

# Коллоквиум №1 (20.11.2019)

GROUPS №19137, №19144

2019

1. Множество: способы задания, операции над множествами  
Не существует явного определения множества.  
Пусть А некоторое мн-во, тогда существует 2 способа задания мн-ва

- (a)  $A = \{1, 2, 3, 4, 5\}$  - явное задание эл-тов мн-ва
- (b) Пусть  $\Phi(x)$ - некоторое условие, тогда  
 $A = \{x \mid \Phi(x)\}$  - Задание множествами с помощью некоторого условия  $\Phi(x)$
- (c) С помощью рекурентного соотношения.  
Пример:  $a_n$  - числа Фибоначчи, тогда  
 $a_1 = a_2 = 1, a_n = a_{n-1} + a_{n-2}$

Пусть А, В- некоторые множества

**Обозначение** (Подмножество). А - подмножество В, если  
 $A \subseteq B = \{x \mid x \in A \Rightarrow x \in B\}$

**Обозначение** (Собственное подмножество). А - собственное подмножество В, если  $A \subset B$ , если  $A \subseteq B$  и  $A \neq B$

**Обозначение** (Пустое множество).  $\emptyset$  - множество, не содержащее эл-тов ("Пустое множество")

**Обозначение** (Множество всех подмножеств множества A).

$$P(A) = \{ C \mid C \subseteq A \}$$

**Обозначение** (Универсум). Универсум (условное множество всех множеств)  $U$

Операции над множествами:

- Объединение множеств:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

- Пересечение множеств:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

- Разность множеств:

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$$

- Дополнение множества:

$$\neg A = \{x \mid x \in U \wedge x \notin A\}$$

- Симметрическая разность множеств:

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (B \cap A)$$

Пусть  $S$  - семейство множеств:

- Объединение семейства множеств

$$\bigcup S = \{x \mid \exists A_i \in S : x \in A_i\}$$

- Пересечение семейства множеств

$$\bigcap S = \{x \mid \forall A_i \in S : x \in A_i\}$$

2. Упорядоченный набор (кортеж), предложение о равенстве n-ок, декартово произведение, декартова степень.

**Определение** (Упорядоченный набор (кортеж)). Упорядоченный набор (кортеж) длины  $n$  определяется по индукции

$$<> = \emptyset$$

$$< a > = a$$

$$< a, b > = \{\{a\}, \{a, b\}\}$$

...

$$< a_1, a_2, \dots, a_{n-1}, a_n > = < a_1, a_2, \dots, a_{n-1} >, a_n >$$

**Определение** (пара). Набор  $\langle a, b \rangle$  длины 2 называют *парой*

**Предложение** (о равенстве n-ок). Если

$$\langle a_1, \dots, a_n \rangle = \langle b_1, \dots, b_n \rangle \Leftrightarrow a_1 = b_1, \dots, a_n = b_n$$

*Доказательство.* для  $n = 1$  очевидно в обе стороны. Докажем для  $n = 2$ :

$$\langle a_1, a_2 \rangle = \langle b_1, b_2 \rangle \Leftrightarrow \{\{a_1\}, \{a_1, a_2\}\} = \{\{b_1\}, \{b_1, b_2\}\}$$

$$\text{Пусть } a_1 = a_2 \Rightarrow \begin{cases} \{a_1\} = \{b_1, b_2\} \\ \{a_1, a_2\} = \{b_1, b_2\} \end{cases} \Rightarrow a_1 = a_2 = b_1 = b_2$$

для  $b_1 = b_2$  аналогично.

Рассмотрим  $a_1 \neq a_2, b_1 \neq b_2$

$$\Rightarrow \begin{cases} \{a_1\} = \{b_1\} \\ \{a_1\} = \{b_1, b_2\} \end{cases} \xrightarrow{\text{Так как } b_1 \neq b_2} \{a_1\} = \{b_1\} \Rightarrow a_1 = b_1$$

По аналогии для  $\{a_1, a_2\} = \{b_1, b_2\}$

Т.к справедливо для  $n = 2$ , а определение n-ок индуктивно следовательно верно для n □

**Определение** (Декартово произведение). Пусть даны множества  $A_1, \dots, A_n$ , тогда их декартовым произведением называют  $A_1 \times A_2 \times \dots \times A_n = \{\langle a_1, \dots, a_n \rangle \mid \forall i \in \{1, \dots, n\} a_i \in A_i\}$

**Определение** (Декартова степень). В случае, если  $A_1 = A_2 = \dots = A_n$ , тогда  $A_1 \times A_2 \times \dots \times A_n$  называют декартовой степенью и обозначают, как  $A^n = A_1 \times A_2 \times \dots \times A_n$

3. Бинарные отношения, обратное отношение, произведение отношений, лемма о бинарных отношениях.

