Введение в математическую логику
Мех-мат МГУ, 1-й курс, весна 2008 г.

Л.Д. Беклемишев*

1 Логика высказываний

1.1 Алфавит, буква, слово

Определение 1.1. *Алфавитом* будем называть любое непустое множество. Его элементы называются *символами* (*буквами*).

Определение 1.2. *Словом* в алфавите Σ называется конечная последовательность элементов Σ.

Пример 1.3. Рассмотрим алфавит $\Sigma = \{a, b, c\}$. Тогда $baaa$ является словом в алфавите Σ.

Определение 1.4. Слово, не содержащее ни одного символа (то есть последовательность длины 0), называется *пустым словом* и обозначается ε.

Определение 1.5. *Длина* слова w, обозначаемая $|w|$, есть число символов в w, причём каждый символ считается столько раз, сколько раз он встречается в w.

Определение 1.6. Если x и y — слова в алфавите Σ, то слово xy (результат приписывания слова y в конец слова x) называется *конкатенацией* слов x и y.

*Данный конспект лекций составлен с использованием лекционных материалов ряда сотрудников кафедры математической логики и теории алгоритмов МГУ, в частности, конспектов лекций профессора М.Р. Пентуса и доцента В.Н. Крпского, на основе программы, разработанной коллективом кафедры.

Определение 1.7. Если x — слово и $n \in \mathbb{N}$, то через x^n обозначается слово

$$\underbrace{xx\ldots x}_{n \text{ раз}}.$$

Положим $x^0 \rightleftharpoons \varepsilon$ (знак $\rightleftharpoons$ читается «равно по определению»).

Пример 1.8. По принятым соглашениям $ba^3 = baaa$ и $(ba)^3 = bababa$.

Определение 1.9. Множество всех слов в алфавите Σ обозначается Σ^*.

Определение 1.10. Подмножества множества Σ^* для некоторого алфавита Σ называются *словарными множествами*. В лингвистике и информатике словарные множества также часто называют *языками*.

Утверждение 1.11. *Если алфавит Σ конечен или счётен, то множество Σ^* счётно.*

В самом деле, для любого конечного подмножества $\Sigma_0 \subseteq \Sigma$ множество всех слов фиксированной длины в алфавите Σ_0 конечно. Следовательно, Σ_0^* является объединением счётного числа конечных множеств, а значит, таково и множество $\Sigma^* = \bigcup_{\Sigma_0 \subseteq \Sigma} \Sigma_0^*$.

1.2 Высказывания и логические операции

Логика высказываний формализует определённые представления о (реальных) высказываниях и логических операциях.

Определение 1.12. *Высказыванием* называется повествовательное предложение, для которого имеет смысл говорить о его истинности или ложности.

Пример 1.13. Предложение «Лиссабон — столица Испании» является высказыванием.

Определение 1.14. Существуют два *истинностных значения* — «истина» и «ложь». Мы будем обозначать их И и Л, соответственно; считаем 1 и 0 синонимами И и Л.

Некоторые сложные высказывания строятся из более простых с помощью *логических операций*, таких как отрицание «не», конъюнкция «и», дизъюнкция «или», импликация «если ..., то ...».

Определение 1.15. *Логическая операция* — это такой способ построения сложного высказывания из данных высказываний, при котором истинностное значение сложного высказывания полностью определяется истинностными значениями исходных высказываний.

Пример 1.16. Отрицание является логической операцией. Предложение «Неверно, что Лиссабон — столица Испании» построено из высказывания «Лиссабон — столица Испании» с помощью отрицания.

Замечание 1.17. Употребляемую в естественном языке импликацию «если A, то B» нельзя в полной мере считать логической операцией, поскольку она, среди прочего, указывает и на причинно-следственную связь между высказываниями A и B, то есть не выражается только лишь через истинностные значения высказываний A и B. Более того, высказывание «если A, то B» *полисемично*, то есть может пониматься по-разному в разных контекстах.

В математическом языке используется *материальная импликация*, которая является логической связкой. При этом высказывание «если A, то B» считается ложным в том и *только том* случае, если A истинно и B ложно.

1.3 Синтаксис логики высказываний

1.3.1 Переменные и связки

Пусть задан некоторый алфавит Var символов, называемых *пропозициональными*[1] *переменными*. Пропозициональные переменные будем обозначать буквами P, Q и т. д. (возможно, с индексами). Интуитивно, пропозициональные переменные интерпретируются как высказывания.

Знаки $\neg$, $\wedge$, $\vee$, $\to$ (и аналогичные знаки, которые будут введены позже) называются *пропозициональными связками* или *булевыми связками*. Интуитивно, связки интерпретируются как логические операции (соответственно, как отрицание, конъюнкция, дизъюнкция, импликация).

1.3.2 Формулы

Формулы логики высказываний являются словами в алфавите, состоящем из пропозициональных переменных, пропозициональных связок и скобок: (и). Множество всех формул индуктивно определяется следующим образом.

[1] Propositio (лат.) = предложение.

Определение 1.18. *Множество формул* Fm логики высказываний порождается из множества Var по следующим правилам:

1. Если $P \in \mathrm{Var}$, то P — формула.
2. Если A — формула, то $\neg A$ — формула.
3. Если A и B — формулы, то $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ — формулы.

Другими словами, множество формул есть наименьшее множество, замкнутое относительно этих трёх правил.

Определение 1.19. *Построением* формулы A называем последовательность формул, каждый элемент которой есть либо переменная, либо получается из предыдущих по правилам 2 или 3, и последний элемент которой есть A.

Смысл определения 1.18 состоит в том, что формулами считаются те и только те слова, которые имеют построение. Определение множества объектов как наименьшего множества, замкнутого относительно некоторых правил образования, называется *индуктивным*. Такого рода определения часто используются в алгебре и логике.

Пример 1.20. Последовательность $P,\ Q,\ (P \to Q),\ (Q \wedge (P \to Q))$ есть построение формулы $(Q \wedge (P \to Q))$.

Формулы логики высказываний будем обозначать буквами A, B и т. д. (возможно, с индексами).

Определение 1.21. Построение формулы A называем *минимальным*, если из этой последовательности нельзя удалить ни одной формулы без того, чтобы она не перестала быть построением A.

Пример 1.22. $P,\ Q,\ (P \to Q),\ (Q \wedge (P \to Q))$ есть минимальное построение, а $P,\ Q,\ (P \to Q),\ (P \wedge Q),\ (Q \wedge (P \to Q))$ — не минимальное построение, поскольку из него можно удалить лишнюю формулу $(P \wedge Q)$.

Определение 1.23. *Подформулами* формулы A называются все те формулы, которые возникают при некотором минимальном построении A. Подформула формулы A, отличная от самой формулы A, называется *собственной подформулой* формулы A.

Замечание 1.24. Не следует путать подформулы с их *вхождениями* в формулу. Одна и та же подформула может иметь несколько вхождений, например подформула P входит три раза в формулу $(P \to (P \wedge P))$.

Предложение 1.25 (однозначность разбора, без доказательства**).**
Каждая пропозициональная формула, не являющаяся переменной, может быть представлена единственным образом как $\neg A$, $(A \wedge B)$, $(A \vee B)$ *или* $(A \to B)$.

Доказательство этого утверждения основывается на соображениях баланса скобок в формуле. Следствием является, например, тот факт, что множество подформул данной формулы не зависит от её построения.

1.3.3 Сокращённая запись формул

Для удобства записи формул принято использовать некоторые сокращения. С формальной точки зрения, такие сокращения являются приёмами изложения, а не элементами языка логики высказываний. Мы рассмотрим два важных вида сокращений.

А. *Соглашения о скобках.*

Во-первых, можно опустить внешнюю пару скобок. Например, запись $P \to (Q \to P)$ обозначает формулу $(P \to (Q \to P))$.

Во-вторых, если в сокращённой записи рядом находятся две операции $\wedge$, то при отсутствии скобок внутренней считается та, которая находится левее. Другими словами, связка $\wedge$ считается *левоассоциативной*. Например, $P \wedge Q \wedge R$ и $(P \wedge Q) \wedge R$ обозначают одну и ту же формулу (длина этой формулы — 9 символов). Однако в записи $P \wedge (Q \wedge R)$ ни одной скобки опустить нельзя. Связка $\vee$ тоже является левоассоциативной, но связка $\to$ не является ни левоассоциативной, ни правоассоциативной (в этом курсе).

В-третьих, если в сокращённой записи рядом находятся разные связки, то при отсутствии скобок внутренней считается та, которая имеет более высокий приоритет согласно следующему списку, составленному в порядке убывания приоритетов: $\neg$, $\wedge$, $\vee$, $\to$. Иными словами, связки с более высоким приоритетом связывают сильнее.

Разрешается также добавить внешнюю пару скобок. Например, запись $(\neg P)$ обозначает формулу $\neg P$. Добавление скобок пригодится, например, в определении 1.46.

Б. *Введение новых логических связок.*

Логическую связку *эквивалентности* $\leftrightarrow$ часто определяют как сокращение. При этом для любых формул A, B запись $A \leftrightarrow B$ понимается как обозначение для формулы $(A \to B) \wedge (B \to A)$. Аналогичным образом можно ввести и другие логические связки, в частности:

$$\begin{aligned}
\bot &\rightleftharpoons (P_0 \wedge \neg P_0), \quad \text{где } P_0 \text{ — фиксированная переменная;} \\
\top &\rightleftharpoons \neg\bot; \\
\bigwedge_{i=1}^{n} A_i &\rightleftharpoons (A_1 \wedge A_2 \wedge \cdots \wedge A_n); \\
\bigvee_{i=1}^{n} A_i &\rightleftharpoons (A_1 \vee A_2 \vee \cdots \vee A_n).
\end{aligned}$$

1.3.4 Другие варианты синтаксиса

Помимо стандартного, изложенного выше, способа записи формул логики высказываний существуют и другие варианты. Отметим три важных способа представления формул.

А. *Польская запись.* Логические связки (как унарные, так и бинарные) записываются префиксным образом, например, вместо $(A \wedge B)$ пишем $\wedge AB$; при этом скобки не употребляются. Так, формула $(A \to (B \wedge C))$ может быть записана «по-польски» как $\to A \wedge BC$. (Почему для польской записи имеет место теорема об однозначности разбора?)

Б. *Представление формул деревьями.* С каждой формулой можно однозначно связать бинарное дерево, называемое иногда *деревом разбора*, листья которого помечены пропозициональными переменными, а внутренние вершины – связками. Вершины этого дерева находятся во взаимно-однозначном соответствии со вхождениями подформул в данную формулу (соответетвующей корню дерева).

Интересно отметить, что одна из первых формулировок логики высказваний, данная в XIX веке немецким учёным Г. Фреге, использовала вариант графического изображения деревьев в качестве записи формул. (Напрашивается сравнение с иероглифическим письмом.)

В. *Представление формул ориентированными ациклическими графами.* Если отождествить в дереве разбора формулы вершины, соответствующие вхождениям одной и той же подформулы, то получится структура, называемая ориентированным ациклическим графом (DAG). При таком представлении вершины графа соответствуют подформулам данной формулы, а стрелки соединяют каждые две подформулы, одна из которых является максимальной собственной подформулой другой.

Этот способ представления формул является наиболее экономным и распостранённым вариантом представления формул в памяти компьютера.

1.4 Таблицы истинности

Определение 1.26. Обозначим $\mathbb{B} \rightleftharpoons \{И, Л\} \rightleftharpoons \{0, 1\}$. Функции $f : \mathbb{B}^n \to \mathbb{B}$ называются *булевыми функциями*.

Определение 1.27. *Оценкой пропозициональных переменных* (или просто *оценкой*) называется произвольная функция $f : \mathrm{Var} \to \mathbb{B}$.

Определение 1.28. *Истинностное значение* (или просто *значение*) формулы при данной оценке f определяется индукцией по построению формулы в соответствии со следующими таблицами.

A	$\neg A$
Л	И
И	Л

A	B	$A \wedge B$	$A \vee B$	$A \to B$
Л	Л	Л	Л	И
Л	И	Л	И	И
И	Л	Л	И	Л
И	И	И	И	И

С формальной точки зрения, оценка $f : \mathrm{Var} \to \mathbb{B}$ продолжается до функции $f : \mathrm{Fm} \to \mathbb{B}$, определённой на множестве всех формул, по следующим правилам.

$$
\begin{aligned}
f(\neg A) = И &\iff f(A) = Л;\\
f(A \wedge B) = И &\iff f(A) = И \text{ и } f(B) = И;\\
f(A \vee B) = И &\iff f(A) = И \text{ или } f(B) = И;\\
f(A \to B) = И &\iff f(A) = Л \text{ или } f(B) = И.
\end{aligned}
$$

Если $f(A) = И$, то говорят, что формула A *истинна* при оценке f. Иначе формула A *ложна* при данной оценке.

Специально рассмотрим случай, когда число переменных конечно, то есть $\mathrm{Var} = \{P_1, \ldots, P_n\}$. Оценка f определяется набором своих истинностных значений на переменных $P_1, \ldots, P_n$. Данному набору $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{B}^n$ сопоставим оценку $f_{\vec{x}}$, определяемую таблицей

P_1	P_2	$\ldots$	P_n
x_1	x_2	$\ldots$	x_n

Таким образом, существует взаимно-однозначное соответствие между оценками и наборами из $\mathbb{B}^n$.

Определение 1.29. *Таблицей истинности* (или *истинностной таблицей*) формулы A над переменными $P_1, \ldots, P_n$ называется таблица, указывающая значения формулы A при всех возможных оценках переменных $P_1, \ldots, P_n$. (Существует 2^n таких оценок, каждая из них записывается в отдельной строке. Обычно оценки $f_{\vec{x}}$ упорядочены в соответствии с лексикографическим порядком на наборах $\vec{x}$.)

Пример 1.30.

P_1	P_2	$P_1 \leftrightarrow P_2$
Л	Л	И
Л	И	Л
И	Л	Л
И	И	И

Таким образом, таблица истинности формулы A над n переменными задаёт булеву функцию $\varphi_A : \mathbb{B}^n \to \mathbb{B}$. Функция φ_A определяется равенством

$$\varphi_A(\vec{x}) = f_{\vec{x}}(A),$$

верным для всех наборов $\vec{x} \in \mathbb{B}^n$.

1.5 Функциональная полнота

Всякую ли булеву функцию можно задать некоторой формулой? Ответ даёт следующая теорема.

Теорема 1.31 (о функциональной полноте). *Для любой функции $\varphi : \mathbb{B}^n \to \mathbb{B}$ найдётся такая формула A от n переменных, что $\varphi = \varphi_A$. При этом можно считать, что A содержит лишь связки $\neg$ и $\vee$.*

Эта теорема показывает, что известных нам логических операций $\vee$, $\neg$ в принципе достаточно, чтобы определить все возможные логические операции.

Доказательство. Равенство $\varphi = \varphi_A$ означает, что для всех $\vec{x} \in \mathbb{B}^n$

$$\varphi(\vec{x}) = \varphi_A(\vec{x}) = f_{\vec{x}}(A).$$

Для $x \in \mathbb{B}$ положим

$$P^x = \begin{cases} P, & \text{если } x = \text{И}; \\ \neg P, & \text{если } x = \text{Л}. \end{cases}$$

Для произвольного $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{B}^n$ обозначим

$$A_{\vec{x}} \rightleftharpoons \bigwedge_{i=1}^{n} P_i^{x_i}.$$

Легко видеть, что формула $A_{\vec{x}}$ истинна лишь при оценке $f_{\vec{x}}$. Другими словами, для любой оценки f

$$f(A_{\vec{x}}) = \text{И} \iff f = f_{\vec{x}}. \tag{1}$$

Для данной функции φ пусть список $\vec{x}_1, \ldots, \vec{x}_m$ исчерпывает все наборы $\vec{x} \in \mathbb{B}^n$ для которых $\varphi(\vec{x}) = \text{И}$, то есть

$$\varphi(\vec{x}) = \text{И} \iff \exists j \ \vec{x} = \vec{x}_j. \tag{2}$$

Положим теперь

$$A \rightleftharpoons \bigvee_{j=1}^{m} A_{\vec{x}_j},$$

тогда

$$\begin{aligned} f_{\vec{x}}(A) = \text{И} \quad &\iff \quad \exists j \ f_{\vec{x}}(A_{\vec{x}_j}) = \text{И} \\ &\iff \quad \exists j \ \vec{x} = \vec{x}_j \quad \text{по (1)} \\ &\iff \quad \varphi(\vec{x}) = \text{И} \quad \text{по (2)}. \end{aligned}$$

Заметим теперь, что конъюнкция выражается через дизъюнкцию и импликацию, поскольку формула $A \wedge B$ равносильна $\neg(\neg A \vee \neg B)$ (см. ниже раздел 1.7). Поэтому, формулы $A_{\vec{x}}$ могут быть переписаны без использования знака $\wedge$. $\boxtimes$

1.6 Выполнимые формулы, тавтологии, логическое следование

1.6.1 Выполнимые формулы и тавтологии

Определение 1.32. Пропозициональная формула, истинная хотя бы при одной оценке пропозициональных переменных, называется *выполнимой*. Множество формул Γ называется *выполнимым*, если существует оценка f, при которой истинны одновременно все формулы из Γ.

Определение 1.33. Пропозициональная формула, истинная при каждой оценке пропозициональных переменных, называется *тавтологией* (*тождественно истинной*).

Важность понятия тавтологии с точки зрения оснований математики (и логики в целом) состоит в том, что они выражают *универсальные законы* логики, верные независимо от содержания составляющих их высказываний. Запись $\models A$ выражает тот факт, что A — тавтология.

Определение 1.34. Пропозициональная формула, ложная при каждой оценке пропозициональных переменных, называется *тождественно ложной.*

Предложение 1.35. *Следующие условия равносильны.*

(i) *Формула A тождественно ложна.*

(ii) *Формула A не является выполнимой.*

(iii) *Формула $\neg A$ — тавтология.*

Доказательство. Предложение непосредственно следует из определений. $\boxtimes$

1.6.2 Проверка формулы на выполнимость

В приложениях часто встречается задача проверки пропозициональной формулы на выполнимость. Наиболее прямолинейный алгоритм её решения состоит в построении всей таблицы истинности формулы, то есть перебора 2^n всех возможных оценок. Этот алгоритм работает экспоненциальное число шагов от числа переменных исходной формулы. Существуют более изощрённые и несколько более эффективные алгоритмы решения этой задачи, однако все они имеют экспоненциальную нижнюю оценку сложности.

Важной открытой проблемой является вопрос о существовании полиномиального по числу шагов алгоритма решения этой задачи. Поскольку выполнимость пропозициональной формулы является классическим примером так называемой NP-полной задачи, этот вопрос эквивалентен знаменитой проблеме P=NP? — одной из самых важных открытых математических проблем. В настоящее время доминирует гипотеза о том, что такого полиномиального алгоритма не существует.

1.6.3 Логическое следование

Определение 1.36. Пусть Γ — некоторое множество формул логики высказываний и A — формула логики высказываний. Говорят, что формула A *логически следует* (или *семантически следует*) из множества Γ

(обозначение $\Gamma \vDash A$), если формула A истинна при каждой оценке пропозициональных переменных, при которой истинны все формулы из Γ.

Пример 1.37. $\{P \vee Q, R, \neg Q\} \vDash P \wedge R$.

Предложение 1.38. $\{B_1, \ldots, B_n\} \vDash A$ *тогда и только тогда, когда формула* $(\bigwedge_{i=1}^{n} B_i) \to A$ *является тавтологией. В частности, формула* A *— тавтология, если и только если* A *логически следует из пустого множества формул.*

1.7 Равносильные формулы в логике высказываний

Определение 1.39. Формулы A и B называются *равносильными* (*эквивалентными*), обозначение $A \equiv B$, если при каждой оценке пропозициональных переменных значение A совпадает со значением B. Другими словами, если $\varphi_A = \varphi_B$.

