П. Е. АЛАЕВ

ЛЕКЦИИ ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ, ЧАСТЬ I

КРАТКИЙ КОНСПЕКТ

ММФ НГУ, 2012

1. ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

1.1. Слова и операции над ними

Алфавитом называется произвольное множество символов. *Слово* в алфавите Δ — произвольная конечная последовательность $A = a_1 a_2 \dots a_n$ символов из Δ. *Длина слова* $|A|$ — количество символов в нём, т. е. число n. *Подслово* слова A — любая его часть, состоящая из идущих подряд символов, т. е. слово вида $a_t a_{t+1} \dots a_s$. *Начало* слова — это подслово вида $a_1 \dots a_s$, а *конец* слова — подслово вида $a_t \dots a_n$. *Пустое слово* — слово длины 0, вообще не содержащее символов.

Замечание. На языке теории множеств слово в алфавите Δ может быть определено как функция $f : \{1, 2, \dots, n\} \to \Delta$.

Вхождением подслова в данное слово называется само подслово вместе с указанием того места, в котором оно расположено в слове (вместе с номером символа, с которого оно начинается). Например, $B = \mathrm{ma}$ является словом в алфавите $\{\mathrm{a}, \mathrm{m}\}$, является подсловом слова $A = \mathrm{mathematics}$, и при этом существует два вхождения слова B в слово A.

Замена некоторого вхождения подслова B в слово A на слово B' производится так: пусть A_1 — та часть слова A, которая расположена перед вхождением B, а A_2 — та часть, которая расположена после него; в этом случае $A = A_1 B A_2$. Тогда результатом замены является слово $A_1 B' A_2$.

Кроме того, используется и операция *подстановки* слова B вместо всех вхождений некоторого символа a в слово A. В этом случае все вхождения a одновременно заменяются на слово B.

1.2. Формулы исчисления высказываний (ИВ)

Алфавит исчисления высказываний состоит из трёх частей:

1) *пропозициональные переменные*: они, как правило, будут обозначаться буквами $P, P_0, P_1, \dots, Q, Q_0, Q_1, \dots, R, R_0, R_1, \dots$

2) логические связки — *конъюнкция:* $\&$
дизъюнкция: $\vee$
импликация: $\to$
отрицание: $\neg$

3) вспомогательные символы — *левая скобка:* (
правая скобка:)

Формулы ИВ являются словами в этом алфавите и строятся по правилам:

1) Пропозициональная переменная является формулой (такая формула называется *атомной*).
2) Если A, B — формулы, то $\neg A$, $(A\&B)$, $(A \vee B)$, $(A \to B)$ — тоже формулы.

Для работы с формулами часто будет использоваться индукция. Пусть $\Phi(n)$ — некоторое утверждение, которое для каждого натурального числа n может быть истинным или ложным.

Принцип математической индукции. Если $\Phi(0)$ истинно, и для всех n из истинности $\Phi(n)$ следует истинность $\Phi(n+1)$, то $\Phi(n)$ истинно для всех n.

Иногда бывает удобно использовать индукцию в следующей усиленной форме.

Возвратная индукция. Пусть для каждого n из того, что $\Phi(k)$ истинно при любом $k < n$, следует, что истинно $\Phi(n)$. Тогда $\Phi(n)$ истинно для всех n.

Лемма (о начале формулы). Если A, B — формулы ИВ и слово B является началом слова A, то $A = B$.

Предложение (о представлении формулы ИВ). Всякая неатомная формула ИВ единственным образом может быть представлена в одной из форм

$$\neg A,\ (A\&B),\ (A \vee B),\ (A \to B),$$

где A, B — формулы ИВ.

До конца Части 1 формулы ИВ будем называть просто *формулами*. Назовём *подформулой* формулы A её подслово, которое само является формулой.

Лемма. Если A, B — формулы и непустой конец слова A совпадает с началом слова B, то этот конец равен B.

Предложение (о подформулах формулы ИВ). Пусть A — формула, B — её подформула и $A \neq B$.
1) Если $A = (A_1 \circ A_2)$, где $\circ \in \{\&, \vee, \to\}$, то любое вхождение B в A является вхождением либо в A_1, либо в A_2.
2) Если $A = \neg A_1$, то любое вхождение B в A является вхождением в A_1.

Следствие. Если в формуле A некоторое вхождение подформулы заменить на другую формулу, то результат вновь будет формулой.

1.3. Исчисление секвенций (ИС)

Алфавит ИС получается из алфавита ИВ добавлением символов $\vdash$ (“следует”) и запятой. *Секвенция* — слово одного из следующих видов:

$A_1, \ldots, A_n \vdash B$ (“из $A_1, \ldots, A_n$ следует B”),
$A_1, \ldots, A_n \vdash$ (“набор $A_1, \ldots, A_n$ противоречив”),
$\vdash B$ (“B истинно”),

где $A_1, \ldots, A_n, B$ — формулы, $n \geqslant 1$. При этом $A_1, \ldots, A_n$ называются *посылками* секвенции, а B — её *заключением*.

Исчисление секвенций ИС задаётся аксиомами и правилами вывода. В приведённом ниже списке правил A, B, C обозначают некоторые формулы, $\Gamma, \Gamma_1, \Gamma_2$ — конечные наборы формул (может быть, пустые).

Аксиомы ИС: все секвенции вида $A \vdash A$

Правила вывода ИС: $\dfrac{\Gamma \vdash A;\quad \Gamma \vdash B}{\Gamma \vdash (A\&B)}$ (введение &),

$\dfrac{\Gamma \vdash (A\&B)}{\Gamma \vdash A}$ (удаление &), $\dfrac{\Gamma \vdash (A\&B)}{\Gamma \vdash B}$ (удаление &),

$\dfrac{\Gamma \vdash A}{\Gamma \vdash (A \vee B)}$ (введение $\vee$), $\dfrac{\Gamma \vdash B}{\Gamma \vdash (A \vee B)}$ (введение $\vee$),

$\dfrac{\Gamma \vdash (A \vee B);\quad \Gamma, A \vdash C;\quad \Gamma, B \vdash C}{\Gamma \vdash C}$ (удаление $\vee$),

$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash (A \to B)}$ (введение $\to$), $\dfrac{\Gamma \vdash A;\quad \Gamma \vdash (A \to B)}{\Gamma \vdash B}$ (удаление $\to$),

$\dfrac{\Gamma, A \vdash}{\Gamma \vdash \neg A}$ (введение $\neg$), $\dfrac{\Gamma, \neg A \vdash}{\Gamma \vdash A}$ (удаление $\neg$),

$\dfrac{\Gamma \vdash}{\Gamma \vdash A}$ (добавление заключения), $\dfrac{\Gamma \vdash A;\quad \Gamma \vdash \neg A}{\Gamma \vdash}$ (сведение к противоречию),

$\dfrac{\Gamma_1, A, B, \Gamma_2 \vdash C}{\Gamma_1, B, A, \Gamma_2 \vdash C}$ (перестановка) $\dfrac{\Gamma \vdash A}{\Gamma, B \vdash A}$ (добавление посылки).

Определим теперь понятие *дерева вывода* в ИС.

1) Аксиома одновременно является деревом вывода этой аксиомы.

2) Если $\dfrac{S_1; \ldots; S_k}{S}$ — правило вывода ИС, $\mathcal{D}_1, \ldots, \mathcal{D}_k$ — деревья выводов секвенций $S_1, \ldots, S_k$, соответственно, то $\dfrac{\mathcal{D}_1; \ldots; \mathcal{D}_k}{S}$ — дерево вывода секвенции S.

Секвенция S *выводима* (*доказуема*) в ИС, если существует дерево вывода этой секвенции.

1.4. Семантика исчисления высказываний

Логические связки можно рассматривать как операции на логических величинах **и** (“истина”) и **л** (“ложь”), которые определяются так:

A	B	$(A\&B)$	$(A \vee B)$	$(A \to B)$
и	**и**	**и**	**и**	**и**
и	**л**	**л**	**и**	**л**
л	**и**	**л**	**и**	**и**
л	**л**	**л**	**л**	**и**

A	$\neg A$
и	**л**
л	**и**

Пусть M — некоторое множество пропозициональных переменных. Назовём *означиванием пропозициональных переменных* из M соответствие γ, которое каждой переменной $P \in M$ сопоставляет значение $\gamma(P)$ из множества $\{\mathbf{и}, \mathbf{л}\}$.

Если A — формула и γ — означивание, при котором каждая переменная из A получает некоторое значение, то *значение формулы* A при означивании γ, $A[\gamma]$, может быть определено индукцией по длине формулы:

1. Если A — переменная P, то $A[\gamma] = \gamma(P)$.
2. Если $A = (A_1 \circ A_2)$, где $\circ \in \{\&, \vee, \to\}$, то $A[\gamma] = A_1[\gamma] \circ A_2[\gamma]$ (см. таблицу выше).
3. Если $A = \neg A_1$, то $A[\gamma] = \neg A_1[\gamma]$.

Замечание. Значение формулы A при означивании γ зависит от значений только тех переменных, которые входят в A.

Ясно, что если не все переменные формулы A получают значения при означивании γ, говорить о $A[\gamma]$, вообще говоря, бессмысленно. Договоримся, что всякий раз, когда речь идёт о значении формулы при означивании γ, неявно подразумевается условие, что γ сопоставляет значения всем переменным, входящим в эту формулу.

Формула называется *тождественно истинной* (*тождественно ложной*), если она принимает значение **и** (**л**) при любом означивании переменных.

Пусть фиксировано некоторое означивание. Секвенция вида $A_1, \ldots, A_n \vdash B$ *истинна* при этом означивании, если B истинна или хотя бы одна из A_i ложна. Секвенция вида $A_1, \ldots, A_n \vdash$ *истинна*, если хотя бы одна из A_i ложна. Секвенция $\vdash B$ *истинна*, если формула B истинна.

Секвенция называется *тождественно истинной*, если она истинна при любом означивании переменных.

Теорема о корректности ИС. Любая выводимая в ИС секвенция тождественно истинна.

1.5. Допустимые правила вывода

Правило $\dfrac{S_1; \ldots; S_k}{S}$ называется *допустимым* в ИС, если из выводимости секвенций $S_1, \ldots, S_k$ следует выводимость S.