**Определение.** Бинарным отношением между элементами множеств  $A$  и  $B$  называется произвольное подмножество  $C \subseteq A \times B$

**Определение.** Обратным бинарным отношением называется  $R^{-1} = \{<y; x> \mid <x; y> \in R\}$

**Определение.** Произведением бинарных отношений называется

$$R_1 \times R_2 = \{<x; z> \mid \exists y \quad <x; y> \in R_1 \wedge <y; z> \in R_2\}$$

**Лемма** (Лемма о бинарных отношениях). Для любых бинарных отношений  $R_1, R_2, R_3$ :

$$(a) \quad R_1 \cdot (R_2 \cdot R_3) = (R_1 \cdot R_2) \cdot R_3$$

$$(b) \quad (R_1 \cdot R_2)^{-1} = R_2^{-1} \cdot R_1^{-1}$$

*Доказательство.* (а) Покажем, что  $R_1 \cdot (R_2 \cdot R_3) \subseteq (R_1 \cdot R_2) \cdot R_3$ .

Пусть  $<x; t> \in R_1 \cdot (R_2 \cdot R_3)$ , тогда существует  $y$  такое, что  $<x; y> \in R_1$  и  $<y; t> \in R_2 \cdot R_3$ . Далее существует  $z$  такое, что  $<y; z> \in R_2$  и  $<z; t> \in R_3$ . Получаем, что  $<x; z> \in R_1 \cdot R_2$  и  $<x; t> \in (R_1 \cdot R_2) \cdot R_3$ . Обратное включение доказывается аналогично.

(б) Покажем, что  $(R_1 \cdot R_2)^{-1} \subseteq R_2^{-1} \cdot R_1^{-1}$ .

Пусть  $<z; x> \in (R_1 \cdot R_2)^{-1}$ , тогда существует  $y$  такое, что  $<x; y> \in R_1$  и  $<y; z> \in R_2$ . Тогда  $<y; x> \in R_1^{-1}$  и  $<z; y> \in R_2^{-1}$ . Получаем, что  $<z; x> \in R_2^{-1} \cdot R_1^{-1}$ . Обратное включение доказывается аналогично.

□

4. Область определения отношения, множество значений отношения, образ и прообраз множества относительно отношений, функция, замечание о равенстве функций, тождественная функция.

**Определение** (Функция). Бинарное отношение  $f$  называется функцией, если выполняется:  $\langle x, y_1 \rangle, \langle x, y_2 \rangle \in f \Rightarrow y_1 = y_2$

**Определение** (Область определения).  $dom(f) = \{x \mid \exists y : \langle x, y \rangle \in f\}$

**Определение** (Область значений).  $ran(f) = \{y \mid \exists x : \langle x, y \rangle \in f\}$

**Обозначение.**  $f$  - функция из  $A$  в  $B$ , если  $f$  - функция,  $dom(f) = A$  и  $ran(f) \subseteq B$

Тогда функцию обозначают  $f : A \rightarrow B$

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

**Замечание** (о равенстве функций). Если  $f, g$  - функции, то  $f = g \Leftrightarrow dom(f) = dom(g)$  и  $\forall x \in dom(f) \quad f(x) = g(x)$

*Доказательство.*

$\Rightarrow$  очевидно

$\Leftarrow$  пусть  $\langle x, y \rangle \in f \Rightarrow x \in dom(f)$  и  $y = f(x) \xrightarrow{\text{т.к } f(x)=g(x)}$   
 $y = g(x) \Rightarrow \langle x, y \rangle \in g \xrightarrow{\text{в силу произвольности выбора}} f(x) \leq g(x)$

Обратное по аналогии  $\square$

**Определение** (Тождественная функция). Для любого множества  $A$

$\exists f = \{\langle x, x \rangle \mid x \in A\} = id_A$ .

Ясно, что  $id_A : A \rightarrow A$

и  $\forall x \in A \quad id_A(x) = x$

5. Композиция функций, лемма о композиции функций:

**Определение** (Композиция функций). Если  $f$  и  $g$  - функции, то их композиция  $g \circ f$  определяется, как произведение бинарных отношений  $f \cdot g$  (В обратном порядке)

**Лемма** (о композиции функций). *Если  $f : A \rightarrow B, g : B \rightarrow C$ , то их композицией  $g \circ f : A \rightarrow C$  и  $[g \circ f](x) = g(f(x))$  при  $x \in A$*

Покажем, что  $g \circ f$  — функция. Пусть  $\langle x, z_1 \rangle, \langle x, z_2 \rangle \in g \circ f$ . Тогда существует  $y_1$  т. ч.  $\langle x, y_1 \rangle \in f$  и  $\langle y_1, z_1 \rangle \in g$ , и существует  $y_2$  т. ч.  $\langle x, y_2 \rangle \in f$  и  $\langle y_2, z_2 \rangle \in g$ . Получаем, что  $y_1 = y_2$  и  $z_1 = z_2$ .