Пример 1.40. $P \to Q \equiv \neg Q \to \neg P$; $P \to Q \not\equiv \neg P \to \neg Q$.

Непосредственно из определений вытекают следующие факты.

Утверждение 1.41. (i) *Отношение* $\equiv$ *рефлексивно, симметрично и транзитивно.*

(ii) *Формулы* A *и* B *равносильны тогда и только тогда, когда формула* $A \leftrightarrow B$ *является тавтологией.*

(iii) *Формула* A *— тавтология тогда и только тогда, когда* $A \equiv \top$.

Основные равносильности:

$A \wedge B$	$\equiv$	$B \wedge A$	$A \vee B$	$\equiv$	$B \vee A$
$A \wedge (B \wedge C)$	$\equiv$	$(A \wedge B) \wedge C$	$A \vee (B \vee C)$	$\equiv$	$(A \vee B) \vee C$
$A \wedge A$	$\equiv$	A	$A \vee A$	$\equiv$	A
$A \wedge (B \vee C)$	$\equiv$	$(A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C)$	$\equiv$	$(A \vee B) \wedge (A \vee C)$
$A \vee (A \wedge B)$	$\equiv$	A	$A \wedge (A \vee B)$	$\equiv$	A
$\neg(A \wedge B)$	$\equiv$	$\neg A \vee \neg B$	$\neg(A \vee B)$	$\equiv$	$\neg A \wedge \neg B$
$\neg\neg A$	$\equiv$	A	$A \to B$	$\equiv$	$\neg A \vee B$

Упражнение 1.42. Равносильны ли формулы $P \to (Q \to R)$ и $(P \to Q) \to R$? Ответ: Нет. Рассмотрим такую оценку g, что $g(P) = g(Q) = g(R) =$ Л.

Упражнение 1.43. Равносильны ли формулы $P \to (Q \to R)$ и $(P \wedge Q) \to R$? Ответ: Да.

Замечание 1.44. В задаче на упрощение формулы необходимо найти равносильную, но более короткую формулу. При этом длина понимается как общее количество всех вхождений символов в формулу.

Упражнение 1.45. *Упростить формулы:*

(i) $(P \leftrightarrow Q) \to P$. *Ответ:* $P \vee Q$.

(ii) $\neg P \to \neg Q$. *Ответ:* $Q \to P$.

(iii) $(P \vee Q) \wedge (P \vee R) \wedge (Q \vee R \vee \neg P)$. *Ответ:* $(P \vee (Q \wedge R)) \wedge (Q \vee R)$.

1.8 Правила подстановки и замены подформулы на эквивалентную

Для доказательства равносильности формул, помимо основных равносильностей, перечисленных в таблице, и правил, соответствующих рефлексивности, симметричности и транзитивности отношения $\equiv$, мы пользуемся правилами подстановки и замены на подформулы на эквивалентную.

Определение 1.46. Если C и D — формулы, а P — пропозициональная переменная, то через $C[P/D]$ обозначим результат подстановки формулы D вместо P в формулу C.

Формальное определение даётся с помощью индукции по построению формулы C.

$$
\begin{array}{l}
P[P/D] \rightleftharpoons D, \\
Q[P/D] \rightleftharpoons Q, \text{ если } Q \text{ — переменная, отличная от } P, \\
(\neg A)[P/D] \rightleftharpoons \neg(A[P/D]), \\
(A \wedge B)[P/D] \rightleftharpoons (A[P/D] \wedge B[P/D]), \\
(A \vee B)[P/D] \rightleftharpoons (A[P/D] \vee B[P/D]), \\
(A \to B)[P/D] \rightleftharpoons (A[P/D] \to B[P/D]).
\end{array}
$$

Пример 1.47. Пусть $C = (P_1 \to P_2) \to P_2$ и $D = P_3 \to P_2$. Тогда

$$C[P_2/D] = (P_1 \to (P_3 \to P_2)) \to (P_3 \to P_2).$$

Теорема 1.48 (о подстановке). *Если A — тавтология, B — произвольная формула, а P — пропозициональная переменная, то $A[P/B]$ — тавтология.*

Доказательство. Рассмотрим произвольную оценку g. Обозначим через g' оценку, полученную из g присвоением переменной P значения $g(B)$. Индукцией по построению C можно доказать, что $g(C[P/B]) = g'(C)$ для любой формулы C. Положим $C = A$. Так как формула A истинна при оценке g', то формула $A[P/B]$ истинна при оценке g. $\boxtimes$

Пример 1.49. Для любой формулы B формула $B \vee \neg B$ является тавтологией. Например, формула $(P_3 \leftrightarrow P_1) \vee \neg(P_3 \leftrightarrow P_1)$ является тавтологией.

Теорема 1.50. *Пусть A, B, C — формулы, а P — пропозициональная переменная. Если $A \equiv B$, то $A[P/C] \equiv B[P/C]$.*

Доказательство. Пусть $A \equiv B$. В силу 1.41 $A \leftrightarrow B$ — тавтология. По теореме 1.48 $(A \leftrightarrow B)[P/C]$ — тавтология. Из определений следует, что $(A \leftrightarrow B)[P/C]$ совпадает с $A[P/C] \leftrightarrow B[P/C]$. В силу 1.41 $A[P/C] \equiv B[P/C]$. $\boxtimes$

Пример 1.51. Пусть $A = (P_1 \to P_2) \to P_2$, $B = P_1 \vee P_2$, $C = P_3 \to P_2$. Так как $(P_1 \to P_2) \to P_2 \equiv P_1 \vee P_2$, то $(P_1 \to (P_3 \to P_2)) \to (P_3 \to P_2) \equiv P_1 \vee (P_3 \to P_2)$.

Лемма 1.52. *Если $A \equiv B$, то $\neg A \equiv \neg B$. Если $A_1 \equiv B_1$ и $A_2 \equiv B_2$, то $A_1 \wedge A_2 \equiv B_1 \wedge B_2$, $A_1 \vee A_2 \equiv B_1 \vee B_2$, $A_1 \to A_2 \equiv B_1 \to B_2$.*

Теорема 1.53 (о замене подформулы на эквивалентную). *Пусть A, B, C — формулы, а P — пропозициональная переменная. Если $A \equiv B$, то $C[P/A] \equiv C[P/B]$.*

Доказательство. Теорема доказывается индукцией по построению формулы C. $\boxtimes$

Пример 1.54. Пусть $A = Q \vee Q$, $B = Q$, $C = P \wedge R$. Так как $Q \vee Q \equiv Q$, то $(Q \vee Q) \wedge R \equiv Q \wedge R$.

Пример 1.55. Существуют ли такие выполнимые формулы A и B, что формула $A[P_1/B]$ не является выполнимой? Ответ: Да. Например, $A = \neg P_1$, $B = P_2 \vee \neg P_2$.

1.9 Нормальные формы

1.9.1 Дизъюнктивные и конъюнктивные нормальные формы

Определение 1.56. *Литералами* называются переменные и их отрицания.

Пример 1.57. Формулы P_3 и $\neg P_1$ являются литералами, а формулы $P_3 \vee P_1$ и $\neg\neg P_3$ — не являются.

Определение 1.58. *Элементарной конъюнкцией* называем формулу вида $\bigwedge_{i=1}^{n} L_i$, где L_i — литералы.

Пример 1.59. Формула $(P \wedge \neg Q) \wedge \neg P$ является элементарной конъюнкцией, а формула $P \wedge (\neg Q \wedge \neg P)$ не является элементарной конъюнкцией.

Определение 1.60. *Дизъюнктивной нормальной формой (ДНФ)* называем формулу вида $\bigvee_{j=1}^{m} C_j$, где C_j — элементарные конъюнкции.

Пример 1.61. Формулы $(P \wedge \neg R) \vee (Q \wedge R)$ и $(P \wedge Q \wedge R) \vee \neg P \vee \neg R$ являются дизъюнктивными нормальными формами.

Упражнение 1.62. *Привести к дизъюнктивной нормальной форме формулу* $(P \vee Q) \to R$. *Ответ:* $(\neg P \wedge \neg Q) \vee R$.

Аналогично определяются элементарные дизъюнкции и конъюнктивные нормальные формы.

Определение 1.63. *Элементарной дизъюнкцией* называем формулу вида $\bigvee_{i=1}^{n} L_i$, где L_i — литералы.

Конъюнктивной нормальной формой (КНФ) называем формулу вида $\bigwedge_{j=1}^{m} D_j$, где D_j — элементарные дизъюнкции.

Упражнение 1.64. *Привести к конъюнктивной нормальной форме формулу* $(P \vee Q) \to R$. *Ответ:* $(\neg P \vee R) \wedge (\neg Q \vee R)$.

Теорема 1.65. *Каждая пропозициональная формула равносильна некоторой дизъюнктивной нормальной форме и некоторой конъюнктивной нормальной форме.*

Доказательство (первый вариант). Если A тождественно ложна, в качестве её ДНФ можно взять формулу $P \wedge \neg P$, где P — любая переменная. В противном случае достаточно заметить, что формула, построенная в доказательстве теоремы о функциональной полноте для функции φ_A есть ДНФ.

Доказательство (второй вариант). Выразим $\to$ через $\neg$ и $\vee$. Далее преобразуем формулу, применяя таблицу основных эквивалентностей и активно пользуясь правилом замены подформулы на эквивалентную. Сначала проносим все отрицания максимально вглубь формулы и удаляем многократные отрицания. Затем, пользуясь дистрибутивностью, выносим все дизъюнкции максимально наружу. Пользуясь ассоциативностью $\wedge$ и $\vee$ расставляем правильно скобки.

Осталось заметить, что если A — дизъюнктивная нормальная форма, то формула $\neg A$ превращается в конъюнктивную нормальную форму после переноса всех отрицаний вглубь и удаления двойных отрицаний. Значит, для того чтобы получить конъюнктивную нормальную форму формулы A, достаточно применить этот процесс к дизъюнктивной нормальной форме формулы $\neg A$. $\boxtimes$

1.9.2 Совершенные ДНФ и КНФ

В этом параграфе считаем фиксированным конечный набор переменных $\mathrm{Var} = \{P_1, \ldots, P_n\}$ и будем рассматривать лишь формулы от этих переменных.

Определение 1.66. Формула A называется *совершенной ДНФ*, если A — ДНФ и

- Каждая элементарная конъюнкция имеет вид $A_{\vec{x}} \rightleftharpoons \bigwedge_{i=1}^{n} P_i^{x_i}$ для некоторого $\vec{x} \in \mathbb{B}^n$.
- $A = \bigvee_{j=1}^{m} A_{\vec{x}_j}$, где $\vec{x}_1, \ldots \vec{x}_m \in \mathbb{B}^n$ попано различны и взяты в лексикографическом порядке.

Определение *совершенной КНФ* аналогично, с заменой дизъюнкций на конъюнкции и наоборот.

Замечание 1.67. Удобно расширить множество формул константами $\bot$ (ложь) и $\top$ (истина). Тем самым, формулами считаются и все выражения, построенные с помощью булевых связок из переменных и этих констант. Считаем $\bot$ совершенной ДНФ, а $\top$ — совершенной КНФ.

Замечание 1.68. Совершенные ДНФ и КНФ перестают быть совершенными, если рассматривать их как формулы от более широкого набора переменных. Поэтому имеет смысл говорить о совершенных ДНФ и КНФ лишь относительно некоторого фиксированного набора переменных.

Теорема 1.69. *Всякая формула A равносильна некоторой совершенной ДНФ.*

Доказательство (первый вариант). Если A тождественно ложна, в качестве её ДНФ можно взять $\bot$. В противном случае достаточно заметить, что формула, построенная в доказательстве теоремы о функциональной полноте для функции φ_A есть совершенная ДНФ. ⊠

Доказательство (второй вариант). Сначала приведём формулу к ДНФ. Удалим противоречивые конъюнкции, воспользовавшись равносильностями:

$$A \wedge \neg A \equiv \bot, \quad \bot \wedge A \equiv \bot, \quad \bot \vee A \equiv A.$$

При этом формула либо приводится к виду $\bot$, либо в формуле останутся лишь элементарные конъюнкции без вхождений пар противоположных литералов. В оставшихся конъюнкциях удалим повторы литералов с помощью равносильности $A \wedge A \equiv A$. Для каждой конъюнкции добавим недостающие до полного набора $P_1, \ldots, P_n$ переменные, пользуясь равносильностью

$$A \equiv (A \wedge B) \vee (A \wedge \neg B).$$

С помощью ассоциативности и коммутативности добьёмся требуемого упорядочения всех членов и правильной расстановки скобок. ⊠

Замечание 1.70. $(A \wedge B) \vee (A \wedge \neg B) \equiv A \wedge (B \vee \neg B) \equiv A \wedge \top \equiv A.$

Теорема 1.71. *Совершенные ДНФ эквивалентных формул (графически) совпадают.*

Доказательство. . Для совершенной ДНФ каждая элементарная конъюнкция определяет некоторую выполняющую оценку, а сама ДНФ — множество всех таких оценок. ⊠

Следствие 1.72. *Совершенная ДНФ любой формулы A единственна.*

Аналогичные теоремы имеют место и для совершенных КНФ.

Упражнение 1.73. *Привести к совершенной конъюнктивной нормальной форме формулу $\neg(P \leftrightarrow Q)$. Ответ:* $(P \vee Q) \wedge (\neg P \vee \neg Q)$.

1.9.3 Полнота исчисления эквивалентностей[2]

Следующая теорема является простым аналогом теоремы о полноте исчисления высказываний, доказываемой ниже. Смысл этого результата в том, что мы сводим (без потери информации) проверку эквивалентности формул к чисто механическим символьным преобразованиям. Исчисление эквивалентностей, фигурирующее неявно в данной теореме — представитель класса так называемых *эквациональных исчислений*, или *исчислений тождеств*, которые распространены в алгебре.

Теорема 1.74. *Всякая равносильность $A \equiv B$ может быть выведена из основных равносильностей (данных в таблице) и дополнительных равносильностей для констант $\top$ и $\bot$*

$$A \wedge \neg A \equiv \bot, \quad A \vee \neg A \equiv \top$$

по правилу замены подформулы на эквивалентную и правилам

$$\frac{B \equiv A}{A \equiv B}, \qquad \frac{A \equiv B \quad B \equiv C}{A \equiv C}.$$

Доказательство. По теореме о СДНФ равносильные формулы приводятся к графически равным СДНФ. При этом достаточно пользоваться лишь основными и дополнительными равносильностями и указанными правилами для вывода новых равносильностей (см. второй способ доказательства теоремы о СДНФ). Нам нужно лишь вывести следующие используемые в доказательстве теоремы о СДНФ равносильности для констант: $\bot \wedge A \equiv \bot$, $\bot \vee A \equiv A$, $A \wedge \top \equiv A$. Получаем:

- $A \wedge \bot \equiv A \wedge (A \wedge \neg A) \equiv (A \wedge A) \wedge \neg A \equiv A \wedge \neg A \equiv \bot$.
- $A \vee \bot \equiv A \vee (A \wedge \neg A) \equiv A$ по закону поглощения.
- $A \wedge \top \equiv A \wedge (A \vee \neg A) \equiv A$, аналогично.

Таким образом, от A к B можно перейти по цепочке эквивалентностей

$$A = A_0 \equiv A_1 \equiv \cdots \equiv A' = B' \equiv \cdots \equiv B_1 \equiv B_0 = B,$$

где A' и B' — СДНФ формул A и B, соответственно, а каждый переход $A_i \equiv A_{i+1}$ и $B_{i+1} \equiv B_i$ получается заменой некоторой подформулы на эквивалентную в соответствии с одной из известных нам основных или дополнительных эквивалентностей. $\boxtimes$

[2]Необязательный материал.

1.10 Другие варианты формальной семантики

1.10.1 Теоретико-множественная семантика

Пусть U — непустое множество; $\mathcal{P}(U)$ — множество всех его подмножеств.

Определение 1.75. *Оценкой* называется функция $f : \mathrm{Var} \to \mathcal{P}(U)$. *Значение* $f(A) \subseteq U$ формулы A при оценке f определяется индуктивно по правилам:

- $f(\neg A) \rightleftharpoons U \setminus f(A)$
- $f(A \wedge B) \rightleftharpoons f(A) \cap f(B)$
- $f(A \vee B) \rightleftharpoons f(A) \cup f(B)$
- $f(A \to B) \rightleftharpoons (U \setminus f(A)) \cup f(B)$

Замечание 1.76. Если взять $U = \{0\}$, теоретико-множественная семантика сводится к стандартной двузначной: Л $= \varnothing$, И $= U$.

Замечание 1.77. Если взять $U = \mathbb{R}^2$ и если для $P \in \mathrm{Var}$ $f(P)$ — круги на плоскости, получаем *диаграммы Венна*, известные из школы.

1.10.2 Алгебраическая семантика[3]

Определение 1.78. Множество $\mathbf{B}$ с заданными на нём константами 0, 1 и операциями $\neg$, $\wedge$, $\vee$, $\to$, которые удовлетворяют равенствам

$$a \wedge \neg a = 0, \quad a \vee \neg a = 1$$

и равенствам, соответствующим таблице основных эквивалентностей, называется *булевой алгеброй*.

В таблице основных эквивалентностей заменяем $\equiv$ на $=$ и большие латинские буквы A, B, C (означающие произвольные формулы) на маленькие a, b, c (означающие элементы множества $\mathbf{B}$), получаем список *тождеств булевой алгебры:*

[3]Необязательный материал.

$a \wedge b$	$=$	$b \wedge a$	$a \vee b$	$=$	$b \vee a$
$a \wedge (b \wedge c)$	$=$	$(a \wedge b) \wedge c$	$a \vee (b \vee c)$	$=$	$(a \vee b) \vee c$
$a \wedge a$	$=$	a	$a \vee a$	$=$	a
$a \wedge (b \vee c)$	$=$	$(a \wedge b) \vee (a \wedge c)$	$a \vee (b \wedge c)$	$=$	$(a \vee b) \wedge (a \vee c)$
$a \vee (a \wedge b)$	$=$	a	$a \wedge (a \vee b)$	$=$	a
$\neg(a \wedge b)$	$=$	$\neg a \vee \neg b$	$\neg(a \vee b)$	$=$	$\neg a \wedge \neg b$
$\neg\neg a$	$=$	a	$a \to b$	$=$	$\neg a \vee b$
$a \wedge \neg a$	$=$	0	$a \vee \neg a$	$=$	1

Примеры булевых алгебр.

- $\mathbb{B} \rightleftharpoons \{0, 1\}$;
- $\mathcal{P}(U)$ для любого U;
- $\mathrm{Fm}/\equiv$ (*алгебра Линденбаума*), то есть множество классов равносильных формул с синтаксически определёнными операциями $\wedge$, $\vee$, $\to$, $\neg$. Более формально, если $[A]$ обозначает класс эквивалентности формулы A, то операция $\wedge$ на классах определяется следующим образом: $[A] \wedge [B] \rightleftharpoons [A \wedge B]$, и аналогично определены остальные операции. Лемма 1.52 гарантирует корректность этих определений.

Определение 1.79. *Оценкой* на булевой алгебре называется функция $f : \mathrm{Var} \to \mathbf{B}$. *Значение* $f(A) \in \mathbf{B}$ формулы A при оценке f вычисляется в соответствии с заданными на $\mathbf{B}$ операциями, в частности $f(A \wedge B) = f(A) \wedge f(B)$ и т.д.