Дерево вывода с допустимыми правилами определяется точно так же, как обычное дерево вывода в ИС, с дополнительным условием, что вместе с исходными правилами ИС могут использовать и любые допустимые.

Предложение (о выводе с допустимыми правилами). Если у секвенции есть дерево вывода с допустимыми правилами, то она выводима в ИС.

Предложение (о допустимых в ИС правилах). Следующие правила допустимы в ИС:

$\dfrac{\Gamma \vdash A;\quad \Gamma, A \vdash B}{\Gamma \vdash B}$ (сечение), $\dfrac{\Gamma, A \vdash C;\quad \Gamma, B \vdash C}{\Gamma, (A \vee B) \vdash C}$ (разбор случаев),

$\dfrac{\Gamma, A, B \vdash C}{\Gamma, (A\&B) \vdash C}$ (соединение посылок), $\dfrac{\Gamma, (A\&B) \vdash C}{\Gamma, A, B \vdash C}$ (разделение посылок),

$\dfrac{\Gamma, A \vdash B}{\Gamma, \neg B \vdash \neg A}$ (контрапозиция), $\dfrac{\Gamma, \neg A \vdash \neg B}{\Gamma, B \vdash A}$ $\dfrac{\Gamma, A \vdash \neg B}{\Gamma, \neg B \vdash A}$ $\dfrac{\Gamma, \neg A \vdash B}{\Gamma, B \vdash \neg A}$

$\dfrac{A_1, \ldots, A_n \vdash B}{C_1, \ldots, C_m \vdash B}$ $\dfrac{A_1, \ldots, A_n \vdash}{C_1, \ldots, C_m \vdash}$ (структурные), где $A_1, \ldots, A_n$ — поднабор в $C_1, \ldots, C_m$.

1.6. Теорема о замене

Формулы A и B *синтаксически эквивалентны* ($A \equiv B$), если выводимы секвенции $A \vdash B$ и $B \vdash A$.

Лемма. Отношение $\equiv$ обладает следующими свойствами:

a) $A \equiv A$;

b) $A \equiv B \Rightarrow B \equiv A$;

c) $A \equiv B$, $B \equiv C \Rightarrow A \equiv C$;

d) $A \equiv A' \Rightarrow \neg A \equiv \neg A'$;

e) $A \equiv A'$, $B \equiv B' \Rightarrow (A \circ B) \equiv (A' \circ B')$, где $\circ \in \{\&, \vee, \to\}$.

Теорема (о замене). Если в формуле A некоторую подформулу заменить на синтаксический эквивалентную ей формулу, то результат будет синтаксически эквивалентен A.

1.7. Нормальные формы

Докажем теперь, что любая формула ИВ может быть приведена через цепочку эквивалентностей к некоторому простому виду. Договоримся, что при записи формул две внешние скобки (в начале и конце формулы) могут быть опущены.

Лемма (основные эквивалентности ИВ-1). Пусть A, B, C — произвольные формулы. Тогда верно, что

a) $A\&B \equiv B\&A$ и $A \vee B \equiv B \vee A$ (коммутативность);

b) $A\&(B\&C) \equiv (A\&B)\&C$ и $A \vee (B \vee C) \equiv (A \vee B) \vee C$ (ассоциативность);

c) $A\&(B \vee C) \equiv (A\&B) \vee (A\&C)$ и

d) $A \vee (B\&C) \equiv (A \vee B)\&(A \vee C)$ (дистрибутивность).

Лемма (основные эквивалентности ИВ-2). Пусть A, B — произвольные формулы. Тогда верно, что

a) $A \to B \equiv \neg A \vee B$;

b) $\neg\neg A \equiv A$;

c) $\neg(A\&B) \equiv \neg A \vee \neg B$;

d) $\neg(A \vee B) \equiv \neg A\&\neg B$;

e) $A \equiv A \vee A$ и $A \equiv A\&A$.

Обозначим через $(A_1 \vee A_2 \vee \ldots \vee A_n)$ формулу $(\ldots((A_1 \vee A_2) \vee A_3)\ldots \vee A_n)$, а через $(A_1\&A_2\&\ldots\&A_n)$ — формулу $(\ldots((A_1\&A_2)\&A_3)\ldots\&A_n)$. Иногда будем кратко обозначать их как $\bigvee\limits_{i=1}^{n} A_i$ и $\bigwedge\limits_{i=1}^{n} A_i$.

Лемма. Пусть A_i, B_j, C — произвольные формулы. Тогда

a) $(A_1 \vee \ldots \vee A_n) \vee (B_1 \vee \ldots \vee B_k) \equiv (A_1 \vee \ldots \vee A_n \vee B_1 \vee \ldots \vee B_k)$;

b) $C\&(A_1 \vee \ldots \vee A_n) \equiv ((C\&A_1) \vee \ldots \vee (C\&A_n))$;

c) пункты (a) и (b) останутся верными при замене & на $\vee$, а $\vee$ на &.

Элементарная конъюнкция — это формула вида $(A_1\&\ldots\&A_n)$, $n \geqslant 1$, где каждая A_i — переменная или отрицание переменной.

Дизъюнктивная нормальная форма (д.н.ф.) — формула вида $(B_1 \vee \ldots \vee B_k)$, $k \geqslant 1$, где каждая B_i — элементарная конъюнкция.

Элементарная дизъюнкция — формула вида $(A_1 \vee \ldots \vee A_n)$, $n \geqslant 1$, где каждая A_i — переменная или отрицание переменной.

Конъюнктивная нормальная форма (к.н.ф.) — формула вида $(B_1\&\ldots\&B_k)$, $k \geqslant 1$, где каждая B_i — элементарная дизъюнкция.

Теорема (о приведении к д.н.ф. и к.н.ф.). Любая формула синтаксически эквивалентна некоторой к.н.ф. и некоторой д.н.ф., содержащим тот же набор переменных, что и она сама.

1.8. Теорема о полноте ИС

Предложение (о тождественно истинных к.н.ф.). К.н.ф. A тождественно истинна тогда и только тогда, когда каждая её элементарная дизъюнкция содержит P и $\neg P$ для некоторой переменной P.

Обратным утверждением к теореме о корректности ИС является

Теорема о полноте ИС. Любая тождественно истинная секвенция выводима в ИС.

Напомним, что запись $A \equiv B$ обозначает синтаксическую эквивалентность. Говорим, что A и B *семантически эквивалентны* ($A \sim B$), если при любом означивании переменных значения A и B совпадают.

Следствие. $A \equiv B$ тогда и только тогда, когда $A \sim B$.

1.9. Совершенные нормальные формы

Совершенная д.н.ф. (с.д.н.ф.) — это такая д.н.ф., что

1) любая входящая в неё переменная входит в каждую элементарную конъюнкцию ровно 1 раз, с отрицанием или без;

2) любые две элементарные конъюнкции *существенно различаются*, т.е. существует такая переменная P, что в одну из них входит P, а в другую $\neg P$.

Совершенная к.н.ф. (с.к.н.ф.) — определяется аналогично, с заменой $\vee$ на $\&$ и наоборот — это такая к.н.ф., что

1) любая входящая в неё переменная входит в каждую элементарную дизъюнкцию ровно 1 раз, с отрицанием или без;

2) любые две элементарные дизъюнкции существенно различаются.

Теорема (о совершенных нормальных формах).

a) Любая не тождественно ложная формула эквивалентна некоторой с.д.н.ф., содержащей тот же набор переменных, что и она сама;

b) Любая не тождественно истинная формула эквивалентна некоторой с.к.н.ф., содержащей тот же набор переменных, что и она сама;

c) Нормальная форма в (a) и (b) единственна с точностью до перестановки элементарных конъюнкций (дизъюнкций) и их компонент.

Замечание. Тождественно истинная формула не имеет эквивалентной ей с.к.н.ф., а тождественно ложная — с.д.н.ф.

2. ТЕОРИЯ МНОЖЕСТВ

2.1. Общие свойства множеств и операции над ними

Изложение математической теории множеств было бы естественно начать с определения множества. К сожалению, попытки дать строгое и исчерпывающее определение этого понятия связаны с трудностями, о которых будет сказано несколько слов позже. Интуитивно, общее представление о множествах является обобщением тех конкретных примеров множеств, которые используются в математике: множества натуральных чисел $\mathbb{N}$, его подмножеств, множества вещественных чисел $\mathbb{R}$, множества $P(\mathbb{N})$ всех подмножеств $\mathbb{N}$, множества функций из $\mathbb{N}$ в $\mathbb{R}$, и т.д.

Любое множество является некоторой совокупностью математических объектов, которые называются его *элементами*. Запись $x \in A$ означает, что x принадлежит множеству A, т. е. является его элементом. Для множеств выполняется
Аксиома экстенсиональности. Пусть A, B — множества. Тогда $A = B \Leftrightarrow$ для любого $x \quad [x \in A \Leftrightarrow x \in B]$.

Эта аксиома говорит, что множество однозначно определяется своими элементами: если у двух множеств набор элементов один и тот же, то эти множества равны.

Введём несколько стандартных обозначений. Пусть A, B — множества.
$\emptyset$ — единственное множество, не содержащее элементов (*пустое множество*);
$A \subseteq B$, если для всех x $[x \in A \Rightarrow x \in B]$ (A — *подмножество* B);
$A \subset B$, если $A \subseteq B$ и $A \neq B$ (A — *собственное подмножество* B);
$A \cup B$ — *объединение* множеств A и B: $\quad x \in A \cup B \Leftrightarrow x \in A$ или $x \in B$;
$A \cap B$ — *пересечение* множеств A и B: $\quad x \in A \cap B \Leftrightarrow x \in A$ и $x \in B$;
$A \setminus B = A - B$ — *разность* множеств A и B: $\quad x \in A - B \Leftrightarrow x \in A$ и $x \notin B$;
$\{a_1, \ldots, a_k\}$ — множество, элементами которого являются $a_1, \ldots, a_k$, и только они.