Покажем, что  $\text{dom}(g \circ f) = A$ . Пусть  $x \in \text{dom}(g \circ f)$ . Тогда существует  $z$  т. ч.  $\langle x, z \rangle \in g \circ f$ , и существует  $y$  т. ч.  $\langle x, y \rangle \in f$ ,  $\langle y, z \rangle \in g$ . Получаем, что  $x \in \text{dom}(f) = A$ . Тем самым

$$\text{dom}(g \circ f) \subseteq A.$$

Пусть  $x \in A$ . Существует  $y$  т. ч.  $\langle x, y \rangle \in f$ . Тогда  $y \in \text{ran}(f)$  и  $y \in B = \text{dom}(g)$ . Следовательно, существует  $z$  т. ч.  $\langle y, z \rangle \in g$ . Получаем, что  $\langle x, z \rangle \in g \circ f$  и  $x \in \text{dom}(g \circ f)$ . Тем самым

$$A \subseteq \text{dom}(g \circ f).$$

Из последнего рассуждения ясно, что  $y = f(x)$ ,  $z = g(y)$  и  $z = [g \circ f](x)$ . Тем самым  $[g \circ f](x) = g(f(x))$ .

Подобным образом можно показать, что  $\text{ran}(g \circ f) \subseteq C$ .

## 6. Сюръекция, инъекция, биекция, обратная функция, лемма о свойствах биекций

Пусть  $f : A \rightarrow B$

**Определение** (Сюръекция).  $f$  - функция из  $A$  на  $B$  (*сюръективная функция, сюрбекция*), если  $\forall y \in B \exists x \in A | f(x) = y$

**Обозначение** (Сюръекция).  $f : A \xrightarrow{\text{на}} B$ .

**Определение** (Инъекция).  $f$  - инъективная функция (*1 - 1 функция, инбекция*), если  $\forall x_1, x_2 \in A$  из  $f(x_1) = f(x_2)$  следует  $x_1 = x_2$

**Обозначение** (Инъекция).  $f : A \xrightarrow{1-1} B$

**Определение** (Биекция).  $f$  - биекция из  $A$  на  $B$ , если  $f$  одновременно и инъекция, и сюръекция.

**Обозначение** (Биекция).  $f : A \xrightarrow[\text{на}]{1-1} B$

**Определение** (Обратная функция). Запись  $f^{-1}$  означает обратное бинарное отношение к  $f$ . Если  $f^{-1}$  при этом является функцией, то она называется *обратной функцией* к  $f$ .

**Лемма** (о свойствах биекций).

(a) Если  $f : A \xrightarrow[\text{на}]{1-1} B$ , то  $f^{-1} : B \xrightarrow[\text{на}]{1-1} A$ ,  $f^{-1}(f(x)) = x \forall x \in A$  и  $f(f^{-1}(y)) = y \forall y \in B$ .

(b) Если  $f : A \xrightarrow[\text{на}]{1-1} B$ ,  $g : B \xrightarrow[\text{на}]{1-1} C$ , то  $g \circ f : A \xrightarrow[\text{на}]{1-1} C$ .

*Доказательство.* (a) Покажем, что  $f^{-1}$  - функция.

Пусть  $\langle y, x_1 \rangle, \langle y, x_2 \rangle \in f^{-1}$ . Тогда  $\langle x_1, y \rangle, \langle x_2, y \rangle \in f$  и  $f(x_1) = f(x_2) = y$ . Поскольку  $f$  инъективна,  $x_1 = x_2$ .

Ясно, что  $\text{dom}(f^{-1}) = \text{ran}(f)$  и  $\text{ran}(f^{-1}) = \text{dom}(f)$ . Поскольку  $f$  сюръективна,  $\text{ran}(f) = B = \text{dom}(f^{-1})$ . Поскольку  $\text{ran}(f^{-1}) = A$ ,  $f^{-1}$  сюръективна. Инъективность  $f^{-1}$  легко проверяется. Тем самым  $f^{-1} : B \xrightarrow[\text{на}]{1-1} A$ .

Покажем, что  $f^{-1}(f(x)) = x$  при  $x \in A$ . Пусть  $x \in A$  и  $y = f(x)$ . Тогда  $\langle x, y \rangle \in f$  и  $\langle y, x \rangle \in f^{-1}$ . Получаем, что  $f^{-1}(y) = x$ .

(b) выше доказано, что  $g \circ f : A \rightarrow C$  и  $[g \circ f](x) = g(f(x))$ .  
Инъективность: если  $g(f(x_1)) = g(f(x_2))$ , то  $f(x_1) = f(x_2)$  и отсюда  $x_1 = x_2$ . Сюръективность доказывается похожим способом.

□

7. Отношения эквивалентности, классы эквивалентности, лемма о классах 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  $a \in A$ .

Отношение эквивалентности на множестве  $A$  — это бинарное отношение  $R \subseteq A^2$ , которое 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 фактормножеством  $A$  по  $R$ .