Непосредственно следует из определений следует

Лемма 1.80. *Для любой оценки $f : \mathrm{Var} \to \boldsymbol{B}$ на булевой алгебре, если $A \equiv B$ — одна из основных или дополнительных эквивалентностей, то $f(A) = f(B)$ в $\boldsymbol{B}$.*

Следующая теорема показывает, что каждая из указанных семантик задаёт одно и то же множество тавтологий.

Теорема 1.81. *Для любого множества U и любой булевой алгебры $\boldsymbol{B}$ равносильны следующие утверждения.*

(i) *A — тавтология;*

(ii) $f(A) = U$ *для любой оценки* $f : \mathrm{Var} \to \mathcal{P}(U)$;

(iii) $f(A) = 1$ *для любой оценки* $f : \mathrm{Var} \to \boldsymbol{B}$.

Доказательство. Утверждение (iii) влечёт (i), поскольку если $f : \mathrm{Var} \to \mathbb{B}$ — оценка, при которой $f(A) = \text{Л}$, мы можем определить соответствующую оценку $f' : \mathrm{Var} \to \mathbf{B}$ на булевой алгебре $\mathbf{B}$ отождествляя И с $1 \in \mathbf{B}$ и Л с $0 \in \mathbf{B}$. При этом для любой формулы C имеем

$$f(C) = \text{И} \iff f'(C) = 1$$

и тем самым $f'(A) = 0$. Аналогично, (ii) влечёт (i).

Докажем, что (i) влечёт (iii). Допустим, что A тавтология. По теореме о полноте исчисления эквивалентностей, равносильность $A \equiv \top$ выводится из основных и дополнительных эквивалентностей по известным правилам. Индукцией по длине цепочки вывода $A \equiv \top$ на основе леммы 1.80 легко установить, что $f(A) = f(\top) = 1$ при любой оценке f.

Отметим, что (i) влечёт (ii) поскольку $\mathcal{P}(U)$ есть булева алгебра. ⊠

2 Исчисление высказываний

В этом разделе буквы A, B и т. д. обозначают формулы логики высказываний, а буквы Γ, Δ и т. д. обозначают множества формул логики высказываний.

2.1 Аксиомы и правила вывода исчисления высказываний

Определение 2.1. *Классическое исчисление высказываний* задаётся следующими аксиомами и правилами вывода:

Аксиомы:
1. $A \to (B \to A)$,
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
3. $A \wedge B \to A$,
4. $A \wedge B \to B$,
5. $A \to (B \to A \wedge B)$,
6. $A \to A \vee B$,
7. $B \to A \vee B$,
8. $(A \to C) \to ((B \to C) \to (A \vee B \to C))$,
9. $(A \to B) \to ((A \to \neg B) \to \neg A)$,
10. $\neg\neg A \to A$.

Правило вывода: $\dfrac{A \quad A \to B}{B}$ (*modus ponens*, MP).

Определение 2.2. *Выводом в исчислении высказываний* (или просто *выводом*) называется конечная последовательность формул, каждая из которых является аксиомой или получается из некоторых предыдущих формул по правилу вывода.

Пример 2.3. Следующая последовательность формул является выводом:

$$
\begin{array}{ll}
P \to Q \vee P & \\
Q \to Q \vee P & \\
(P \to Q \vee P) \to ((Q \to Q \vee P) \to (P \vee Q \to Q \vee P)) & \\
(Q \to Q \vee P) \to (P \vee Q \to Q \vee P) & \text{(MP)} \\
P \vee Q \to Q \vee P & \text{(MP)}.
\end{array}
$$

Определение 2.4. Формула A называется *выводимой* в исчислении высказываний или *теоремой* исчисления высказываний (обозначение $\vdash A$), если существует вывод, в котором последняя формула есть A.

Пример 2.5. $\vdash P \vee Q \to Q \vee P$.

Пример 2.6. $\vdash A \to A$.

Доказательство. В аксиоме 2 возьмём $B = (A \to A)$ и $C = A$.

$$
\begin{array}{ll}
(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)) & \\
A \to ((A \to A) \to A) & \\
(A \to (A \to A)) \to (A \to A) & \text{(MP)} \\
A \to (A \to A) & \\
A \to A & \text{(MP).}
\end{array}
$$

$\boxtimes$

2.2 Выводимость из гипотез

Определение 2.7. Пусть Γ — некоторое множество формул. *Выводом из* Γ называется конечная последовательность формул, каждая из которых либо принадлежит множеству Γ, либо является аксиомой, либо получается из предыдущих формул по правилу вывода. Элементы множества Γ называются *гипотезами*.

Пример 2.8. Следующая последовательность формул является выводом из множества гипотез $\{P \wedge Q\}$:

$$
\begin{array}{ll}
P \wedge Q & \text{(гипотеза)} \\
P \wedge Q \to P & \\
P & \text{(MP)} \\
P \wedge Q \to Q & \\
Q & \text{(MP)} \\
Q \to (P \to Q \wedge P) & \\
P \to Q \wedge P & \text{(MP)} \\
Q \wedge P & \text{(MP).}
\end{array}
$$

Определение 2.9. Формула A называется *выводимой из множества формул* Γ (обозначение $\Gamma \vdash A$), если существует вывод из Γ, в котором последняя формула есть A.

Замечание 2.10. Вместо $\{B_1, \ldots, B_n\} \vdash A$ обычно пишут $B_1, \ldots, B_n \vdash A$. Выражение $\Gamma \vdash A, B$ означает $\Gamma \vdash A$ и $\Gamma \vdash B$.

Пример 2.11. $P \wedge Q \vdash Q \wedge P$.

Замечание 2.12. Выводимость из гипотез обладает следующими простыми свойствами.

- Если $\Delta \subseteq \Gamma$ и $\Delta \vdash A$, то $\Gamma \vdash A$ (*монотонность*).
- Если $\Gamma \vdash A$, то существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vdash A$ (*компактность*).
- Если $\Gamma \vdash A$ и для каждой формулы $B \in \Gamma$ имеет место $\Delta \vdash B$, то $\Delta \vdash A$ (*транзитивность*).

2.3 Корректность исчисления высказываний

Предложение 2.13 (корректность). *Всякая выводимая формула является тавтологией.*

Доказательство. Теорема доказывается индукцией по длине вывода формулы A. $\boxtimes$

Аналогично доказывается несколько более общее утверждение, связывающее синтаксическое и семантическое отношения следования.

Предложение 2.14. *Если* $\Gamma \vdash A$, *то* $\Gamma \vDash A$.

2.4 Теорема о дедукции для исчисления высказываний

Следующая теорема существенно упрощает построение выводов в исчислении высказываний.

Теорема 2.15 (о дедукции). *Если* $\Gamma \cup \{A\} \vdash B$, *то* $\Gamma \vdash (A \to B)$.

Доказательство. Теорема доказывается индукцией по длине вывода формулы B из множества гипотез $\Gamma \cup \{A\}$.

Если B является аксиомой или принадлежит Γ, то искомый вывод выглядит так:

$$\begin{array}{ll} B & \\ B \to (A \to B) & \\ (A \to B) & \text{(MP)}. \end{array}$$

Если B совпадает с A, то используем пример 2.6.

Если B получена из некоторых предыдущих формул по правилу вывода modus ponens, то эти формулы имеют вид C и $C \to B$. Согласно предположению индукции $\Gamma \vdash (A \to C)$ и $\Gamma \vdash (A \to (C \to B))$. Искомый вывод формулы B из множества гипотез $\Gamma \cup \{A\}$ состоит из этих двух выводов и следующих формул:

$$\begin{array}{ll} (A \to (C \to B)) \to ((A \to C) \to (A \to B)) & \\ (A \to C) \to (A \to B) & \text{(MP)} \\ A \to B & \text{(MP)}. \end{array}$$

$\boxtimes$

Замечание 2.16. Вместо $\Gamma \cup \{A\} \vdash B$ обычно пишут $\Gamma, A \vdash B$.

Пример 2.17. Из примера 2.11 и теоремы 2.15 следует, что $\vdash P \wedge Q \to Q \wedge P$.

Следствие 2.18. *Пусть* Γ — *некоторое множество формул. Тогда* $\Gamma \vdash (A \to B)$ *в том и только том случае, когда* $\Gamma \cup \{A\} \vdash B$.

Доказательство. Достаточность доказана в теореме 2.15. Необходимость доказывается одним применением правила modus ponens. $\boxtimes$

2.5 Полезные выводимые правила

Приведём несколько полезных примеров выводимых правил, обосновываемых с помощью теоремы о дедукции.

Пример 2.19. (*силлогизм*) $A \to B, B \to C \vdash A \to C$.

Доказательство. Дважды по правилу modus ponens выводим

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

Отсюда получаем требуемое по теореме о дедукции. ⊠

Пример 2.20. (*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

Доказательство. По модулю теоремы о дедукции достаточно вывести $A \to B,\ \neg B \vdash \neg A$. Строим следующий вывод:

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

⊠

Пример 2.21. (*ex falso*) $A, \neg A \vdash B$.

ex falso sequitur quodlibet (лат.) «из ложного следует всё, что угодно»

Доказательство. Выводим, опираясь на аксиомы 1 (дважды), 9 и 10:

$$A, \neg A \vdash \neg B \to A, \neg B \to \neg A \vdash \neg\neg B \vdash B.$$

⊠

2.6 Непротиворечивые множества формул

Определение 2.22. Множество формул Γ называется *противоречивым*, если для некоторой формулы A имеем $\Gamma \vdash A$ и $\Gamma \vdash \neg A$. В противном случае Γ называется *непротиворечивым*.

Замечание 2.23. Если Γ противоречиво, то $\Gamma \vdash B$ для любой формулы B в силу выводимости $A, \neg A \vdash B$.

Замечание 2.24. Γ противоречиво, если и только если существует конечное противоречивое подмножество $\Gamma_0 \subseteq \Gamma$.

Лемма 2.25. $\Gamma \cup \{B\}$ *противоречиво* $\iff$ $\Gamma \vdash \neg B$.

Доказательство. Если $\Gamma \vdash \neg B$, то $\Gamma \cup \{B\}$ противоречиво, поскольку в качестве A можно взять B.

Если $\Gamma, B \vdash A, \neg A$, то по теореме о дедукции $\Gamma \vdash B \to A, B \to \neg A$. По аксиоме $(B \to A) \to ((B \to \neg A) \to \neg B)$ отсюда следует $\Gamma \vdash \neg B$. $\boxtimes$

Определение 2.26. Γ называется *максимальным непротиворечивым* множеством, если Γ непротиворечиво и для любой формулы $A \notin \Gamma$ $\Gamma \cup \{A\}$ противоречиво.

Пример 2.27. Пусть f — фиксированная оценка, тогда множество $\Gamma_f \rightleftharpoons \{A : f(A) = \text{И}\}$ — максимальное непротиворечивое.

Теорема 2.28 (Линденбаума). *Для всякого непротиворечивого множества формул* Γ_0 *найдётся максимальное непротиворечивое* $\Gamma \supseteq \Gamma_0$.

Доказательство (для счётного числа переменных). Пусть $A_0, A_1, \ldots$ — пересчёт всех формул языка. Определим последовательность множеств, начинающуюся с данного множества Γ_0,

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \cdots \subseteq \Gamma_n \subseteq \ldots$$

по следующему правилу:

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{A_n\}, \text{ если } \Gamma_n \cup \{A_n\} \text{ непротиворечиво;} \\ \Gamma_n, \text{ иначе.} \end{cases}$$

Положим $\Gamma \rightleftharpoons \bigcup_{n \geq 0} \Gamma_n$. Утверждение теоремы вытекает из следующей леммы.

Лемма 2.29. (i) *Для любого* n *множество* Γ_n *непротиворечиво.*

(ii) Γ — *максимальное непротиворечивое множество.*

Доказательство. Утверждение (i) доказывается индукцией по n. Из (i) вытекает непротиворечивость Γ (в силу свойства компактности). Поэтому для доказательства утверждения (ii) достаточно установить максимальность.

Допустим $A \notin \Gamma$. Поскольку в исходном пересчёте встречаются все формулы, для некоторого k формула A есть A_k. Поскольку $A_k \notin \Gamma$, множество $\Gamma_k \cup \{A_k\}$ противоречиво (иначе мы присоединили бы A_k на шаге k). Значит, противоречиво и объемлющее множество $\Gamma \cup \{A_k\}$. $\boxtimes$

Замечание 2.30. Для несчётного языка теорема Линденбаума доказывается, опираясь на лемму Цорна (эквивалентную аксиоме выбора). Как нетрудно показать, объединение возрастающей цепи непротиворечивых множеств непротиворечиво. Отсюда непосредственно вытекает требуемый результат.

Предложение 2.31. *Пусть* Γ *— максимальное непротиворечивое множество. Тогда для любых формул* A, B

(i) $\neg A \in \Gamma \iff A \notin \Gamma$;

(ii) $(A \wedge B) \in \Gamma \iff A \in \Gamma$ *и* $B \in \Gamma$;

(iii) $(A \vee B) \in \Gamma \iff A \in \Gamma$ *или* $B \in \Gamma$;

(iv) $(A \to B) \in \Gamma \iff A \notin \Gamma$ *или* $B \in \Gamma$.

Доказательство. (i) Рассуждаем от противного. Если обе формулы $A, \neg A \in \Gamma$, то Γ противоречиво. Если же $A, \neg A \notin \Gamma$, то противоречивы, соответственно, множества $\Gamma \cup \{A\}$ и $\Gamma \cup \{\neg A\}$ в силу максимальности. Отсюда по лемме 2.25 получаем $\Gamma \vdash \neg A, \neg\neg A$, т.е. Γ противоречиво.

(ii) Пусть $(A \wedge B) \in \Gamma$, $A \notin \Gamma$. Тогда, в силу максимальности, $\Gamma \cup \{A\}$ противоречиво, откуда $\Gamma \vdash \neg A$. С другой стороны, по аксиоме $(A \wedge B) \to A$ имеем $A \wedge B \vdash A$. Значит, $\Gamma \vdash A$, т.е. Γ противоречиво.

Аналогично рассматриваем случай $(A \wedge B) \in \Gamma$, $B \notin \Gamma$.

Пусть теперь $(A \wedge B) \notin \Gamma$ и $A, B \in \Gamma$. Тогда по максимальности $\Gamma \vdash \neg(A \wedge B)$. С другой стороны, по аксиоме $A \to (B \to (A \wedge B))$ имеем $\Gamma \vdash A \wedge B$, т.е. Γ противоречиво.

(iii) доказывается аналогично (ii).

(iv) Допустим $(A \to B) \in \Gamma$, $A \in \Gamma$, $B \notin \Gamma$. Тогда $\Gamma \cup \{B\}$ противоречиво, откуда $\Gamma \vdash \neg B$. С другой стороны, по правилу modus ponens $\Gamma \vdash B$, т.е. Γ противоречиво.

Допустим $(A \to B) \notin \Gamma$, $A \notin \Gamma$. Тогда в силу максимальности $\Gamma \vdash \neg A$, $\Gamma \vdash \neg(A \to B)$.

Заметим, что $\neg(A \to B) \vdash A$. Действительно, из $A, \neg A \vdash B$ получаем $\neg A \vdash A \to B$, отсюда с помощью контрапозиции и снятия двойного отрицания $\neg(A \to B) \vdash \neg\neg A \vdash A$.

Поскольку $\Gamma \vdash \neg(A \to B)$, отсюда получаем $\Gamma \vdash A$, т.е. Γ противоречиво.

Случай $(A \to B) \notin \Gamma$, $B \in \Gamma$ рассматривается аналогично, с использованием выводимости $\neg(A \to B) \vdash \neg B$. Последняя вытекает с помощью контрапозиции из очевидного $B \vdash A \to B$. $\boxtimes$

2.7 Теорема о полноте исчисления высказываний

Теорема 2.32. *Множество* Γ *непротиворечиво тогда и только тогда, когда* Γ *выполнимо.*

Доказательство. Выполнимость влечёт непротиворечивость. Пусть f — такая оценка, что $f(A) = \text{И}$ для всех формул $A \in \Gamma$. Простой индукцией по построению вывода убедимся, что $f(B) = \text{И}$ для любой формулы B такой, что $\Gamma \vdash B$. Тем самым, B не может быть противоречием.

Непротиворечивость влечёт выполнимость. Допустим Γ непротиворечиво. По теореме Линденбаума расширим Γ до максимального непротиворечивого множества формул Γ'. Определим оценку f следующим образом: для любой переменной P

$$f(P) = \text{И} \overset{\text{def}}{\iff} P \in \Gamma'.$$

Утверждение теоремы вытекает из следующей леммы.

Лемма 2.33. *Для любой формулы A*

$$f(A) = \text{И} \iff A \in \Gamma'.$$

Доказательство. Индукция по построению формулы A.

Если A — переменная, то утверждение верно непосредственно по определению f.

Если $A = \neg B$, то пользуясь последовательно определением оценки, предположением индукции и предложением 2.31 (i) имеем

$$f(\neg B) = \text{И} \iff f(B) \neq \text{И} \iff B \notin \Gamma' \iff (\neg B) \in \Gamma'.$$

Если $A = (B \to C)$, то аналогично по предложению 2.31 (iv) получаем

$$\begin{aligned} f(B \to C) = \text{И} &\iff (f(B) \neq \text{И} \text{ или } f(C) = \text{И}) \iff \\ &\iff (B \notin \Gamma' \text{ или } C \in \Gamma') \iff (B \to C) \in \Gamma'. \end{aligned}$$

Оставшиеся случаи рассматриваются аналогично. ⊠

Поскольку $\Gamma \subseteq \Gamma'$, для любой $A \in \Gamma$ получаем $f(A) = \text{И}$, что и требовалось. ⊠

Теорема 2.34 (полнота). *Всякая тавтология выводима в исчислении высказываний.*

Полнота исчисления высказываний следует из более общего свойства *сильной полноты*.

Теорема 2.35 (сильная полнота). *Для любого множества формул Γ и любой формулы A*

$$\Gamma \vDash A \;\Rightarrow\; \Gamma \vdash A.$$

Доказательство. Заметим, что $\Gamma \vDash A$ влечёт невыполнимость множества $\Gamma \cup \{\neg A\}$. По теореме 2.32 множество $\Gamma \cup \{\neg A\}$ противоречиво и тем самым $\Gamma \vdash \neg\neg A \vdash A$. ⊠

Таким образом, семантическое следование в логике высказываний равносильно выводимости из гипотез:

Следствие 2.36. $\Gamma \vDash A \iff \Gamma \vdash A$.

Следствие 2.37 (компактность). $\Gamma \vDash A \iff \Gamma_0 \vDash A$ *для некоторого конечного подмножества* $\Gamma_0 \subseteq \Gamma$.

3 Логика предикатов первого порядка

3.1 Модели.

Алгебраические системы или модели являются естественной семантикой логики первого порядка.

Пусть M — непустое множество. *n-арным предикатом на M* называется произвольное подмножество $Q \subseteq M^n = M \times M \times \cdots \times M$ (n раз). *n-арной функцией на M* называется функция $f : M^n \to M$. Если Q — n-арный предикат, то часто пишут $Q(x_1, \ldots, x_n)$ вместо $\langle x_1, \ldots, x_n \rangle \in Q$; аналогично, $f(x_1, \ldots, x_n)$ означает $f(\langle x_1, \ldots, x_n \rangle)$. *Константами* называем произвольные элементы множества M.

Сигнатурой называется некоторая совокупность имён функций, предикатов и констант. Сигнатура Σ задаётся тремя непересекающимися алфавитами Pred_Σ, Func_Σ и Const_Σ *предикатных*, *функциональных символов* и *символов констант*, соответственно, и функцией *валентности*

$$\mathrm{arity} : \mathrm{Pred}_\Sigma \cup \mathrm{Func}_\Sigma \to \mathbb{N} \setminus \{0\},$$

сопоставляющей каждому предикатному и функциональному символу число его аргументов.