Если $\Phi(x)$ — некоторое условие, которое в зависимости от x может быть истинным или ложным, то запись $\{x \mid \Phi(x)\}$ обозначает множество всех x, для которых $\Phi(x)$ истинно (если такое множество существует). Через $P(A)$ обозначим множество всех подмножеств A, т.е. $\{B \mid B \subseteq A\}$.

Использование теории множеств в качестве основания математики опирается, в частности, на идею о том, что любой математический объект можно представить в виде множества. Тем самым понятия “множество” и “математический объект” являются синонимами. Натуральные числа могут быть представлены в виде множеств так:

$0 = \emptyset$
$1 = \{0\} = \{\emptyset\}$
$2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$
$3 = \{0, 1, 2\}$
$\vdots$
$n + 1 = n \cup \{n\}$
$\vdots$

Множество натуральных чисел $\{0, 1, 2, \ldots\}$ будем обозначать $\mathbb{N}$ или ω. Иногда вместо термина "множество" будем употреблять его синоним "семейство".

Если S — непустое множество, то $\bigcap S = \{x \mid x \in A \text{ для всех } A \in S\}$,
$\bigcup S = \{x \mid \text{существует } A \in S \text{ такое, что } x \in A\}$.
Иногда эти операции обозначаются как $\bigcap_{A \in S} A$ и $\bigcup_{A \in S} A$.

2.2. Упорядоченные пары и n-ки

Упорядоченный набор (*кортеж*) длины n (n-*ка*) определяется индукцией по n:
$\langle\rangle = \emptyset$
$\langle a \rangle = a$
$\langle a, b \rangle = \{\{a\}, \{a, b\}\}$
$\langle a_1, \ldots, a_n, a_{n+1} \rangle = \langle \langle a_1, \ldots, a_n \rangle, a_{n+1} \rangle$.

Набор $\langle a, b \rangle$ длины 2 часто называют *парой*.

Предложение (о равенстве n-ок). Если $\langle a_1, \ldots, a_n \rangle = \langle b_1, \ldots, b_n \rangle$, то все их компоненты попарно равны, т. е. $a_1 = b_1, \ldots, a_n = b_n$.

Пусть $A_1, \ldots, A_n$ — множества. Их *декартово произведение* — это множество
$A_1 \times \ldots \times A_n = \{\langle a_1, \ldots, a_n \rangle \mid a_1 \in A_1, \ldots, a_n \in A_n\}$.
Если $A_1 = \ldots = A_n = A$, то это декартово произведение называется *декартовой степенью* множества A и обозначается A^n.

2.3. Функции

Бинарным отношением называется любое множество R, состоящее из пар. Если при этом $R \subseteq A \times B$, то R называют *бинарным отношением между* A *и* B, а если $R \subseteq A^2$, то R — *бинарное отношение* на A. *Обратное отношение* R^{-1} равно $\{\langle b, a \rangle \mid \langle a, b \rangle \in R\}$.

Бинарное отношение f называется *функцией*, если выполняется условие:

$$\langle x, y_1 \rangle, \langle x, y_2 \rangle \in f \Rightarrow y_1 = y_2;$$

$\mathrm{dom}(f) = \{x \mid$ существует y т.ч. $\langle x, y \rangle \in f\}$ — *область определения* функции f;
$\mathrm{ran}(f) = \{y \mid$ существует x т.ч. $\langle x, y \rangle \in f\}$ — *множество значений* функции f;

f — *функция из* A *в* B, если f — функция, $\mathrm{dom}(f) = A$ и $\mathrm{ran}(f) \subseteq B$.
В последнем случае используется обозначение $f : A \to B$.

Замечание. Если $f : A \to B$ и $x \in A$, то существует единственный y такой, что $\langle x, y\rangle \in f$. Этот y лежит в B, называется *значением* функции f в точке x, и обозначается $f(x)$.

Замечание (о равенстве функций). Если f, g — функции, то $f = g \Leftrightarrow \mathrm{dom}(f) = \mathrm{dom}(g)$ и $f(x) = g(x)$ при любом $x \in \mathrm{dom}(f)$.

Для любого множества A существует *тождественная функция* $\mathrm{id}_A = \{\langle x, x\rangle \mid x \in A\}$. Ясно, что $\mathrm{id}_A : A \to A$ и $\mathrm{id}_A(x) = x$ при $x \in A$.

Если f и g — функции, то их *композиция* $g \circ f$ определяется так:
$g \circ f = \{\langle x, z\rangle \mid$ существует y т.ч. $\langle x, y\rangle \in f$ и $\langle y, z\rangle \in g\}$.

Лемма (о композиции функций). Пусть f, g и h — функции. Тогда
a) $h \circ (g \circ f) = (h \circ g) \circ f$;
b) если $f : A \to B$, $g : B \to C$, то $g \circ f : A \to C$ и $[g \circ f](x) = g(f(x))$ при $x \in A$.

Пусть $f : A \to B$. Говорим, что
f — функция из A *на* B (*сюръекция*), если для любого $y \in B$ найдётся $x \in A$ такой, что $f(x) = y$; будем обозначать это как $f : A \xrightarrow{\text{на}} B$;
f — *разнозначная функция* (1–1 *функция*, *инъекция*), если для любых $x_1, x_2 \in A$ из $f(x_1) = f(x_2)$ следует, что $x_1 = x_2$; пишем, что $f : A \xrightarrow{1-1} B$;
f — *биекция* из A на B, если f — одновременно инъекция и функция из A на B.

Лемма (о свойствах биекций).
a) если $f : A \xrightarrow[\text{на}]{1-1} B$, то $f^{-1} : B \xrightarrow[\text{на}]{1-1} A$, $f^{-1}(f(x)) = x$ при любом $x \in A$ и $f(f^{-1}(y)) = y$ при любом $y \in B$;
b) если $f : A \xrightarrow[\text{на}]{1-1} B$, $g : B \xrightarrow[\text{на}]{1-1} C$, то $g \circ f : A \xrightarrow[\text{на}]{1-1} C$ и $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Функция f^{-1} в (a) называется *обратной функцией* к f.

2.4. Отношения эквивалентности

Пусть R — бинарное отношение на множестве A, т.е. $R \subseteq A^2$. Говорим, что
R *симметрично*, если $\langle a, b\rangle \in R \Rightarrow \langle b, a\rangle \in R$,
R *антисимметрично*, если $\langle a, b\rangle, \langle b, a\rangle \in R \Rightarrow a = b$,
R *транзитивно*, если $\langle a, b\rangle, \langle b, c\rangle \in R \Rightarrow \langle a, c\rangle \in R$,
R *иррефлексивно*, если $\langle a, a\rangle \notin R$ для любого a,
R *рефлексивно на* A, если $\langle a, a\rangle \in R$ для любого $a \in A$.

Бинарное отношение $R \subseteq A^2$ называется *отношением эквивалентности* на A, если оно симметрично, транзитивно и рефлексивно на A.
Вместо записи $\langle x, y\rangle \in R$ часто будем использовать краткое обозначение xRy и говорить, что x и y *эквивалентны* относительно R.

Если $x \in A$, то множество $x/R = \{y \in A \mid xRy\}$ называется *классом эквивалентности* элемента x. Множество всех классов эквивалентности $A/R = \{x/R \mid x \in A\}$ называется *фактор-множеством* A по R.

Семейство $D \subseteq P(A)$ назовём *разбиением множества* A, если
1) любое множество $B \in D$ непусто;
2) если $B_1, B_2 \in D$ и $B_1 \neq B_2$, то $B_1 \cap B_2 = \emptyset$;
3) для любого $x \in A$ существует $B \in D$ такое, что $x \in B$.

Лемма (о классах эквивалентности). Если R — отношение эквивалентности на A, то A/R — разбиение множества A.

Теорема (об отношениях эквивалентности). Для любого множества A существует биекция между множеством всех отношений эквивалентности на A и множеством всех разбиений A.

2.5. Частично упорядоченные множества

Бинарное отношение $R \subseteq A^2$ — *частичный порядок* на A, если оно антисимметрично, транзитивно и рефлексивно на A. *Частично упорядоченное множество* (ч.у.м.) — это пара (A, R), где R — частичный порядок на A.

В дальнейшем, как правило, для частичных порядков будет использоваться символ $\leqslant$ и его модификации. Как и раньше, вместо записи $\langle x, y\rangle \in \leqslant$ используем сокращение $x \leqslant y$.

Пусть $\leqslant$ — частичный порядок на A, $x \in A$. Говорим, что
x — *наибольший* элемент в A, если $y \leqslant x$ для всех $y \in A$;
x — *наименьший* элемент, если $x \leqslant y$ для всех $y \in A$;
x — *максимальный* элемент, если для любого $y \in A$ из $x \leqslant y$ следует, что $x = y$;
x — *минимальный* элемент, если для любого $y \in A$ из $y \leqslant x$ следует, что $x = y$;

Замечание. Наибольший элемент (если он существует) единственен и является максимальным, а наименьший (если существует) единственен и является минимальным.

Обозначим через $x < y$ то, что $x \leqslant y$ и $x \neq y$.

Замечание. Если $\leqslant$ — частичный порядок на A, то $<$ — иррефлексивное и транзитивное отношение на A.

Пусть $(A, \leqslant_A)$ — ч.у.м. и $B \subseteq A$. Тогда мы можем перенести порядок $\leqslant_A$ на B, определяя $\leqslant_B$ как $\leqslant_A \cap B^2$: это просто означает, что $x \leqslant_B y \Leftrightarrow x \leqslant_A y$ при $x, y \in B$. Отношение $\leqslant_B$ называется *индуцированным порядком* на B; легко проверить, что это действительно частичный порядок на B. Иногда мы будем говорить о множестве B как о ч.у.м., подразумевая под этим ч.у.м. $(B, \leqslant_A \cap B^2)$.

Частичный порядок $\leqslant$ на A называется *фундированным*, если любое непустое $X \subseteq A$ содержит минимальный (в X) элемент.

Предложение (критерий фундированности порядка). Частичный порядок $\leqslant$ на A является фундированным $\Leftrightarrow$ в A нет бесконечно убывающей последовательности $a_0 > a_1 > a_2 > \ldots$

Предложение (о индукции в фундированном ч.у.м.). Пусть A — ч.у.м. с фундированным порядком $\leqslant$, B — некоторое подмножество A. Допустим, что для любого $x \in A$ из того, что $y \in B$ для всех $y < x$, следует, что $x \in B$. Тогда $B = A$.

