 4x^3 + b,\ f_2(x) = -3bx - 4c,\ f_3(x) = \frac{D(f)}{b^3}.$$

Обозначим через $V(\pm\infty)$ число перемен знаков в последовательности $f_0(\pm\infty), f_1(\pm\infty), f_2(\pm\infty), f_3(\pm\infty)$, где $f_i(\pm\infty)$ – знак многочлена $f_i(x)$ при $x \to \pm\infty$, который очевидным образом определяется по знаку старшего коэффициента многочлена f_i. Здесь возможны 4 случая :

a). $b > 0, D(f) > 0$: $V(-\infty) = 2,\ V(+\infty) = 2$;
b). $b > 0, D(f) < 0$: $V(-\infty) = 2, V(+\infty) = 1$;
c). $b < 0, D(f) > 0$: $V(-\infty) = 1, V(+\infty) = 1$;
d). $b < 0, D(f) < 0$: $V(-\infty) = 2, V(+\infty) = 1$.

В силу теоремы Штурма число вещественных корней многочлена f равно $V(-\infty) - V(+\infty)$, т.е. корни существуют в случаях b) и d).

Если $D(f) = 0$, то $(f, f') = f_2$, т.е. $g = \frac{f}{(f,f')}$ – многочлен третьей степени, а значит он имеет по крайней мере один вещественный корень, который является корнем многочлена f (напомним, что g имеет те же корни, что и f, но все они входят в g с кратностью, равной единице). Окончательно формула (9.3) равносильна формуле

$$b = 0 \wedge c \leq 0 \vee \neg b = 0 \wedge (D(f) = 0 \vee D(f) < 0).$$

Таким образом теорема Тарского по существу представляет собой обобщение теоремы Штурма на случай систем полиномиальных неравенств. Из описанного выше общего вида атомарных формул в $Th(\mathbb{R})$ следует, что каждое бескванторное атомарное предложение сигнатуры σ равносильно в $\mathbb{R}$ либо предложению $n > 0$, либо предложению $n \geq 0$ для некоторого $n \in \mathbb{Z}$. Отсюда видно, что существует алгоритм, распознающий по любому бескванторному атомарному предложению является оно истинным или ложным. Теперь, применяя предложение 7.8, получаем

Следствие 2. *Теория упорядоченного поля вещественных чисел* $Th(\mathbb{R})$ *разрешима.*

Именно последнее утверждение и было доказано А.Тарским в его знаменитой работе "A decision method for elementary algebra and geometry", появившейся в конце 40-х годов (второе издание в 1951 году). Первоначальное доказательство Тарского было очень сложным – работа имела более сотни страниц. Впоследствии это доказательство было упрощено Зайденбергом, Коэном

и другими авторами. Сравнительно короткое доказательство теоремы Тарского, основанное на идеях Коэна можно найти в книге [6].

Результат Тарского показал существование алгоритма для значительного формализованного фрагмента элементарной математики. По существу был предложен алгоритм решения задач элементарной алгебры, например, выяснения совместности произвольной системы алгебраических уравнений и неравенств. Пользуясь декартовыми системами координат можно и большинство предложений элементарной геометрии сформулировать в виде предложений языка теории $\mathrm{Th}(\mathbb{R})$. Например, предложение

$$\forall x_1, y_1, x_2, y_2((x_1 \neq x_2 \vee y_1 \neq y_2) \longrightarrow \exists A, B, C(Ax_1 + By_1 + C = 0 \wedge$$
$$\wedge Ax_2 + By_2 + C = 0 \wedge \forall A_1, B_1, C_1(A_1x_1 + B_1y_1 + C_1 = 0 \wedge$$
$$\wedge A_1x_2 + B_1y_2 + C_1 = 0 \longrightarrow \exists t(A_1 = tA \wedge B_1 = tB \wedge C_1 = tC)))$$

выражает геометрическую аксиому о том, что через две различные точки на плоскости проходит единственная прямая.

Аналогичным образом большинство теорем школьной геометрии может быть записано в языке теории $\mathrm{Th}(\mathbb{R})$. Это не относится к теоремам, в которых фигурируют площадь круга, объем шара и т.п., поскольку можно доказать, что добавление к сигнатуре σ еще одной константы, которая интерпретируется как число π делает теорию неразрешимой. Не имея возможности доказывать это утверждение, докажем аналогичное, но более простое предложение.

Рассмотрим сигнатуру σ_1, которая получается из σ добавлением одного одноместного функционального символа. Этот символ мы будем обозначать sin и интерпретировать в $\mathbb{R}$ как функцию $\sin(x)$. Множество всех предложений сигнатуры σ_1, истинных в $\mathbb{R}$ будем обозначать $\mathrm{Th}_1(\mathbb{R})$.

Предложение 9.2. *Теория $Th_1(\mathbb{R})$. не допускает исключения кванторов и неразрешима.*

Доказательство. Мы будем пользоваться тем фактом, что теория алгебры $\mathbb{N}$ в сигнатуре $\sigma_2 < \{0\}, \{+, \cdot\}, \emptyset >$ неразрешима. Это будет доказано в нашем курсе позднее. Из предложения 7.8 следует, что если бы теория $\mathrm{Th}(\mathbb{N})$ допускала эффективное исключение кванторов, то она была бы разрешима. Значит она не допускает эффективного исключения кванторов. На самом деле можно доказать, что эта теория вообще не допускает исключения кванторов.

Покажем, что теория $\mathrm{Th}(\mathbb{N})$ эффективно интерпретируется в теории $\mathrm{Th}_1(\mathbb{R})$ (см. определение 8.4). После этого наше утверждение будет следовать из предложения 8.5.

Сначала покажем, что в сигнатуре σ_1 можно определить одноместный предикат $Nat(x)$, такой, что в $\mathbb{R}$

$$Nat(x) = \mathbf{И} \Longleftrightarrow x - - \text{натуральное число}$$

Идея состоит в том, что натуральное число есть отношение произвольного неотрицательного периода к наименьшему положительному периоду. Определим предикат

$$P(t) \rightleftharpoons \forall x(\sin(x+t) = \sin x) \wedge t \geq 0.$$

Ясно, что $P(t) = \mathbf{И} \Longleftrightarrow t$ – неотрицательный период функции $\sin(x)$. Наименьший положительный период определяется формулой

$$MP(t) \rightleftharpoons P(t) \wedge t > 0 \wedge \forall s(P(s) \wedge s > 0 \longrightarrow t \leq s$$

Теперь очевидно, что

$$Nat(x) \equiv \exists t \exists s(P(t) \wedge MP(s) \wedge t = x \cdot s.$$

Доказательство нашего предложения непосредственно вытекает из следующего утверждения (см. определение 8.4 и предложение 8.5).

По любой формуле $F(x_1, \ldots, x_n)$ сигнатуры σ_2 можно построить такую формулу $F'(x_1, \ldots, x_n)$ сигнатуры σ_1, что для любых $k_1, \ldots, k_n \in \mathbb{N}$

$$\mathbb{N} \models F(k_1, \ldots, k_n) \Longleftrightarrow \mathbb{R} \models F'(k_1, \ldots, k_n)$$

Это утверждение легко доказывается индукцией по построению формулы F

Для атомарной формулы F сигнатуры σ_2 очевидно $F' = F$.

Если для формул F и G требуемые формулы F' и G' уже построены, то очевидно, что:

$$(F \wedge G)' = F' \wedge G';\ (F \vee G)' = F' \vee G';\ (\neg F)' = \neg F';$$
$$(\forall x F)' = \forall x(Nat(x) \longrightarrow F');\ (\exists x F)' = \exists x(Nat(x) \wedge F'). \blacksquare$$

Естественный вопрос, который здесь возникает – является ли разрешимой аналогичная теория $\mathrm{Th}_2(\mathbb{R})$, которая получается если интерпретировать одноместный функциональный символ сигнатуры σ_1 не как синус, а как экспоненту (естественно в этом случае его следует и обозначать exp). Эта проблема поставленная еще в 50-х годах оказалась очень трудной. Она не решена и до сих пор, но в последнее время в ее исследовании достигнут существенный прогресс – доказано, что области истинности одноместных предикатов, определимых формулами этой теории, содержат лишь конечное число граничных точек, т.е. представляют собой конечные объединения интервалов всевозможных видов (открытых, замкнутых, полуоткрытых, полуограниченных и т.п.). Отметим, что вопрос о разрешимости этой теории связан с известной в теории чисел классической проблемой об алгебраической независимости чисел e и π, которая состоит в том, чтобы доказать, что не существует многочлена

$p(x,y) \in \mathbb{Z}[x,y]$, удовлетворяющего условию $p(\pi, e) = 0$. В самом деле, если бы такой многочлен существовал, то константа π была бы определима в теории $\mathrm{Th}_2(\mathbb{R})$, что влекло бы неразрешимость ее, т.к., как отмечалось уже добавление π к теории Тарского приводит к неразрешимой теории. Таким образом доказательство разрешимости $\mathrm{Th}_2(\mathbb{R})$ привело бы к доказательству гипотезы об алгебраической независимости e и π.

ЛЕКЦИЯ 10

Изучим более подробно области истинности предикатов, определимых формулами сигнатуры σ теории Тарского. Из рассмотрений в начале предыдущей лекции следует, что каждая бескванторная формула сигнатуры σ равносильна дизъюнкции конечного числа конъюнкций формул вида $p(x_1, \ldots, x_n) > 0$ и $q(x_1, \ldots, x_n) \geq 0$, где $p, q \in \mathbb{Z}[x_1, \ldots, x_n]$. Область истинности каждой такой конъюнкции есть решение системы полиномиальных неравенств. Эти соображения приводят к следующему определению.

Определение 10.1. Подмножество $M \subseteq \mathbb{R}^n$ называется *элементарным полуалгебраическим*, если оно является множеством решений системы полиномиальных неравенств вида

$$\begin{aligned} &p_1(x_1, \ldots, x_n) > 0, \\ &\ldots\ldots\ldots\ldots\ldots \\ &p_k(x_1, \ldots, x_n) > 0, \\ &q_1(x_1, \ldots, x_n) \geq 0, \\ &\ldots\ldots\ldots\ldots\ldots \\ &q_l(x_1, \ldots, x_n) \geq 0, \end{aligned} \tag{10.1}$$

где p_i и q_j – многочлены с *вещественными* коэффициентами.

Конечное объединение элементарных полуалгебраических множеств называется *полуалгебраическим* множеством.

Таким образом область истинности предиката в $\mathbb{R}^n$, определяемого любой бескванторной формулой сигнатуры σ представляет собой полуалгебраическое множество.

Класс полуалгебраических множеств включает в себя класс алгебраических многообразий (множеств решений систем алгебраических уравнений).

Очевидно класс полуалгебраических множеств замкнут относительно булевых операций и декартова произведения. Следующая теорема, которая легко следует из теоремы 9.1, показывает, что этот класс замкнут и относительно проекций.

Теорема 10.2 (Тарский – Зайденберг). *Проекция элементарного полуалгебраического множества вдоль любой координатной оси есть полуалгебраическое множество.*

Доказательство. . Пусть $A \subseteq \mathbb{R}^{n+k}$ – полуалгебраическое множество $c_1, \ldots, c_k \in \mathbb{R}$. Поскольку для любого многочлена $f(x_1, \ldots, x_n, y_1, \ldots, y_k)$ функция $f(x_1, \ldots, x_n, c_1, \ldots, c_k)$ представляет собой многочлен от переменных $x_1, \ldots, x_n$, то множество $\{\langle x_1, \ldots, x_n\rangle \mid \langle x_1, \ldots, x_n, c_1, \ldots, c_k\rangle \in A\}$ тоже является полуалгебраическим.

Пусть теперь A – множество решений системы (10.1). Покажем, что проекция A вдоль оси x_1 является полуалгебраическим множеством.