Алгебраическая система (или *модель*) *сигнатуры* Σ есть непустое множество M вместе с отображением, сопоставляющим каждому предикатному символу P из Σ некоторый предикат P_M на M той же валентности, каждому функциональному символу f функцию f_M на M той же валентности, и каждой символу $c \in \mathrm{Const}_\Sigma$ константу $c_M \in M$. Такое отображение называется *интерпретацией Σ на M*. Множество M называется *универсумом* или *носителем* данной интерпретации (модели). Модель сигнатуры Σ с носителем M обозначается $(M; \Sigma)$.

Замечание 3.1. В математике используются многочисленные стандартные имена для предикатов и функций. Например, на множестве целых чисел «+» означает обычную функцию сложения, «=» означает предикат равенства, «0» константу 0. Так, $(\mathbb{Z}; =, +, 0)$ означает модель с универсумом $\mathbb{Z}$ и заданными на нём бинарным отношением $=$, бинарной функцией $+$ и константой 0. Мы также используем другие стандартные соглашения об обозначениях, например, пишем $a_1 = a_2$ вместо формального $=(a_1, a_2)$ и $a_1 + a_2$ вместо $+(a_1, a_2)$.

3.2 Примеры

Пример 3.2. [Стандартная модель арифметики] $(\mathbb{N}; =, S, +, \times, 0)$

Здесь $S(x) \rightleftharpoons x+1$ есть одноместная функция следования на множестве $\mathbb{N}$, а все остальные функции и предикаты имеют стандартный смысл.

Пример 3.3. [Кольцо целых чисел] $(\mathbb{Z}; =, +, -, \times, 0, 1)$

Здесь «$-$» есть одноместная функция, отображающая x на $-x$.

Пример 3.4. Любое другое кольцо (с единицей) может рассматриваться как модель той же сигнатуры, например

- $\mathbb{Q}[X]$ — кольцо многочленов над полем $\mathbb{Q}$.
- $\mathbb{Z}_n$ — кольцо вычетов по модулю n.
- $M_n(\mathbb{R})$ — кольцо матриц порядка n над $\mathbb{R}$.

Пример 3.5. [Элементарная геометрия плоскости] $(\mathbb{R}^2; =, \cong, B)$, где

- $\mathbb{R}^2$ — множество точек евклидовой плоскости;
- $B(a, b, c)$ — трёхместный предикат «*точка b лежит на прямой ac между точками a и c*»;
- $\cong$ — четырёхместный предикат (записываемый $ab \cong cd$) «*отрезки, задаваемые парами точек ab и cd, имеют равные длины*».

Пример 3.6. [Модель Пуанкаре геометрии Лобачевского] $(\mathbf{H}^2; =, \cong, B)$, где

- $\mathbf{H}^2 \rightleftharpoons \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ — множество точек верхней евклидовой полуплоскости;
- $B(a, b, c)$ — трёхместный предикат «*точка b лежит между точками a и c на полуокружности (или полупрямой), проходящей через a, c и ортогональной вещественной оси*»;
- $\cong$ — четырёхместный предикат (записываемый $ab \cong cd$) «*отрезки, задаваемые парами точек ab и cd, имеют равные длины в смысле метрики Пуанкаре*», то есть

$$ab \cong cd \overset{\text{def}}{\iff} \frac{|a-b|}{|a-\bar{b}|} = \frac{|c-d|}{|c-\bar{d}|},$$

где $\bar{b}$ означает комплексно сопряжённое к b.

Пример 3.7. [Упорядоченные множества] $(\mathbb{N}; <)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}; <)$, $(\mathbb{R}; <)$.

Пример 3.8. [Частично упорядоченные множества]

(i) $(\mathcal{P}(U); \subseteq)$, где U — любое множество;

(ii) $(\mathbb{Z}; |)$, где $a \mid b$ — бинарное отношение «быть делителем»;

(iii) $(Sub(G); \subseteq)$, где $Sub(G)$ — множество всех подгрупп группы G.

Пример 3.9. [Упорядоченные поля рациональных и действительных чисел] $(\mathbb{Q}; =, <, +, -, \times, 0, 1)$ и $(\mathbb{R}; =, <, +, -, \times, 0, 1)$

Естественно было бы обогатить сигнатуру поля операцией взятия обратного элемента (или операцией деления), но эта операция не определена в нуле. Однако, эту операцию можно выразить из уже имеющихся средствами логики первого порядка (см. ниже), поэтому включать её в сигнатуру нет необходимости.

Пример 3.10. [Булева алгебра] $(B; =, \underline{\wedge}, \underline{\vee}, \underline{\neg}, \underline{\rightarrow}, 0, 1)$

Подчёркнутые символы здесь означают операции булевой алгебры (а не логические связки), то есть функции на B.

3.3 Синтаксис логики первого порядка

Язык логики первого порядка $\mathcal{L}_\Sigma$ определяется его сигнатурой Σ. Помимо всех символов сигнатуры, в алфавит языка $\mathcal{L}_\Sigma$ входят два фиксированных счётных алфавита *свободных* и *связанных переменных*

$$\begin{aligned} \mathrm{FrVar} &= \{a_0, a_1, a_2, \dots\}, \\ \mathrm{BdVar} &= \{v_0, v_1, v_2, \dots\}, \end{aligned}$$

и следующие специальные символы:

Булевы связки: $\rightarrow$, $\neg$, $\wedge$, $\vee$;

Кванторы: $\forall$ (квантор общности, «для всех»);
$\exists$ (квантор существования, «существует»);

Знаки пунктуации: «(», «)» (скобки) и «,» (запятая).

Произвольное слово в описанном алфавите называем *выражением*. Некоторые выражения называются *термами* и *формулами*. Множества термов и формул языка $\mathcal{L}_\Sigma$ определяются индуктивно.

Определение 3.11. Множество термов Tm_Σ есть наименьшее множество, замкнутое относительно следующих правил:

1. Свободные переменные и константы суть термы.
2. Если f — функциональный символ валентности n и $t_1, \dots, t_n$ — термы, то выражение $f(t_1, \dots, t_n)$ есть терм.

Пример 3.12. Если $f \in \mathrm{Func}_\Sigma$ — бинарный функциональный символ, то $f(a_0, a_1)$ — терм, а $f(v_0, a_1)$ — не терм.

Определение 3.13. Множество формул Fm_Σ есть наименьшее множество, замкнутое относительно следующих правил:

1. Если P — предикатный символ валентности n и $t_1, \ldots, t_n$ — термы, то $P(t_1, \ldots, t_n)$ есть формула (называемая *атомарной формулой*).
2. Если A, B — формулы, то формулами являются также выражения $(A \to B)$, $\neg A$, $(A \wedge B)$, $(A \vee B)$.
3. Если A — формула, и a — свободная переменная, то для любой связанной переменной x, *не входящей в* A, выражения $(\forall x A[a/x])$ и $(\exists x A[a/x])$ — формулы. (Здесь $A[a/x]$ означает результат замены всех вхождений a в A на x.)

Пример 3.14. $f(a_0, a_1) = f(a_0, a_1)$ и $(\forall v_0(\forall v_1 f(v_0, v_1) = f(v_0, v_1)))$ — формулы (с учётом соглашения о написании предиката $=$), а $g(a_0) = g(v_1)$ — не формула.

Формулы, в которые не входят кванторы, называются *бескванторными*. Формулы и термы, в которые не входят свободные переменные, называются *замкнутыми*. Замкнутые формулы также называются *предложениями*.

Так же как и в логике высказываний, в логике предикатов действуют стандартные соглашения об опускании скобок, сокращения для логических связок, и другие сокращения. В частности,

- пишут буквы a, b, c вместо a_0, a_1, a_2 и т.д.; x, y, z вместо v_0, v_1, v_2 и т.д.;
- пишут $\forall x_1 \ldots x_n A$ вместо $(\forall x_1(\forall x_2(\ldots(\forall x_n A)\ldots)))$ и аналогично для последовательностей кванторов существования.

3.4 Семантика логики первого порядка

Пусть M — модель сигнатуры Σ. Обозначим через $\Sigma(M)$ сигнатуру, получаемую из Σ добавлением новых символов констант $\{\underline{c} : c \in M\}$. Для каждого элемента $c \in M$ добавляется ровно одна константа $\underline{c}$, и все эти символы отличны друг от друга и от символов сигнатуры Σ.

Определение 3.15. Пусть t — замкнутый терм языка $\mathcal{L}_{\Sigma(M)}$. *Значение терма* t *в модели* M есть элемент $t_M \in M$, определяемый индукцией по построению t.

(i) Если $a \in M$, то $\underline{a}_M \rightleftharpoons a$.

(ii) Если $c \in \mathrm{Const}_\Sigma$, то $c_M \in M$ есть данная нам интерпретация c.

(iii) Если t есть $f(t_1, \ldots, t_n)$, где $f \in \mathrm{Func}_\Sigma$, то $t_M \rightleftharpoons f_M((t_1)_M, \ldots, (t_n)_M)$.

Определение 3.16. Пусть A — замкнутая формула языка $\mathcal{L}_{\Sigma(M)}$. *Истинностное значение формулы* A *в модели* M определяется индукцией по построению A (отношение $M \vDash A$ читается «формула A истинна в модели M»).

1. $M \vDash P(t_1, \ldots, t_n) \overset{\text{def}}{\iff} P_M((t_1)_M, \ldots, (t_n)_M)$, если $A = P(t_1, \ldots, t_n)$ — атомарная формула;
2. $M \vDash (B \to C) \overset{\text{def}}{\iff} (M \nvDash B$ или $M \vDash C)$;
3. $M \vDash \neg B \overset{\text{def}}{\iff} M \nvDash B$;
4. $M \vDash (B \wedge C) \overset{\text{def}}{\iff} (M \vDash B$ и $M \vDash C)$;
5. $M \vDash (B \vee C) \overset{\text{def}}{\iff} (M \vDash B$ или $M \vDash C)$;
6. $M \vDash (\forall x B[a/x]) \overset{\text{def}}{\iff}$ для всех $x \in M$ $M \vDash B[a/\underline{x}]$;
7. $M \vDash (\exists x B[a/x]) \overset{\text{def}}{\iff}$ существует $x \in M$ $M \vDash B[a/\underline{x}]$.

Если список $b_1, \ldots, b_n$ содержит все свободные переменные формулы A, а $x_1, \ldots, x_n \in M$, то $M \vDash A[b_1/\underline{x}_1, \ldots, b_n/\underline{x}_n]$ сокращённо записываем как $M \vDash A[b_1/x_1, \ldots, b_n/x_n]$ или даже $M \vDash A[x_1, \ldots, x_n]$.

Замечание 3.17. Нельзя говорить об истинности или ложности незамкнутых формул, поскольку их истинностные значения зависят от выбора значений параметров — входящих в формулу свободных переменных.

Пример 3.18. Формула $a + 1 = b$ в стандартной модели арифметики может быть как истинна, так и ложна, в зависимости от значений a и b.

Пример 3.19. В модели $(\mathbb{N}; =, S, +, \cdot, 0)$ истинна формула

$$\exists x, y, z\, (\neg x = 0 \wedge \neg y = 0 \wedge x \cdot x + y \cdot y = z \cdot z)$$

и ложна формула

$$\exists x, y, z\, (\neg x = 0 \wedge \neg y = 0 \wedge x \cdot x \cdot x + y \cdot y \cdot y = z \cdot z \cdot z).$$

Пример 3.20. В модели $(\mathbb{R}^2; =, \cong, B)$ истинна формула

$$\forall x, y, y', z\, (B(x, y, z) \wedge B(x, y', z) \to B(x, y, y') \vee B(x, y', y)).$$

Эта же формула верна и в модели $(\mathbf{H^2}; =, \cong, B)$.

3.5 Определимые предикаты и функции

Пусть $b_1, \ldots, b_n$ — упорядоченный набор свободных переменных. Запись $A(b_1, \ldots, b_n)$ означает, что все свободные переменные формулы A входят в набор $b_1, \ldots, b_n$.

Для фиксированного набора переменных любая формула $A(b_1, \ldots, b_n)$ определяет n-местный предикат A_M в модели M:

$$A_M(x_1, \ldots, x_n) \overset{\text{def}}{\iff} M \vDash A[b_1/x_1, \ldots, b_n/x_n].$$

Определение 3.21. Предикат $P(x_1, \ldots, x_n)$ называется *определимым (или выразимым) в модели* $(M; \Sigma)$, если $P = A_M$ для некоторой формулы $A(a_1, \ldots, a_n)$ в языке $\mathcal{L}_\Sigma$.

Определение 3.22. Функция f называется *определимой в модели* M, если определим её график, то есть предикат

$$G_f(x_1, \ldots, x_n, y) \overset{\text{def}}{\iff} f(x_1, \ldots, x_n) = y.$$

Пример 3.23. *В модели* $(\mathbb{Z}; \leq)$ *предикат* $a_2 = a_1 + 1$ *определим формулой*

$$a_1 \leq a_2 \wedge \forall v_0 \, (v_0 \leq a_2 \to (v_0 \leq a_1 \vee a_2 \leq v_0)).$$

Следовательно, функция последователя $s(x) \rightleftharpoons x + 1$ *определима в модели* $(\mathbb{Z}; \leq)$.

Пример 3.24. (Аксиома о параллельных)
Определим следующие предикаты в $(\mathbb{R}^2; =, \cong, B)$.

- $a \neq b \rightleftharpoons \neg\, a = b$
- $c \in ab$ «c лежит на прямой ab»:

$$c \in ab \rightleftharpoons (B(c, a, b) \vee B(a, c, b) \vee B(a, b, c)).$$

- $ab \| cd$ «прямые ab и cd параллельны»:

$$ab \| cd \rightleftharpoons (a \neq b \wedge c \neq d \wedge \neg \exists x \, (x \in ab \wedge x \in cd)).$$

Аксиома о параллельных

> «*Через точку* z *вне прямой* xy *можно провести не более одной прямой параллельной данной.*»

может быть выражена следующим образом:

$$\forall x, y, z \, (x \neq y \wedge \neg\, z \in xy \to \forall u, v \, (zu \| xy \wedge zv \| xy \to v \in zu)).$$

Это утверждение верно в $\mathbb{R}^2$, но не в $\mathbf{H}^2$.

Пример 3.25. В модели $(\mathbb{R}; =, +, \cdot, 0, 1)$ выразимы порядок и деление.

- $a \leq b \rightleftharpoons \exists x \, (b = a + (x \cdot x))$
- Предикат «$a/b = c$» выразим формулой

$$D(a, b, c) \rightleftharpoons (b \neq 0 \wedge c \cdot b = a).$$

3.6 Изоморфизм моделей.

Пусть M и M' — модели сигнатуры Σ.

Определение 3.26. *Гомоморфизм* $\varphi : M \to M'$ есть отображение из M в M', сохраняющее все предикаты, функции и константы Σ. То есть, $\varphi : M \to M'$ — гомоморфизм, если для всех $P \in \mathrm{Pred}_\Sigma$, $f \in \mathrm{Func}_\Sigma$ и $c \in \mathrm{Const}_\Sigma$ валентности n, для всех $x_1, \ldots, x_n \in M$

$$\begin{array}{rcl} P_M(x_1, \ldots, x_n) & \Rightarrow & P_{M'}(\varphi(x_1), \ldots, \varphi(x_n)) \\ \varphi(f_M(x_1, \ldots, x_n)) & = & f_{M'}(\varphi(x_1), \ldots, \varphi(x_n)) \\ \varphi(c_M) & = & c_{M'} \end{array}$$

Предложение 3.27. *Композиция гомоморфизмов — гомоморфизм.*

Определение 3.28. *Изоморфизм* $\varphi : M \to M'$ есть гомоморфизм, у которого есть обратный, то есть гомоморфизм $\psi : M' \to M$ такой, что

$$\varphi \circ \psi = id_{M'}, \qquad \psi \circ \varphi = id_M,$$

где $id_M : M \to M$ — тождественный гомоморфизм $id_M(x) = x$.

Определение 3.29. M и M' изоморфны, если существует изоморфизм $\varphi : M \to M'$.

Теорема 3.30. *Если* $\varphi : M \to M'$ *— изоморфизм, то для любой формулы* $A(a_1, \ldots, a_n)$ *и любых* $c_1, \ldots, c_n \in M$

$$M \vDash A[c_1, \ldots, c_n] \iff M' \vDash A[\varphi(c_1), \ldots, \varphi(c_n)].$$

Доказательство. Индукция по построению A. $\boxtimes$

Следствие 3.31. *В изоморфных моделях истинны одни и те же предложения.*

3.7 Доказательство невыразимости с помощью автоморфизмов.

Определение 3.32. *Автоморфизмом* $\varphi : M \to M$ называется изоморфизм модели на себя.

Поскольку все определимые предикаты и функции сохраняются при автоморфизмах модели, для доказательства невыразимости достаточно построить автоморфизм, не сохраняющий ту или иную функцию или предикат.

Пример 3.33. В модели $(\mathbb{Z}; =, +)$ не выразим предикат $\leq$.

Доказательство. Отображение $\varphi : x \mapsto -x$ есть автоморфизм $(\mathbb{Z}; =, +)$, не сохраняющий $\leq$, поскольку $\mathbb{Z} \vDash 0 \leq 1$, но $\mathbb{Z} \nvDash \varphi(0) \leq \varphi(1)$. $\boxtimes$

Пример 3.34. В модели $(\mathbb{Z}; \leq)$ не выразима функция $+$.

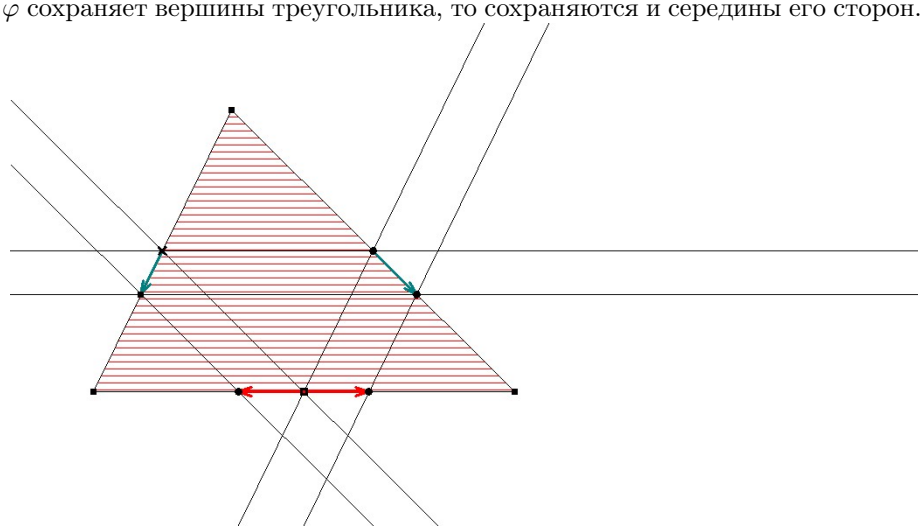
Доказательство. Отображение $\varphi : x \mapsto x + 1$ есть автоморфизм $(\mathbb{Z}; \leq)$, не сохраняющий $+$. $\boxtimes$

Пример 3.35. Автоморфизмами модели $(\mathbb{R}^2; =, B)$ являются все взаимно однозначные аффинные преобразования плоскости и только они.

Этот факт вытекает из следующих соображений.