Пусть даны два ч.у.м. $(A, \leqslant_A)$ и $(B, \leqslant_B)$.

Функция $f : A \to B$ называется *монотонной*, если $x \leqslant_A y \Rightarrow f(x) \leqslant_B f(y)$;

f — *изоморфизм между* $(A, \leqslant_A)$ и $(B, \leqslant_B)$, если f — биекция из A на B и $x \leqslant_A y \Leftrightarrow f(x) \leqslant_B f(y)$ при любых $x, y \in A$.

Ч.у.м. называются *изоморфными*, если между ними существует изоморфизм. Обозначим это как $(A, \leqslant_A) \cong (B, \leqslant_B)$.

Замечание. Изоморфность обладает свойствами отношения эквивалентности:

a) $(A, \leqslant_A) \cong (A, \leqslant_A)$;

b) если $(A, \leqslant_A) \cong (B, \leqslant_B)$, то $(B, \leqslant_B) \cong (A, \leqslant_A)$;

c) если $(A, \leqslant_A) \cong (B, \leqslant_B)$ и $(B, \leqslant_B) \cong (C, \leqslant_C)$, то $(A, \leqslant_A) \cong (C, \leqslant_C)$.

2.6. Линейно упорядоченные множества

Пусть $\leqslant$ — частичный порядок на A, $x, y \in A$. Говорим, что x, y *сравнимы* относительно $\leqslant$, если $x \leqslant y$ или $y \leqslant x$. Частичный порядок $\leqslant$ называется *линейным*, если $x \leqslant y$ или $y \leqslant x$ для любых $x, y \in A$, т.е. если любые два элемента в A сравнимы. В этом случае пара $(A, \leqslant)$ называется *линейно упорядоченным множеством* (л.у.м.).

Замечание. Если $(A, \leqslant)$ — л.у.м. и $x \in A$, то

a) x является минимальным тогда и только тогда, когда является наименьшим;

b) x является максимальным тогда и только тогда, когда является наибольшим.

Пусть $(A, \leqslant)$ — л.у.м. Подмножество $S \subseteq A$ называется *начальным сегментом* A, если для любых $x, y \in A$ из $x \in S$ и $y \leqslant x$ следует, что $y \in S$.

Замечание. Если S_1, S_2 — начальные сегменты л.у.м., то $S_1 \subseteq S_2$ или $S_2 \subseteq S_1$.

Начальным отрезком A, отсекаемым элементом $x \in A$, называется множество $A_x = \{y \in A \mid y < x\}$.

Замечание. Начальный отрезок всегда является начальным сегментом.

Лемма. Если $(A, \leqslant)$, $(B, \leqslant)$ — л.у.м. и $f : A \to B$ — монотонная биекция, то f — изоморфизм.

2.7. Вполне упорядоченные множества

Вполне упорядоченное множество (в.у.м.) — это пара $(A, \leqslant)$, где $\leqslant$ — линейный фундированный порядок на A. Иногда такой порядок называют *полным*.

Замечание 1. Любой начальный сегмент в.у.м. $(A, \leqslant)$ либо равен A, либо является начальным отрезком.

Замечание 2. Если $(A, \leqslant)$ — в.у.м. и $B \subseteq A$, то B с порядком, индуцированным из A, тоже является в.у.м.

Лемма. Если $(A, \leqslant)$ — в.у.м. и $f : A \xrightarrow{1-1} A$ — монотонная функция, то $f(x) \geqslant x$ при всех $x \in A$.

Предложение (о начальных сегментах в.у.м.). Различные начальные сегменты в.у.м. не могут быть изоморфны друг другу.

Предложение (о изоморфизме в.у.м.). Если два в.у.м. изоморфны, то изоморфизм между ними единственен.

Предположим, что $f : A \to C$ и $B \subseteq A$. Определим *сужение* функции f на B, $f|_B$, как $\{\langle x, y\rangle \in f \mid x \in B\}$. Легко проверить, что $f|_B$ — функция, $\mathrm{dom}(f|_B) = B$ и $f|_B(x) = f(x)$ при $x \in B$.

Теорема (о сравнении в.у.м.). Если даны два в.у.м., то одно из них изоморфно начальному сегменту другого.

2.8. Аксиома выбора, лемма Цорна, теорема Цермело

Ещё одна важная аксиома теории множеств —

Аксиома выбора. Для любого множества A существует $f : P(A) \setminus \{\emptyset\} \to A$ такая, что $f(X) \in X$ для всех $X \in P(A) \setminus \{\emptyset\}$.

Мы уже использовали её выше в некоторых доказательствах. Она играет ключевую роль и в доказательстве леммы Цорна.

Пусть $(A, \leqslant)$ — ч.у.м. Подмножество $B \subseteq A$ называется *цепью*, если любые два элемента из B сравнимы, т.е. $x \leqslant y$ или $y \leqslant x$ при $x, y \in B$.

Элемент $x \in A$ называется *верхней гранью* подмножества $B \subseteq A$, если $y \leqslant x$ для всех $y \in B$, и *нижней гранью*, если $x \leqslant y$ для всех $y \in B$. Если в множестве всех верхних граней B есть наименьший элемент, то он называется *супремумом* B, и обозначается $\sup(B)$. Наибольший элемент множества всех нижних граней называется *инфимумом* B, и обозначается $\inf(B)$.

Лемма Цорна (принцип максимума). Если в ч.у.м. у каждой цепи есть верхняя грань, то в этом ч.у.м. есть максимальный элемент.

Говорим, что множество можно *вполне упорядочить*, если на нём существует линейный фундированный порядок, т.е. порядок, при котором оно станет вполне упорядоченным.

Теорема Цермело. Любое множество можно вполне упорядочить.

Ниже будет показано, что эти три утверждения в некотором смысле равносильны.

2.9. Парадокс Рассела

Рассмотрим M_R — совокупность всех множеств A таких, что $A \notin A$. Предположим, что само M_R является множеством. Возможны два варианта:
1) $M_R \notin M_R$. Тогда $A = M_R$ подходит под определение выше, и $M_R \in M_R$. Противоречие.
2) $M_R \in M_R$. Вновь полагая $A = M_R$, получаем, что по определению $M_R \notin M_R$. Противоречие.

Это рассуждение называется парадоксом Рассела. Оно показывает, что совокупность M_R нельзя считать множеством. Подход, который первоначально использовался в работах основателя теории множеств Георга Кантора и предполагал, что множеством можно считать любую совокупность математических объектов, иногда называют наивной теорией множеств. Парадокс Рассела показывает, что наивная теория множеств нуждается в корректировке. Открытие парадоксов наивной теории множеств привело к появлению аксиоматических теорий множеств.

Заметим, что к противоречию приводит и существование множества всех множеств. Если совокупность $M = \{A \mid A \text{ — множество}\}$ является множеством, то стандартные правила работы с множествами говорят, что $M_R = \{A \in M \mid A \notin A\}$ тоже является множеством.

2.10. Аксиоматическая теория множеств ZFC

Аксиомы теории множеств Цермело–Френкеля (ZF) выглядят так:
1. Аксиома экстенсиональности. Множества a и b равны тогда и только тогда, когда для любого x $[x \in a \Leftrightarrow x \in b]$.
2. Аксиома пары. Для любых множеств a, b существует множество $\{a, b\}$.
3. Аксиома объединения. Для любого множества a существует множество $\bigcup a = \{y \mid \text{существует } x \in a \text{ такой, что } y \in x\}$.
4. Аксиома множества подмножеств. Для любого множества a существует множество $P(a) = \{b \mid b \subseteq a\}$.
5. Аксиома подстановки. Пусть a — множество, а $\Phi(x, y)$ — условие, обладающее свойством: для каждого $x \in a$ существует не более одного y такого, что $\Phi(x, y)$. Тогда существует множество $a' = \{y \mid \text{существует } x \in a \text{ такой, что } \Phi(x, y)\}$.
6. Аксиома бесконечности. Существует множество, которое содержит $\emptyset$ и вместе с каждым x содержит и $x \cup \{x\}$.

7. Аксиома регулярности. Для любого непустого множества a существует элемент $x \in a$ такой, что $x \cap a = \emptyset$.

Точная формализация понятия "условие $\Phi(x, y)$" из Аксиомы 5 может быть дана с помощью формул исчисления предикатов (ИП), которые появятся в нашем курсе позже. Тем самым список аксиом является пока не совсем формальным. Теория множеств Цермело-Френкеля с аксиомой выбора (ZFC) получается из ZF добавлением аксиомы выбора.

8. Аксиома выбора. Для любого множества A существует $f : P(A) \setminus \{\emptyset\} \to A$ такая, что $f(X) \in X$ для всех $X \in P(A) \setminus \{\emptyset\}$.

ZFC является наиболее известной и широко распространённой теорией множеств. В нашем курсе мы пользуемся её аксиомами, считая, что они выполняются для множеств. При этом мы не ставим перед собой задачу строго вывести все результаты курса из её аксиом. Если мы работаем в рамках ZFC и хотим использовать некоторое множество, то сначала нужно доказать, используя аксиомы ZFC, что такое множество существует. Приведём два примера таких доказательств.

Пример 1. Если A — множество и $\Psi(x)$ — некоторое условие, то существует множество $B = \{x \in A \mid \Psi(x)\}$.

Пример 2. Для любых множеств A и B существуют множества $A \cup B$, $A \cap B$ и $A \times B$.

Аксиомы 1 и 7 просто фиксируют некоторые важные свойства множеств, а Аксиомы 2–6 задают некоторые конструкции, которые позволяют строить новые, однозначно заданные множества из уже имеющихся. Аксиома выбора является в этом смысле особой — она утверждает существование некоторого объекта, но не указывает, как его можно построить или задать в явном виде. Из-за этого доказательства, использующие только ZF без аксиомы выбора, иногда рассматриваются как более конструктивные.

Предложение. В теории множеств ZF аксиома выбора следует из теоремы Цермело. Тем самым аксиома выбора, теорема Цермело и лемма Цорна равносильны в ZF.