Семейство  $D \subseteq P(A)$  назовём разбиением множества  $A$ , если верно:

- 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  $B \in D$  т. ч.  $x \in B$ .

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

Если  $x \in A$ , то  $x \in x/R$ . Отсюда сразу получаем 1) и 3).

2): пусть  $x/R, y/R \in A/R$  и  $x/R \cap y/R \neq \emptyset$ . Покажем, что тогда  $x/R = y/R$ . Пусть  $z \in x/R \cap y/R$ . Тогда верно  $xRz$  и  $yRz$ , отсюда  $zRy$  в силу симметричности и  $xRy$  в силу транзитивности, а отсюда  $yRx$ .

Покажем, что  $x/R \subseteq y/R$ . Если  $t \in x/R$ , то  $xRt$  и  $yRt$ . Следовательно,  $t \in y/R$ . Аналогично получаем, что  $y/R \subseteq x/R$ .

8. Частичный порядок, ч.у.м., минимальные, максимальные, наименьшие, наибольшие элементы, связи между ними. Замечание о строгом порядке.

## 2.5. Частично упорядоченные множества

*Частичный порядок* на множестве  $A$  — это бинарное отношение  $R \subseteq A^2$ , которое 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  $x \leqslant y$  и говорим, что  $x$  меньше или равен  $y$  относительно порядка  $\leqslant$ .

Пусть  $\leqslant$  — частичный порядок на  $A$ ,  $x \in A$ . Говорим, что:

$x$  — наибольший элемент в ч.у.м.  $(A, \leqslant)$ , 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.

Допустим, что  $x_1, x_2$  — два наибольших элемента. Тогда по определению  $x_1 \leqslant x_2$  и  $x_2 \leqslant x_1$ . В силу антисимметричности  $x_1 = x_2$ .

Покажем, что  $x_1$  — максимальный элемент. Пусть  $x_1 \leqslant y$ . Тогда по определению наибольшего элемента  $y \leqslant x_1$ , следовательно,  $x_1 = y$ .

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

**Замечание (о строгом порядке).** Если  $\leqslant$  — частичный порядок на  $A$ , то  $<$  — иррефлексивное и транзитивное отношение на  $A$ .

Иррефлексивность  $<$  верна по определению. Покажем, что  $<$  транзитивно. Пусть  $x < y$  и  $y < z$ . Тогда  $x \leqslant y$ ,  $y \leqslant z$ ,  $x \neq y$  и

$y \neq z$ . Отсюда  $x \leq z$ . Допустим, что  $x = z$ . Тогда  $x \leq y, y \leq x$  и  $x = y, \uparrow\downarrow$ .

Пусть  $(A, \leq_A)$  — ч.у.м. и  $B \subseteq A$ . Тогда мы можем сузить порядок  $\leq_A$  на  $B$ , определяя порядок  $\leq_B$  как  $\leq_A \cap B^2$ . Это означает, что  $x \leq_B y \Leftrightarrow x \leq_A y$  при  $x, y \in B$ .

**Замечание.**  $\leq_A \cap B^2$  — частичный порядок на  $B$ .

Отношение  $\leq_B$  называется *индуцированным порядком* на  $B$ .

Иногда мы будем говорить о множестве  $B$  как о ч.у.м., подразумевая под этим ч.у.м.  $(B, \leq_A \cap B^2)$ .

Частичный порядок  $\leq$  на  $A$  называется *фундированным*, если в любом непустом  $B \subseteq A$  есть минимальный (в  $B$ ) элемент.

## 9. Фундированные частичные порядки, критерий фундированности порядка.

Частичный порядок  $\leq$  на  $A$  называется *фундированным*, если в любом непустом  $B \subseteq A$  есть минимальный (в  $B$ ) элемент.

**Предложение (критерий фундированности порядка).**

Частичный порядок  $\leq$  на  $A$  является фундированным  $\Leftrightarrow$  в  $A$  нет бесконечно убывающей последовательности  $a_0 > a_1 > a_2 > \dots$

$(\Rightarrow)$ : пусть  $\leq$  является фундированным порядком. Допустим, что в  $A$  есть последовательность  $a_0 > a_1 > \dots$ . Рассмотрим множество  $B = \{a_0, a_1, \dots\}$ . По условию в  $B$  есть минимальный элемент  $a_n$ . Но  $a_{n+1} < a_n, \uparrow\downarrow$ .

$(\Leftarrow)$ : пусть в  $A$  нет бесконечно убывающих последовательностей. Допустим, что  $\leq$  не является фундированным. Тогда существует непустое  $B \subseteq A$ , в котором нет минимального элемента. Выберем произвольный  $a_0 \in B$ . Поскольку он не минимален, в  $B$  существует  $a_1 \leq a_0$  т. ч.  $a_1 \neq a_0$ , т. е.  $a_1 < a_0$ . Далее, существует  $a_2 < a_1, a_3 < a_2$  и т. д. Получаем убывающую последовательность,  $\uparrow\downarrow$ .