Пусть $c_1, \ldots, c_k$ – полный набор вещественных коэффициентов многочленов, входящих в систему (10.1). Выберем переменные Рассмотрим многочлены $\bar{p}_i(x_1, \ldots, x_n, y_1, \ldots, y_k)$, $\bar{q}_j(x_1, \ldots, x_n, y_1, \ldots, y_k) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_k]$, $i = 1, \ldots, k, j = 1, \ldots, l$, такие, что $\bar{p}_i(x_1, \ldots, x_n, c_1, \ldots, c_k) = p_i(x_1, \ldots, x_n)$, $\bar{q}_j(x_1, \ldots, x_n, c_1, \ldots, c_k) = q_j(x_1, \ldots, x_n)$. В силу теоремы 8.1 формула $F(x_2, \ldots, x_n, y_1, \ldots, y_k)$, равная

$$\exists x_1(\bar{p}_1(x_1, \ldots, x_n, y_1, \ldots, y_k) \wedge \cdots \wedge \bar{p}_2(x_1, \ldots, x_n, y_1, \ldots, y_k) \wedge$$
$$\wedge \bar{q}_1(x_1, \ldots, x_n, y_1, \ldots, y_k) \wedge \cdots \wedge \bar{q}_1(x_1, \ldots, x_n, y_1, \ldots, y_k)),$$

равносильна в $Th(\mathbb{R})$ некоторой бесквантворной формуле, т.е. ее область истинности есть полуалгебраическое множество B. Теперь проекция множества A вдоль оси x_1 равна $\{\langle x_2, \ldots, x_n\rangle \mid \langle x_2, \ldots, x_n, c_1, \ldots, c_k\rangle \in B\}$ т.е. является полуалгебраическим множеством в силу замечания, сделанного в первом абзаце доказательства ■.

Пример.
Гипербола $xy = 1$ – алгебраическое многообразие и, следовательно – элементарное полуалгебраическое множество . Его проекция вдоль оси OY представляет собой полуалгебраическое множество, $\{x \in \mathbb{R} \mid x \neq 0\}$, которое является объединением двух элементарных полуалгебраических множеств $\{x \in \mathbb{R} \mid x > 0\} \cup \{x \in \mathbb{R} \mid x < 0\}$.
Задача*. Доказать, что это множество не является элементарным полуалгебраическим.

Рассмотрим теперь сигнатуру σ', которая получается добавлением к σ всевозможных константных символов вида c_α, $\alpha \in \mathbb{R}$. Будем считать, что каждый символ c_α интерпретируется в $\mathbb{R}$ как α. Из теоремы 10.2 немедленно вытекает следующая теорема, которую мы также будем называть теоремой Тарского – Зайденберга.

Теорема 10.3. *Подмножество $A \subseteq \mathbb{R}^n$ представляет собой область истинности предиката, определяемого некоторой бескванторной формулой сигнатуры σ' в том и только в том случае, когда A – полуалгебраическое множество.*

Теорема Тарского – Зайденберга имеет важные применения в анализе и алгебраической геометрии. Проиллюстрируем возможность ее применений на нескольких примерах.

Отображение подмножеств $\mathbb{R}^n$ назовем *полуалгебраическим*, если его график есть полуалгебраическое множество.

Предложение 10.4. *Если $A \subseteq \mathbb{R}^n$, $B \subseteq \mathbb{R}^k$ и $f : A \longrightarrow B$ – полуалгебраическое отображение, то $A = domf$ и $rngf$ – область значений отображения f – полуалгебраические множества.*

Доказательство. Из теоремы 10.3 следует, что любое подмножество $\mathbb{R}^m$, определимое формулой сигнатуры σ' есть полуалгебраическое множество. Пусть формула $F(\bar{x}, \bar{y})$ определяет график отображения f. Тогда $A = \{\bar{x} \in \mathbb{R}^n \mid \exists \bar{y} F(\bar{x}, \bar{y})\}$, а $\mathrm{rng} f = \{\bar{y} \in \mathbb{R}^k \mid \exists \bar{x} F(\bar{x}, \bar{y})\}$, т.е. оба эти множества определимы формулами сигнатуры σ'■.

Следствие. *Образ полуалгебраического множества при полуалгебраическом отображении есть полуалгебраическое множество.*

Напомним, что расстоянием от точки $\bar{x} \in \mathbb{R}^n$ до множества $A \subseteq \mathbb{R}^n$ называется число $\mathrm{dist}(\bar{x}, A) = \inf\{|\bar{x} - \bar{y}| \mid \bar{y} \in A\}$.

Предложение 10.5. *Если $A \subseteq \mathbb{R}^n$ – полуалгебраическое множество, то функция $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ такая, что $f(\bar{x}) = dist(\bar{x}, A)$ есть полуалгебраическая функция.*

Доказательство. Пусть $G(\bar{x})$ – формула сигнатуры σ', определяющая множество A. Напишем формулу $F(\bar{x}, y)$, определяющую график функции f. Тем самым предложение будет доказано. Легко видеть, что эта формула имеет следующий вид:

$$y \geq 0 \wedge \forall \bar{y}(G(\bar{y}) \longrightarrow y^2 > (x_1 - y_1)^2 + \cdots + (x_n - y_n)^2 \wedge$$
$$\wedge \forall b > 0 \exists \bar{y}(G(\bar{y}) \wedge (x_1 - y_1)^2 + \ldots (x_n - y_n)^2 > y^2 - b) \blacksquare$$

Предложение 10.6. *Производная от полуалгебраической функции сама является полуалгебраической функцией*

Доказательство. Упражнение ■

Доказательство теоремы Тарского – Зайденберга и ее приложения, важные для исследования уравнений в частных производных, можно найти в книге:

Л.Хермандер. Анализ линейных дифференциальных операторов с частными производными. Т.2. Дифференциальные операторы с постоянными коэффициентами. М.:Мир. 1986 (Добавление А).

В настоящее время ведутся интенсивные исследования различных расширений теории Тарского. Ниже приводится очень короткое введение в полученные здесь результаты. Сделаем сначала несколько замечаний общего характера. Пусть имеется произвольная алгебраическая система $\mathcal{M} = \langle M, i\rangle$ сигнатуры $\sigma = \langle \mathcal{C}, \mathcal{F}, \mathcal{P}\rangle$. Обозначим через $\mathcal{S}^n_\sigma(M)$ – семейство всех n-местных предикатов на M, определимых формулами сигнатуры σ, $\mathcal{S}_\sigma(M) = \bigcup\limits_{n\in\mathbb{N}} \mathcal{S}^n_\sigma(M)$. Отождествляя предикаты с их областями истинности можно считать, что $\mathcal{S}^n_\sigma(M)$ есть семейство подмножеств M^n для каждого $n \in \mathbb{N}$. Легко видеть, что эти семейства обладают следующими свойствами.

S1 $\mathcal{S}^n_\sigma(M)$ – булева алгебра подмножеств M^n;
S2 $\Delta_{ij}(M) = \{\bar{x} \in M^n \mid x_i = x_j\} \in \mathcal{S}^n_\sigma(M),\ 1 \le i \le j \le n$;
S3 $A \in \mathcal{S}^n_\sigma(M) \Longrightarrow M \times A, A \times M \in \mathcal{S}^n_\sigma(M)$;
S4 $A \in \mathcal{S}^{n+1}_\sigma(M) \Longrightarrow \pi(A) \in \mathcal{S}^n_\sigma(M)$, где $\pi(x_1, \ldots, x_n, x_{n+1}) = (x_1, \ldots, x_n,)$;
S5 графики функций $i(f),\ f \in \mathcal{F}$, а также области истинности предикатов $i(P),\ P \in \mathcal{P}$ лежат в $\mathcal{S}_\sigma(M)$.

Назовем *структурой* на M семейство подмножеств $\mathcal{T} = \bigcup\limits_{n\in\mathbb{N}} \mathcal{T}^n$, где $\mathcal{T}^n \subseteq 2^{M^n}$, удовлетворяющих свойствам S1 – S4. Тогда очевидно, что $\mathcal{S}_\sigma(M)$ – наименьшая структура на M, обладающая свойством S5.

Теорема Тарского - Зайденберга показывает, что полуалгебраические множества образуют структуру на $\mathbb{R}$. Эта структура есть в точности $\mathcal{S}_{\sigma'}(\mathbb{R})$, где σ' – сигнатура, фигурирующая в теореме 10.3. Заметим, что поскольку $x \le y \equiv \exists z(y = x + z^2)$, то полуалгебраические множества образуют наименьшую структуру, содержащую графики функций $x + y = z$ и $x \cdot y = z$. Очевидно также, что $\mathcal{S}^1_{\sigma'}(\mathbb{R})$ состоит из множеств, имеющих конечное число компонент связности, т.е. представляющих собой конечные объединения интервалов всех видов. Эти замечания приводят к следующему определению.

Определение 10.7. Структура $\mathcal{T}$ на $\mathbb{R}$ называется о-минимальной (order minimal), если она содержит графики функций $x + y = z$ и $x \cdot y = z$ и $\mathcal{T}^1$ состоит из множеств, имеющих конечное число компонент связности.

Таким образом полуалгебраические множества образуют наименьшую о-минимальную структуру на $\mathbb{R}$.

Ниже $\bar{x} = (x_1, \ldots, x_n)$, а $e^{\bar{x}} = (e^{x_1}, \ldots, e^{x_n})$. Множества вида $\{\bar{x} \in \mathbb{R}^n \mid P(\bar{x}, e^{\bar{x}}) = 0\}$, где P – многочлен с вещественными коэффициентами от $2n$ переменных, назовем *экспоненциальными*, а образы экспоненциальных множеств при отображении проектирования $\pi : \mathbb{R}^{n+k} \to \mathbb{R}^n$ назовем *субэкспоненциальными* множествами.

Теорема 10.8(Вильке). *Субэкспоненциальные множества образуют о-минимальную структуру на* $\mathbb{R}$

Поскольку замкнутость субэкспоненциальных множеств относительно объединений, пересечений, декартовых произведений и проектирований очевидна, то для доказательства теоремы Вильке достаточно доказать лишь, что дополнение до субэкспоненциального множества есть субэкспоненциальное множество. Это и было сделано Вильке на основании глубокого исследования теории $Th(\mathbb{R})$ в сигнатуре σ'', которая получается из σ' добавлением одноместного функционального символа exp со стандартной интерпретацией. Теорема 10.8 показывает, что структура $\mathcal{S}_{\sigma''}(\mathbb{R})$ совпадает со структурой субэкспоненциальных множеств. Таким образом можно утверждать, что каждая формула в языке сигнатуры σ'' равносильна в $\mathbb{R}$ формуле вида $\exists \bar{y} F(\bar{x}, \bar{y})$, где $F(\bar{x}, \bar{y})$ – бескванторная формула. Мы не имеем здесь возможности доказывать теорему Вильке, а также следующую теорему, в которой описана наиболее общая известная в настоящее время о-минимальная структура.

Теорема 10.9 (Ван ден Дрис, Макинтайр). *Образы в* $\mathbb{R}^n$ *для* $n = 0, 1, 2 \ldots$ *при отображениях проектирования* $\pi : \mathbb{R}^{n+k} \to \mathbb{R}^n$ *множеств вида*

$$\{(\bar{x}, \bar{y}) \in \mathbb{R}^{(n+k)} \mid P(\bar{x}, \bar{y}, \varepsilon^{\bar{x}}, e^{\bar{y}}) = 0, f(\bar{x}, \bar{y}) = 0\},$$

где P *– многочлен с вещественными коэффициентами от* $2(n+k)$ *переменных, а* f *– вещественная функция, аналитическая в некотором параллелепипеде* $[a_1, b_1] \times \cdots \times [a_{n+k}, b_{n+k}]$ *и тождественно равная нулю вне его, образуют о-минимальную структуру.*

Из этой теоремы в частности следует, что если к сигнатуре теории Тарского добавить одноместный функциональный символ f интерпретировать его как функцию, равную $\sin x$ на произвольном конечном интервале и нулю, вне этого интервала, то подмножества $\mathbb{R}$, определимые в полученной теории, имеют лишь конечное число компонент связности. Это неверно, если интерпретировать этот функциональный символ как функцию, равную $\sin x$ всюду на $\mathbb{R}$, поскольку тогда в этой теории определимо множество $\mathbb{N}$ (см. доказательство предложения 9.2).