Если некоторая совокупность множеств сама не является множеством, но может быть задана как совокупность всех множеств, обладающих некоторым фиксированным свойством, то такие совокупности часто называют *классами*. Например, мы можем говорить о классе всех множеств, всех бинарных отношений, или всех функций.

2.11. Мощности

Немного позже мы дадим точное определение *мощности множества* A, которая обозначается $|A|$. Базисным понятием для теории мощностей является, однако, не само понятие мощности, а понятие равномощности множеств. Говорим, что множества A и B *равномощны*, если существует биекция $f : A \xrightarrow[\text{на}]{1-1} B$. Обозначим это символической записью $|A| = |B|$. Это определение — точная формализация того, что в A и B содержится одинаковое количество элементов.

Замечание. Равномощность обладает свойствами отношения эквивалентности — для любых множеств A, B, C верно:

a) $|A| = |A|$;

b) $|A| = |B| \Rightarrow |B| = |A|$;

c) $|A| = |B|$ и $|B| = |C| \Rightarrow |A| = |C|$.

Запись $|A| \leqslant |B|$ означает, что существует инъекция $f : A \xrightarrow{1-1} B$. Это понятие формализует то, что количество элементов в A меньше или равно количества элементов в B. Запись $|A| < |B|$ означает, что $|A| \leqslant |B|$ и $|A| \neq |B|$.

Замечание. Из $|A| \leqslant |B|$ и $|B| \leqslant |C|$ следует, что $|A| \leqslant |C|$.

Лемма. Если A и B — непустые множества, то равносильно:

a) $|A| \leqslant |B|$;

b) существует функция $g : B \xrightarrow{\text{на}} A$;

c) A равномощно некоторому подмножеству B.

Если $f : A \to B$ и $A_1 \subseteq A$, то через $f[A_1]$ обозначим множество $\{f(x) \mid x \in A_1\}$. Его называют *образом* A_1 относительно f, и иногда обозначают как $f(A_1)$.

Теорема Кантора–Бернштейна. Если $|A| \leqslant |B|$ и $|B| \leqslant |A|$, то $|A| = |B|$.

Теорема (о сравнимости мощностей). Мощности любых двух множеств сравнимы, т.е. $|A| \leqslant |B|$ или $|B| \leqslant |A|$ для любых множеств A, B.

Теорема Кантора. $|A| < |P(A)|$ для любого множества A.

Множество A называется *конечным множеством мощности* k, если $|A| = |\mathbb{N}_k|$, где $k \in \mathbb{N}$, а $\mathbb{N}_k = \{x \in \mathbb{N} \mid x < k\} = \{0, 1, \ldots, k-1\}$. Множество *бесконечно*, если оно не является конечным. Множество A *счётно*, если $|A| = |\mathbb{N}|$, и *континуально*, если $|A| = |\mathbb{R}|$, где $\mathbb{R}$ — множество вещественных чисел.

Мы не будем доказывать некоторые свойства конечных множеств, считая их (почти) очевидными. Например то, что подмножество конечного множества является конечным. Они могут быть доказаны через свойства натуральных чисел.

Предложение. Любое бесконечное множество содержит счётное подмножество.

Множество A называется *не более, чем счётным*, если $|A| \leqslant |\mathbb{N}|$.

Следствие. Множество не более, чем счётно, тогда и только тогда, когда оно конечно или счётно.

2.12. Мощности объединения и произведения множеств

Лемма. a) Если $|A| = |A_1|$ и $|B| = |B_1|$, то $|A \times B| = |A_1 \times B_1|$;
b) если при этом $A \cap B = A_1 \cap B_1 = \emptyset$, то $|A \cup B| = |A_1 \cup B_1|$.

Лемма. $|\mathbb{N}^2| = |\mathbb{N}|$.

Лемма. Если A — бесконечное множество, а B — конечное, то $|A \cup B| = |A|$.

Если A, B — два множества, то они сравнимы по мощности: $|A| \leqslant |B|$ или $|B| \leqslant |A|$. Обозначим через $\max\{|A|, |B|\}$ бóльшую из этих мощностей, т.е. $|B|$ в первом случае и $|A|$ во втором.

Теорема (о мощности объединения). Если одно из множество A, B бесконечно, то $|A \cup B| = \max\{|A|, |B|\}$.

Теорема. Если A — бесконечное множество, то $|A^2| = |A|$.

Теорема (о мощности произведения). Если A, B — непустые множества и одно из них бесконечно, то $|A \times B| = \max\{|A|, |B|\}$.

Индексированное семейство $\{A_i\}_{i \in I}$ — это функция f такая, что $\mathrm{dom}(f) = I$ и $f(i) = A_i$ при $i \in I$.

Теорема (об объединении семейства). Пусть A — бесконечное множество. Если $\{A_i\}_{i \in I}$ — индексированное семейство множеств, $|I| \leqslant |A|$ и $|A_i| \leqslant |A|$ при всех $i \in I$, то $|\bigcup\limits_{i \in I} A_i| \leqslant |A|$.

Предложение. Если Δ — непустой алфавит, то мощность множества слов в этом алфавите равна $\max\{|\Delta|, |\mathbb{N}|\}$.

2.13. Ординалы

Отношение изоморфизма разбивает класс всех в.у.м. на подклассы: каждый подкласс состоит из всех в.у.м., которые изоморфны некоторому фиксированному в.у.м. Оказывается, что в каждом таком подклассе можно выбрать одно фиксированное в.у.м., которое можно считать его каноническим представителем. Оно является множеством специального вида, которое называется ординалом. Ординалы иногда называют также *трансфинитными числами*.

Замечание. Если $n \geqslant 1$ — натуральное число, то не существует множеств $x_1, \ldots, x_n$ таких, что $x_1 \in x_2 \in \ldots \in x_n \in x_1$. В частности, не существует x такого, что $x \in x$.

Множество α называется *транзитивным*, если из $x \in \alpha$ и $y \in x$ следует, что $y \in \alpha$. Множество α — *ординал*, если оно транзитивно и любые различные элементы в нём сравнимы относительно $\in$. Последнее означает, что один из случаев $x \in y$, $x = y$, $y \in x$ выполняется для любых $x, y \in \alpha$. В дальнейшем ординалы часто будут обозначаться греческими буквами $\alpha, \beta, \ldots$

Лемма. Если α — ординал и $\beta \in \alpha$, то β — ординал.

Определим на классе ординалов порядок $\leqslant$ так: $\alpha \leqslant \beta$, если $\alpha \in \beta$ или $\alpha = \beta$. Запись $\alpha < \beta$, как обычно, обозначает $\alpha \leqslant \beta$ и $\alpha \neq \beta$.

Лемма. Любой ординал α с порядком $\leqslant$ на его элементах является в.у.м.

Далее, говоря об ординале как о в.у.м., мы будем подразумевать, что на его элементах задан этот порядок $\leqslant$ (*естественный порядок* на ординале).

Лемма (о порядке на ординалах). Для любых ординалов α, β равносильно:
a) $\alpha \leqslant \beta$;
b) $\alpha \subseteq \beta$;
c) α — начальный сегмент в β.

Теорема (о порядке на ординалах). Класс ординалов с порядком $\leqslant$ обладает свойствами в.у.м. — для любых ординалов α, β, γ верно:
a) $\alpha \leqslant \alpha$;
b) $\alpha \leqslant \beta$ и $\beta \leqslant \alpha \Rightarrow \alpha = \beta$;
c) $\alpha \leqslant \beta$ и $\beta \leqslant \gamma \Rightarrow \alpha \leqslant \gamma$;
d) $\alpha \leqslant \beta$ или $\beta \leqslant \alpha$;
e) в любом непустом множестве ординалов есть минимальный элемент.

Определим $\alpha + 1$ как $\alpha \cup \{\alpha\}$.

Замечание. Если α — ординал, то $\alpha + 1$ тоже является ординалом, $\alpha < \alpha + 1$ и не существует ординала β такого, что $\alpha < \beta < \alpha + 1$.

Предложение (о супремуме множества ординалов). Объединение любого множества ординалов A вновь является ординалом, который является супремумом множества A.

Обозначим ординал из предыдущего предложения как $\sup(A)$.

Выше мы определяли натуральные числа так: $0 = \emptyset$ и $n+1 = n \cup \{n\}$. Поскольку $\emptyset$ является наименьшим ординалом, ординалами будут и все множества $1, 2, \ldots$ Они образуют начальный сегмент в классе всех ординалов. Их объединение равно множеству всех натуральных чисел $\omega = \{0, 1, 2, \ldots\}$. Тем самым ω — ординал, следующий за всеми натуральными числами. Далее будут идти $\omega + 1$, $(\omega + 1) + 1$, и т.д.

Теорема (о полноте класса ординалов). Для любого в.у.м. существует единственный изоморфный ему ординал.

Предложение (принцип трансфинитной индукции). Пусть $\Phi(x)$ — некоторое условие. Пусть для любого ординала α из того, что $\Phi(\beta)$ верно для всех $\beta < \alpha$, следует, что верно $\Phi(\alpha)$. Тогда $\Phi(\alpha)$ верно для всех ординалов α.

Как и аксиоме подстановки ZFC, точное определение условия $\Phi(x)$ требует использования формул ИП. Тем самым предложение сформулировано пока не совсем формальной. Приведём в ещё более неформальном виде другой важный факт.

Предложение (принцип трансфинитной рекурсии). Пусть существует условие, которое для каждого ординала α однозначно задаёт некоторое множество f_α в предположении, что при $\beta < \alpha$ множества f_β уже определены. Тогда каждому ординалу α действительно можно сопоставить множество f_α так, чтобы указанная связь между f_α и f_β, $\beta < \alpha$, выполнялась. При этом f_α определено однозначно.

Ординал α — *предельный*, если $\alpha \neq 0$ и его нельзя представить в виде $\beta + 1$ для некоторого ординала β.

Пример. Для любых двух ординалов α, β существует ординалы $\alpha + \beta$ и $\alpha \cdot \beta$, обладающие свойствами:
a) $\alpha + 0 = \alpha$ и $\alpha \cdot 0 = 0$;
b) $\alpha + (\beta + 1) = (\alpha + \beta) + 1$ и $\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha$;
c) $\alpha + \lambda = \sup\{\alpha + \beta \mid \beta < \lambda\}$ и $\alpha \cdot \lambda = \sup\{\alpha \cdot \beta \mid \beta < \lambda\}$, если λ — предельный ординал.