## 10. Предложение об индукции в фундированном ч.у.м., изоморфизм ч.у.м., замечание об изоморфизме ч.у.м.

**Предложение (об индукции в фундированном ч.у.м.).**

Пусть  $(A, \leq)$  — ч.у.м. с фундированным порядком,  $B$  — некоторое подмножество  $A$ . Предположим, что для любого  $x \in A$  из того, что  $y \in B$  для всех  $y < x$ , следует, что  $x \in B$ . Тогда  $B = A$ .

|| Допустим, что  $B \neq A$ . Тогда  $C = A \setminus B$  непусто. Пусть  $x$  — минимальный элемент в  $C$ . Если  $y < x$ , то  $y \notin C$ , следовательно,  $y \in B$ . По условию из этого следует, что  $x \in B$ ,  $\uparrow\downarrow$ .

Пусть даны два ч.у.м.  $(A, \leq_A)$  и  $(B, \leq_B)$ . Функция  $f : A \rightarrow B$  называется *монотонной*, если

$$x \leq_A y \Rightarrow f(x) \leq_B f(y);$$

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

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

**Замечание.** Изоморфность обладает свойствами отношения эквивалентности:

- $(A, \leq_A) \cong (A, \leq_A)$ ;
- если  $(A, \leq_A) \cong (B, \leq_B)$ , то  $(B, \leq_B) \cong (A, \leq_A)$ ;
- если  $(A, \leq_A) \cong (B, \leq_B)$  и  $(B, \leq_B) \cong (C, \leq_C)$ , то  $(A, \leq_A) \cong (C, \leq_C)$ .

|| а): функция  $\text{id}_A$  является искомым изоморфизмом; б): если  $f : A \rightarrow B$  — изоморфизм, то  $f^{-1} : B \rightarrow A$  — тоже изоморфизм; в): если  $f : A \rightarrow B$  и  $g : B \rightarrow C$  — изоморфизмы, то  $g \circ f$  — тоже изоморфизм. Всё это легко проверяется.

11. Линейные порядки, л.у.м., начальные сегменты и отрезки, лемма о свойствах начальных сегментов.

## 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 элемент  $x \in A$ , то:

- $x$  является минимальным тогда и только тогда, когда является наименьшим;
- $x$  является максимальным тогда и только тогда, когда является наибольшим.

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

**Лемма (о свойствах начальных сегментов).** Пусть дано л.у.м.  $(A, \leqslant)$ . Тогда:

- если  $S_1, S_2$  — начальные сегменты, то  $S_1 \subseteq S_2$  или  $S_2 \subseteq S_1$ ;
- если  $S$  — начальный сегмент, а  $x$  — минимальный элемент в  $A \setminus S$ , то  $S \cup \{x\}$  — тоже начальный сегмент;
- объединение любого семейства начальных сегментов — снова начальный сегмент.

a): предположим, что  $S_1 \not\subseteq S_2$ , и покажем, что  $S_2 \subseteq S_1$ . Пусть  $x \in S_1 \setminus S_2$ . Рассмотрим  $y \in S_2$ . Случай  $x \leqslant y$  невозможен, так как тогда  $x \in S_2$ . Значит,  $y \leqslant x$ . Получаем, что  $y \in S_1$ .

b): пусть  $z \in S \cup \{x\}$  и  $y \leqslant z$ . Покажем, что  $y \in S \cup \{x\}$ . Если  $z \in S$ , то  $y \in S$ . Пусть  $z = x$ . Если  $y = x$ , то  $y \in S \cup \{x\}$ . Если же  $y < x$ , то  $y$  не может лежать в  $A \setminus S$ . Значит,  $y \in S$ .

c): пусть  $D$  — семейство начальных сегментов и  $S' = \bigcup_{S \in D} S$ . Проверим, что  $S'$  — начальный сегмент. Пусть  $x \in S'$  и  $y \leqslant x$ . Тогда существует  $S \in D$  т. ч.  $x \in S$ . Следовательно,  $y \in S$  и  $y \in S'$ .

*Начальным отрезком* л.у.м.  $(A, \leqslant)$ , отсекаемым элементом  $x \in A$ , называется множество  $A_x = \{y \in A \mid y < x\}$ .

**Замечание.** Начальный отрезок всегда является начальным сегментом.

12. Изоморфизм ч.у.м., изоморфизм л.у.м., признак изоморфизма л.у.м., лемма о монотонной инъекции в.у.м.