Интерес к о-минимальным структурам связан с тем, что множества, входящие в 0-минимальные структуры обладают многими хорошими топологическими свойствами – например, каждое такое множество имеет лишь конечное число компонент линейной связности. С другой стороны, как показывает последняя теорема, класс таких множеств достаточно широк. Для иллюстрации приведем одну весьма эффектную теорему о функциях, входящих в о-минимальные структуры.

Теорема 10.10. *Пусть график функции f, определенной на некотором интервале (a, b), принадлежит какой-то о-минимальной структуре. Тогда для любого натурального числа r существует возрастающая конечная последовательность $a = a_0 < a_1 < \cdots < a_N = b$, что ограничение функции f на каждый интервал (a_i, a_{i+1}) имеет r непрерывных производных и либо постоянно, либо строго монотонно.*

Более подробную информацию об о-минимальных структурах и ссылки на относящуюся к ним литературу можно найти в книге А.Г.Хованский. Малочлены. М.: Фазис, 1997.

В заключение сделаем еще одно важное замечание. Внимательный анализ пропущенного здесь доказательства теоремы Тарского (теорема 9.1) показывает, что оно проходит в любом вещественно замкнутом поле (см. пример 4 лекции 5). В частности доказательство теоремы Штурма в вещественно замкнутом поле содержится в известных учебниках по алгебре Б.Л. ван дер Вардена и С.Ленга. Следовательно, имеет место

Предложение 10.11. *Теория класса вещественно замкнутых полей допускает эффективное исключение кванторов.*

Легко понять, что всякое вещественно замкнутое поле имеет характеристику ноль, т.е. содержит простое подполе, изоморфное $\mathbb{Q}$. Следовательно все не содержащие переменных термы сигнатуры σ имеют одинаковые значения во всех вещественно замкнутых полях, поскольку эти значения получается в результате конечного числа применений операций сложения и умножения к константам 0,1,-1, а все эти вычисления проходят в кольце $\mathbb{Z} \subseteq \mathbb{Q}$. А это значит, что любое атомарное бескванторное предложение истинно или ложно во всех вещественно замкнутых полях одновременно. Тем самым это справедливо и для произвольных бескванторных предложений. Теперь из предложения 7.8 немедленно вытекает такое

Следствие. *i). Теория класса вещественно замкнутых полей разрешима.*
ii). Любые два вещественно замкнутых поля элементарно эквивалентны.

Отсюда, например, следует, что в любом вещественно замкнутом поле, любое непрерывное полуалгебраическое отображение замкнутого отрезка в себя имеет неподвижную точку. Для этого, используя формулу для графика данного отображения f следует записать предложение сигнатуры σ, утверждающее, что если f непрерывно и отображает замкнутый отрезок в себя то оно имеет неподвижную точку. Это предложение, будучи истинным в $\mathbb{R}$, истинно по предыдущему следствию и в любом другом вещественно замкнутом поле. Примером вещественно замкнутого поля, отличного от $\mathbb{R}$, является поле вещественных алгебраических чисел. Известно, что любое упорядоченное поле

является подполем некоторого вещественно замкнутого поля. Наименьшее такое поле называется вещественным замыканием исходного поля.

ЛЕКЦИЯ 11

ГЛАВА III. Исчисление предикатов и формальные теории

§1. Исчисление предикатов.

Мы переходим к изучения понятия формального доказательства. Понятие доказательства формализуется в рамках так называемого исчисления предикатов (ИП). В исчислении предикатов выделяется некоторый класс предложений языка L_σ, которые называются аксиомами исчисления предикатов и определяются *формальные* правила, по которым одни предложения считаются следствиями других. Эти правила называются правилами вывода. Слово "формальные" здесь означает, что правила вывода определяются только видом предложений как слов в алфавите $\mathcal{S}$ и не зависят от их истинности или ложности. Формальными теоремами ИП называются предложения, которые получаются из аксиом исчисления предикатов многократным последовательным применением правил вывода. Тем самым выделяется некоторый класс предложений – теорем исчисления предикатов.

Этот формальный или, как еще говорят, *синтаксический* подход к определению теорем исчисления предикатов оказывается адекватным описанному выше содержательному подходу, основанному на понятии истинности (который еще называется *семантическим*). Аксиомы ИП выделяются среди логически общезначимых предложений языка L_σ и правила вывода определены так, что предложения, которые следуют из логически общезначимых предложений, сами являются логически общезначимыми. Отсюда следует, что все теоремы ИП тоже логически общезначимы. Значительно более нетривиальный факт состоит в том, что *все* логически общезначимые предложения являются теоремами ИП. Этот факт является следствием теоремы Геделя о полноте. Эквивалентность синтаксического и семантического подходов имеет важные приложения не только в логике, но и в алгебре и даже в анализе. Эти приложения изучает *теория моделей*.

Ниже считается, что сигнатура σ содержит не менее, чем счетный набор константных символов. Если это не так, то такой набор к сигнатуре присоединяется. Начнем с перечисления аксиом ИП.

Определение 11.1 (Аксиомы исчисления предикатов).

I. Аксиомы логики высказываний.

Пусть $F(p_1, \ldots, p_n)$ – ФЛВ, причем $\vdash F(p_1, \ldots, p_n)$, а $A_1, \ldots, A_n$ – предложения языка L_σ. Тогда $F(A_1, \ldots, A_n)$ – аксиома ИП. Аксиомы такого вида называются аксиомами логики высказываний.

II. Аксиомы равенства.

Пусть c и d – термы, не содержащие переменных (в частности, константы). Тогда следующие предложения являются аксиомами ИП, которые называются аксиомами равенства:

(1) c=c;

(2) $c = d \longrightarrow (A(c) \longleftrightarrow A(d))$, где предложение $A(d)$ получается заменой в предложении $A(c)$ всех или части вхождений терма c на d.

III. Аксиомы замены переменной.

Пусть A – предложение языка L_σ, а переменная x' не входит в A. Обозначим через A' – предложение, которое получается из A заменой всех вхождений переменной x на x'. Тогда $A \longleftrightarrow A'$ – аксиома ИП, которая называется аксиомой замены переменной.

IV. Аксиомы для кванторов.

Пусть $A(x)$ – формула языка L_σ с единственной свободной переменной x, B – предложение языка L_σ, не содержащее переменной x. Тогда следующие предложения являются аксиомами ИП, которые называются аксиомами для кванторов.

(1) $\forall x A(x) \longrightarrow A(t)$, где t – терм, не содержащий переменных.

(2) $\neg\forall x A(x) \longleftrightarrow \exists x \neg A(x)$.

(3) $\neg\exists x A(x) \longleftrightarrow \forall x \neg A(x)$.

(4) $\forall x(B \longrightarrow A(x)) \longleftrightarrow (B \longrightarrow \forall x A(x))$.

Предложение 11.2. *Все аксиомы ИП логически общезначимы.*

Доказательство. Логическая общезначимость аксиом типов I и II а также аксиомы 1 типа IV вытекает непосредственно из определения интерпретации формул в алгебраических системах (определение 6.4). Логическая общезначимость аксиом типа III и остальных аксиом типа IV следует из основных тождеств логики предикатов. В самом деле. Пусть $\mathcal{M} =< M, i >$ – а.с. сигнатуры σ. Тогда аксиома 4 для кванторов интерпретируется, как нульместный предикат

$$\forall x(i(B) \longrightarrow i(A)(x)) \longleftrightarrow (i(B) \longrightarrow \forall x i(A)(x)),$$

который истинен, если значения предикатов, стоящих слева и справа от эквивалентности, равны. Заменяя импликацию в обеих частях последнего равенства через дизъюнкцию и отрицание и воспользовавшись вторым из равенств (4) теоремы 3.1, получаем требуемое ■

Каждое правило вывода записывается в виде:

$$\frac{A_1, \ldots, A_n}{B}. \tag{11.1}$$

Эта запись означает, что предложение B следует по данному правилу из предложений $A_1, \ldots, A_n$.

Определение 11.3. В исчислении предикатов имеется два правила вывода – правило заключения (по латыни modus ponens):

$$\frac{A, A \longrightarrow B}{B},$$

и правило обобщения:

$$\frac{A(c) \longrightarrow B}{\exists x A(x) \longrightarrow B},$$

если предложение B не содержит константы c и переменной x.

Предложение 11.4. *Если предложение A следует по одному из правил вывода из логически общезначимых предложений, то оно само логически общезначимо.*

Доказательство. Для правила modus ponens утверждение очевидно. Чтобы доказать его для правила обобщения рассмотрим произвольную а.с. $\mathcal{M} =< M, i >$ сигнатуры σ. Пусть $\mathcal{M} \models \exists x A(x)$, т.е. существует $m \in M$, такое, что $\mathcal{M} \models A(m)$. Рассмотрим а.с. $\mathcal{M}' =< M, i' >$, где $i'(c) = m$, а на всех остальных объектах сигнатуры i' совпадает с i. Тогда $\mathcal{M}' \models A(c)$, а поскольку, по условию, $A(c) \longrightarrow B$ логически общезначимо, то $\mathcal{M}' \models B$. Но $i'(B) = i(B)$, т.е. $\mathcal{M} \models B$. Это означает, что $\mathcal{M} \models \exists x A(x) \longrightarrow B$, а поскольку $\mathcal{M}$ выбрана произвольно, то предложение $\exists x A(x) \longrightarrow B$ логически общезначимо ■

Определение 11.5. Последовательность $A_1, \ldots, A_n$ предложений языка L_σ называется доказательством предложения A_n, если каждое A_i $(i \leq n)$ есть либо аксиома ИП, либо следует из каких-нибудь предшествующих предложений этой последовательности по одному из правил вывода. Предложение A называется теоремой ИП (обозначение $\vdash A$), если существует хотя бы одно доказательство этого предложения.

Из предложений 11.2 и 11.4 немедленно вытекает следующее

Предложение 11.6. *Всякая теорема ИП логически общезначима* ■

Замечания. 1. Очевидно, что каждый начальный отрезок доказательства сам является доказательством, т.е. каждое предложение, входящее в доказательство, является теоремой ИП.

2. Если последовательность $A_1, \ldots, A_n$ предложений языка L_σ такова, что каждое A_i $(i \leq n)$ есть либо теорема ИП, либо следует из каких-нибудь предшествующих предложений этой последовательности по одному из правил вывода, то последнее предложение этой последовательности является теоремой ИП. Чтобы построить доказательство этой теоремы, нужно к каждому предложению A_i этой последовательности, являющемуся теоремой, приписать слева ее доказательство.

3. Легко понять, что определение доказательства является эффективным, т.е. в случае, когда сигнатура задана эффективно (например, когда она конечна), существует алгоритм, который по любой конечной последовательности предложений отвечает на вопрос о том, является ли эта последовательность доказательством. Это следует из того, что аксиомы ИП и правила вывода описаны эффективно, т.е. существует алгоритм, позволяющий по любому предложению за конечное число шагов определить является ли это предложение аксиомой ИП, а также алгоритм, позволяющий по любому набору (из не более, чем трех) предложений, определить следует ли одно из предложений этого набора из других по правилам вывода.

Построение доказательств тех или иных предложений является весьма непростым делом (позднее в нашем курсе будет показана алгоритмическая неразрешимость проблемы распознавания теорем). Чтобы несколько его облегчить введем несколько вспомогательных правил вывода. Ниже запись (11.1) означает, что если $A_1, \ldots, A_n$ – теоремы ИП, то и B – теорема ИП.