Отметим, что на языке ординалов определение натурального числа звучит так: α — *натуральное число*, если α — непредельный ординал и любой $\beta \in \alpha$ — тоже непредельный ординал.

2.14. Кардиналы

Ординал μ называется *кардиналом*, если он неравномощен никакому меньшему ординалу.

Теорема (основное свойство кардиналов). Для любого множества A существует единственный кардинал μ_A такой, что $|\mu_A| = |A|$.

Предложение. Если A, B — множества, то
a) $|A| = |B| \Leftrightarrow \mu_A = \mu_B$;
b) $|A| \leqslant |B| \Leftrightarrow \mu_A \leqslant \mu_B$.

Определим теперь понятие мощности: $|A|$, *мощность* множества A — это кардинал, равномощный A, то есть μ_A. Последнее предложение показывает, что это определение согласуется с нашей прошлой системой обозначений.

Пример. Ординал ω и все натуральные числа $n \in \omega$ являются кардиналами.

3. ЯЗЫК ИСЧИСЛЕНИЯ ПРЕДИКАТОВ И ЕГО СЕМАНТИКА

3.1 Формулы исчисления предикатов (ИП)

Чтобы определить понятие формулы ИП, нужно в первую очередь зафиксировать некоторое множество символов, которое называется сигнатурой (или языком). Это множество соответствует тому набору исходных понятий, о которых мы собираемся говорить на языке формул. Оно состоит из трёх частей — из предикатных, функциональных и константных символов.

Формально определим *сигнатуру* Σ как четвёрку вида $(\mathrm{Pr}_\Sigma, \mathrm{Fn}_\Sigma, \mathrm{Cn}_\Sigma, \nu)$, где $\nu : \mathrm{Pr}_\Sigma \cup \mathrm{Fn}_\Sigma \to \mathbb{N} \setminus \{0\}$, а множества $\mathrm{Pr}_\Sigma, \mathrm{Fn}_\Sigma, \mathrm{Cn}_\Sigma$ попарно не пересекаются. Элементы множества Pr_Σ называются *предикатными символами*, элементы Fn_Σ — *функциональными символами*, а элементы Cn_Σ — *константными символами*. Функция ν каждому предикатному и функциональному символу сопоставляет ненулевое натуральное число, которое называется *местностью* этого символа.

Поскольку сигнатура — всего лишь набор символов, её строгое определение не очень существенно. Если, например, $\mathrm{Pr}_\Sigma = \{P_1, \ldots, P_t\}$, $\mathrm{Fn}_\Sigma = \{f_1, \ldots, f_s\}$, $\mathrm{Cn}_\Sigma = \{c_1, \ldots, c_r\}$, то сигнатуру Σ будем иногда обозначать так:

$$\Sigma = (P_1^{n_1}, \ldots, P_t^{n_t}; f_1^{m_1}, \ldots, f_s^{m_s}; c_1, \ldots, c_r),$$

где n_i — местность символа P_i, а m_j — местность f_j.

Выбрав сигнатуру Σ, можно определить исчисление $\mathrm{ИП}_\Sigma$. Определим сначала термы и формулы $\mathrm{ИП}_\Sigma$. Алфавит $\mathrm{ИП}_\Sigma$ состоит из четырёх непересекающихся частей:

1) символы из Σ

2) *предметные переменные*: $v_0, v_1, v_2, \ldots$

3) *логические символы*: $\&, \vee, \to, \neg, \exists, \forall, =$

4) *вспомогательные символы*: запятая и две скобки, левая и правая.

Символ $\exists$ называется *квантором существования*, а $\forall$ — *квантором всеобщности*. Предметные переменные в этом разделе часто будут называться просто *переменными* и обозначаться символами x, y, z и производными от них.

Терм $\mathrm{ИП}_\Sigma$ — слово в этом алфавите, которое строится по правилам:

1) любая переменная x — терм;

2) любой константный символ c из Σ — терм;

3) если f — функциональный символ из Σ местности m, а $t_1, \ldots, t_m$ — термы, то $f(t_1, \ldots, t_m)$ — терм.

Формула ИП_Σ — слово в этом алфавите, которое строится по правилам:

1) если P — предикатный символ из Σ местности n, а $t_1, \ldots, t_n$ — термы, то $P(t_1, \ldots, t_n)$ — формула;

2) если t_1, t_2 — термы, то $t_1 = t_2$ — формула;

3) если A, B — формулы, то $\neg A$, $(A\&B)$, $(A \vee B)$, $(A \to B)$ — тоже формулы;

4) если A — формула, x — переменная, то $\exists x A$ и $\forall x A$ — тоже формулы.

Формулы из пунктов (1) и (2) называются *атомными*. Две последние формулы могут читаться так: "существует x такой, что верно A" и "для всех x верно A".

Как и для ИВ, *подформулой* формулы A называется её подслово, которое само является формулой. Отметим без доказательства, что для формул ИП_Σ нетрудно получить аналоги ряда утверждений, доказанных для формул ИВ в Части 1.

Лемма. Если A, B — формулы ИП_Σ и слово A является началом слова B, то $A = B$.

Предложение (о представлении термов и формул ИП). a) Любой терм ИП_Σ может быть единственным образом представлен в одной из форм

$$x, c, f(t_1, \ldots, t_k),$$

где x — переменная, c — константный символ, f — функциональный символ, t_i — термы ИП_Σ;

b) любая формула ИП_Σ единственным образом может быть представлена в одной из форм

$$P(t_1, \ldots, t_k), t_1 = t_2, \neg A, (A\&B), (A \vee B), (A \to B), \exists x A, \forall x A,$$

где P — предикатный символ, t_i — термы, A, B — формулы ИП_Σ, x — переменная.

Как правило, в дальнейшем мы будем работать с некоторой фиксированной сигнатурой Σ. До конца Части 3 термы и формулы ИП_Σ будем называть просто *термами* и *формулами*. Если нужно будет подчеркнуть то, что их сигнатурные символы лежат в Σ, они будут называться термами и формулами сигнатуры Σ.

Предложение (о подформулах формулы ИП). Пусть A — формула, B — её подформула.

a) Если A — атомная формула, то $B = A$.

b) Если $A = (A_1 \circ A_2)$, где $\circ \in \{\&, \vee, \to\}$, и при этом $B \neq A$, то любое вхождение B в A является вхождением либо в A_1, либо в A_2.

c) Если $A = \neg A_1$, $A = \exists x A_1$ или $A = \forall x A_1$, и при этом $B \neq A$, то любое вхождение B в A является вхождением в A_1.

Из этих утверждений легко следует

Замечание. В любой формуле для каждого вхождения квантора $\forall$ или $\exists$ существует единственное вхождение подформулы, которое начинается с этого квантора.

Это вхождение подформулы называется *областью действия* данного квантора. Квантор, за которым следует переменная x, называется *квантором по переменной* x. Вхождение переменной x в формулу называется *связанным вхождением*, если оно находится в области действия квантора по переменной x. В противном случае оно называется *свободным вхождением*.

Переменная x называется *свободной переменной* формулы A, если в A есть свободные вхождения x. Смысл этого определения состоит в том, что свободные переменные формулы A — те переменные, от которых зависит значение A. Формула, у которой нет свободных переменных, называется *предложением*. Обозначим через $\mathrm{Fv}(A)$ множество свободных переменных формулы A.

Лемма (о свободных переменных). a) Если A — атомная формула, то $\mathrm{Fv}(A)$ состоит из всех переменных, входящих в A;
b) если $A = (A_1 \circ A_2)$, где $\circ \in \{\&, \vee, \to\}$, то $\mathrm{Fv}(A) = \mathrm{Fv}(A_1) \cup \mathrm{Fv}(A_2)$;
c) если $A = \neg A_1$, то $\mathrm{Fv}(A) = \mathrm{Fv}(A_1)$;
d) если $A = \exists x A_1$ или $A = \forall x A_1$, то $\mathrm{Fv}(A) = \mathrm{Fv}(A_1) \setminus \{x\}$.

3.2. Алгебраические системы

Пусть A — множество, $n \geqslant 1$ — натуральное число. Любое отображение $P : A^n \to \{\mathbf{и}, \mathbf{л}\}$ называется n-местным *предикатом на множестве* A, а любая функция $f : A^n \to A$ — n-местной *функцией на множестве* A.

Пусть фиксирована сигнатура Σ. *Алгебраическая система* $\mathfrak{A}$ сигнатуры Σ — это пара вида $\mathfrak{A} = (A, \Sigma^{\mathfrak{A}})$, где A — непустое множество, а $\Sigma^{\mathfrak{A}}$ — интерпретация сигнатуры в A. *Интерпретация сигнатуры* — это соответствие, которое каждому символу из Σ сопоставляет его интерпретацию по следующим правилам:
1) $P \in \mathrm{Pr}_\Sigma$ и $\nu(P) = n \Rightarrow$ его интерпретация $P^{\mathfrak{A}}$ — n-местный предикат на A;
2) $f \in \mathrm{Fn}_\Sigma$ и $\nu(f) = m \Rightarrow$ его интерпретация $f^{\mathfrak{A}}$ — m-местная функция на A;
3) $c \in \mathrm{Cn}_\Sigma \Rightarrow$ его интерпретация $c^{\mathfrak{A}}$ — элемент A.