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

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

**Замечание.** Изоморфность обладает свойствами отношения эквивалентности:

- a)  $(A, \leq_A) \cong (A, \leq_A)$ ;
- b) если  $(A, \leq_A) \cong (B, \leq_B)$ , то  $(B, \leq_B) \cong (A, \leq_A)$ ;
- c) если  $(A, \leq_A) \cong (B, \leq_B)$  и  $(B, \leq_B) \cong (C, \leq_C)$ , то  $(A, \leq_A) \cong (C, \leq_C)$ .

||| a): функция  $\text{id}_A$  является искомым изоморфизмом; b): если  $f : A \rightarrow B$  — изоморфизм, то  $f^{-1} : B \rightarrow A$  — тоже изоморфизм; c): если  $f : A \rightarrow B$  и  $g : B \rightarrow C$  — изоморфизмы, то  $g \circ f$  — тоже изоморфизм. Всё это легко проверяется.

**Лемма (признак изоморфизма л.у.м.).** Если  $(A, \leq)$ ,  $(B, \leq)$  — л.у.м. и  $f : A \rightarrow B$  — монотонная биекция, то  $f$  — изоморфизм.

||| Нужно лишь проверить переход  $f(x) \leq f(y) \Rightarrow x \leq y$ . Пусть  $f(x) \leq f(y)$ . Допустим, что  $x \not\leq y$ . Тогда  $y \leq x$ ,  $f(y) \leq f(x)$  и  $f(y) = f(x)$ . В силу инъективности  $x = y$ ,  $\uparrow\downarrow$ .

**Лемма.** Если  $(A, \leq)$  — в.у.м. и  $f : A \xrightarrow{\text{1-1}} A$  — монотонная инъекция, то  $f(x) \geq x$  при всех  $x \in A$ .

||| Заметим: если  $x, y \in A$  и  $x < y$ , то  $f(x) < f(y)$ . Из монотонности получаем, что  $f(x) \leq f(y)$ , а из инъективности — что  $f(x) \neq f(y)$ .

Допустим, что утверждение неверно: существует  $x \in A$  т. ч.  $f(x) \not\geq x$ . Поскольку порядок линеен,  $f(x) < x$ . Тогда

$$f(f(x)) < f(x), f(f(f(x))) < f(f(x)), \text{ и т. д.}$$

Получаем последовательность  $x > f(x) > f(f(x)) > \dots, \uparrow\downarrow$ .

13. Полный порядок, в.у.м., лемма о начальных сегментах в.у.м.

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

**Лемма** (о начальных сегментах в.у.м.). *Любой начальный сегмент в.у.м.  $(A, \leq)$  либо равен  $A$ , либо является начальным отрезком.*

*Доказательство.* Пусть  $S$  - начальный сегмент в  $A$  и  $S \neq A$ . Тогда  $A \setminus S \neq \emptyset$ . Пусть  $x$  - минимальный элемент в  $A \setminus S$ . Покажем, что  $S = A_x$ . Если  $y \in S$ , то либо  $y < x$ , либо  $x \leq y$ . Второй случай невозможен, так как тогда  $x \in S$ .  $\square$

14. Предложение об изоморфизме начальных сегментов, теорема о сравнимости в.у.м. (без доказательства).

**Предложение** (об изоморфизме начальных сегментов). *Различные начальные сегменты в.у.м. не могут быть изоморфны друг другу.*

*Доказательство.* Пусть  $S_1$  и  $S_2$  - два различных сегмента в.у.м.  $(A, \leq)$ . Тогда сначала докажем лемму о том, что если  $(A, \leq)$  - в.у.м. и  $f : A \xrightarrow{1-1} A$  - монотонная инъекция, то  $f(x) \geq x \forall x \in A$ . Заметим: если  $x, y \in A$  и  $x < y$ , то  $f(x) < f(y)$ . Из монотонности получаем, что  $f(x) \leq f(y)$ , а из инъективности - что  $f(x) \neq f(y)$ . Допустим, что утверждение неверно: существует  $x \in A$  |  $f(x) \not\geq x$ . Поскольку ряд линеен,  $f(x) < x$ . Тогда  $f(f(x)) < f(x)$ ,  $f(f(f(x))) < f(f(x))$ , и т.д. Получаем последовательность  $x > f(x) > f(f(x)) > \dots$ , противоречие.

По доказанной лемме  $S_1 \subseteq S_2$  или  $S_2 \subseteq S_1$ . Пусть  $S_1 \subseteq S_2$ . Выберем  $x_0 \in S_2 \setminus S_1$ .

Мы рассматриваем эти сегменты как в.у.м. с индуцированным из  $A$  порядком. Допустим, что  $f : S_2 \rightarrow S_1$  - изоморфизм. Рассматривая  $f$  как функцию из  $S_2$  в  $S_2$ , видим, что она инъективна и монотонна. Следовательно,  $f(x_0) \geq x_0$ . Поскольку  $S_1$  начальный сегмент и  $f(x_0) \in S_1$ , получаем, что  $x_0 \in S_1$ , противоречие.  $\square$

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

15. Аксиома выбора, лемма Цорна (без доказательства), теорема Цермело (без доказательства), эквивалентность утверждений.