Предложение 11.7. *Имеют место следующие правила вывода:*

(1) *Правило цепочки импликаций.*

$$\frac{A_1 \longrightarrow A_2, A_2 \longrightarrow A_3, \ldots, A_{n-1} \longrightarrow A_n}{A_1 \longrightarrow A_n}$$

(2) *Правило цепочки эквивалентностей.*

$$\frac{A_1 \longleftrightarrow A_2, A_2 \longleftrightarrow A_3, \ldots, A_{n-1} \longleftrightarrow A_n}{A_1 \longleftrightarrow A_n}$$

(3) *Правила дизъюнкции.*

$$\frac{A}{A \vee B};\ \frac{B}{A \vee B};\ \frac{A \longrightarrow C, B \longrightarrow C}{(A \vee B) \longrightarrow C}$$

(4) *Правила конъюнкции.*

$$\frac{A \wedge B}{A};\ \frac{A \wedge B}{B};\ \frac{A \longrightarrow B, A \longrightarrow C}{A \longrightarrow B \wedge C};\ \frac{A, B}{A \wedge B}$$

(5) *Правило эквивалентной замены.*

$$\frac{A_1 \longleftrightarrow B_1, A_2 \longleftrightarrow B_2, \ldots, A_n \longleftrightarrow B_n}{F(A_1, \ldots, A_n) \longleftrightarrow F(B_1, \ldots, B_n)},$$

где $F(p_1, \ldots, p_n)$ *– произвольная ФЛВ.*

(6) *Правило эквивалентных преобразований.*

Пусть F *и* G *– такие ФЛВ, что* $\vdash F(p_1,\ldots,p_n) \longleftrightarrow G(p_1,\ldots,p_n)$, *а* $A_1,\ldots,A_n$ *– произвольные предложения языка* L_σ, *тогда*

$$\frac{F(A_1,\ldots,A_n)}{G(A_1,\ldots,A_n)}$$

Замечания. 1. Последнее правило показывает, что над теоремами ИП можно производить тождественные преобразования логики высказываний. При этом снова получаются теоремы ИП.

2. Последовательность предложений $A_1,\ldots,A_n$, в котором каждое A_i либо является теоремой ИП, либо следует из предшествующих по одному из основных или вспомогательных правил вывода, назовем обобщенным доказательством. Очевидно, что все предложения, входящие в обобщенное доказательство являются теоремами ИП.

3. Первые два правила для конъюнкции часто используется в виде

$$\frac{A \longleftrightarrow B}{A \longrightarrow B};\ \frac{A \longleftrightarrow B}{B \longrightarrow A}$$

Доказательство. Для доказательства правила (1) ограничимся для наглядности случаем $n = 3$. Общий случай рассматривается аналогично. Нам дано, что $A_1 \longrightarrow A_2$ и $A_2 \longrightarrow A_3$ – теоремы ИП. Построим обобщенное доказательство предложения $A_1 \longrightarrow A_3$.

1.$(A_1 \longrightarrow A_2) \longrightarrow ((A_2 \longrightarrow A_3) \longrightarrow (A_1 \longrightarrow A_3))$ (тавтология)

2.$A_1 \longrightarrow A_2$ (теорема ИП по условию)

3.$(A_2 \longrightarrow A_3) \longrightarrow (A_1 \longrightarrow A_3)$ (следует из 1. и 2. по modus ponens)

4.$A_2 \longrightarrow A_3$ (теорема ИП по условию)

5.$(A_1 \longrightarrow A_3)$ (следует из 3. и 4. по modus ponens)

Правило (2) доказывается аналогично. Рассмотрим одно из правил для конъюнкции:

$$\frac{A \longrightarrow B, A \longrightarrow C}{A \longrightarrow B \wedge C};$$

Пусть $A \longrightarrow B$ и $A \longrightarrow C$ – теоремы ИП. Тогда следующая последовательность является обобщенным доказательством предложения $A \longrightarrow B \wedge C$.

1.$(A \longrightarrow B) \longrightarrow ((A \longrightarrow C) \longrightarrow (A \longrightarrow B \wedge C))$ (тавтология)

2.$A \longrightarrow B$ (теорема ИП по условию)

3.$(A \longrightarrow C) \longrightarrow (A \longrightarrow B \wedge C)$ (следует из 1. и 2. по modus ponens)

4.$A \longrightarrow C$ (теорема ИП по условию)

5.$(A \longrightarrow B \wedge C)$ (следует из 3. и 4. по modus ponens)

Остальные правила для конъюнкции и правила для дизъюнкции доказываются аналогично.

Докажем правило эквивалентной замены. Легко видеть, что следующая ФЛВ

$$(A_1 \longleftrightarrow B_1) \longrightarrow ((A_2 \longleftrightarrow B_2) \longrightarrow \ldots \longrightarrow ((A_n \longleftrightarrow B_n) \longrightarrow \\ \longrightarrow (F(A_1, \ldots, A_n) \longleftrightarrow F(B_1, \ldots, B_n) \ldots) \tag{11.2}$$

В самом деле, применяя тождественные преобразования (выражение импликации через дизъюнкцию и отрицание, а также закон де Моргана) приходим к эквивалентной (11.2) формуле

$$(A_1 \longleftrightarrow B_1) \wedge (A_2 \longleftrightarrow B_2) \wedge \cdots \wedge (A_n \longleftrightarrow B_n) \longrightarrow \\ \longrightarrow (F(A_1, \ldots, A_n) \longleftrightarrow F(B_1, \ldots, B_n) \tag{11.3}$$

Покажем, что (11.3) – тавтология. В самом деле, если хотя бы одна из эквивалентностей $(A_i \longleftrightarrow B_i)$ то ложна и вся посылка импликации (11.3), а следовательно сама импликация истинна. Если же все эти эквивалентности истинны, то A_i и B_i имеют одинаковы истинностные значения при любом i, а следовательно $F(A_1, \ldots, A_n)$ и $F(B_1, \ldots, B_n)$ также принимают одинаковые значения. В этом случае и посылка и заключение импликации (11.3) истинны, т.е. и сама она истинна. Теперь, применяя к (11.2) n раз правило modus ponens, получаем требуемое.

Приведем также доказательство правила эквивалентных преобразований.

1. $F(A_1, \ldots, A_n) \longleftrightarrow G(A_1, \ldots, A_n)$ (тавтология по условию)
2. $F(A_1, \ldots, A_n) \longrightarrow G(A_1, \ldots, A_n)$ (правило 3а., см. замечание 3)
3. $F(A_1, \ldots, A_n)$ (теорема ИП по условию)
4. $G(A_1, \ldots, A_n)$ (2,3 - modus ponens)■

Приведем теперь для примера доказательства симметричности и транзитивности равенства. Здесь мы будем пользоваться самодистрибутивностью импликации:

$$\vdash (p \longrightarrow (q \longrightarrow r)) \longleftrightarrow ((p \longrightarrow q) \longrightarrow (p \longrightarrow r)) \tag{11.4}$$

Выпишем теперь доказательство предложения $c = d \longrightarrow d = c$.

1.$c = d \longrightarrow (c = c \longleftrightarrow d = c)$ (аксиома равенства 2)

2.$(c = c \longleftrightarrow d = c) \longrightarrow (c = c \longrightarrow d = c)$ (тавтология)

3.$c = d \longrightarrow (c = c \longrightarrow d = c)$ (цепочка импликаций)

4.$(c = d \longrightarrow c = c) \longrightarrow (c = d \longrightarrow d = c)$ (11.4 и правило экв. преобр.)

5.$c = c$ (аксиома равенства 1)

6.$c = c \longrightarrow (c = d \longrightarrow c = c)$ (тавтология)

7.$(c = d \longrightarrow c = c)$ (5,6 modus ponens)

8.$(c = d \longrightarrow d = c)$ (4,7 modus ponens)

Докажем теперь транзитивность равенства. Здесь мы воспользуемся эквивалентностью

$$\vdash (p \longrightarrow (q \longrightarrow r)) \longleftrightarrow (p \wedge q \longrightarrow r) \tag{11.5}$$

Теперь доказательство имеет вид:

1.$a = b \longrightarrow (a = c \longleftrightarrow b = c)$ (аксиома равенства 2)

2.$(a = c \longleftrightarrow b = c) \longrightarrow (b = c \longrightarrow a = c)$ (тавтология)

3.$a = b \longrightarrow (b = c \longleftrightarrow a = c)$ (цепочка импликаций)

4.$a = b \wedge b = c \longrightarrow a = c$ (11.5 и правило экв. преобр.)

Докажем теперь обобщение второй аксиомы равенства: для любой формулы $F(x_1, \ldots, x_n)$ языка L_σ

$$\vdash a_1 = b_1 \wedge \cdots \wedge a_n = b_n \longrightarrow (F(a_1, \ldots, a_n) \longleftrightarrow F(b_1, \ldots, b_n)) \tag{11.6}$$

Доказательство проведем для $n = 2$ поскольку переход от n к $n + 1$ такой же как от 1 к 2.

Применяя вторую аксиому равенства, получаем

$$\vdash a = c \longrightarrow (F(a, b) \longleftrightarrow F(c, b)); \vdash b = d \longrightarrow (F(c, b) \longleftrightarrow F(c, d))$$

Теперь, используя тавтологию

$$\vdash p \longrightarrow q \longrightarrow ((r \longrightarrow s) \longrightarrow (p \wedge r \longrightarrow q \wedge s)),$$

и применяя два раза правило MP, получаем

$$\vdash a = c \wedge b = d \longrightarrow (F(a, b) \longleftrightarrow F(c, b)) \wedge (F(c, b) \longleftrightarrow F(c, d)).$$

Теперь, применяя тавтологию

$$(F(a, b) \longleftrightarrow F(c, b)) \wedge (F(c, b) \longleftrightarrow F(c, d)) \longrightarrow (F(a, b) \longleftrightarrow F(c, d)),$$

и цепочку импликаций, получаем

$$\vdash a = c \wedge b = d \longrightarrow (F(a, b) \longleftrightarrow F(c, d)),$$

что и требовалось.

ЛЕКЦИЯ 12

Рассмотрим теперь три вспомогательных правила вывода, включающих кванторы.

Предложение 12.1. *Пусть x – переменная не входящая в формулы $A(c)$ и $B(c)$, где c – константа сигнатуры σ. Тогда имеют место следующие правила вывода:*

$$(1).\ \frac{A(c)}{\forall x A(x)};\ (2).\ \frac{A(c) \longleftrightarrow B(c)}{\forall x A(x) \longleftrightarrow \forall x B(x)};\ (3).\ \frac{A(c) \longleftrightarrow B(c)}{\exists x A(x) \longleftrightarrow \exists x B(x)}$$

Доказательство. (1). Предположим, что $A(c)$ – теорема. Выпишем доказательство $\forall x A(x)$.

1.$A(c)$ (теорема по условию)

2.$A(c) \longrightarrow (\neg A(c) \longrightarrow \mathbf{Л})$ (тавтология)

3.$\neg A(c) \longrightarrow \mathbf{Л}$ (1,2 – modus ponens)

4.$\exists x \neg A(x) \longrightarrow \mathbf{Л}$ (3 – правило обобщения)

5.$(\exists x \neg A(x) \longrightarrow \mathbf{Л}) \longrightarrow \neg \exists x \neg A(x)$ (тавтология)

6.$\neg \forall x A(x) \longleftrightarrow \neg \exists x \neg A(x)$ (аксиома для кванторов)

7.$(\neg \forall x A(x) \longleftrightarrow \neg \exists x \neg A(x)) \longrightarrow (\neg \exists x \neg A(x) \longrightarrow \forall x A(x))$ (тавтология $(\neg p \longleftrightarrow q) \longrightarrow (\neg q \longrightarrow p)$)

8.$\neg \exists x \neg A(x) \longrightarrow \forall x A(x)$ (6,7 – modus ponens)

9.$(\exists x \neg A(x) \longrightarrow \mathbf{Л}) \longrightarrow \forall x A(x)$ (5,8 – цепочка импликаций)

10.$\forall x A(x)$ (4,9 – modus ponens)

Докажем правило (2).

1.$\forall x A(x) \longrightarrow A(c)$ (аксиома для кванторов)

2.$A(c) \longleftrightarrow B(c)$ (теорема по условию)

3.$\forall x A(x) \longrightarrow B(c)$ (1,2 – цепочка импликаций)

4.$\forall y(\forall x A(x) \longrightarrow B(y))$ (3 – правило (1) этого предложения)

5.$\forall y(\forall x A(x) \longrightarrow B(y)) \longrightarrow (\forall x A(x) \longrightarrow \forall y B(y))$ (аксиома для кванторов)

6.$\forall x A(x) \longrightarrow \forall y B(y)$ (4,5 – modus ponens)

7.$\forall y B(y) \longrightarrow \forall x B(x)$ (аксиома замены переменной)

8.$\forall x A(x) \longrightarrow \forall x B(x)$ (6,7 – цепочка импликаций)

9.$\forall x B(x) \longrightarrow \forall x A(x)$ (доказательство аналогично)

10.$\forall x A(x) \longleftrightarrow \forall x B(x)$ (8,9 – правило конъюнкции – см. предл. 11.7)

Докажем правило (3).