- Всякий автоморфизм переводит отрезки в отрезки.
- Всякий автоморфизм сохраняет параллельность прямых, поскольку предикат параллельности $ab \| cd$ выразим в этой модели.
- Для любого автоморфизма φ существует аффинное преобразование h такое, что $h \circ \varphi$ сохраняет три различные точки. Действительно, выберем произвольно точки a, b, c, не лежащие на одной прямой. Их образы при автоморфизме φ также не лежат на одной прямой. Каждое аффинное преобразование определяется однозначно образами трёх вершин треугольника. Выберем h таким образом, чтобы $\varphi(a) \mapsto a$, $\varphi(b) \mapsto b$, $\varphi(c) \mapsto c$.
- Если автоморфизм φ имеет три различные неподвижные точки, то $\varphi = id$.

Докажем последнее утверждение. Следующий рисунок показывает, что если φ сохраняет вершины треугольника, то сохраняются и середины его сторон.



Повторяя эту конструкцию для каждого из треугольников, образованных разбиением сторон данного, получаем, что на каждой из сторон треугольника есть всюду плотное множество неподвижных точек φ. Отсюда следует, что все точки сторон треугольника должны быть неподвижны: если $x \neq \varphi(x)$, рассмотрим неподвижную точку, лежащую между x и $\varphi(x)$, и легко придём к противоречию. Но если неподвижны все точки сторон треугольника, то неподвижными должны быть и все его внутренние точки и даже все точки большего треугольника, образованного прямыми, проходящими через вершины данного треугольника и параллельными его противоположным сторонам (каждая точка большего треугольника определяется своими проекциями на пару сторон данного треугольника). Итерируя эту конструкцию мы замостим всю плоскость треугольниками, точки которых неподвижны.

Следствие 3.36. *В модели* $(\mathbb{R}^2; =, B)$ *не определимы:*

- *никакая конкретная точка;*
- *никакая конкретная фигура (множество точек), за исключением всей плоскости;*
- *предикат* $\cong$*;*
- *равенство углов, то есть шестиместный предикат* $\angle abc \cong \angle a_1 b_1 c_1$*.*

Пример 3.37. Автоморфизмы модели $(\mathbb{R}^2; =, B, \cong)$ суть все преобразования плоскости, являющиеся композицией гомотетии и движения.

Для доказательства этого факта отметим, что

- Предикаты B и $\cong$ сохраняются при движениях и гомотетиях.
- Аффинное преобразование, сохраняющее длины сторон некоторого треугольника, есть движение.
- Любой автоморфизм φ переводит равносторонний треугольник в (подобный ему) равносторонний.
- Для некоторой гомотетии h автоморфизм $h \circ \varphi$ сохраняет длины сторон заданного равностороннего треугольника.

Значит, $h \circ \varphi$ — движение.

Следствие 3.38. *В модели* $(\mathbb{R}^2; =, B, \cong)$ *не определимы:*

- *никакая конкретная фигура, за исключением всей плоскости;*
- *единица длины, то есть предикат «длина отрезка* ab *равна 1»;*
- *ориентация, то есть предикат «вершины треугольника* abc *обходятся против часовой стрелки»;*
- *направление «вдоль оси* x*».*

3.8 Выполнимость, общезначимость, логическое следование.

Определение 3.39. Формула $A(b_1, \ldots, b_n)$ сигнатуры Σ *выполнима в модели* (M, Σ), если для некоторых констант $c_1, \ldots, c_n \in M$ предложение $A[b_1/\underline{c}_1, \ldots, b_n/\underline{c}_n]$ сигнатуры $\Sigma(M)$ истинно. Формула A сигнатуры Σ *выполнима*, если она выполнима в некоторой модели $(M; \Sigma)$.

Определение 3.40. Множество формул Γ сигнатуры Σ *выполнимо в модели* M, если существует функция $f : \mathrm{FrVar} \to M$ такая, что при подстановке вместо каждой переменной a_i константы $\underline{f(a_i)}$ сигнатуры $\Sigma(M)$ все формулы Γ истинны в M. Такую функцию f будем называть *выполняющей оценкой* для Γ.

Множество формул Γ *выполнимо*, если Γ выполнимо в некоторой модели.

Определение 3.41. Формула A *общезначима* (*тождественно истинна*), если $\neg A$ не выполнима.

Определение 3.42. Формула A *тождественно ложна*, если A не выполнима.

Пример 3.43. Формулы $P(a) \vee \neg P(a)$, $\exists x \forall y A(x, y) \to \forall y \exists x\, A(x, y)$ общезначимы. Формула $P(a_0) \to P(a_1)$ выполнима, но не общезначима.

Определение 3.44. Пусть Γ — некоторое множество формул сигнатуры Σ и A — формула той же сигнатуры. Говорят, что A *логически следует* (или *семантически следует*) из множества Γ (обозначение $\Gamma \vDash A$), если для любой модели M сигнатуры Σ формула A истинна в M при любой выполняющей оценке для множества Γ.

Пример 3.45. $\{P(a) \to Q(b), P(a)\} \vDash P(a) \wedge \exists x Q(x)$.

Пример 3.46. $P(a) \nvDash \forall x P(x)$.

Соотношения между понятиями выполнимости, общезначимости и логическим следованием в логике предикатов такие же, как и в логике высказываний.

Предложение 3.47. (i) A *— общезначима* $\iff \varnothing \vDash A$.

(ii) Γ *выполнимо* $\iff \Gamma \nvDash \bot$.

(iii) $\Gamma \vDash A \iff \Gamma \cup \{\neg A\}$ *не выполнимо.*

Предложение 3.48. $\{B_1, \ldots, B_n\} \vDash A \iff (\bigwedge_{i=1}^{n} B_i) \to A$ *общезначима.*

3.9 Эквивалентность формул.

Определение 3.49. Формулы A и B сигнатуры Σ равносильны (обозначение $A \equiv B$), если для любой модели $(M;\Sigma)$ и оценки f на M

$$M \vDash f(A) \iff M \vDash f(B).$$

Пусть список $b_1, \ldots, b_n$ содержит все свободные переменные A, B.

Утверждение 3.50. *$A \equiv B$, если и только если в любой модели M формулы A и B определяют один и тот же предикат, то есть если $A_M = B_M$ (для данного набора переменных).*

Утверждение 3.51. (i) *Отношение $\equiv$ рефлексивно, симметрично и транзитивно.*

(ii) *$A \equiv B$, если и только если формула $A \leftrightarrow B$ общезначима.*

(iii) *Формула A общезначима тогда и только тогда, когда $A \equiv \top$.*

Перечислим основные равносильности с кванторами.

Лемма 3.52 (замена связанной переменной). *Если $x, y \in BdVar$ не входят в формулу A, то $\forall x\, A[a/x] \equiv \forall y\, A[a/y]$ и $\exists x\, A[a/x] \equiv \exists y\, A[a/y]$.*

Доказательство.

$$\begin{array}{rcl} M \vDash \forall x\, A[a/x] & \iff & M \vDash A[a/c] \quad \text{для всех } c \in M \\ & \iff & M \vDash \forall y\, A[a/y]. \end{array}$$

Для квантора существования рассуждение аналогично. $\boxtimes$

Лемма 3.53. *Если $x \in BdVar$ не входит в формулы A, B, то*

$$(\forall x\, A[a/x] \vee B) \equiv \forall x\, (A[a/x] \vee B).$$

Доказательство. Прежде всего заметим, что правая часть эквивалентности, так же как и левая часть, является формулой. В самом деле, выберем $a' \in$ FrVar, не входящую в A, B. Тогда $B[a'/x] = B$, $A[a/x] = A[a/a'][a'/x]$ и тем самым $\forall x\, (A[a/x] \vee B)$ совпадает с $\forall x\, (A[a/a'] \vee B)[a'/x]$. Получаем

$$\begin{array}{rcl} M \vDash \forall x\, (A[a/x] \vee B) & \iff & M \vDash (A[a/c] \vee B) \quad \text{для всех } c \in M \\ & \iff & (M \vDash B \text{ или для всех } c \in M\ M \vDash A[a/c]) \\ & \iff & (M \vDash B \text{ или } M \vDash \forall x\, A[a/x]) \\ & \iff & M \vDash (\forall x\, A[a/x] \vee B). \end{array}$$

$\boxtimes$

Аналогично обосновываются остальные равносильности, входящие в следующую таблицу (где предполагается, что переменные x, y не входят в формулы A и B).

$\forall x\, A[a/x]$	$\equiv$	$\forall y\, A[a/y]$	$\exists x\, A[a/x]$	$\equiv$	$\exists y\, A[a/y]$
$(\forall x\, A[a/x] \vee B)$	$\equiv$	$\forall x\, (A[a/x] \vee B)$	$(\exists x\, A[a/x] \vee B)$	$\equiv$	$\exists x\, (A[a/x] \vee B)$
$(\forall x\, A[a/x] \wedge B)$	$\equiv$	$\forall x\, (A[a/x] \wedge B)$	$(\exists x\, A[a/x] \wedge B)$	$\equiv$	$\exists x\, (A[a/x] \wedge B)$
$\neg\forall x A[a/x]$	$\equiv$	$\exists x \neg A[a/x]$	$\neg\exists x A[a/x]$	$\equiv$	$\forall x \neg A[a/x]$

3.10 Правила подстановки и замены подформулы на эквивалентную.

Определение 3.54. Обогатим язык логики первого порядка пропозициональной переменной P. Можно считать P нульместным предикатным символом. Распространим на расширенный язык все синтаксические понятия, включая понятие формулы (P считается атомарной формулой). Запись $C[P/A]$ означает результат замены всех вхождений P в формулу C на A.

Заметим, что $C[P/A]$ не всегда является формулой. Для этого достаточно, чтобы связанные переменные A не входили в C. Необходимое и достаточное условие формулируется следующим образом.

Лемма 3.55. *$C[P/A]$ — формула, если и только если любое вхождение P в формулу C не находится в области действия квантора по переменной $x \in BdVar$, входящей в A.*

Доказательство. Необходимость этого условия очевидна. Достаточность доказывается простой индукцией по построению формулы C. $\boxtimes$

Определение 3.56. Говорим, что *разрешена подстановка формулы A вместо P в C*, если выполнено условие предыдущей леммы.

Лемма 3.57. (i) *Если $A \equiv B$, то $\neg A \equiv \neg B$. Если $A_1 \equiv B_1$ и $A_2 \equiv B_2$, то $A_1 \wedge A_2 \equiv B_1 \wedge B_2$, $A_1 \vee A_2 \equiv B_1 \vee B_2$, $A_1 \to A_2 \equiv B_1 \to B_2$.*

(ii) *Если $A \equiv B$ и $x \in BdVar$ не входит в A, B, то $\forall x A[a/x] \equiv \forall x B[a/x]$ и $\exists x A[a/x] \equiv \exists x B[a/x]$.*

Теорема 3.58 (замена подформулы на эквивалентную). *Если $A \equiv B$ и разрешена подстановка формул A, B вместо P в C, то $C[P/A] \equiv C[P/B]$.*

Доказательство. Теорема доказывается индукцией по построению формулы C на основе очевидной леммы 3.57. Рассмотрим лишь один наиболее интересный случай.

Допустим C имеет вид $\forall x D[a/x]$. Поскольку $C = \forall x D[a/a'][a'/x]$, переходя в случае необходимости к формуле $D[a/a']$ мы можем считать, что переменная a не входит в A, B. По предположению индукции $D[P/A] \equiv D[P/B]$. Так как подстановка формул A, B в C разрешена, переменная x не входит в A, B. Отсюда по лемме 3.57 (ii) получаем

$$\forall x D[P/A][a/x] \equiv \forall x D[P/B][a/x].$$

Поскольку a не входит в A, B мы имеем $D[P/A][a/x] = D[a/x][P/A]$, откуда

$$(\forall x D[a/x])[P/A] = (\forall x D[P/A][a/x]) \equiv (\forall x D[P/B][a/x]) = (\forall x D[a/x])[P/B].$$

$\boxtimes$

Комбинируя эту теорему вместе с леммой 3.52 мы получаем следующее утверждение о переименовании связанных переменных в формуле.

Лемма 3.59. *Пусть $y \in BdVar$ не входит в формулу B. Тогда $B[x/y]$ есть формула и $B[x/y] \equiv B$.*

Доказательство. Применяем индукцию по числу вхождений кванторов $\forall x$ в B. Если таких вхождений нет, то утверждение очевидно. Иначе $B = B'[P/C]$, где $C = \forall x A[a/x]$ для некоторых формул B' и A. По предположению индукции $B' \equiv B'' \rightleftharpoons B'[x/y]$. По лемме 3.52 $C \equiv C' \rightleftharpoons \forall y A[a/y]$, поэтому

$$B'[P/C] \equiv B''[P/C] \equiv B''[P/C'].$$

Но формула $B''[P/C']$ совпадает с $B[x/y]$. $\boxtimes$

Понятие модели также распространяется на формулы языка, расширенного пропозициональной переменной P. При этом P в модели M интерпретируется как логическая константа, то есть $P_M \in \mathbb{B}$. Считается $M \vDash P_M$, если $P_M = \text{И}$ и $M \nvDash P_M$, если $P_M = \text{Л}$. При этих соглашениях понятие общезначимой формулы и равносильности формул распространяется на расширенный язык.

Теорема 3.60 (о подстановке). *Пусть формула A общезначима и разрешена подстановка формулы C вместо P в A, тогда общезначима формула $A[P/C]$.*

Доказательство. Рассуждаем от противного. Допустим, $M \nvDash A[P/C]$ при некоторой подстановке элементов M вместо свободных переменных этой формулы. Поскольку формула C не содержит других свободных переменных, при данной подстановке она истинна или ложна. Положим

$$P_M = \text{И} \iff M \vDash C.$$

Тем самым мы доопределили модель M до модели языка с пропозициональной переменной P. Индукцией по построению формулы B этого языка легко проверяется, что

$$M \vDash B[P/C] \iff M \vDash B$$

для любой формулы B, в которую разрешена подстановка C вместо P. Отсюда получаем $M \nvDash A$. $\boxtimes$

3.11 Предварённые формулы

Определение 3.61. Формула A называется *предварённой*, если A имеет вид $\mathsf{Q}x_1\mathsf{Q}x_2\ldots\mathsf{Q}x_nA_0[b_1/x_1,\ldots,b_n/x_n]$, где Q означает квантор $\forall$ или $\exists$, а формула A_0 бескванторная.

Теорема 3.62 (о предварённой форме). *Для каждой формулы A можно указать эквивалентную ей предварённую формулу A' от тех же свободных переменных.*

Такую формулу A' называем *предварённой формой* формулы A.

Доказательство. Применяя основные эквивалентности с кванторами постепенно выносим все кванторы наружу. Более формально, доказываем теорему индукцией по построению A.

Удобно ввести следующее обозначение. Пусть α, β означают произвольные последовательности кванторов вида $\mathsf{Q}x_1\mathsf{Q}x_2\ldots\mathsf{Q}x_n$, а αA означает результат применения последовательности кванторов α к формуле A.

Лемма 3.63. *Для любых α, β и любых формул A, B, не содержащих переменных из α, β, имеем:*

(i) $\alpha A\wedge B\equiv\alpha(A\wedge B)$; $\alpha A\vee B\equiv\alpha(A\vee B)$;

(ii) $\neg\,\alpha A\equiv\bar\alpha\neg A$, *где $\bar\alpha$ получается из α заменой всех символов $\exists$ на $\forall$ и наоборот.*

Доказательство. Утверждение (i) доказывается индукцией по длине α. Шаг индукции есть вторая и третья строка таблицы основных эквивалентностей. Утверждение (ii) получается по индукции из последней строки таблицы эквивалентностей. ⊠

Доказательство теоремы. Можем считать, что формула A не содержит связки импликации.

Если A атомарна, то можно взять $A'=A$.

Если $A=\forall xB[a/x]$, пусть B' — предварённая форма B. Переходя к эквивалентной формуле $B''=B'[x/x']$, где x' — новая переменная, добиваемся того, что x не входит в B''. Тогда $A'\rightleftharpoons\forall xB''[a/x]$ — требуемая формула.

Если $A=\neg B$ и B' — предварённая форма B, то применяем утверждение (ii) предыдущей леммы.

Если $A=(B\vee C)$, по теореме о замене подформулы на эквивалентную получаем $A\equiv(B'\vee C')$, где $B'=\alpha B_0$ и $C'=\beta C_0$ — предварённые формы B и C, соответственно (формулы B_0 и C_0 бескванторные). Произведя замену связанных переменных, входящих в C', на новые, можно считать, что последовательности α и β содержат не пересекающиеся множества переменных. Тогда дважды применимо утверждение (i) предыдущей леммы и мы получаем

$$A\equiv\alpha B_0\vee\beta C_0\equiv\alpha(B_0\vee\beta C_0)\equiv\alpha\beta(B_0\vee C_0),$$

что и требовалось доказать.

Случай конъюнкции рассматривается аналогично. ⊠

3.12 Теории и их модели

Определение 3.64. *Теорией* сигнатуры Σ называем произвольное множество T замкнутых формул языка $\mathcal{L}_\Sigma$. Элементы $A \in T$ называем *нелогическими аксиомами* T.

Пример 3.65. Теория отношения эквивалентности в сигнатуре с единственным бинарным предикатным символом R задаётся следующими тремя нелогическими аксиомами:

1. $\forall x\, R(x, x)$;
2. $\forall x, y\, (R(x, y) \to R(y, x))$;
3. $\forall x, y, z\, (R(x, y) \wedge R(y, z) \to R(x, z))$.

Определение 3.66. Модель $(M; \Sigma)$ есть *модель теории* T (обозначение $M \vDash T$), если для любой $A \in T$ $M \vDash A$.

Пример 3.67. R есть отношение эквивалентности на множестве M, если и только если $(M; R) \vDash T$, где T — теория отношения эквивалентности.

Пример 3.68. Модель $(M; <)$ есть *строгий частичный порядок*, если в $(M; <$) истинны следующие предложения:

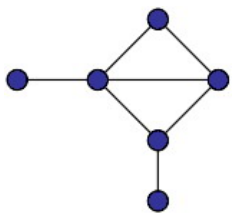
1. $\forall x, y, z\, (x < y \wedge y < z \to x < z)$
2. $\forall x \neg\, x < x$

Это можно считать определением строгих частичных порядков. Аксиомы 1 и 2 задают *теорию строгих частичных порядков*.

Пример 3.69. *Простой граф* — это модель вида $(V; E)$, где V — множество (называемое множеством вершин графа), а E — бинарный предикат *смежности*, причём отношение E симметрично и иррефлексивно:

1. $\forall x \neg\, E(x, x)$
2. $\forall x, y\, (E(x, y) \to E(y, x))$

Аксиомы 1 и 2 задают *теорию простых графов*.



Пример 3.70. $(M; =, \cdot, 1)$ есть *группа*, если M есть модель следующей теории (при условии, что «=» в M понимается как равенство):

1. $\forall x, y, z \;\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\forall x \, (1 \cdot x = x \wedge x \cdot 1 = x)$
3. $\forall x \exists y \, (x \cdot y = 1 \wedge y \cdot x = 1)$

Под *теорией групп*, однако, обычно понимают несколько иную теорию, формулируемую в языке с дополнительным функциональным символом для операции взятия обратного элемента. В таком языке аксиомы теории групп выразимы предварёнными формулами, не содержащими кванторов существования.

3.13 Теории с равенством

Пусть Σ — сигнатура, содержащая выделенный предикатный символ «=».

Определение 3.71. *Нормальной моделью* называем модель $(M; \Sigma)$, в которой «=» интерпретируется как равенство $\{\langle x, x\rangle \mid x \in M\}$.

Определение 3.72. *Аксиомы равенства* для Σ суть универсальные замыкания следующих формул:

1. аксиомы отношения эквивалентности для «=»;
2. $a_1 = b_1 \wedge a_2 = b_2 \wedge \cdots \wedge a_n = b_n \to (P(a_1, \ldots, a_n) \leftrightarrow P(b_1, \ldots, b_n))$;
3. $a_1 = b_1 \wedge a_2 = b_2 \wedge \cdots \wedge a_n = b_n \to (f(a_1, \ldots, a_n) = f(b_1, \ldots, b_n))$.