**Аксиома выбора.** Для любого множества  $A$  существует функция  $f : P(A) \setminus \{\emptyset\} \rightarrow A$  т. ч.  $f(X) \in X$  для всех  $X \in P(A) \setminus \{\emptyset\}$ .

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

Элемент  $x \in A$  называется *верхней гранью* подмножества  $B \subseteq A$ , если  $y \leq x$  для всех  $y \in B$ , и *нижней гранью*, если  $x \leq y$  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 аксиома выбора, лемма Цорна и теорема Цермело в некотором смысле равносильны.

16. Парадокс Рассела, аксиоматика ZFC.

**Парадокс** (Парадокс Рассела). Рассмотрим совокупность:  $M_R = \{A \mid A - \text{множество и } A \notin A\}$ .

Предположим, что само  $M_R$  является множеством. Возможны два варианта:

- (a)  $M_R \notin M_R$ . Тогда  $A - M_R$  подходит под определение, и  $M_R \notin M_R$ . Противоречие.
- (b)  $M_R \in M_R$ . Вновь полагая,  $A = M_R$ , получаем, что по определению  $M_R \notin M_R$ . Противоречие.

Это рассуждение показывает, что совокупность  $M_R$  нельзя считать множеством.

Аксиоматика ZFC.

Можно с собой на листочке!!!

17. Равномощные множества, замечание о равномощности.

**Обозначение** (мощность множества). Мощность множества  $A$  обозначается  $|A|$ .

**Определение** (равномощные множества). Говорим, что множества  $A$  и  $B$  равномощные, если существует биекция  $f : A \xrightarrow[\text{на}]{} B$ . Обозначим это символической записью  $|A| = |B|$ .

**Замечание** (о равномощности). 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  $|B| = |C| \Rightarrow |A| = |C|$ ;

*Доказательство.* Следует из леммы о свойствах биекций. □

18. Лемма о порядке на мощностях.

**Лемма** (Лемма о порядке на мощностях). Для всяких непустых множеств  $A$  и  $B$  следующие условия эквивалентны:

- (a)  $|A| \leq |B|$
- (b) Существует функция  $g : B \xrightarrow[\text{на}]{} A$
- (c)  $A$  равномочно некоторому подмножеству  $B$

*Доказательство.*

(a)  $a \Rightarrow c$

Пусть  $|A| \leq |B|$ .

Тогда существует  $f : A \xrightarrow{\text{на}^{1-1}} B$ .

Тогда  $\text{ran}(f) \subseteq B$  и  $f : A \xrightarrow[\text{на}]{1-1} \text{ran}(f)$ .

(b)  $c \Rightarrow b$

Пусть  $h : B_1 \xrightarrow[\text{на}]{1-1} A$ , где  $B_1 \subseteq B$ .

Выберем произвольное  $a_0 \in A$  и построим  $g : B \xrightarrow[\text{на}]{} A$  так:

$$g(y) = \begin{cases} h(y), & \text{если } y \in B_1 \\ a_0, & \text{если } y \in B \setminus B_1 \end{cases}$$

(c)  $b \Rightarrow a$

Пусть  $g : B \xrightarrow[\text{на}]{} A$ .

Построим  $f : B \rightarrow A$ .

Рассмотрим  $x \in A$

Множество  $\{y \in B \mid g(y) = x\}$  непусто.

Выберем в качестве  $f(x)$  некоторый элемент из этого множества. Проверим, что  $f$  инъективна. Пусть  $f(x_1) = f(x_2)$

Тогда  $g(f(x_1)) = g(f(x_2))$ , а по построению  $g(f(x_i)) = x_i$  при  $i = 1, 2$ .

□

19. Теорема Кантора-Бернштейна.

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

По условию существуют  $f : A \xrightarrow{1-1} B$  и  $g : B \xrightarrow{1-1} A$ . Тогда  $g \circ f : A \xrightarrow{1-1} A$ . Построим последовательность  $\{A_n\}_{n \in \mathbb{N}}$  так:  $A_0 = A$ ,  $A_1 = \text{ран}(g)$  и  $A_{n+2} = g \circ f[A_n]$  при  $n \in \mathbb{N}$ .

Проверим, что  $A_n \supseteq A_{n+1}$  индукцией по  $n$ . При  $n = 0, 1$  это очевидно. Если  $n \geq 2$ , то уже доказано, что  $A_{n-2} \supseteq A_{n-1}$ , отсюда  $g \circ f[A_{n-2}] \supseteq g \circ f[A_{n-1}]$ .

Положим  $M_n = A_n \setminus A_{n+1}$  при  $n \in \mathbb{N}$  и  $D = \bigcap_{n \in \mathbb{N}} A_n$ .