1.$A(c) \longleftrightarrow B(c)$ (теорема по условию)
2.$\neg A(c) \longleftrightarrow \neg B(c)$ (правило эквивалентных преобразований)
3.$\forall x \neg A(x) \longleftrightarrow \forall x \neg B(x)$ (1 – правило (2) этого предложения)
4.$\forall x \neg A(x) \longleftrightarrow \neg \exists x A(x)$ (аксиома для кванторов)
5.$\forall x \neg B(x) \longleftrightarrow \neg \exists x B(x)$ (аксиома для кванторов)
6.$\neg \exists x A(x) \longleftrightarrow \neg \exists x B(x)$ (3,4,5 – цепочка эквивалентностей)
7.$\exists x A(x) \longleftrightarrow \exists x B(x)$ (правило эквивалентных преобразований)

Докажем теперь, что все основные тождества логики предикатов (теорема 3.1) являются теоремами ИП.

Предложение 12.2. *Пусть предложение D не имеет свободных вхождений переменной x. Тогда следующие предложения являются теоремами ИП:*

$(1). \vdash (\exists x(A(x) \vee B(x)) \longleftrightarrow (\exists x A(x) \vee \exists x B(x))$;
$(2). \vdash \forall x(A(x) \wedge B(x)) \longleftrightarrow (\forall x A(x) \wedge \forall x B(x))$;
$(3). \vdash \exists x(A(x) \wedge D) \longleftrightarrow (\exists x A(x) \wedge D)$;
$(4). \vdash \forall x(A(x) \vee D) \longleftrightarrow (\forall x A(x) \vee D)$;
$(5). \vdash \mathcal{Q}x\mathcal{Q}yA(x,y) = \mathcal{Q}y\mathcal{Q}xA(x,y)$,

где $\mathcal{Q}$ есть либо $\forall$, либо $\exists$.

Доказательство. Доказательство (4):

1.$(A(c) \vee D) \longleftrightarrow (\neg D \longrightarrow A(c))$ (тавтология)
2.$\forall x(A(x) \vee D) \longleftrightarrow \forall x(\neg D \longrightarrow A(x))$ (1 – правило 3 предложения 12.1)
3.$\forall x(\neg D \longrightarrow A(x)) \longleftrightarrow (\neg D \longrightarrow \forall x A(x))$ (аксиома для кванторов)
4.$(\neg D \longrightarrow \forall x A(x)) \longleftrightarrow (\forall x A(x) \vee D)$ (тавтология)
5.$\forall x(A(x) \vee D) \longleftrightarrow (\forall x A(x) \vee D)$ (2,3,4,5 – цепочка эквивалентностей)

Доказательство (3):

1.$\neg\exists x(A(x) \wedge D) \longleftrightarrow \forall x\neg(A(x) \wedge D)$ (аксиома для кванторов)
2.$\neg(A(c) \wedge D) \longleftrightarrow (\neg A(c) \vee \neg D)$ (тавтология)
3.$\forall x\neg(A(x) \wedge D) \longleftrightarrow \forall x(\neg A(x) \vee \neg D)$ (2, правило 2 предложения 12.1)
4.$\forall x(\neg A(x) \vee \neg D) \longleftrightarrow (\forall x\neg A(x) \vee \neg D)$
(теорема ИП (4) настоящего предложения)
5.$\forall x\neg A(x) \longleftrightarrow \neg\exists x A(x)$ (аксиома для кванторов)
6.$(\forall x\neg A(x) \vee \neg D) \longleftrightarrow (\neg\exists x A(x) \vee \neg D)$ (правило эквивалентной замены)
7.$(\neg\exists x A(x) \vee \neg D) \longleftrightarrow \neg(\exists x A(x) \wedge D)$ (тавтология)
8.$\neg\exists x(A(x) \wedge D) \longleftrightarrow \neg(\exists x A(x) \wedge D)$ (1 – 7 – цепочка эквивалентностей)
9.$\exists x(A(x) \wedge D) \longleftrightarrow (\exists x A(x) \wedge D)$(правило эквивалентных преобразований)

Доказательство (2):

1.$\forall x(A(x) \wedge B(x)) \longrightarrow A(c) \wedge B(c)$ (аксиома для кванторов)
2.$A(c) \wedge B(c) \longrightarrow A(c)$ (тавтология)
3.$\forall x(A(x) \wedge B(x)) \longrightarrow A(c)$ (1,2 – цепочка импликаций)
4.$\forall y(\forall x(A(x) \wedge B(x)) \longrightarrow A(y))$ (1 – правило 1 предложения 12.1)
5.$\forall y(\forall x(A(x) \wedge B(x)) \longrightarrow A(y)) \longleftrightarrow (\forall x(A(x) \wedge B(x)) \longrightarrow \forall y A(y))$
(аксиома для кванторов)
6.$\forall y A(y) \longleftrightarrow \forall x A(x)$ (аксиома замены переменной)
7.$\forall x(A(x) \wedge B(x)) \longrightarrow \forall x A(x)$ (1 – 6 – цепочка импликаций)
8.$\forall x(A(x) \wedge B(x)) \longrightarrow \forall x B(x)$ (доказательство аналогично)
9.$\forall x(A(x) \wedge B(x)) \longrightarrow \forall x A(x) \wedge \forall x B(x)$ (7,8 – правило для конъюнкции)
10.$\forall x A(x) \wedge \forall x B(x) \longrightarrow \forall x A(x)$ (тавтология)
11.$\forall x A(x) \longrightarrow A(c)$ (аксиома для кванторов)
12.$\forall x A(x) \wedge \forall x B(x) \longrightarrow A(c)$ (10,11 – цепочка импликаций)
13.$\forall x A(x) \wedge \forall x B(x) \longrightarrow B(c)$ (доказательство аналогично)
14.$\forall x A(x) \wedge \forall x B(x) \longrightarrow A(c) \wedge B(c)$ (12,13 – правило для конъюнкции)

15.$\forall y(\forall x A(x) \wedge \forall x B(x) \longrightarrow A(y) \wedge B(y))$ (14 – правило 1 предложения 12.1)

16.$\forall y(\forall x A(x) \wedge \forall x B(x) \longrightarrow A(y) \wedge B(y)) \longleftrightarrow (\forall x A(x) \wedge \forall x B(x) \longrightarrow$
$\longrightarrow \forall y(A(y) \wedge B(y)))$ (аксиома для кванторов)

17.$\forall x A(x) \wedge \forall x B(x) \longrightarrow \forall y(A(y) \wedge B(y))$ (15,16 – modus ponens)

18.$\forall y(A(y) \wedge B(y)) \longleftrightarrow \forall x(A(x) \wedge B(x))$ (аксиома замены переменной)

19.$\forall x A(x) \wedge \forall x B(x) \longrightarrow \forall x(A(x) \wedge B(x))$ (цепочка импликаций)

20.$\forall x(A(x) \wedge B(x)) \longleftrightarrow (\forall x A(x) \wedge \forall x B(x))$ (9,19 – правило для конъюнкции)

Доказательства теорем (1) и (5) предоставляются читателю в качестве упражнения. ■

Замечание. Рассмотренные выше вспомогательные правила вывода и доказанные только что теоремы ИП показывают, что если к теореме ИП применить тождественные преобразования, использующие как основные тождества логики высказываний, так и основные тождества логики предикатов, то вновь получится теорема ИП.

Упражнение. Доказать следующие теоремы ИП:

1. $\vdash (\forall x A(x) \vee \forall x B(x)) \longrightarrow \forall x(A(x) \vee B(x))$
2. $\vdash \exists x(A(x) \wedge B(x)) \longrightarrow (\exists x A(x) \wedge \exists x B(x))$
3. $\vdash \exists x \forall y A(x, y) \longrightarrow \forall y \exists x A(x)$

§2. Формальные теории.

Определение 12.3. Пусть Γ – множество предложений языка L_σ. Говорят, что предложение A выводится из Γ и пишут $\Gamma \vdash A$, если существует такое конечное множество предложений $A_1, \ldots, A_k \in \Gamma$, что $\vdash A_1 \wedge \cdots \wedge A_k \longrightarrow A$.

Предложение 12.4. *Если* $\vdash A$, *то для любого множества* Γ *выполняется* $\Gamma \vdash A$

Доказательство. Пусть $B \in \Gamma$ тогда

$\vdash A \longrightarrow (B \longrightarrow A)$ (тавтология)

$\vdash A$ (по условию)

$\vdash B \longrightarrow A$ modus ponens

Последняя теорема ИП и показывает требуемое ■

Предложение 12.5. *Если* $\Gamma \vdash A$ *и для любого* $B \in \Gamma$ *имеет место* $\Gamma' \vdash B$, *то* $\Gamma' \vdash A$.

Доказательство. Пусть $B_1, \ldots, B_k \in \Gamma$ и $\vdash B_1 \wedge \cdots \wedge B_k \longrightarrow A$. Пусть, также $A_1^{(1)}, \ldots, A_{s_1}^{(1)}, \ldots A_1^{(k)}, \ldots, A_{s_k}^{(k)} \in \Gamma'$ таковы, что $\vdash A_1^{(i)}, \ldots, A_{s_i}^{(i)} \longrightarrow B_i$ $i = 1, \ldots k$. Имеем

$$\vdash A_1^{(1)} \wedge \cdots \wedge A_{s_1}^{(1)} \wedge \cdots \wedge A_1^{(k)} \wedge \cdots \wedge A_{s_k}^{(k)} \longrightarrow A_1^{(i)} \wedge \cdots \wedge A_{s_i}^{(i)} \; i = 1, \ldots, k,$$

поскольку это тавтологии. Следовательно

$$\vdash A_1^{(1)} \wedge \cdots \wedge A_{s_1}^{(1)} \wedge \cdots \wedge A_1^{(k)} \wedge \cdots \wedge A_{s_k}^{(k)} \longrightarrow B_i \; i = 1, \ldots, k$$

по правилу цепочки импликаций. Теперь, применяя несколько раз правило для конъюнкции, получаем

$$\vdash A_1^{(1)} \wedge \cdots \wedge A_{s_1}^{(1)} \wedge \cdots \wedge A_1^{(k)} \wedge \cdots \wedge A_{s_k}^{(k)} \longrightarrow B_1 \wedge \cdots \wedge B_k$$

и, наконец,

$$\vdash A_1^{(1)} \wedge \cdots \wedge A_{s_1}^{(1)} \wedge \cdots \wedge A_1^{(k)} \wedge \cdots \wedge A_{s_k}^{(k)} \longrightarrow A$$

по правилу цепочки импликаций, что и доказывает требуемое ■

Следствие 12.6. $\Gamma \vdash A_1, \ldots, \Gamma \vdash A_k \Longleftrightarrow \Gamma \vdash A_1 \wedge \cdots \wedge A_k$ ■

Определение 12.7. Множество T предложений языка L_σ называется формальной теорией, если оно замкнуто относительно выводимости, т.е., если $\forall A \in \text{Ł}_\sigma \; T \vdash A \Longrightarrow A \in T$.

.

Следствие 12.8. *Если* T *– формальная теория, то* $A_1, \ldots, A_k \in T \Longleftrightarrow A_1 \wedge \cdots \wedge A_k \in T$ ■

Предложение 12.9. *Если* Γ *– произвольное множество предложений, а* $T(\Gamma) = \{A \mid \Gamma \vdash A\}$, *то* $T(\Gamma)$ *– наименьшая формальная теория, содержащая* Γ.