Множество A называется *носителем* системы $\mathfrak{A}$. Алгебраические системы называют также *моделями* или *структурами*. Для краткости иногда будем называть их просто системами. Если сигнатура задана в виде

$$\Sigma = (P_1, \ldots, P_t; f_1, \ldots, f_s; c_1, \ldots, c_r),$$

то алгебраическая система этой сигнатуры часто будет обозначаться как

$$\mathfrak{A} = (A, P_1^{\mathfrak{A}}, \ldots, P_t^{\mathfrak{A}}, f_1^{\mathfrak{A}}, \ldots, f_s^{\mathfrak{A}}, c_1^{\mathfrak{A}}, \ldots, c_r^{\mathfrak{A}}).$$

Пусть $\mathfrak{A}, \mathfrak{B}$ — две системы сигнатуры Σ с носителями A и B, соответственно. Функция $\beta : A \to B$ называется *изоморфизмом* между $\mathfrak{A}$ и $\mathfrak{B}$, если β является биекцией, для каждого символа из Σ удовлетворяющей условию:
1) $P \in \mathrm{Pr}_\Sigma \Rightarrow P^{\mathfrak{A}}(a_1, \ldots, a_n) = P^{\mathfrak{B}}(\beta(a_1), \ldots, \beta(a_n))$ для любых $a_i \in A$;
2) $f \in \mathrm{Fn}_\Sigma \Rightarrow \beta(f^{\mathfrak{A}}(a_1, \ldots, a_m)) = f^{\mathfrak{B}}(\beta(a_1), \ldots, \beta(a_m))$ для любых $a_i \in A$;
3) $c \in \mathrm{Cn}_\Sigma \Rightarrow \beta(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$.

Если между $\mathfrak{A}$ и $\mathfrak{B}$ существует изоморфизм, они называются *изоморфными* ($\mathfrak{A} \cong \mathfrak{B}$). Изоморфные системы являются по сути одной и той же системой, с точностью до замены одного носителя на другой. Свойства носителя системы часто переносят на саму систему: например, мощностью системы называют мощность её носителя, элементами системы — элементы носителя и т. д.

Замечание. Если две системы изоморфны, то их мощности равны.

Система $\mathfrak{B}$ называется *подсистемой* системы $\mathfrak{A}$, если $B \subseteq A$ и интерпретация любого символа из Σ в $\mathfrak{A}$ и $\mathfrak{B}$ совпадает на B. Последнее означает, что:
1) $P \in \mathrm{Pr}_\Sigma \Rightarrow P^{\mathfrak{A}}(a_1, \ldots, a_n) = P^{\mathfrak{B}}(a_1, \ldots, a_n)$ для любых $a_i \in B$;
2) $f \in \mathrm{Fn}_\Sigma \Rightarrow f^{\mathfrak{A}}(a_1, \ldots, a_m) = f^{\mathfrak{B}}(a_1, \ldots, a_m)$ для любых $a_i \in B$;
3) $c \in \mathrm{Cn}_\Sigma \Rightarrow c^{\mathfrak{A}} = c^{\mathfrak{B}}$.

Это определение означает, что интерпретация Σ в $\mathfrak{B}$ — просто сужение интерпретации Σ в $\mathfrak{A}$ на множество B. В силу этого подсистемой иногда называют и само множество B.

Предложение. Пусть $\mathfrak{A}$ — алгебраическая система с носителем A, а $X \subseteq A$. Тогда в $\mathfrak{A}$ существует наименьшая (по включению) подсистема, содержащая X.

Подсистема с указанным свойством называется *подсистемой, порождённой множеством* X.

3.3. Истинность формул в алгебраических системах

Введём несколько обозначений, облегчающих работу с формулами и термами. Часто терм бывает удобно обозначать как $t(x_1, \ldots, x_k)$. Договоримся, что такая запись может быть использована только в том случае, когда все переменные этого терма входят в набор $x_1, \ldots, x_k$, и все переменные из этого набора различны. Аналогичная запись $A(x_1, \ldots, x_k)$ может быть использована для формулы, но только в том случае, когда все её свободные переменные входят в набор $x_1, \ldots, x_k$, и все его элементы различны. При этом запись A может обозначать как предложение, так и произвольную формулу. Кроме того, набор $x_1, \ldots, x_k$ часто будем сокращать до $\bar{x}$.

Пусть фиксирована сигнатура Σ и $\mathfrak{A}$ — система этой сигнатуры. Если дан терм $t(x_1, \ldots, x_k)$ и $a_1, \ldots, a_k \in \mathfrak{A}$, то мы можем определить *значение* этого *терма* в системе $\mathfrak{A}$ при значениях переменных $x_1 = a_1, \ldots, x_k = a_k$. Обозначим это значение как $t^{\mathfrak{A}}(a_1, \ldots, a_k)$. Оно определяется индукцией по длине терма:

1) если $t(\bar{x})$ — переменная x_i, то $t^{\mathfrak{A}}(\bar{a}) = a_i$;

2) если $t(\bar{x})$ — константный символ c, то $t^{\mathfrak{A}}(\bar{a}) = c^{\mathfrak{A}}$;

3) если $t(\bar{x}) = f(t_1(\bar{x}), \ldots, t_n(\bar{x}))$, то $t^{\mathfrak{A}}(\bar{a}) = f^{\mathfrak{A}}(t_1^{\mathfrak{A}}(\bar{a}), \ldots, t_n^{\mathfrak{A}}(\bar{a}))$.

Тем самым значение терма — элемент $\mathfrak{A}$.

Замечание. Значение терма зависит только от системы и значений входящих в него переменных.

Значением формулы ИП в системе является истина или ложь, т.е. она является либо истинной, либо ложной. Пусть дана формула $A(x_1, \ldots, x_k)$ и $a_1, \ldots, a_k \in \mathfrak{A}$. Дадим определение того, что эта *формула истинна* в $\mathfrak{A}$ при значениях переменных $x_1 = a_1, \ldots, x_k = a_k$. Обозначим это как $\mathfrak{A} \models A(a_1, \ldots, a_k)$. Если формула не является истинной, то по определению является *ложной*, и это обозначается как $\mathfrak{A} \not\models A(a_1, \ldots, a_k)$. Определим истинность индукцией по длине формулы:

1) если $A(\bar{x}) = P(t_1(\bar{x}), \ldots, t_n(\bar{x}))$, то $\mathfrak{A} \models A(\bar{a}) \Leftrightarrow P^{\mathfrak{A}}(t_1^{\mathfrak{A}}(\bar{a}), \ldots, t_n^{\mathfrak{A}}(\bar{a})) = \mathbf{и}$;

2) если $A(\bar{x})$ — формула $t_1(\bar{x}) = t_2(\bar{x})$, то $\mathfrak{A} \models A(\bar{a}) \Leftrightarrow t_1^{\mathfrak{A}}(\bar{a}) = t_2^{\mathfrak{A}}(\bar{a})$;

3) если $A(\bar{x}) = \neg B(\bar{x})$, то $\mathfrak{A} \models A(\bar{a}) \Leftrightarrow \mathfrak{A} \not\models B(\bar{a})$;

4) если $A(\bar{x}) = (A_1(\bar{x}) \& A_2(\bar{x}))$, то $\mathfrak{A} \models A(\bar{a}) \Leftrightarrow \mathfrak{A} \models A_1(\bar{a})$ и $\mathfrak{A} \models A_2(\bar{a})$;

5) если $A(\bar{x}) = (A_1(\bar{x}) \vee A_2(\bar{x}))$, то $\mathfrak{A} \models A(\bar{a}) \Leftrightarrow \mathfrak{A} \models A_1(\bar{a})$ или $\mathfrak{A} \models A_2(\bar{a})$;

6) если $A(\bar{x}) = (A_1(\bar{x}) \to A_2(\bar{x}))$, то $\mathfrak{A} \models A(\bar{a}) \Leftrightarrow \mathfrak{A} \not\models A_1(\bar{a})$ или $\mathfrak{A} \models A_2(\bar{a})$;

7) если $A(\bar{x}) = \exists y B(\bar{x}, y)$, где $y \notin \{x_1, \ldots, x_k\}$, то

$\mathfrak{A} \models A(\bar{a}) \Leftrightarrow$ существует $b \in \mathfrak{A}$ такой, что $\mathfrak{A} \models B(\bar{a}, b)$;

8) если $A(\bar{x}) = \forall y B(\bar{x}, y)$, где $y \notin \{x_1, \ldots, x_k\}$, то

$\mathfrak{A} \models A(\bar{a}) \Leftrightarrow$ для всех $b \in \mathfrak{A}$ выполняется $\mathfrak{A} \models B(\bar{a}, b)$.

Можно заметить, что в этом списке отсутствуют ещё два пункта: случаи, когда $A(x_1, \ldots, x_k)$ равна $\exists x_i B$ или $\forall x_i B$ для некоторого $i \leqslant k$. Поскольку x_i в этом случае не является свободной переменной $A(\bar{x})$, значение a_i просто отбрасывается: можно переобозначить формулу как $A(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$ и использовать пункт (7) или (8). Приведём для ясности формальное определение:

7') если $A(x_1, \ldots, x_k) = \exists x_i B(x_1, \ldots, x_k)$, то

$\mathfrak{A} \models A(a_1, \ldots, a_k) \Leftrightarrow$ существует $b \in \mathfrak{A}$ такой, что $\mathfrak{A} \models B(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_k)$;

8') если $A(x_1, \ldots, x_k) = \forall x_i B(x_1, \ldots, x_k)$, то

$\mathfrak{A} \models A(a_1, \ldots, a_k) \Leftrightarrow$ для всех $b \in \mathfrak{A}$ выполняется $\mathfrak{A} \models B(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_k)$.

Замечание. Истинность формулы зависит только от системы и значений её свободных переменных. В частности, истинность предложения зависит только от системы: оно либо является истинным в системе, либо ложным.

Предложение (о сохранении формул при изоморфизме). Пусть $\mathfrak{A}, \mathfrak{B}$ — две системы сигнатуры Σ, $\beta : \mathfrak{A} \to \mathfrak{B}$ — изоморфизм и $A(x_1, \ldots, x_k)$ — формула. Если $a_1, \ldots, a_k \in \mathfrak{A}$, то $\mathfrak{A} \models A(a_1, \ldots, a_k) \Leftrightarrow \mathfrak{B} \models A(\beta(a_1), \ldots, \beta(a_k))$.

Если Γ — бесконечное множество формул, то множество его свободных переменных тоже может быть бесконечным. В такой ситуации удобно использовать понятие означивания. Назовём *означиванием переменных в системе* $\mathfrak{A}$ любую функцию $\gamma : V \to \mathfrak{A}$, где V — некоторое множество переменных. Как и в случае с ИВ, договоримся, что всякий раз, когда речь идёт о значении терма или формулы при данном означивании, неявно подразумевается условие, что все переменные терма и все свободные переменные формулы получают какие-то значения при этом означивании.