для всех $f \in \mathrm{Func}_\Sigma$ and $P \in \mathrm{Pred}_\Sigma$.

Следующее предложение вытекает непосредственно из определений.

Предложение 3.73. *Если $(M; \Sigma)$ — нормальная модель, то в M истинны все аксиомы равенства.*

Определение 3.74. *Теорией с равенством* называем теорию в языке с равенством, содержащую все аксиомы равенства.

Теорема 3.75. *Пусть T — теория с равенством. Если T выполнима, то T имеет нормальную модель.*

Доказательство. Пусть $M \models T$. Предикат $=_M$ есть отношение эквивалентности на M. Положим $M' \rightleftharpoons M/{=_M}$ — множество классов эквивалентности

и пусть $\varphi : M \to M'$ сопоставляет любому $x \in M$ его класс эквивалентности $\varphi(x) \in M'$. Все функции и предикаты сигнатуры Σ естественным образом переносятся с M на M': полагаем

$$\begin{array}{rcl} P_{M'}(\varphi(x_1), \ldots, \varphi(x_n)) & \stackrel{\text{def}}{\iff} & P_M(x_1, \ldots, x_n) \\ f_{M'}(\varphi(x_1), \ldots, \varphi(x_n)) & \rightleftharpoons & \varphi(f_M(x_1, \ldots, x_n)) \\ c_{M'} & \rightleftharpoons & \varphi(c_M). \end{array}$$

Заметим, что в силу истинности аксиом равенства в M все функции и предикаты корректно определены на M', и M' — нормальная модель.

Индукцией по построению формулы A проверяем

$$M \vDash A[x_1, \ldots, x_n] \iff M' \vDash A[\varphi(x_1), \ldots, \varphi(x_n)].$$

Отсюда следует $M' \vDash T$.

Упражнение 3.76. *Выпишете аксиомы теории коммутативных колец с единицей в сигнатуре* $=, +, -, \cdot, 0, 1$.

Упражнение 3.77. *Выпишете аксиомы теории полей в той же сигнатуре.*

3.14 Элементарная геометрия

Полная система аксиом для элементарной геометрии была построена Давидом Гильбертом. В дальнейшем аксиоматика Гильберта была оптимизирована целым рядом исследователей. По-видимому, наиболее простая аксиоматика (на основе понятия точки и отношений $B, \cong$) была предложена Альфредом Тарским. Им же были получены фундаментальные результаты о полноте и разрешимости элементарной геометрии.

Элементарная геометрия Тарского представляет собой теорию первого порядка с равенством в сигнатуре $=, B, \cong$, задаваемую следующими аксиомами G1–G11.

Аксиоматика Тарского:

G1. $ab \cong ba$

G2. $ab \cong pq \wedge ab \cong rs \to pq \cong rs$

G3. $ab \cong cc \to a = b$

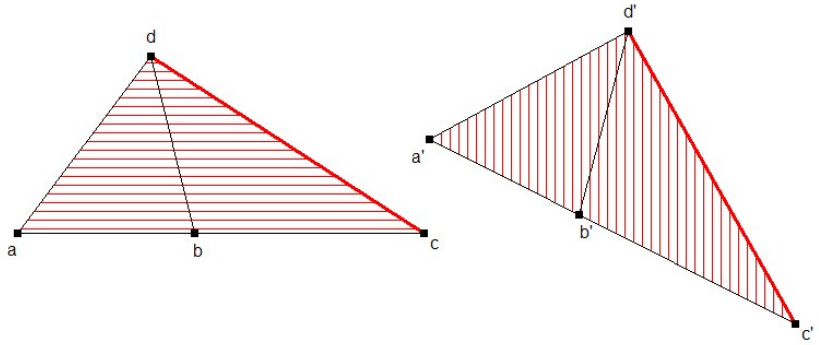
G4. $Babd \wedge Bbcd \to Babc$

G5. $\exists x\, (Bqax \wedge ax \cong bc)$

На прямой qa в сторону от точки a противоположную q можно отложить отрезок заданной длины.

G6. (аксиома о пяти отрезках)

$$(a \neq b \wedge Babc \wedge Ba'b'c' \wedge ab \cong a'b' \wedge bc \cong b'c' \\ \wedge ad \cong a'd' \wedge bd \cong b'd') \rightarrow cd \cong c'd'$$

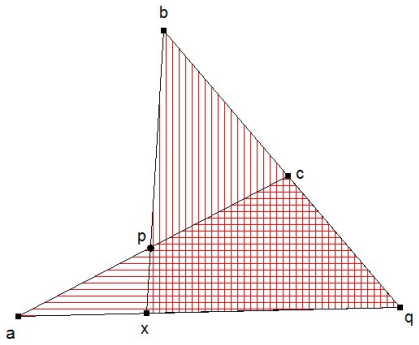


Если даны четыре точки $abcd$ и соответствующие им точки $a'b'c'd'$ такие, что длины соответствующих рисунку четырёх (помеченных чёрным цветом) отрезков равны, то равны и длины пятых (помеченных красным) отрезков.

Эта аксиома заменяет признак равенства треугольников по двум сторонам и углу между ними и позволяет избежать использования понятия «угол» в аксиомах геометрии.

G7. (аксиома Паша)

$$Bapc \wedge Bqcb \rightarrow \exists x\,(Baxq \wedge Bbpx)$$



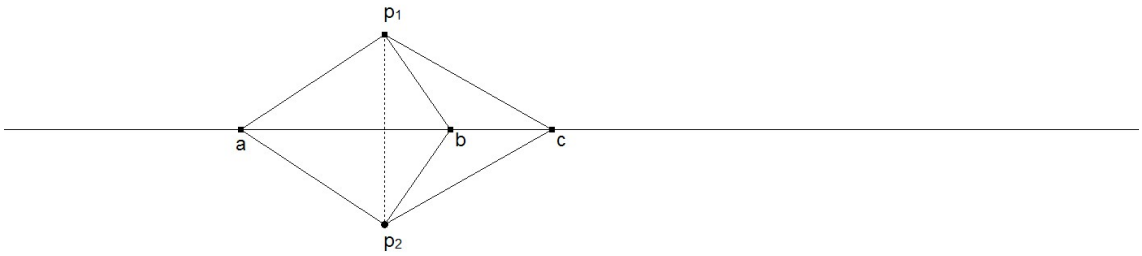
Следующие аксиомы G8 и G9 называются аксиомами размерности. G8 влечёт, что размерность пространства не менее двух, а G9 — что она не более двух.

G8. $(dim \geq 2)$
$\exists x, y, z\ (\neg Bxyz \wedge \neg Byzx \wedge \neg Bzxy)$

Существуют три точки, не лежащие на одной прямой.

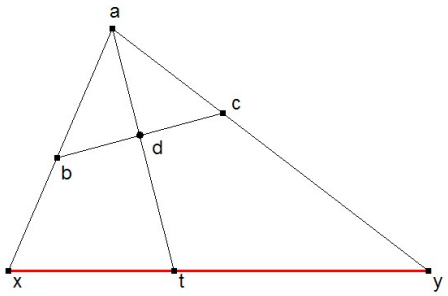
G9. $(dim \leq 2)$
$(p_1 \neq p_2 \wedge ap_1 \cong ap_2 \wedge bp_1 \cong bp_2 \wedge cp_1 \cong cp_2) \rightarrow a \in bc$

Точки, находящиеся на равном расстоянии от двух данных точек p_1, p_2, лежат на одной прямой.



G10. (аксиома Евклида)

$Badt \wedge Bbdc \wedge a \neq d \rightarrow \exists x, y\,(Babx \wedge Bacy \wedge Bytx)$



Эта аксиома является одной из эквивалентных форм аксиомы о параллельных.

G11. (схема аксиом непрерывности)

Для любых формул C, D имеем аксиому

$$\exists u \forall x, y\,(C[a/x] \wedge D[a/y] \rightarrow Buxy) \rightarrow \exists v \forall x, y\,(C[a/x] \wedge D[a/y] \rightarrow Bxvy)$$

Переменные x, y, u, v не входят в C, D.

Если точки, удовлетворяющие свойству C, лежат между фиксированной точкой u и любой из точек, удовлетворяющих свойству D, то найдётся точка v разделяющая точки из C и D.

Таким образом, эта аксиома является разновидностью известной из курса анализа аксиомы полноты (для действительной прямой). Принципиально, что здесь речь идёт лишь о множествах точек *определимых* формулами C и D языка элементарной геометрии.

В полном своём объёме, то есть для произвольных подмножеств прямой, эта аксиома не выразима в логике первого порядка (без использования понятия множества).

Замечание 3.78. В геометрии второго порядка наряду с переменными по точкам пространства имеются переменные $X, Y, \ldots$ по произвольным множествам точек и бинарное отношение $\in$ между точками и множествами. Замена схемы $G11$ на нижеследующую аксиому непрерывности второго порядка $G11'$ даёт полную аксиоматику геометрии евклидовой плоскости, эквивалентную известной аксиоматике Гильберта. Эта система аксиом обладает свойством *категоричности*, состоящим в том, что любая модель системы аксиом $G1 - G11'$ *изоморфна* евклидовой плоскости. Ниже мы установим, что никакое множество аксиом первого порядка не обладает этим свойством.

G11′. (аксиома непрерывности 2-го порядка)

$$\forall X, Y\,(\exists u \forall x, y\,(x \in X \wedge y \in Y \to Buxy) \to\ \exists v \forall x, y\,(x \in X \wedge y \in Y \to Bxvy)).$$

3.15 Теоремы Тарского о полноте и разрешимости элементарной геометрии

Приведём без доказательства следующие два важных результата, принадлежащих Альфреду Тарскому.

Теорема 3.79. *Для любого предложения A языка элементарной геометрии, если $(\mathbb{R}^2; =, B, \cong) \vDash A$, то A логически следует из аксиом G1–G11.*

Теорема 3.80. *Существует алгоритм проверки произвольной формулы A языка элементарной геометрии на выполнимость в $\mathbb{R}^2$.*

4 Исчисление предикатов

4.1 Аксиомы и правила вывода

Исчисление предикатов сигнатуры Σ задаётся следующими схемами аксиом и правилами вывода.

Аксиомы:

A1. аксиомы исчисления высказываний,

A2. $\forall x A[a/x] \to A[a/t]$,

A3. $A[a/t] \to \exists x A[a/x]$.

Схему аксиом A1 более аккуратно мы понимаем следующим образом. Если $A(P_1, \ldots, P_n)$ — аксиома исчисления высказываний, то формула $A[P_1/C_1, \ldots, P_n/C_n]$ есть аксиома исчисления предикатов для любых формул $C_1, \ldots, C_n$ сигнатуры Σ.

В аксиомах A2 и A3 A — любая формула сигнатуры Σ и t — любой терм (переменная x не входит в A).

Правила вывода:

R1. $\dfrac{A \quad A \to B}{B}$ (*modus ponens*)

R2. $\dfrac{A \to B}{A \to \forall x B[a/x]}$

R3. $\dfrac{B \to A}{\exists x B[a/x] \to A}$

В правилах R2 и R3 переменная a не входит в A (и x не входит в B). Правила R2 и R3 называются *правилами Бернайса*.

Определение 4.1. *Выводом в исчислении предикатов* называется конечная последовательность формул, каждая из которых либо является аксиомой, либо получается из предыдущих формул по одному из правил вывода $R1 - R3$.

Пример 4.2.

$$\begin{array}{ll} \forall x A[a/x] \to A & \text{(A2)} \\ \forall x A[a/x] \to \forall y A[a/y] & \text{(R2)} \end{array}$$

Определение 4.3. Формула A называется *выводимой* в исчислении предикатов или *теоремой* исчисления предикатов (обозначение $\vdash A$), если существует вывод, в котором последняя формула есть A.

Пример 4.4. $\vdash \forall x A[a/x] \to \forall y A[a/y]$ для любой формулы A.

4.2 Выводимость в теории

Для исчисления предикатов мы рассматриваем понятие *выводимости в теории*, которое является аналогом понятия выводимости из гипотез для исчисления высказываний. Нам будет удобно считать, что гипотезы являются замкнутыми формулами, что соответствует понятию теории как множеству *замкнутых* формул.

Определение 4.5. *Выводом в теории* T называется конечная последовательность формул, каждая из которых либо принадлежит множеству T, либо является логической аксиомой вида $A1 - A3$, либо получается из предыдущих формул по одному из правил вывода $R1 - R3$.

Определение 4.6. Формула A называется *выводимой (доказуемой) в теории* T или *теоремой* T (обозначение $T \vdash A$), если существует вывод в T, в котором последняя формула есть A.

Определение 4.7. Формула A *опровержима* в T, если $T \vdash \neg A$.

Определение 4.8. Формула A *независима* от T, если $T \nvdash A$ и $T \nvdash \neg A$.

Простейшие свойства отношения выводимости в теории для исчисления предикатов аналогичны свойствам отношения выводимости из гипотез для исчисления высказываний.

- Если $T \subseteq U$ и $T \vdash A$, то $U \vdash A$ (*монотонность*).
- Если $T \vdash A$, то существует такое конечное множество $T_0 \subseteq T$, что $T_0 \vdash A$ (*компактность*).
- Если $T \vdash A$ и для каждой аксиомы $B \in T$ имеет место $U \vdash B$, то $U \vdash A$ (*транзитивность*).

Пусть T, U — теории сигнатуры Σ.

Определение 4.9. Теория U *содержит* T, если для любой $A \in T$ $U \vdash A$ (обозначение $U \vdash T$).

Определение 4.10. Теории T и U *(дедуктивно) эквивалентны*, если $T \vdash U$ и $U \vdash T$ (обозначение $T \equiv U$).

4.3 Теорема о тавтологии

Предложение 4.11. *Если* $A(P_1, \ldots, P_n)$ *выводима в исчислении высказываний, то для любых формул* $C_1, \ldots, C_n$ *сигнатуры* Σ *формула*

$$A[P_1/C_1, \ldots, P_n/C_n]$$

выводима в исчислении предикатов.

Доказательство. Индукция по построению вывода формулы A. Если A — аксиома исчисления высказываний, то результат подстановки является аксиомой вида A1. Если A получена из B и $B \to A$ по правилу modus ponens, то по предположению индукции в исчислении предикатов выводимы формулы $B[P_1/C_1, \ldots, P_n/C_n]$ и $B[P_1/C_1, \ldots, P_n/C_n] \to A[P_1/C_1, \ldots, P_n/C_n]$. Отсюда $A[P_1/C_1, \ldots, P_n/C_n]$ выводится по правилу modus ponens. $\boxtimes$

Замечание 4.12. Это предложение удобно применять в комбинации с теоремой о полноте для исчисления высказываний. Поскольку любая тавтология выводима в исчислении высказываний, аналогичное утверждение имеет место в предположении, что $A(P_1, \ldots, P_n)$ — тавтология.

Пример 4.13. Для любой формулы A сигнатуры Σ формулы $A \to A$ и $A \vee \neg A$ выводимы в исчислении предикатов.

4.4 Теорема о дедукции

Как обычно, пишем $T, A \vdash B$ вместо $T \cup \{A\} \vdash B$.

Теорема 4.14. *Для любой теории T и* замкнутой *формулы A*

$$T, A \vdash B \iff T \vdash A \to B.$$

Доказательство. Индукция по длине вывода $T, A \vdash B$. Разбираем лишь новые случаи, относящиеся к правилам R2 и R3.

Допустим $B = (C \to \forall x D[a/x])$ получена из $C \to D$ по R2. По предположению индукции

$$T \vdash A \to (C \to D).$$

Надо построить вывод

$$T \vdash A \to (C \to \forall x D[a/x]).$$

Рассмотрим тавтологию

$$(P \to (Q \to R)) \leftrightarrow (P \wedge Q \to R).$$

Подставляя A вместо P, C вместо Q и D вместо R получаем, что формула

$$(A \to (C \to D)) \leftrightarrow (A \wedge C \to D)$$

выводима в исчислении предикатов.

Таким образом, вывод $A \to (C \to D)$ в T можно продолжить:

$A \to (C \to D)$	
$(A \to (C \to D)) \to (A \wedge C \to D)$	(тавтология)
$(A \wedge C) \to D$	(MP)
$(A \wedge C) \to \forall x D[a/x]$	(R2, A замкнута)
$A \to (C \to \forall x D[a/x])$	(аналогично)

Правило R3 рассматривается аналогично. $\boxtimes$

4.5 Непротиворечивость и корректность

Определение 4.15. Теория T *противоречива*, если существует формула A такая, что $T \vdash A$ и $T \vdash \neg A$. В противном случае теория T называется *непротиворечивой*.

Из теоремы о дедукции получаем следующее следствие.

Следствие 4.16. *Пусть формула A замкнута. Тогда теория $T \cup \{A\}$ противоречива $\iff T \vdash \neg A$.*

Следующая теорема называется *теоремой о корректности исчисления предикатов*.

Теорема 4.17. *Если $M \vDash T$ и $T \vdash B(b_1, \ldots, b_n)$, то $M \vDash B[b_1/x_1, \ldots, b_n/x_n]$ для любых $x_1, \ldots, x_n \in M$.*

Доказательство. Индукция по длине вывода формулы B в T. Если $B \in T$, то $M \vDash B$, поскольку $M \vDash T$.

Рассмотрим случай, когда B — логическая аксиома вида A3, то есть $B = (A[a/t] \to \exists x A[a/x])$. Можно считать B (после подстановки констант вместо свободных переменных) замкнутой формулой, а t — замкнутым термом сигнатуры $\Sigma(M)$.

Допустим $M \vDash A[a/t]$. Пусть $c \rightleftharpoons t_M$, тогда $M \vDash A[a/\underline{c}]$, а значит и $M \vDash \exists x\, A[a/x]$ (см. определение истинности формул). Тем самым доказано, что $M \vDash A[a/t] \to \exists x A[a/x]$.

Аксиомы вида A3 рассматриваются аналогично.

Рассмотрим случай, когда B — аксиома A1, то есть B имеет вид $B_0[P_1/C_1, \ldots, P_n/C_n]$, где $B_0(P_1, \ldots, P_n)$ — аксиома исчисления высказываний. Считаем $C_1, \ldots, C_n$ замкнутыми формулами сигнатуры $\Sigma(M)$ и докажем $M \vDash B$.

Допустим $M \nvDash B$. Рассмотрим оценку f пропозициональных переменных $P_1, \ldots, P_n$ такую, что

$$f(P_i) = \text{И} \overset{\text{def}}{\iff} M \vDash C_i.$$

Тогда для любой пропозициональной формулы $D(P_1, \ldots, P_n)$ индукцией по построению D легко доказывается эквивалентность

$$f(D) = \text{И} \iff M \vDash D[P_1/C_1, \ldots, P_n/C_n].$$

В частности, для $D = B_0$ получаем $f(B_0) = \text{Л}$, поскольку $M \nvDash B$. Это противоречит предположению о том, что B_0 — тавтология.

Рассмотрим теперь случай, когда B получена по одному из правил вывода R1–R3.

Если B получена из A и $A \to B$ по правилу modus ponens, мы имеем по предположению индукции $M \vDash A$ и $M \vDash A \to B$ (считая A и B замкнутыми формулами сигнатуры $\Sigma(M)$). Тогда $M \vDash B$ в силу определения истинности для импликации.