Доказательство. Очевидно, достаточно показать, что $T(\Gamma)$ – формальная теория. Пусть $T(\Gamma) \vdash B$. Поскольку, по определению $T(\Gamma)$ любое предложение $C \in T(\Gamma)$ выводимо из Γ, то в силу предложения 12.5 $\Gamma \vdash B$, т.е. $B \in T(\Gamma)$ ■

Определение 12.10. Теория T называется непротиворечивой, если не существует такого предложения A, что $T \vdash A$ и $T \vdash \neg A$. В противном случае теория T называется противоречивой. Множество предложений Γ называется непротиворечивым, если непротиворечива теория $T(\Gamma)$.

Предложение 12.11. *Теория T противоречива тогда и только тогда, когда ей принадлежит любое предложение A языка L_σ. Соответственно множество предложений Γ противоречиво тогда и только тогда, когда любое предложение A языка L_σ выводится из Γ.*

Доказательство. Ясно, что если Tсодержит все предложения, то она противоречива. Пусть, наоборот, теория T противоречива и предложение A языка L_σ таково, что $T \vdash A$ и $T \vdash \neg A$, т.е. по следствию 12.6 $A \wedge \neg A \in T$ Для любого предложения $B \in L_\sigma$ $\vdash A \wedge \neg A \longrightarrow B$, т.к. это тавтология. Теперь из определения выводимости следует, что $B \vdash T$, т.е. $B \in T$ ■

Предложение 12.12. *Если теория T непротиворечива, $A \notin T$ и $\neg A \notin T$, то множества предложений $T \cup \{A\}$ и $T \cup \{\neg A\}$ непротиворечивы.*

.

Доказательство. Докажем непротиворечивость $T \cup \{A\}$ от противного. Пусть $T \cup \{A\} \vdash B$ и $T \cup \{A\} \vdash \neg B$. Тогда существуют такие предложения $A_1, \ldots, A_k \in T$, что $\vdash A_1 \wedge \cdots \wedge A_k \wedge A \longrightarrow B$ и такие предложения $B_1, \ldots, B_l \in T$, что $\vdash B_1 \wedge \cdots \wedge B_l \wedge A \longrightarrow \neg B$. В силу следствия 12.6 $C = A_1 \wedge \cdots \wedge A_k \in T$, $D = B_1 \wedge \cdots \wedge B_l \in T$ и $F = C \wedge D \in T$. Поскольку $\vdash (C \wedge A \longrightarrow B) \longrightarrow (C \wedge D \wedge A \longrightarrow B)$, то $F \wedge A \longrightarrow B \in T$, аналогично $F \wedge A \longrightarrow \neg B \in T$. Далее $\vdash (F \wedge A \longrightarrow B) \longrightarrow (F \longrightarrow (A \longrightarrow B)$, т.е. $F \longrightarrow (A \longrightarrow B) \in T$, а т.к. $F \in T$, то $A \longrightarrow B \in T$. Аналогично $A \longrightarrow \neg B \in T$. Но $\vdash (A \longrightarrow B) \wedge (A \longrightarrow \neg B) \longrightarrow \neg A$ (закон приведения к противоречию), т.е. $\neg A \in T$. Противоречие. Непротиворечивость $T \cup \{\neg A\}$ доказывается аналогично ■

Определение 12.13. 1. Непротиворечивая теория T называется максимальной, если для любого предложения $A \notin T$ множество формул $T \cup \{A\}$ противоречиво.

2. Непротиворечивая теория T называется полной, если для любого предложения A либо $A \in T$, либо $\neg A \in T$.

Замечание. Множество предложений Γ полно, если полна теория $T(\Gamma)$, т.е. если для любого предложения A либо $\Gamma \vdash A$, либо $\Gamma \vdash \neg A$.

Предложение 12.14. *Теория T максимальна тогда и только тогда, когда она полна.*

Доказательство. Пусть теория T максимальна и $A \notin T$. Если при этом $\neg A \notin T$, то по предложению 12.12 множество формул $T \cup \{A\}$ непротиворечиво, что противоречит максимальности T.

Пусть, наоборот, теория T полна. Предположим, что она не максимальна. Тогда существует такое предложение $B \notin T$, что множество $T' = T \cup \{B\}$

непротиворечиво. Ввиду полноты T $\neg B \in T$, т.е. $\neg B \in T'$, но по определению $B \in T'$, т.е. T' противоречиво. ■

Теорема 12.15 (Лемма Линденбаума). *Всякая непротиворечивая теория T содержится в некоторой полной теории.*

Доказательство. Данная теорема является простым следствием леммы Цорна. Обозначим через $\mathcal{T}$ множество всех непротиворечивых теорий языка L_σ. Это множество частично упорядочено отношением включения и его максимальные элементы есть как раз всевозможные полные теории. Для применения леммы Цорна достаточно показать, что любая цепь $\mathcal{S} \subseteq \mathcal{T}$ имеет верхнюю грань. Для этого, в свою очередь, достаточно показать, что $T_0 = \bigcup\limits_{T \in \mathcal{S}} T$ – непротиворечивая теория. Предположим, что T_0 – противоречива. Тогда существуют предложение B и предложения $A_1, \ldots, A_k \in T_0$, такие, что $\vdash A_1 \wedge \cdots \wedge A_k \longrightarrow B \wedge \neg B$, но это значит, что множество предложений $\{A_1, \ldots, A_k\}$ – противоречиво. Поскольку это множество лежит в T_0, то существуют непротиворечивые теории $T_1, \ldots, T_k \in \mathcal{S}$, такие, что $A_1 \in T_1, \ldots, A_k \in T_k$. Но из линейной упорядоченности $\mathcal{S}$ следует, что среди теорий $T_1, \ldots, T_k$ имеется наибольшая по включению, например, T_k. Тогда, $\{A_1, \ldots, A_k\} \subseteq T_k$, т.е. T_k – противоречива. Но элементами $\mathcal{S}$ являются непротиворечивые теории ■

Замечание. Мы показали лишь, что T_0 – непротиворечивое множество формул. Этого достаточно для доказательства леммы Линденбаума. Однако, аналогичными рассуждениями несложно показать, что T_0 – формальная теория. Это предоставляется читателю в качестве упражнения.

Пример. Пусть $\mathcal{K}$ – класс алгебраических систем сигнатуры σ. Тогда теория класса $\mathcal{K}$ – $Th(\mathcal{K})$ есть формальная теория. В самом деле. Если $Th(\mathcal{K}) \vdash A$, то существуют такие предложения $A_1, \ldots, A_k \in Th(\mathcal{K})$, что $\vdash A_1 \wedge \cdots \wedge A_k \longrightarrow A$. Рассмотрим произвольную а.с. $\mathcal{M} \in \mathcal{K}$. Поскольку $\mathcal{M} \models A_1 \wedge \cdots \wedge A_k$ и $\mathcal{M} \models A_1 \wedge \cdots \wedge A_k \longrightarrow A$ (как логически общезначимая формула), то $\mathcal{M} \models A$, т.е. $A \in Th(\mathcal{K})$. Из определения ясно, что $Th(\mathcal{K}) \subseteq Th(\mathcal{M})$. Но для любой а.с. $\mathcal{M}$ теория $Th(\mathcal{M})$ полна, поскольку для любого предложения A либо $\mathcal{M} \models A$, либо $\mathcal{M} \models \neg A$.

ЛЕКЦИЯ 13

§3. Теорема Геделя о полноте и ее следствия.

Пусть T – формальная теория. Говорят, что а.с. $\mathcal{M}$ является моделью теории T, если $\forall A \in T$ $\mathcal{M} \models A$, т.е. другими словами, $T \subseteq Th(\mathcal{M})$. Соответственно $\mathcal{M}$ – модель множества предложений Γ, если $\mathcal{M}$ – модель теории $T(\Gamma)$. Из этого определения видно, что если формальная теория имеет модель, то она

непротиворечива (поскольку теория любой модели очевидно непротиворечива). Обратное утверждение является одной из наиболее важных и известных теорем математической логики.

Теорема 13.1 (Теорема Геделя о полноте). *Всякая непротиворечивая формальная теория имеет модель.*

В доказательстве этой теоремы мы ограничимся предположением, что сигнатура σ не содержит функциональных символов поскольку, во-первых, наличие функциональных символов в сигнатуре приводит лишь к некоторому техническому усложнению доказательства, не требуя никаких новых идей, а во-вторых, как объяснялось в лекции 5, от функциональных символов всегда можно отказаться, не обедняя выразительных возможностей формального языка, но делая запись в нем более громоздкой, что, конечно же, не имеет значения для доказательства теоремы Геделя.

Итак, пусть T – непротиворечивая теория сигнатуры σ. Каждой формуле с одной свободной переменной $A(x)$ языка L_σ поставим в соответствие некоторую константу c_A, не входящую в сигнатуру σ, добавим ее к сигнатуре, а к теории T добавим все предложения вида $\exists x A(x) \longrightarrow A(c_A)$. Обозначим полученную теорию через T^*.

Лемма 13.2. *Теория T^* непротиворечива.*

Доказательство. Докажем сначала, что непротиворечива теория T', полученная добавлением к T только одного предложения $\exists x A(x) \longrightarrow A(c_A)$. Предположим, что T' противоречива. Тогда существует такое предложение $U \in T$, что

$$\vdash U \wedge (\exists x A(x) \longrightarrow A(c_A) \longrightarrow B \wedge \neg B,$$

для некоторого предложения B в языке расширенной сигнатуры. По правилу эквивалентных преобразований (предложение 11.7(6))

$$\vdash U \longrightarrow ((\exists x A(x) \longrightarrow A(c_A)) \longrightarrow B \wedge \neg B),$$

Теперь, используя тавтологию

$$\vdash ((\exists x A(x) \longrightarrow A(c_A)) \longrightarrow B \wedge \neg B) \longrightarrow \neg(\exists x A(x) \longrightarrow A(c_A)),$$

и правило цепочки импликаций, получаем

$$\vdash U \longrightarrow \neg(\exists x A(x) \longrightarrow A(c_A)).$$

Пусть переменная y, не входит в последнее предложение. Тогда по предложению 12.1(1)

$$\vdash \forall y(U \longrightarrow \neg(\exists x A(x) \longrightarrow A(y))).$$

Применяя к последнему предложению тождественные преобразования логики предикатов (см. Замечание после доказательства предложения 13.2), получаем

$$\vdash U \longrightarrow (\exists x A(x) \wedge \neg \exists y A(y)),$$

т.е. $\exists x A(x) \wedge \neg \exists y A(y) \in T$, что невозможно, поскольку T непротиворечива.

Теперь, если теория T^* противоречива, то существует конечное множество предложений $B_1, \ldots, B_n$, где каждое B_i имеет вид $\exists x A_i(x) \longrightarrow A_i(c_{A_i})$, такое что для некоторого предложения $U \in T$ и некоторого предложения B $\vdash U \wedge B_1 \wedge, \ldots, B_n \longrightarrow B \wedge \neg B$, т.е. уже множество формул $T \cup \{B_1, \ldots, B_n\}$ противоречиво. Но это невозможно, поскольку по доказанному выше множество $T \cup \{B_1\}$ непротиворечиво, следовательно множество $T \cup \{B_1\} \cup \{B_2\}$ непротиворечиво, и т.д. ■

Построим теперь последовательность теорий $T_0 = T$, $T_{n+1} = T_n^*$, $n = 0, 1, \ldots$ и положим $\widetilde{T} = \bigcup\limits_{n=0}^{\infty} T_n$. Тогда легко видеть, что $\widetilde{T}$ – непротиворечивая теория. В самом деле, если эта теория противоречива, то $\exists A_1, \ldots, A_n \in \widetilde{T}$, такие, что $\vdash A_1 \wedge \cdots \wedge A_n \longrightarrow B \wedge \neg B$ для некоторого предложения B, но тогда по построению существует такое m, что $A_1, \ldots, A_n \in T_m$, т.е. уже теория T_m противоречива, что невозможно в силу леммы 13.2.