Скажем, что формула $A(x_1, \ldots, x_k)$ истинна в $\mathfrak{A}$ при означивании γ, если $\mathfrak{A} \models A(\gamma(x_1), \ldots, \gamma(x_k))$. Формула называется *тождественно истинной (ложной)*, если она истинна (ложна) в любой системе при любом означивании. Формулы A и B *семантически эквивалентны* ($A \sim B$), если в любой системе при любом означивании они истинны или ложны одновременно. Множество формул Γ называется *выполнимым*, если существует система и означивание, при которых все формулы из Γ истинны.

Лемма. Для любой формулы A выполняются эквивалентности $\neg\exists x A \sim \forall x \neg A$ и $\neg\forall x A \sim \exists x \neg A$.

3.4. Прямые и фильтрованные произведения алгебраических систем

Пусть I — некоторое множество. Семейство подмножеств $F \subseteq P(I)$ называется *центрированным*, если $A_1 \cap A_2 \cap \ldots \cap A_n \neq \emptyset$ для любых $A_1, \ldots, A_n \in F$. Семейство F называется *фильтром на* I, если выполняются условия:
1) $\emptyset \notin F$ и $I \in F$;
2) если $A, B \in F$, то $A \cap B \in F$;
3) если $A \subseteq B \subseteq I$ и $A \in F$, то $B \in F$.

Фильтр F — *ультрафильтр*, если $A \in F$ или $I \setminus A \in F$ для любого $A \subseteq I$.

Теорема (о существовании ультрафильтров). a) Любое непустое центрированное семейство в $P(I)$ может быть расширено до фильтра на I;
b) любой фильтр на I может быть быть расширен до ультрафильтра.

Пусть $\{A_i\}_{i \in I}$ — индексированное семейство множеств. Его *прямое произведение* $\prod_{i \in I} A_i = \{\alpha$ — функция $\mid \mathrm{dom}(\alpha) = I$ и $\alpha(i) \in A_i$ при $i \in I\}$.

Пусть фиксирована сигнатура Σ, $\{\mathfrak{A}_i\}_{i\in I}$ — семейство систем этой сигнатуры и A_i — носитель $\mathfrak{A}_i$. *Прямое произведение* семейства $\prod_{i\in I}\mathfrak{A}_i$ — это система $\mathfrak{A}$ с носителем $\prod_{i\in I}A_i$, в которой интерпретация символов из Σ задаётся так:
1) $P\in \mathrm{Pr}_\Sigma \Rightarrow P^{\mathfrak{A}}(\alpha_1,\ldots,\alpha_n)=\mathbf{и}\Leftrightarrow P^{\mathfrak{A}_i}(\alpha_1(i),\ldots,\alpha_n(i))=\mathbf{и}$ для всех $i\in I$;
2) $f\in \mathrm{Fn}_\Sigma \Rightarrow f^{\mathfrak{A}}(\alpha_1,\ldots,\alpha_n)(i)=f^{\mathfrak{A}_i}(\alpha_1(i),\ldots,\alpha_n(i))$ для всех $i\in I$;
3) $c\in \mathrm{Cn}_\Sigma \Rightarrow c^{\mathfrak{A}}(i)=c^{\mathfrak{A}_i}$ для всех $i\in I$.

Пусть теперь на I задан фильтр F. Чтобы определить фильтрованное произведение семейства $\{\mathfrak{A}_i\}_{i\in I}$, определим на $\prod_{i\in I}A_i$ бинарное отношение $\sim_F$ так: $\alpha\sim_F\beta\Leftrightarrow\{i\in I\mid\alpha(i)=\beta(i)\}\in F$.

Лемма. Отношение $\sim_F$ является отношением эквивалентности.

Кратко обозначим класс эквивалентности $\alpha/\!\sim_F$ как α/F.

Пусть $\mathfrak{A}=\prod_{i\in I}\mathfrak{A}_i$ — определённое выше прямое произведение. Определим $\mathfrak{A}/F$, *фильтрованное произведение* семейства $\{\mathfrak{A}_i\}_{i\in I}$ по фильтру F, как систему с носителем $\{\alpha/F\mid\alpha\in\prod_{i\in I}A_i\}$, в которой интерпретация символов из Σ задаётся так:
1) $P\in \mathrm{Pr}_\Sigma \Rightarrow P^{\mathfrak{A}/F}(\alpha_1/F,\ldots,\alpha_n/F)=\mathbf{и}\Leftrightarrow\{i\in I\mid P^{\mathfrak{A}_i}(\alpha_1(i),\ldots,\alpha_n(i))=\mathbf{и}\}\in F$;
2) $f\in \mathrm{Fn}_\Sigma \Rightarrow f^{\mathfrak{A}/F}(\alpha_1/F,\ldots,\alpha_n/F)=f^{\mathfrak{A}}(\alpha_1,\ldots,\alpha_n)/F$;
3) $c\in \mathrm{Cn}_\Sigma \Rightarrow c^{\mathfrak{A}/F}=c^{\mathfrak{A}}/F$.

Лемма. Указанное определение системы $\mathfrak{A}/F$ является корректным.

Обозначим построенную систему $\mathfrak{A}/F$ как $\prod^F_{i\in I}\mathfrak{A}_i$. Если F — ультрафильтр на I, то эту систему называют *ультрапроизведением* семейства $\{\mathfrak{A}_i\}_{i\in I}$ по F.

Скажем, что формула $A(x_1,\ldots,x_n)$ *фильтруется по фильтру* F, если для любого семейства систем $\{\mathfrak{A}_i\}_{i\in I}$ и любых элементов $\alpha_1/F,\ldots,\alpha_n/F\in\prod^F_{i\in I}\mathfrak{A}_i$

$$\prod\nolimits^F_{i\in I}\mathfrak{A}_i\models A(\alpha_1/F,\ldots,\alpha_n/F)\Leftrightarrow\{i\in I\mid\mathfrak{A}_i\models A(\alpha_1(i),\ldots,\alpha_n(i))\}\in F.$$

Лемма 1. Атомная формула фильтруется по любому фильтру.

Лемма 2. Любая формула A семантически эквивалентна формуле A', в которой нет $\vee$, $\to$ и $\forall$.

Теорема Лося. Любая формула фильтруется по любому ультрафильтру.

3.5. Теорема компактности Мальцева

Пусть фиксирована сигнатура Σ. Напомним, что множество формул Γ называется выполнимым, если существует система $\mathfrak{A}$ и означивание, при которых все формулы из Γ истинны. Назовём множество Γ *локально выполнимым*, если любое его конечное подмножество выполнимо. Ясно, что выполнимое множество является и локально выполнимым.

Теорема компактности Мальцева. Любое локально выполнимое множество формул является выполнимым.

Пусть Γ — множество предложений, $\mathfrak{A}$ — алгебраическая система. Обозначим через $\mathfrak{A} \models \Gamma$ то, что $\mathfrak{A} \models A$ для всех $A \in \Gamma$. Система $\mathfrak{A}$ называется *моделью* множества Γ, если $\mathfrak{A} \models \Gamma$.

Предложение. Если для каждого натурального n у множества предложений Γ есть модель мощности больше или равной n, то у Γ есть бесконечная модель.

3.6. Формулировка аксиом ZFC на языке формул ИП

Обозначим класс всех множеств как $\mathbb{V}$. Это класс иногда называют *универсумом* теории множеств. Мы предполагаем, для любых двух множеств $A, B \in \mathbb{V}$ выполнен ровно один из двух случаев: $A \in B$ или $A \notin B$. Заменяя запись $A \in B$ на $\in(A, B) = \mathbf{и}$, а $A \notin B$ — на $\in(A, B) = \mathbf{л}$, мы можем рассматривать пару $(\mathbb{V}, \in)$ как объект, "похожий" на алгебраическую систему сигнатуры $\Sigma = (\in^2)$, где $\in$ — предикатный символ.

Он не является алгебраической системой, поскольку $\mathbb{V}$ не является множеством. Тем не менее некоторые свойства алгебраических систем могут быть перенесены на $\mathbb{V}$. В частности, мы можем говорить об истинности формул сигнатуры Σ в $\mathbb{V}$. Значениями свободных переменных при этом являются элементы $\mathbb{V}$, т.е. произвольные множества. Истинность атомных формул, которые имеют вид $\in(x, y)$ и $x = y$, считается заданной изначально, логические связки определяются стандартно, а значение кванторов $\exists x$ и $\forall x$ понимается в том смысле, что "существует множество x такое, что ..." и "для всех множеств x верно, что ...".

Тогда аксиомы ZFC, о которых шла речь выше, могут быть переписаны в виде предложений ИП_Σ, истинных в $\mathbb{V}$. Например, аксиома пары приобретает вид

$$\forall x \forall y \exists z \forall t \ \big(\in(t, z) \leftrightarrow (t = x \vee t = y)\big),$$

где запись $A \leftrightarrow B$ является сокращением для $(A \to B)\&(B \to A)$.

Выше мы говорили, что классом множеств может быть названа совокупность всех множеств, удовлетворяющих некоторому условию. Теперь можно привести более строгую формулировку: под "условием" мы понимаем свойство, которое может быть записано в виде формулы ИП_Σ. В этой формуле можно использовать дополнительные параметры, поэтому общее определение звучит так: (определимый) *класс множеств* — это совокупность всех множеств b, для которых в $\mathbb{V}$ верно $A(d, b)$, где $A(z, x)$ — формула ИП_Σ, а d — некоторое фиксированное множество, которое называется *параметром*.

То же самое относится и к другим упоминаниям о неформальных “условиях” выше. Например, условие $\Phi(x, y)$ из аксиомы подстановки — это любое условие, записанное в виде формулы с параметрами. Тогда точная формулировка аксиомы становится такой: пусть $a, d \in \mathbb{V}$, $A(z, x, y)$ — формула ИП_Σ, и для любого $b \in a$ существует не более одного $c \in \mathbb{V}$ такого, что $A(d, b, c)$. Тогда существует множество $a' = \{c \mid \text{существует } b \in a \text{ такой, что } A(d, b, c)\}$.