Допустим $B = (A \to \forall x C[a/x])$ получена из $A \to C$ по правилу R2. Считаем B замкнутой формулой в сигнатуре $\Sigma(M)$. По предположению индукции $M \vDash A \to C[a/\underline{c}]$ для всех $c \in M$. Если $M \nvDash A$, то очевидно $M \vDash A \to \forall x\, C[a/x]$. Иначе $M \vDash C[a/\underline{c}]$ для всех $c \in M$ и тем самым $M \vDash \forall x\, C[a/x]$. Правило R3 рассматривается аналогично. $\boxtimes$

Следствие 4.18. *Если $\vdash A$, то A общезначима.*

Теорема о корректности исчисления предикатов играет роль при доказательстве непротиворечивости теорий и доказательстве независимости утверждений относительно данной теории.

Следствие 4.19. *Если теория T имеет модель, то T непротиворечива.*

Пример 4.20. Следующие теории непротиворечивы:

- исчисление предикатов данной сигнатуры (с пустым множеством нелогических аксиом);
- теория отношения эквивалентности;
- теория групп;
- элементарная геометрия.

Для доказательства независимости утверждений полезно следующее следствие теоремы о корректности.

Следствие 4.21. *Если существует модель M теории T для которой $M \nvDash A$, то $T \nvdash A$.*

Пример 4.22. Модель Пуанкаре $\mathbf{H}^2$ показывает, что аксиома Евклида не выводима из остальных аксиом элементарной геометрии. Модель $\mathbb{R}^2$ показывает, что отрицание аксиомы Евклида не выводимо из остальных аксиом.

5 Теоремы о полноте и компактности

5.1 Теорема Гёделя о полноте

Теорема 5.1. *1. Всякая непротиворечивая теория T выполнима, то есть имеет модель $M \vDash T$.*

2. Если $T \nvdash A$, то найдётся модель $M \vDash T$ для которой $M \nvDash A$.

3. $T \vDash A$ влечёт $T \vdash A$.

Мы не доказываем теорему Гёделя о полноте, но установим равносильность этих утверждений.

$(1 \Rightarrow 2)$: Если $T \nvdash A$, то по теореме о дедукции $T \cup \{\neg A\}$ непротиворечива. Следовательно, $T \cup \{\neg A\}$ имеет модель M.

$(2 \Rightarrow 3)$: очевидно.

$(3 \Rightarrow 1)$: Возьмём $A = (B \wedge \neg B)$. Тогда $T \nvdash A$, следовательно $T \not\models A$ и у теории T должна быть модель (опровергающая A).

5.2 Теорема Мальцева о компактности

Теорема 5.2. *1. Теория T выполнима $\iff$ любое конечное подмножество $T_0 \subseteq T$ выполнимо.*

2. $T \vDash A \iff$ существует такое конечное множество $T_0 \subseteq T$, что $T_0 \vDash A$.

Теорема о компактности вытекает из теоремы о полноте и свойства компактности отношения выводимости. Она является полезным инструментом при построении моделей теорий первого порядка. В качестве важного примера мы рассмотрим нестандартные модели арифметики.

5.3 Нестандартные модели арифметики

Пример 5.3. Пусть $(\mathbb{N}; =, S, +, \cdot, 0)$ — стандартная модель арифметики и $Th(\mathbb{N})$ есть множество *всех* истинных в $\mathbb{N}$ предложений.

Добавим к сигнатуре новую константу c и рассмотрим теорию

$$T \rightleftharpoons Th(\mathbb{N}) \cup \{\neg c = 0, \neg c = S0, \neg c = SS0, \dots\}.$$

Терм $\bar{n} \rightleftharpoons SS \dots S0$ (n раз) называем *нумералом*. Нумералы служат именами натуральных чисел.

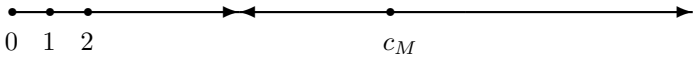
Утверждение 5.4. *Каждая конечная подтеория $T_0 \subseteq T$ выполнима.*

Доказательство. T_0 содержит лишь конечное число аксиом вида $c \neq \bar{n}_1$, …, $c \neq \bar{n}_k$. Интерпретируем константу c в стандартной модели как любое число $m > n_1, \dots, n_k$. $\boxtimes$

По теореме о компактности существует (нормальная) модель $M \vDash T$. Модель M обладает следующими свойствами:

- $\mathbb{N}$ изоморфна начальному сегменту M; вложение $\mathbb{N} \to M$ задаётся функцией $\varphi : n \longmapsto \bar{n}_M$.

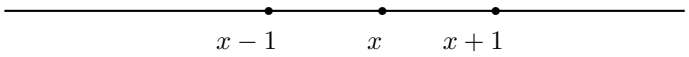
- $M \vDash Th(\mathbb{N})$;
- $M \ncong \mathbb{N}$, в частности $c_M \in M$ есть «бесконечно большое число», поскольку c_M отлично от всякого $n \in \mathbb{N}$.



Формула $a < b \rightleftharpoons \exists x (x \neq 0 \wedge a + x = b)$ определяет порядок в $\mathbb{N}$. Для данной формулы в $\mathbb{N}$ выполнены аксиомы строгого линейного порядка и следующие предложения:

- $\forall x\ (0 < x \vee 0 = x)$;
- $\forall x \exists y\ (x < y \wedge \forall z\ (z < y \to z = x \vee z < x))$;
- $\forall y\ (y \neq 0 \to \exists x\ (x < y \wedge \forall z\ (z < y \to z = x \vee z < x)))$.

Следовательно, те же аксиомы выполнены и в M. Поэтому предикат $<_M$ на M представляет собой строгий линейный порядок с наименьшим элементом 0. При этом каждый элемент имеет последователя, и каждый элемент, кроме 0, имеет непосредственного предшественника.



Определение 5.5. Элементы $x, y \in M$ *близки*, если для некоторого $n \in \mathbb{N}$ выполнено $y = SS \ldots S(x)$ или $x = SS \ldots S(y)$ (n символов S).

Классы эквивалентности по отношению близости называем *галактиками*.

Утверждение 5.6. *Если G — галактика в M, $G \neq \mathbb{N}$, то порядок $(G, <_M)$ изоморфен $(\mathbb{Z}, <)$.*

Пусть $\mathcal{G}$ есть множество всех галактик в M. Определим $G_1 <_M G_2$, если для любых $x \in G_1$, $y \in G_2$ $x <_M y$.

Теорема 5.7. *Порядок $(\mathcal{G}, <_M)$ есть плотный порядок без наибольшего элемента, наименьшим элементом которого является $\mathbb{N}$.*

Доказательство. Если $G_1 < G_2$, возьмём чётные $x_1 \in G_1$ и $x_2 \in G_2$ и рассмотрим $y = (x_1 + x_2)/2$ (функция $g(x) = x/2$ определима в $\mathbb{N}$, а значит и в M).

Если $y \in G_1$, то $(x_1 + x_2)/2 = x + \bar{n}$ для некоторого $n \in \mathbb{N}$. Тогда $2x_1 + 2\bar{n} = x_1 + x_2$, откуда $x_1 + 2\bar{n} = x_2$, то есть $x_2 \in G_1$.

Аналогично показываем $y \notin G_2$.

Доказательство отсутствия наибольшего элемента оставляем в качестве упражнения. $\boxtimes$

Упражнение 5.8. *Доказать, что для любой галактики G_1 в M найдётся галактика G_2 такая, что $G_1 < G_2$.*

5.4 Элементарная эквивалентность

Пусть St_Σ — множество предложений сигнатуры Σ

Определение 5.9. *Элементарная теория модели* M есть множество $Th(M) \rightleftharpoons \{A \in \mathrm{St}_\Sigma : M \vDash A\}$.

Определение 5.10. Модели M и N сигнатуры Σ *элементарно эквивалентны* ($M \equiv N$), если в M и в N истинны одни и те же предложения Σ, т.е. если $Th(M) \equiv Th(N)$.

Утверждение 5.11. *$M \cong N$ влечёт $M \equiv N$. Обратное, вообще говоря, неверно.*

5.5 Подмодели

Определение 5.12. $(N;\Sigma)$ есть *подмодель* модели $(M;\Sigma)$, если $N \subseteq M$ и для всех $P \in \mathrm{Pred}_\Sigma$, $f \in \mathrm{Func}_\Sigma$, $c \in \mathrm{Const}_\Sigma$ имеем $P_N = P_M \restriction N$, $c_M \in N$, N замкнуто относительно f_M и $f_N = f_M \restriction N$.

Пример 5.13. Если $(G;=,\cdot,1,(\cdot)^{-1})$ — группа, то подмодели G суть подгруппы группы G. Если же G рассматривается как модель $(G;=,\cdot,1)$, то её подмоделями будут подполугруппы с единицей группы G.

5.6 Элементарные подмодели

Определение 5.14. Подмодель $(N;\Sigma)$ модели $(M;\Sigma)$ *элементарна* (обозначение $N \preccurlyeq M$), если для всех $A \in \mathrm{Fm}_\Sigma$

$$\forall \vec{x} \in N\ (N \vDash A[\vec{x}] \iff M \vDash A[\vec{x}]).$$

Утверждение 5.15. *$N \preccurlyeq M$ влечёт $N \equiv M$.*

Пример 5.16. Если M — модель $Th(\mathbb{N})$, то $\mathbb{N}$ изоморфна некоторой элементарной подмодели $N \preccurlyeq M$.

Доказательство. Вложение $\varphi : \mathbb{N} \to M$ действует по формуле $\varphi(n) \rightleftharpoons (\overline{n})_M$. Докажем, что $N \rightleftharpoons \varphi(\mathbb{N})$ есть подмодель M.

Ясно, что подмножество $\varphi(\mathbb{N}) \subseteq M$ замкнуто относительно функции S_M и $S_M(\varphi(n)) = \varphi(S_{\mathbb{N}}(n))$. Рассмотрим теперь функцию сложения $+$. Надо установить, что $\varphi(\mathbb{N})$ замкнуто относительно $+_M$ и

$$\varphi(n) +_M \varphi(m) = \varphi(n+m).$$

Это вытекает из равенства $\overline{n} + \overline{m} = \overline{n+m}$, которое является истинным в $\mathbb{N}$ и потому входит в $Th(\mathbb{N})$. Функция умножения рассматривается аналогично. Таким образом, $\varphi : \mathbb{N} \to N$ — изоморфизм.

Элементарность вложения следует из цепочки эквивалентностей, верной для любых $n_1, \ldots, n_k \in \mathbb{N}$:

$$N \vDash A[\varphi(n_1), \ldots, \varphi(n_k)] \iff \mathbb{N} \vDash A[n_1, \ldots, n_k] \iff \mathbb{N} \vDash A(\overline{n_1}, \ldots, \overline{n_k})$$
$$\iff M \vDash A(\overline{n_1}, \ldots, \overline{n_k}) \iff M \vDash A[\varphi(n_1), \ldots, \varphi(n_k)].$$

Третья эквивалентность следует из $M \vDash Th(\mathbb{N})$. $\boxtimes$

5.7 Теорема Лёвенгейма–Сколема

Пусть Σ — счётная сигнатура.

Теорема 5.17. *Всякая модель $(M; \Sigma)$ имеет (конечную или) счётную элементарную подмодель.*

Доказательство. Построим последовательность счётных подмножеств модели M

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \ldots$$

следующим образом:

- N_0 — любое непустое счётное подмножество M.
- Для каждой формулы $A[a, \vec{b}]$ и набора $\vec{y} \in N_k$, если $M \vDash \exists v A[v, \vec{y}]$ выберем $x \in M$ такой, что $M \vDash A[x, \vec{y}]$. Добавим все такие x к N_k и получим N_{k+1}.

Положим $N \rightleftharpoons \bigcup_{k \geq 0} N_k$. По построению множества N получаем следующее свойство.

Лемма 5.18. *Для любой формулы A и всех $\vec{y} \in N$*

$$M \vDash \exists v A[v, \vec{y}] \iff \exists x \in N \quad M \vDash A[x, \vec{y}].$$

Лемма 5.19. *N есть подмодель M.*

Доказательство. Пусть $\vec{x} \in N$, $f \in \mathrm{Func}_\Sigma$. Поскольку $M \vDash \exists v\, f(\vec{x}) = v$, имеем $y \in N$ такой, что $M \vDash f(\vec{x}) = y$, т.е. $f_M(\vec{x}) \in N$. $\boxtimes$

Индукцией по построению A теперь покажем

$$\forall \vec{y} \in N \; (N \vDash A[\vec{y}] \iff M \vDash A[\vec{y}]).$$

- Для атомарных формул A следует из того, что N — подмодель M.
- Для $A = \neg B,\ B \wedge C,\ B \vee C$ вытекает из предположения индукции.
- Допустим $A = \exists v B[a/v]$. Тогда

$$M \vDash \exists v B[a/v, \vec{y}] \iff \exists x \in N \quad M \vDash B[x, \vec{y}]$$
$$\iff \exists x \in N \quad N \vDash B[x, \vec{y}] \iff N \vDash \exists v B[a/v, \vec{y}].$$

⊠

Следствие 5.20. *Всякая непротиворечивая теория в счётной сигнатуре имеет (конечную или) счётную модель.*

Следствие 5.21. (i) *Существуют счётные модели $Th(\mathbb{R})$ и $Th(\mathbb{C})$.*

(ii) *Существует счётная модель элементарной геометрии.*

(iii) *Если теория множеств ZFC непротиворечива, то существует и счётная модель ZFC.*

Следующее утверждение, несколько обобщающее предыдущую теорему, иногда называют теоремой Лёвенгейма–Сколема о понижении мощности.[4]

Теорема 5.22. *Пусть $(M;\Sigma)$ — бесконечная модель в счётной сигнатуре и $\lambda \le |M|$ — бесконечная мощность. Тогда найдётся подмодель $N \preccurlyeq M$ такая, что $|N| = \lambda$.*

Доказательство. Та же конструкция, но начинаем с любого подмножества $N_0 \subseteq M$ мощности λ. Поскольку сигнатура счётна, нетрудно показать по индукции, что все множества N_k, так же как и их объединение N, имеют мощность λ. ⊠

5.8 Теорема Лёвенгейма–Сколема о повышении мощности

Пусть Σ — счётная сигнатура с равенством.

Теорема 5.23. *Для любой бесконечной модели $(M;\Sigma)$ и мощности $\lambda \ge |M|$ найдётся модель $(N;\Sigma)$ такая, что $M \preccurlyeq N$ и $|N| = \lambda$.*

Доказательство. Возьмём $X \supseteq M$, $|X| = \lambda$. Рассмотрим сигнатуру $\Sigma_X \rightleftharpoons \Sigma \cup \{\underline{c} : c \in X\}$ и теорию

$$T := Th(M;\Sigma_X) \cup \{\underline{c} \ne \underline{d} : c, d \in X, c \ne d\}.$$

Каждая конечное подмножество теории T совместно. По теореме о компактности T имеет нормальную модель N. Но функция $\varphi : c \longmapsto (\underline{c})_N$ инъективна в силу аксиом T, следовательно $|N| \ge |X| = \lambda$. Т.к. $N \vDash Th(M;\Sigma_X)$, то $\varphi(M)$ есть подмодель N изоморфная M и $\varphi(M) \preccurlyeq N$. Это рассуждение совершенно аналогично уже разобранному нами более детально примеру 5.16. ⊠

Следствие 5.24. *Если теория T имеет бесконечную модель, то T имеет модели любой бесконечной мощности.*

Следствие 5.25. *Множество $Th(\mathbb{N})$ всех предложений, истинных в стандартной модели арифметики, имеет модели любой бесконечной мощности.*

[4]Это предложение предполагает знакомство с понятием мощности множества и не входит в обязательную программу.

5.9 Полные теории

Определение 5.26. Теория T *полна*, если

- T непротиворечива;
- Для любого предложения A в языке T $T \vdash A$ или $T \vdash \neg A$.

Предложение 5.27. *Для любой модели M теория $Th(M)$ полна.*

Доказательство. Действительно, $Th(M)$ непротиворечива, поскольку имеет модель M. Так как любое предложение A либо истинно, либо ложно в M, получаем, что $A \in Th(M)$ или $\neg A \in Th(M)$. $\boxtimes$

Предложение 5.28. *Если T полна и $M \vDash T$, то $T \equiv Th(M)$.*

Доказательство. Условие $T \equiv Th(M)$ означает, что множество теорем T совпадает с $Th(M)$. Поскольку $M \vDash T$ имеем $Th(M) \vdash T$. Если $A \in Th(M)$ и $T \nvdash A$, то в силу полноты $T \vdash \neg A$. Отсюда $M \vDash \neg A$ и $M \nvDash A$, что противоречит $A \in Th(M)$. $\boxtimes$

Теорема 5.29 (Линденбаум). *Всякая непротиворечивая теория имеет полное расширение.*

Эта теорема доказывается совершенно аналогично теореме Линденбаума для логики высказываний.

5.10 Аксиоматизируемость

Определение 5.30. Теория T *эффективно аксиоматизируема*, если существует алгоритм, распознающий аксиомы T.

Замечание 5.31. В следующей главе мы дадим точное понятие алгоритма. Сейчас мы пользуемся неформальным представлением об алгоритмах.

Определение 5.32. Теория T *разрешима*, если существует алгоритм, распознающий теоремы T.

Теорема 5.33. *Если T полна и эффективно аксиоматизируема, то T разрешима.*

Доказательство. Пусть дано предложение A. Перебираем все возможные выводы в T до тех пор, пока не встретим доказательство A или доказательство $\neg A$. Полнота гарантирует, что одно из этих двух событий произойдёт. $\boxtimes$

5.11 Примеры полных эффективно аксиоматизируемых теорий

Элементарная геометрия. Для случая размерности два эта теория задаётся аксиомами Тарского (G1–G11) и эквивалентна $Th(\mathbb{R}^2; =, \cong, B)$.

Теория ACF_0 алгебраически замкнутых полей характеристики 0. Эта теория эквивалентна $Th(\mathbb{C}; =, +, \cdot, 0, 1)$ и задаётся обычными аксиомами поля вместе с двумя бесконечными сериями аксиом:

C_p: $0 \neq (1 + 1 + \cdots + 1)$ (p раз), для каждого простого p.

A_n: $\forall y_0 \ldots y_{n-1} \exists x \, (y_0 + y_1 x + \ldots y_{n-1} x^{n-1} + x^n = 0)$, для каждого $n \geq 1$.

Первая серия аксиом выражает тот факт, что характеристика поля равна нулю. Вторая серия аксиом выражает алгебраическую замкнутость.

Теория RCF вещественно замкнутых упорядоченных полей. Эта теория эквивалентна $Th(\mathbb{R}; =, \leq, +, \cdot, 0, 1)$ и задаётся аксиомами поля, аксиомами линейного порядка для отношения $\leq$, а также следующими формулами:

1. $\forall x, y, z \, (x \leq y \wedge 0 \leq z \to xz \leq yz)$;
2. $\forall x, y, z \, (x \leq y \to x + z \leq y + z)$;
3. $\forall x \exists y \, (0 \leq x \to y^2 = x)$;
4. A_n, для каждого нечётного $n \in \mathbb{N}$.

Как и выше, аксиома A_n выражает тот факт, что произвольный полином степени n над данным полем имеет корень.

Теория DLO плотных линейных порядков без первого и последнего элементов. Эта теория эквивалентна $Th(\mathbb{Q}; =, <)$ и задаётся аксиомами линейного порядка вместе с двумя дополнительными аксиомами:

1. $\forall x, y \, (x < y \to \exists z \, (x < z \wedge z < y))$;
2. $\forall x \exists y, z \, (z < x \wedge x < y)$.

5.12 Примеры неполных теорий

Примеры неполных теорий легко получить, удаляя аксиомы из известных теорий (не меняя при этом сигнатуры).