Обозначим через $\mathfrak{M}$ – множество всех констант языка сигнатуры теории $\widetilde{T}$. Заметим для дальнейшего, что

$$|\mathfrak{M}| \leq \max\{\aleph_0, |\sigma|\}. \tag{13.1}$$

В самом деле, если σ_i, $i \in \mathbb{N}$ – сигнатура языка теории T_i, то мощность множества предложений языка L_{σ_i} равна $\max\{\aleph_0, |\sigma|\}$ (см. Замечание 2 к определению 5.1), т.е. на $i+1$-ом шаге к сигнатуре добавляется не более, чем $\max\{\aleph_0, |\sigma_i|\}$ констант. Это значит, что начиная с 1-го шага, $|L_{\sigma_i}| = \max\{\aleph_0, |\sigma|\}$, т.е. они все имеют одинаковую бесконечную мощность. Значит такую же мощность имеет и объединение всех этих множеств, т.е. и множество всех построенных констант не превосходит этой мощности.

Пусть S – полная теория, содержащая T (см. лемму Линденбаума). Определим на множестве $\mathfrak{M}$ отношение $\sim$, положив

$$c \sim c' \rightleftharpoons c = c' \in S.$$

Покажем, что $\sim$ – отношение эквивалентности. Поскольку $c = c$ – аксиома равенства, то $c = c \in S$, т.е. отношение $\sim$ – рефлексивно. Предложение $c = d \longrightarrow d = c$ – теорема ИП (см. конец лекции 11), т.е. если $c = d \in S$, то $S \vdash d = c$, а значит и $d = c \in S$. Тем самым доказана симметричность

отношения $\sim$. Аналогично с использованием теоремы ИП $a = b \wedge b = c \longrightarrow a = c$ доказывается транзитивность $\sim$.

Пусть теперь $M = \mathfrak{M}/\sim$. Это множество и будет являться носителем модели для теории T. Интерпретация i для констант определяется естественным образом: если $c \in \mathfrak{M}$, то $i(c)$ есть класс элемента c по отношению $\sim$. Если P – n-местный предикатный символ, то положим

$$i(P)(i(c_1), \ldots, i(c_n)) = \mathbf{И} \Longleftrightarrow P(c_1, \ldots, c_n) \in S.$$

Покажем прежде всего, что это определение корректно. Пусть $c_1 \sim d_1, \ldots, c_n \sim d_n$ и $i(P)(i(c_1), \ldots, i(c_n)) = \mathbf{И}$, т.е. $c_1 = d_1, \ldots, c_n = d_n$, $P(c_1, \ldots, c_n) \in S$. Используя (11.6), легко доказать следующую теорему ИП:

$$\vdash c_1 = d_1 \wedge \cdots \wedge c_n = d_n \longrightarrow (P(c_1, \ldots, c_n) \longrightarrow P(d_1, \ldots, d_n)).$$

Отсюда немедленно следует, что $(P(c_1, \ldots, c_n) \longrightarrow P(d_1, \ldots, d_n)) \in S$, а следовательно и $P(d_1, \ldots, d_n)) \in S$, т.е. $i(P)(i(d_1), \ldots, i(d_n)) = \mathbf{И}$.

Если $i(P)(i(c_1), \ldots, i(c_n)) = \mathbf{Л}$, то, по определению, $P(c_1, \ldots, c_n) \notin S$. Тогда в силу полноты S $\neg P(c_1, \ldots, c_n) \in S$. Теперь, рассуждая также, как в предыдущем абзаце, получаем, что $\neg P(d_1, \ldots, d_n)) \in S$, т.е. $P(d_1, \ldots, d_n)) \notin S$, т.е. $i(P)(i(d_1), \ldots, i(d_n)) = \mathbf{Л}$.

Для того, чтобы показать, что а.с. $\mathcal{M} = \langle M, i\rangle$ является моделью для S, а следовательно и для T, очевидно достаточно доказать следующее утверждение.

Для любой формулы $F(x_1, \ldots, x_n)$ и для любых $c_1, \ldots, c_n \in \mathfrak{M}$

$$\mathcal{M} \models F(i(c_1), \ldots, i(c_n)) \Longleftrightarrow F(c_1, \ldots, c_n) \in S. \tag{13.2}$$

Это утверждение, как обычно, будем доказывать индукцией по построению формулы F. Заметим, что для атомарных формул оно непосредственно следует из интерпретации предикатных символов.

Покажем, что, если (13.2) верно для F_1 и для F_2, то оно верно для $F_1 \wedge F_2$. В самом деле, $\mathcal{M} \models F_1 \wedge F_2$ эквивалентно тому, что $\mathcal{M} \models F_1$ и $\mathcal{M} \models F_2$. По предположению, это эквивалентно тому, что $F_1 \in S$ и $F_2 \in S$. Последнее равносильно условию $F_1 \wedge F_2 \in S$ (следствие 12.6).

Покажем теперь, что, если 13.2 верно для F, то оно верно также для $\neg F$. Если $\mathcal{M} \models \neg F$, то F ложно в $\mathcal{M}$ и, в силу (13.2), $F \notin S$, т.е., ввиду полноты S, $\neg F \in S$. Если $\neg F$ ложно в $\mathcal{M}$, то $\mathcal{M} \models F$, а поскольку для F эквивалентность (13.2) выполняется, то $F \in S$, т.е. $\neg F \notin S$.

Пусть теперь F имеет вид $\exists x G(x, x_1, \ldots, x_n)$ и для G утверждение (13.2) уже доказано. Рассмотрим произвольные константы $c_1, \ldots, c_n \in \mathfrak{M}$. Предположим, что $\mathcal{M} \models \exists x G(x, i(c_1), \ldots, i(c_n))$. По определению истинности формулы

в модели, это означает, что для некоторого $c \in \mathfrak{M}\ \mathcal{M} \models G(i(c), i(c_1), \ldots, i(c_n))$, т.е., ввиду (13.2), $G(c, c_1, \ldots, c_n) \in S$. Но легко видеть, что для любой формулы $A(x) \vdash A(c) \longrightarrow \exists x A(x)$. В самом деле, используя основные тождества логики предикатов (см. замечание после доказательства предложения 12.2), получаем, что

$$A(c) \longrightarrow \exists x A(x) \equiv \forall x \neg A(x) \longrightarrow \neg A(c),$$

а предложение, стоящее справа, есть первая аксиома для кванторов. Тем самым $\exists x G(x, c_1, \ldots, c_n) \in S$.

Пусть, наоборот, дано, что $\exists x G(x, c_1, \ldots, c_n) \in S$. По построению найдется такое n, что последнее предложение принадлежит языку теории T_n, а значит существует такая, константа c, что $\exists x G(x, c_1, \ldots, c_n) \longrightarrow G(c, c_1, \ldots, c_n) \in S$, т.е. и $G(c, c_1, \ldots, c_n) \in S$ в силу тавтологии $\vdash p \wedge (p \longrightarrow q) \longrightarrow q$. Теперь по предположению индукции $\mathcal{M} \models G(i(c), i(c_1), \ldots, i(c_n))$, а значит $\mathcal{M} \models \exists x G(x, i(c_1), \ldots, i(c_n))$.

Как всегда, рассмотрение остальных логических связок и квантора всеобщности можно опустить, поскольку они выражаются через уже рассмотренные. Утверждение (13.2), а с ним и теорема Геделя о полноте, доказаны.

Следствие 13.3 (Теорема Левенгейма – Сколема). *Если теория T сигнатуры σ непротиворечива, то она имеет модель, мощность которой не превосходит* $\max\{\aleph_0, |\sigma|\}$.

Данное следствие непосредственно вытекает из неравенства (13.1).

Следствие 13.4. *Всякое общезначимое предложение в языке логики предикатов является теоремой ИП.*

Доказательство. Пусть предложение A общезначимо, но не является теоремой ИП. Тогда множество $\{\neg A\}$ непротиворечиво. В самом деле, если $\vdash \neg A \longrightarrow B \wedge \neg B$, то, используя тавтологию $\vdash (\neg A \longrightarrow B \wedge \neg B) \longrightarrow A$ и правило MP, немедленно получаем, что $\vdash A$. Если теперь $\mathcal{M}$ – модель для $\neg A$, то в силу общезначимости A, одновременно выполняется $\mathcal{M} \models A$ и $\mathcal{M} \models \neg A$, что невозможно ■

Следствие 13.5 (Теорема компактности А.И.Мальцева). *Если каждое конечное подмножество множества предложений* Γ *имеет модель, то и само* Γ *имеет модель.*

Доказательство. Если Γ не имеет модели, то Γ противоречиво. Следовательно существуют такие предложения $A_1, \ldots, A_n \in \Gamma$, что $\vdash A_1 \wedge \cdots \wedge A_n \longrightarrow B \wedge \neg B$ для некоторого предложения B. Но тогда уже множество $\{A_1, \ldots, A_n\}$ противоречиво, что невозможно поскольку оно имеет модель как конечное подмножество G ■

Доказанная только что теорема компактности А.И.Мальцева имеет многочисленные применения не только в логике, но и в алгебре, где она используется для доказательства *локальности* свойств алгебраических систем.

Определение 13.6. Пусть $\mathcal{K}$ некоторый класс алгебраических систем сигнатуры σ, замкнутый относительно подсистем (т.е. содержащий вместе с каждой системой все ее подсистемы). Свойство P алгебраических систем класса $\mathcal{K}$ называется локальным, если из того, что все конечно порожденные подсистемы системы $\mathcal{M} \in \mathcal{K}$ обладают свойством P, следует, что и сама система M обладает этим свойством.

Например, если $\mathcal{K}$ – класс групп, то свойство коммутативности является локальным, поскольку, если каждая конечно порожденная подгруппа группы G коммутативна, то для любых $a, b \in G$ подгруппа, порожденная $\{a, b\}$ коммутативна, т.е. для любых $a, b \in G$ выполняется равенство $a \cdot b = b \cdot a$.

Простейшим примером не локального свойства является свойство групп быть конечно порожденными, т.к. каждая конечно порожденная подгруппа любой группы конечно порождена по определению. Свойство конечности тоже не является локальным, поскольку существуют бесконечные группы, у которых все конечно порожденные подгруппы конечны (такие группы называются локально конечными). Примером такой группы служит группа всех таких подстановок множества $\mathbb{N}$, которые оставляют неподвижными все точки $\mathbb{N}$, кроме конечного числа (докажите!). Еще один пример не локального свойства – это свойство групп быть циклическими: каждая конечно порожденная подгруппа аддитивной группы поля $\mathbb{Q}$ – циклическая (докажите!), но сама группа $\mathbb{Q}$ очевидно циклической не является.

А.И.Мальцев был первым, кто открыл возможность применения теоремы Геделя о полноте для доказательства локальности некоторых свойств алгебраических систем. Его работа, опубликованная в 1941 году в Ученых записках Ивановского пед. института, так и называлась "Об одном общем методе получения локальных теорем теории групп". Эта работа положила начало новой математической дисциплине, расположенной на стыке алгебры и логики, – теории моделей.

ЛЕКЦИЯ 14

Суть метода А.И.Мальцева состоит в том, что локальность свойства вытекает из возможности его записи некоторым конечным или бесконечным множеством формул специального вида в языке L_σ или каком-нибудь его расширении. Мы проиллюстрируем этот метод на примере доказательства локальности свойства упорядочиваемости групп.

Напомним, что коммутативная группа G называется упорядочиваемой, если на множестве ее элементов можно ввести такое отношение линейного порядка $\leq$, что

$$\forall a, b, c \in G(a \leq b \longrightarrow a + c \leq b + c). \tag{14.1}$$

Ясно, что если группа G упорядочиваема, то и любая ее подгруппа H упорядочиваема, т.к. если отношение $\leq$ удовлетворяет (14.1) на всей группе, то оно удовлетворяет этому условию и на любой подгруппе.

Примерами упорядочиваемых групп служат аддитивная группа поля $\mathbb{R}$ и все ее подгруппы, в частности, группы $\mathbb{Z}$ и $\mathbb{Q}$. Отношением, которое упорядочивает все эти группы является естественное отношение порядка на $\mathbb{R}$.

Любая конечная циклическая группа служит примером группы, которую нельзя упорядочить. В самом деле, пусть $\mathbb{Z}_m = \{0, 1, \ldots m-1\}$ – группа вычетов по $\mod m$. Предположим, что на $\mathbb{Z}_m$ можно ввести какое-нибудь отношение линейного порядка $\preccurlyeq$, удовлетворяющее (14.1). Тогда, либо $0 \preccurlyeq 1$, либо $1 \preccurlyeq 0$. В первом случае, применив m раз условие (14.1) при $c = 1$ и учитывая, что $m = 0$ в $\mathbb{Z}_m$, получим, что

$$0 \preccurlyeq 1 \preccurlyeq 2 \preccurlyeq \cdots \preccurlyeq m-1 \preccurlyeq 0,$$

т.е. в силу свойств отношения порядка все элементы $\mathbb{Z}_m$ равны, что неверно. Второй случай рассматривается аналогично.

Мы сейчас докажем, что свойство упорядочиваемости групп является локальным. Пусть G – абелева группа, каждая конечно порожденная подгруппа которой упорядочиваема. Каждому элементу $g \in G$ поставим в соответствие константный символ c_g (элемент $0 \in G$ и соответствующий ему константный символ отождествляем). Рассмотрим сигнатуру $\sigma = \langle \{c_g \mid g \in G\}, \{+\}, \{\leq\}$ (в соответствии со сказанным только что, 0 входит в множество константных символов). Пусть $LOAG$ – конечное множество аксиом теории линейно упорядоченных абелевых групп в сигнатуре σ (выписать самим!). Рассмотрим множество предложений языка L_σ

$$\Gamma = LOAG \cup \{\neg c_{g_1} = c_{g_2} \mid g_1 \neq g_2, g_1, g_2 \in G\} \cup$$
$$\cup \{c_{g_1} + c_{g_2} = c_{g_3} \mid g_1 + g_2 = g_3, g_1, g_2, g_3 \in G\}.$$

Каждое конечное множество $\mathcal{H} \subseteq \Gamma$ имеет модель. В самом деле. Очевидно имеется лишь конечное множество констант $\{c_{g_1}, \ldots, c_{g_n}\}$, входящих в предложения из $\mathcal{H}$. Рассмотрим подгруппу H группы G, порожденную элементами $g_1, \ldots, g_n$. По условию это группа упорядочиваема. Упорядочив ее и интерпретируя каждую константу c_{g_n} как элемент g_i, мы очевидно получаем, что H модель для $\mathcal{H}$.

Теперь по теореме компактности Мальцева и все множество Г имеет модель $\mathcal{M} = \langle M, i\rangle$. Поскольку $\mathcal{M} \models LOAG$, то M – линейно упорядоченная абелева группа. Определим отображение $\varphi : G \to M$, положив $\varphi(g) = i(c_g)$. Если $g_1 \neq g_2$, то $\mathcal{M} \models \neg c_{g_1} = c_{g_2}$, т.е. $i(c_{g_1}) \neq i(c_{g_2})$. Это показывает, что φ инъективно. Аналогично, если $g_1 + g_2 = g_3$, то $\mathcal{M} \models c_{g_1} + c_{g_2} = c_{g_3}$, т.е. $i(c_{g_1}) + i(c_{g_2}) = i(c_{g_3})$. Это показывает, что $\varphi(g_1 + g_2) = \varphi(g_1) + \varphi(g_2)$. Таким образом φ – инъективный гомоморфизм, т.е. $\varphi(G)$ изоморфна G, но $\varphi(G)$ упорядочена, как подгруппа упорядоченной группы M. Следовательно и G упорядочиваема ■

Задачи 1. Если некоторая теория имеет модели сколь угодно большой конечной мощности, то она имеет и бесконечные модели.

2. Если какое-нибудь предложение языка теории полей истинно в полях сколь угодно большой простой характеристики, то оно истинно и в некотором поле характеристики ноль.

§4. Полнота и категоричность теорий.

Теорема 14.1 (Теорема Левенгейма – Сколема – Тарского). *Если теория T в сигнатуре σ имеет хотя бы одну бесконечную модель, то она имеет модель произвольной мощности $k \geq \max\{\aleph_0, |\sigma|\}$*

Доказательство. Пусть $\mathcal{M}$ – некоторая бесконечная модель теории T. Добавим к сигнатуре σ множество дополнительных константных символов $\{d_\alpha \mid \alpha \in A\}$, где $|A| = k$, а к теории T – множество предложений $\{d_\alpha \neq d_\beta \mid \alpha \neq \beta \in A\}$. Полученное множество формул T' непротиворечиво. В самом деле, любое конечное подмножество $F \subseteq T'$ содержит лишь конечное множество новых констант $\{d_{\alpha_1}, \ldots, d_{\alpha_n}\}$. Рассмотрим в качестве модели множества предложений F модель $\mathcal{M}$, проинтерпретировав константы множества $\{d_{\alpha_1}, \ldots, d_{\alpha_n}\}$ произвольными *различными* элементами $\mathcal{M}$. Очевидно, что таким образом действительно получается модель для F – все предложения F, входящие в T истинны, поскольку они истинны в $\mathcal{M}$, а предложения вида $\{d_{\alpha_i} \neq d_{\beta_j},\ i \neq j,\ i, j = 1, \ldots, n$ истинны, поскольку эти константы проинтерпретированы попарно различными элементами. Тем самым, каждое конечное подмножество T' имеет модель, т.е. по теореме компактности Мальцева и все множество T' имеет модель, причем по теореме Левенгейма – Сколема существует модель, мощность которой не превосходит k, т.к. мощность расширенной сигнатуры равна k. С другой стороны мощность любой модели теории T' больше либо равна k, поскольку подмножество этой модели, состоящее из интерпретаций констант d_α имеет мощность k (интерпретации различных констант различны в силу определения множества T'). Таким образом T', а следовательно и T имеет модель мощности k ■

Главный вывод, который можно сделать из теоремы Левенгейма – Сколема – Тарского состоит в том, что ни одна алгебраическая система не может быть описана никаким множеством предложений однозначно с точностью до изоморфизма В самом деле, если $\mathcal{M} = \langle M, i\rangle$ – алгебраическая система сигнатуры σ, а $T = Th(\mathcal{M})$, то по теореме Левенгейма – Сколема – Тарского для произвольной мощности $k > max\{|\sigma|, |M|\}$ найдется модель $\mathcal{M}' = \langle M', i'\rangle$ теории T, мощность которой равна k. Ввиду того, что теория T полна, $Th(\mathcal{M}') = Th(\mathcal{M})$, но эти системы не могут быть изоморфными, поскольку они имеют разные мощности.

Ситуация изменится, если расширить язык логики предикатов, допустив переменные хотя бы для одноместных предикатов и разрешив применять кванторы по этим переменным. При этом интерпретировать эти переменные следует как *всевозможные* одноместные предикаты на носителе алгебраической системы. Такой логический язык называется языком второго порядка. Читателю предоставляется возможность самостоятельно сформулировать формальное определение языка второго порядка и его интерпретации, а мы ограничимся одним примерам. Если язык теории упорядоченных полей расширить до языка второго порядка, то в нем можно сформулировать аксиому точной верхней грани. Будем обозначать предикатные переменные заглавными латинскими буквами. Поскольку одноместные предикаты отождествляются с подмножествами носителя, то можно говорить о точных верхней и нижней грани одноместного предиката. Тогда формула $t = \sup X$ запишется следующим образом:

$$\forall x(X(x) \longrightarrow x \leq t) \wedge \forall s(\forall x(X(x) \longrightarrow x \leq s) \longrightarrow s \leq t).$$

Теперь аксиома точной верхней грани запишется так:

$$\forall X(\exists s(\forall x(X(x) \longrightarrow x \leq s)) \longrightarrow \exists t(t = \sup X)).$$

Из курса математического анализа известно, что любое упорядоченное поле, удовлетворяющее аксиоме точной верхней грани, изоморфно полю вещественных чисел.

Задача*. Записать в данном языке второго порядка тот факт, что область истинности предиката X есть множество натуральных чисел.

Возвращаясь к логике первого порядка (а в нашем курсе изучается только такая логика), заметим, что теореме Левенгейма – Сколема – Тарского не противоречит ситуация, при которой все модели некоторой теории, мощность которых фиксирована, изоморфны.

Определение 14.2. Говорят, что теория T категорична в некоторой мощности k, если все ее модели мощности k изоморфны.

Теорема 14.3 (Воот). *Если теория T в языке сигнатуры σ категорична в некоторой мощности $k \geq \max\{|\sigma|, \aleph_0\}$, то T полна.*

Доказательство. Если T не полна, то существует такое предложение A языка L_σ, что $A \notin T$ и $\neg A \notin T$. В этом случае по предложению 12.12 множества $\Gamma = T \cup \{A\}$ и $\Gamma' = T \cup \{\neg A\}$ непротиворечивы. По теореме Левенгейма – Сколема – Тарского существует модель $\mathcal{M}$ для множества Γ, мощность которой равна k и модель $\mathcal{M}'$ множества Γ', мощность которой также равна k. Поскольку обе эти системы являются моделями теории T, то по условию нашей теоремы они изоморфны. Тогда, в силу предложения 6.9, эти системы элементарно эквивалентны, что невозможно, т.к. $\mathcal{M} \models A$, а $\mathcal{M}' \models \neg A$ ■

Примеры. 1°. Известна следующая

Теорема Хаусдорфа. *Любые два счетные плотные неограниченные линейно упорядоченные множества изоморфны*

Доказательство этой теоремы можно найти, например, в книге [9]. Из нее следует, что теория $Th(DL)$ класса плотных неограниченных л.у. множеств, рассмотренная в лекции 7, категорична в счетной мощности и, следовательно, полна. По существу этот факт был нами доказан в лекции 7 при помощи исключения кванторов, поскольку из того факта, что любые две модели некоторой теории элементарно эквивалентны (см. предложение 7.7 и его следствие) очевидно следует ее полнота.

2°. В теории полей известна

Теорема Штейница. *Все алгебраически замкнутые поля фиксированной характеристики и фиксированной* **несчетной** *мощности изоморфны.*

Отсюда следует, что теория алгебраически замкнутых полей категорична в любой несчетной мощности и, следовательно, полна. Аксиомы этой теории (см. пример 3 лекции 5) есть аксиомы поля к которым добавлены аксиомы ACl_n для любого $n \in \mathbb{N}$ и либо аксиома $ACh ar(p)$ для некоторого простого p, либо все аксиомы $ACh ar(0)_n$, $n \in \mathbb{N}$.

Отметим, что ситуация, встречавшаяся в этих двух примерах, является общей. В теории моделей доказана следующая

Теорема Морли. *Если некоторая теория в языке не более чем счетной сигнатуры категорична в некоторой несчетной мощности, то она категорична в любой несчетной мощности.*

Отметим, что теория алгебраически замкнутых полей в счетной мощности не категорична. В самом деле, поле алгебраических чисел – алгебраическое замыкание поля $\mathbb{Q}$ не изоморфно алгебраическому замыканию, например, поля $\mathbb{Q}(e)$, полученного присоединением к $\mathbb{Q}$ числа e, поскольку в первом из этих

полей все элементы алгебраические, а во втором – нет. С другой стороны – оба эти поля счетны.

Литература

1. Э.Мендельсон. Введение в математическую логику. логике и теории алгоритмов. – М.: Наука, 1971.

2. Н.Катленд. Вычислимость. Введение в теорию рекурсивных функций. – М.: Мир, 1983.

3. Д.Булос, Р.Джеффри. Вычислимость и логика. – М.: Мир, 1994.

4. Э.Энгелер. Метаматематика элементарной математики. – М.: Мир, 1987.

5. П.Коэн. Теория множеств и континуум-гипотеза. – М.: Мир, 1969.

6. Е.И.Гордон, Г.М.Полотовский. Мощность бесконечных множеств. Учебное пособие. – Изд-во ННГУ, Нижний Новгород, 1998.

7. Е.И.Гордон, Г.М.Полотовский. Элементы математической логики и теории множеств. Часть 2. Методическая разработка. – Изд-во ННГУ, Нижний Новгород, 1988.

8. Е.И.Гордон, Г.М.Полотовский. Элементы математической логики и теории множеств. Часть III. Методическая разработка. – Изд-во ННГУ, Нижний Новгород, 1990.