Пример 5.34. Рассмотрим сигнатуру с бинарными предикатными символами $=, <$. Неполными теориями в этой сигнатуре являются:

- пустая теория;
- чистая теория равенства;

- теория частичных порядков;
- теория линейных порядков;
- теория плотных линейных порядков.

Все указанные теории содержатся в полной теории DLO плотных линейных порядков без первого и последнего элементов. Указав соответствующие модели, нетрудно убедиться в том, что все эти теории попарно различны и, тем самым, неполны (упражнение).

Пример 5.35. Рассмотрим сигнатуру элементарной геометрии Тарского: $=$, B, $\cong$. Неполными теориями в этой сигнатуре являются, например,

- «безразмерная» геометрия, получаемая выбрасыванием аксиом размерности G8 и G9.
- *абсолютная геометрия*, получаемая удалением аксиомы Евклида G10.

Другой класс составляют теории, сформулированные с целью формализации всей математики в целом или достаточно богатых её частей. Для таких теорий нет — и не должно быть — очевидных принципов, «пропущенных» или «забытых» при выписывании списка их аксиом. Наиболее важные, с точки зрения оснований математики, теории такого универсального типа — это арифметика Пеано и теория множеств Цермело–Френкеля (с аксиомой выбора).

Арифметика Пеано PA. Эта теория формализует математику конечного, то есть ту часть математики, для развития которой не требуется использование бесконечных множеств. Арифметика Пеано основана на аксиомах для натуральных чисел в сигнатуре $=$, 0, S, $+$, $\cdot$, приводимых ниже.

Аксиомы арифметики Пеано:

1. аксиомы равенства для S, $+$, $\cdot$;
2. $\neg S(a) = 0, \quad S(a) = S(b) \to a = b$,
3. $a + 0 = a, \quad a + S(b) = S(a + b)$,
4. $a \cdot 0 = a, \quad a \cdot S(b) = a \cdot b + a$,
5. (Схема аксиом индукции)
   $A[a/0] \wedge \forall x\,(A[a/x] \to A[a/S(x)]) \to \forall x\,A[a/x]$,
   для любой формулы A.

Теория множеств Цермело–Френкеля (с аксиомой выбора) ZFC. Эта теория формализует всю «обычную» математику. Она основана на аксиомах для множеств и отношения принадлежности $\in$. В этом курсе мы не будем рассматривать аксиомы теории множеств.

Глубокий факт неполноты таких теорий как формальная арифметика и теория множеств, и даже более сильный факт их, в определённом смысле, *непополняемости*, составляет содержание знаменитых теорем Гёделя о неполноте. Здесь мы приведём первую теорему Гёделя о неполноте в формулировке Россера. Доказательству этой теоремы посвящена отдельная глава курса.

Пусть язык теории T содержит арифметический.

Теорема 5.36. *Если T содержит* PA*, непротиворечива и эффективно аксиоматизируема, то T неполна.*

Следствие 5.37. (i) PA *неполна.*

(ii) ZFC *неполна при условии её непротиворечивости.*

Замечание 5.38. Формально говоря, язык теории множеств не содержит арифметический. Однако, множество натуральных чисел вместе с операциями сигнатуры арифметики можно определить в языке теории множеств, что обеспечивает применимость теоремы Гёделя к ZFC. Определения такого рода называются *(относительными) интерпретациями*. Они будут рассмотрены в следующем разделе.

6 Интерпретации

Определение 6.1. Модель $(M;\Omega)$ *интерпретируема в* $(N;\Sigma)$, если её носитель M и все предикаты, функции и константы сигнатуры Ω на M определимы в N.

Более явно, это определение можно выразить с помощью понятия перевода.

Определение 6.2. *Перевод* I сигнатуры Ω в сигнатуру Σ задаётся:

- формулой $D_I(a) \in \mathrm{Fm}_\Sigma$, определяющей носитель M;
- сопоставляет каждому символу Ω формулу сигнатуры Σ соответствующей валентности:

$$\begin{aligned} P &\longmapsto P_I(a_1,\dots,a_n) \\ f &\longmapsto F_I(a_1,\dots,a_n,b) \\ c &\longmapsto C_I(a) \end{aligned}$$

Для данного перевода I и модели $(N;\Sigma)$ положим

$$M_I \rightleftharpoons \{x \in N : N \vDash D_I[x]\}.$$

Определение 6.3. Перевод I есть *интерпретация* M *в* N, если

$$(M_I; P_I, f_I, c_I) \cong (M; P, f, c),$$

где P_I, f_I и c_I — предикат, функция и константа на M_I, определимые в N формулами P_I, F_I и C_I, соответственно. (Для простоты мы рассматриваем сигнатуру с единственным предикатным, функциональным и константным символами.)

Замечание 6.4. Для нормальной модели M условие изоморфизма

$$(M_I; =_I) \cong (M; =)$$

говорит о том, что $=_I$ есть отношение равенства на множестве M_I, т.е. можно считать, что $=_I$ есть $=$.

Пример 6.5. $(\mathbb{Z}; <)$ интерпретируема в $(\mathbb{N}; +, =)$.

Интерпретируем чётные натуральные числа как отрицательные, а нечётные как положительные. Чётность числа a выражается формулой $E(a) \overset{\text{def}}{\iff} (\exists x\ x+x=a)$, а порядок на натуральных числах формулой $a<b \overset{\text{def}}{\iff} (\exists x\ b = a + x \wedge \neg(x+x=x))$. Тогда перевод I можно задать формулами

$$\begin{array}{rcl} D_I(a) & \overset{\text{def}}{\iff} & (a=a) \\ a <_I b & \overset{\text{def}}{\iff} & (E(a) \wedge E(b) \wedge b < a) \vee \\ & & (E(a) \wedge \neg E(b)) \vee \\ & & (\neg E(b) \wedge \neg E(a) \wedge a < b). \end{array}$$

На практике, требование определимости с точностью до изоморфизма является слишком жёстким и малоупотребительным. Обобщить определение интерпретации M в N можно несколькими естественными способами (или всеми сразу):

- Допускается интерпретация одного объекта из M набором объектов из N (*многомерные интерпретации*).
- Рассматривается *мягкое* (или *неабсолютное*) понятие равенства.
- Допускаются параметры (*параметрические интерпретации*).

Мы разберём эти условия по очереди. Окончательное общее определение интерпретации будет использовать все три условия.

6.1 Многомерные интерпретации

Элементу $a \in M$ сопоставляем набор $\vec{a} = (a_1, \ldots, a_n) \in N^n$ элементов N.

В этом случае перевод I задаётся формулой $D_I(\vec{a})$ и переводом символов Ω следующего вида:

$$\begin{array}{rcl} P & \longmapsto & P_I(\vec{a}_1, \ldots, \vec{a}_n) \\ f & \longmapsto & F_I(\vec{a}_1, \ldots, \vec{a}_n, \vec{b}) \\ c & \longmapsto & C_I(\vec{a}) \end{array}$$

Положим

$$M_I \rightleftharpoons \{\vec{x} \in N^n : N \vDash D_I[\vec{x}]\}.$$

Как обычно, I — интерпретация, если

$$(M_I; P_I, f_I, c_I) \cong (M; P, f, c),$$

а P_I, f_I и c_I — предикат, функция и константа на M_I, определимые в N формулами P_I, F_I и C_I, соответственно.

Пример 6.6. Модель $(\mathbb{R}^2; =, B, \cong)$ интерпретируема в $(\mathbb{R}; =, +, \cdot, 0, 1)$.

Эта интерпретация — классическое сведение элементарной геометрии к теории действительных чисел, восходящее к Декарту.

Сначала определим на множестве $\mathbb{R}$ отношение порядка и функцию разности:

$$\begin{array}{rcl} a \leq b & \overset{\text{def}}{\Longleftrightarrow} & (\exists z\, a + z \cdot z = b) \\ a - b = c & \overset{\text{def}}{\Longleftrightarrow} & (c + b = a). \end{array}$$

После этого перевод можно задать формулами

$$\begin{array}{rcl} D_I(a_1, a_2) & \overset{\text{def}}{\Longleftrightarrow} & (a_1 = a_1 \wedge a_2 = a_2) \\ B_I(\vec{a}, \vec{b}, \vec{c}) & \overset{\text{def}}{\Longleftrightarrow} & \exists \lambda, \mu\, (0 \leq \lambda \wedge 0 \leq \mu \wedge \lambda + \mu = 1 \wedge \\ & & \qquad \wedge\, b_1 = \lambda a_1 + \mu c_1 \wedge b_2 = \lambda a_2 + \mu c_2) \\ \vec{a}\vec{b} \cong_I \vec{c}\vec{d} & \overset{\text{def}}{\Longleftrightarrow} & (a_1 - b_1)^2 + (a_2 - b_2)^2 = (c_1 - d_1)^2 + (c_2 - d_2)^2. \end{array}$$

6.2 Мягкое равенство

Определение 6.7. Пусть $(M; =, P, f)$ — нормальная модель, I — перевод. Вместо изоморфизма $(M_I; =_I, P_I, f_I) \cong M$ требуем:

- Формула $\vec{a} =_I \vec{b}$ удовлетворяет в N аксиомам равенства для сигнатуры Ω, в частности $=_I$ есть отношение эквивалентности и

  $N \vDash \forall \vec{x}, \vec{y}\, (D_I(\vec{x}) \wedge D_I(\vec{y}) \wedge \vec{x} =_I \vec{y} \to (P_I(\vec{x}) \leftrightarrow P_I(\vec{y})))$;

  и аналогично для F_I.

- $(M;=,P,f) \cong (M_I;=_I,P_I,f_I)/=_I$.

Пример 6.8. $(\mathbb{Z};=,+,\cdot,0,1)$ интерпретируема в $(\mathbb{N};=,S,+,\cdot)$.

Число $z \in \mathbb{Z}$ представляем парой $(m,n) \in \mathbb{N}^2$, где $z = m - n$.

$$\begin{aligned}
D_I(a_1,a_2) &\overset{\text{def}}{\iff} (a_1 = a_1 \wedge a_2 = a_2)\\
(a_1,a_2) =_I (b_1,b_2) &\overset{\text{def}}{\iff} (a_1 + b_2 = a_2 + b_1)\\
(a_1,a_2) +_I (b_1,b_2) = (c_1,c_2) &\overset{\text{def}}{\iff} (c_1 = a_1 + b_1 \wedge c_2 = a_2 + b_2)\\
(a_1,a_2) \cdot_I (b_1,b_2) = (c_1,c_2) &\overset{\text{def}}{\iff} (c_1 = a_1b_1 + a_2b_2 \wedge c_2 = a_1b_2 + a_2b_1)\\
0_I(a_1,a_2) &\overset{\text{def}}{\iff} (a_1 = a_2)\\
1_I(a_1,a_2) &\overset{\text{def}}{\iff} (a_1 = S(a_2))
\end{aligned}$$

6.3 Интерпретации с параметрами

Здесь мы даём наиболее общее определение интерпретации. *Перевод* I задаётся формулой $D_I(\vec{a},\vec{p})$ со свободными переменными $\vec{p}$ и переводами символов Ω вида:

$$\begin{aligned}
P &\longmapsto P_I(\vec{a}_1,\ldots,\vec{a}_n,\vec{p})\\
f &\longmapsto F_I(\vec{a}_1,\ldots,\vec{a}_n,\vec{b},\vec{p})\\
c &\longmapsto C_I(\vec{a},\vec{p})
\end{aligned}$$

Определение 6.9. Перевод I есть *интерпретация* M *в* N, если для некоторого набора констант $\vec{c} \in N$:

- $=_I(\vec{a},\vec{b},\vec{c})$ удовлетворяет в N аксиомам равенства для сигнатуры Ω;
- $(M_I;P_I,f_I)/=_I$ изоморфна M, где $M_I = \{\vec{x} \in N^n : N \vDash D_I[\vec{x},\vec{c}]\}$, а P_I и f_I — предикат и функция на M_I определимые в $(N;\vec{c})$ формулами P_I и F_I, соответственно.

Определение 6.10. Набор констант $\vec{c}$, для которого выполнены эти условия, называется *допустимым* для данной интерпретации I.

Определение 6.11. Интерпретация I имеет *определимые параметры*, если для некоторой формулы $\mathrm{Par}_I(\vec{p})$ сигнатуры Σ

- $N \vDash \exists\vec{x}\,\mathrm{Par}_I(\vec{x})$;
- если $N \vDash \mathrm{Par}_I[\vec{c}]$, то набор $\vec{c}$ допустим для I.

Пример 6.12. $(\mathbb{R};=,+,\cdot,0,1)$ интерпретируема в $(\mathbb{R}^2;=,B,\cong)$.

Параметры p_0, p_1 — две различные точки. Действительные числа интерпретируем точками прямой p_0p_1.

$$D_I(a) \overset{\text{def}}{\iff} (a \in p_0p_1),\ 0_I \rightleftharpoons p_0,\ 1_I \rightleftharpoons p_1$$

$$a +_I b = c \overset{\text{def}}{\iff} (Bp_0ac \wedge Bp_0bc \wedge p_0b \cong ac) \vee (Bap_0b \wedge Bacb \wedge ap_0 \cong bc)$$

$$a \cdot_I b = c \overset{\text{def}}{\iff} \exists u, v\,(Bp_0uv \wedge p_0u \cong p_0b \wedge p_1u \| av \wedge p_0v \cong p_0c) \wedge \\ \wedge (Bap_0b \leftrightarrow Bcp_0p_1).$$

Для определения произведения действительных чисел мы используем теорему Фалеса. Первый конъюнктивный член утверждает $|a| \cdot |b| = |c|$, а второй учитывает знак произведения (знак отрицательный, если и только если a и b лежат по разные стороны от p_0).

Упражнение 6.13. *Определить интерпретации:*

- $(\mathbb{C}; =, +, \cdot, 0, 1)$ *в поле* $\mathbb{R}$.
- $(\mathbb{Q}; =, +, \cdot, 0, 1)$ *в стандартной модели* $\mathbb{N}$.
- *Доказать, что поле* $\mathbb{R}$ *не интерпретируемо в поле* $\mathbb{Q}$.

6.4 Перевод формул при интерпретации

Нам будет удобно иметь дело с формулами некоторого упрощённого вида.

Определение 6.14. Формула A *упрощённая*, если всякая атомарная подформула, входящая в A, имеет вид $P(a_1, \ldots, a_n)$ или $f(a_1, \ldots, a_n) = b$, где $a_1, \ldots, a_n, b$ — переменные, а P и f — предикатный и функциональный символы сигнатуры.

Лемма 6.15. *Всякая формула A логически эквивалентна некоторой упрощённой формуле A'.*

Доказательство. Поскольку $P(t) \equiv \exists x\,(P(x) \wedge t = x)$ достаточно доказать эту лемму для случая, когда A — атомарная формула вида $t(\vec{a}) = b$ для некоторого терма t. Рассуждаем индукцией по построению t. Если t — переменная или функциональнй символ, то мы уже имеем требуемое представление (символ равенства входит в сигнатуру).

Иначе $t(\vec{a})$ имеет вид $f(t_1(\vec{a}), \ldots, t_n(\vec{a}))$, где t_i — термы меньшей глубины. Тогда имеем

$$t(\vec{a}) = b \equiv \exists x_1 \ldots x_n\,(f(x_1, \ldots, x_n) = b \wedge t_1(\vec{a}) = x_1 \wedge \cdots \wedge t_n(\vec{a}) = x_n).$$

Применяя предположение индукции к термам t_1,…,t_n и теорему о замене подформулы на эквивалентную получаем требуемое. ⊠

Определение 6.16. Пусть I — перевод сигнатуры Ω в Σ. Перевод A^I упрощённой формулы $A \in \mathrm{Fm}_\Omega$ определим индуктивно:

- $P(a,b)^I \rightleftharpoons P_I(\vec{a},\vec{b},\vec{p})$, $(f(a)=b)^I \rightleftharpoons F_I(\vec{a},\vec{b},\vec{p})$,
- $(\neg A)^I \rightleftharpoons \neg A^I$, $(A \wedge B)^I \rightleftharpoons (A^I \wedge B^I)$,
- $(\forall x A[a/x])^I \rightleftharpoons \forall \vec{x}\,(D_I(\vec{x},\vec{p}) \to A^I[\vec{a}/\vec{x}])$,
- $(\exists x A[a/x])^I \rightleftharpoons \exists \vec{x}\,(D_I(\vec{x},\vec{p}) \wedge A^I[\vec{a}/\vec{x}])$.

Переводом произвольной формулы A сигнатуры Ω считаем перевод эквивалентной ей упрощённой формулы. Этот перевод определён однозначно с точностью до логической эквивалентности.

Пусть $\vec{x}_I$ означает элемент модели M_I, соответствующий $x \in M$.

Теорема 6.17. *Для любой A в языке M, любых $\vec{x} \in M$ и допустимых $\vec{c} \in N$*

$$M \vDash A[\vec{x}] \iff N \vDash A^I[\vec{x}_I, \vec{c}].$$

Доказательство. Индукция по построению A. ⊠

Следствие 6.18. *Если M интерпретируема в N с определимыми параметрами и $Th(N)$ разрешима, то такова и $Th(M)$.*

Доказательство. Для данного предложения A в языке M имеем

$$M \vDash A \iff N \vDash \forall \vec{x}\,(\mathrm{Par}_I(\vec{x}) \to A^I(\vec{x})).$$

Таким образом, для проверки выполнимости формулы A в N достаточно проверить выполнимость $\forall \vec{x}\,(\mathrm{Par}_I(\vec{x}) \to A^I(\vec{x}))$ в модели N. ⊠

Следствие 6.19. *Разрешимость элементарной геометрии равносильна разрешимости $Th(\mathbb{R})$.*

6.5 Интерпретируемость теорий

Определение 6.20. Перевод I с определимыми параметрами есть *интерпретация теории T в U*, если

- для любой аксиомы $A \in T$ $U \vdash \mathrm{Par}_I(\vec{p}) \to A^I$;
- $U \vdash \mathrm{Par}_I(\vec{p}) \to \exists \vec{x} D_I(\vec{x},\vec{p})$;
- в U выводимы переводы аксиом равенства для сигнатуры Ω;
- $U \vdash \mathrm{Par}_I(\vec{p}) \to (\forall x \exists! y\, f(x)=y)^I$ для всех $f \in \mathrm{Func}_\Omega$.

Определение 6.21. Теория T *интерпретируема в U*, если существует интерпретация T в U.

Предложение 6.22. *Если T интерпретируема в U и $T \vdash A$, то $U \vdash \forall \vec{x}\,(Par_I(\vec{p}) \wedge D_I(\vec{x},\vec{p}) \to A^I(\vec{x},\vec{p}))$.*

Доказательство. Индукция по длине вывода формулы A. $\boxtimes$

Следствие 6.23. *Если T интерпретируема в U и теория U непротиворечива, то такова и T.*

Замечание 6.24. Этот результат установлен элементарными (синтаксическими) методами, не опирающимися на теорию множеств. Заметим, что доказательства непротиворечивости, опирающиеся на существование модели, как правило, выходят за рамки элементарных методов, так как обычно модели являются бесконечными и строятся в рамках теории множеств. Метод интерпретаций позволяет избавиться от ненужных гипотез о существовании бесконечных множеств и приводит к «чистому» сведению одной теории к другой.

Следствие 6.25. *Если непротиворечива элементарная евклидова геометрия, то непротиворечива элементарная геометрия Лобачевского.*

Следствие 6.26. *Если непротиворечива арифметика Пеано, то непротиворечива $Th(\mathbb{R})$ и элементарная евклидова геометрия.*

Этот факт вытекает из существования интерпретации $Th(\mathbb{R})$ в арифметике Пеано, которую можно построить исходя из интерпретации поля *вещественных алгебраических* чисел в стандартной модели арифметики.