**Лемма 1.** Множества  $D, M_0, M_1, \dots$  попарно не пересекаются, а их объединение равно  $A$ .

▷ Допустим, что  $D \cap M_n \neq \emptyset$ , и  $x \in D \cap M_n$ . Тогда  $x \in A_{n+1}$  и  $x \in A_n \setminus A_{n+1}$ ,  $\uparrow\downarrow$ .

Допустим, что  $M_n \cap M_k \neq \emptyset$  при  $n < k$ , и  $x \in M_n \cap M_k$ . Тогда  $x \in A_n \setminus A_{n+1}$  и  $x \in A_k$ , где  $A_k \subseteq A_{n+1}$ ,  $\uparrow\downarrow$ .

Тем самым эти множества попарно не пересекаются. Рассмотрим  $x \in A$  и покажем, что он попадёт в одно из них. Предположим, что  $x \notin D$ . Тогда существует  $n \in \mathbb{N}$  т. ч.  $x \notin A_n$ . Найдём наименьшее  $n$  с таким свойством. Тогда  $n \neq 0$  и  $x \in A_{n-1} \setminus A_n$ .  $\square$

**Лемма 2.**  $g \circ f[M_n] = M_{n+2}$ .

▷ ( $\subseteq$ ) : пусть  $x \in M_n = A_n \setminus A_{n+1}$ . Тогда  $g \circ f(x) \in A_{n+2} = g \circ f[A_n]$ . Допустим, что  $g \circ f(x) \in A_{n+3} = g \circ f[A_{n+1}]$ . Тогда существует  $x' \in A_{n+1}$  т. ч.  $g \circ f(x) = g \circ f(x')$ . Из инъективности  $x = x'$  и  $x \in A_{n+1}$ ,  $\uparrow\downarrow$ .

( $\supseteq$ ) : пусть  $y \in A_{n+2} \setminus A_{n+3}$ . Найдётся  $x \in A_n$  т. ч.  $y = g \circ f(x)$ . Если  $x \in A_{n+1}$ , то  $y \in A_{n+3}$ , что невозможно. Получаем, что  $x \in A_n \setminus A_{n+1} = M_n$ .  $\square$

Построим  $h : A \rightarrow A$  так:

$$h(x) = \begin{cases} x, & \text{если } x \in D \text{ или } x \in M_{2t+1}, t \in \mathbb{N}; \\ g \circ f(x), & \text{если } x \in M_{2t}, t \in \mathbb{N}. \end{cases}$$

Легко проверить, что  $h : A \xrightarrow{1-1} A$  и  $\text{ран}(h) = D \cup \bigcup_{n \geq 1} M_n$ .

Последнее множество равно  $A_1$ , следовательно,  $h : A \xrightarrow[\text{на}]{1-1} A_1$  и  $|A| = |A_1|$ . Поскольку  $g : B \xrightarrow[\text{на}]{1-1} A_1$ , получаем, что  $|A_1| = |B|$ .

## 20. Теорема о сравнимости мощностей, теорема Кантора.

**Теорема (о сравнимости мощностей).** Если  $A, B$  — множества, то  $|A| \leq |B|$  или  $|B| \leq |A|$ .

По теореме Цермело  $A$  и  $B$  можно вполне упорядочить: найдутся порядки  $\leq_A$  и  $\leq_B$  т. ч.  $(A, \leq_A)$  и  $(B, \leq_B)$  — в.у.м. По теореме о сравнимости в.у.м. одно из них изоморфно начальному сегменту второго. Предположим, что  $(A, \leq_A)$  изоморфно  $S$  — начальному сегменту  $(B, \leq_B)$ . Тогда  $|A| = |S| \leq |B|$ .

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

Покажем, что  $|A| \leq |P(A)|$ . Построим  $f : A \rightarrow P(A)$  так:  $f(x) = \{x\}$ . Ясно, что  $f$  инъективна.

Допустим теперь, что  $|A| = |P(A)|$ . Тогда существует биекция  $g : A \xrightarrow[\text{на}]{1-1} P(A)$ . Положим  $B = \{x \in A \mid x \notin g(x)\}$ . Поскольку  $B \in P(A)$ , найдётся  $x_0 \in A$  т. ч.  $g(x_0) = B$ . Тогда либо  $x_0 \in B$ , либо  $x_0 \notin B$ . Если  $x_0 \in B$ , то  $x_0 \in g(x_0)$  и  $x_0 \notin B$ . Если же  $x_0 \notin B$ , то  $x_0 \notin g(x_0)$  и  $x_0 \in B$ .  $\uparrow \downarrow$ .

Заметим, что теорема Кантора тоже показывает, что множества всех множеств не существует: если  $M$  — множество всех множеств, то  $P(M) \subseteq M$ , и тем самым  $|P(M)| \leq |M|$ . Это рассуждение называется *парадоксом Кантора*.

Множество  $A$  называется *конечным множеством мощности*  $k$ , если  $|A| = |\mathbb{N}_k|$ , где  $k \in \mathbb{N}$ , а  $\mathbb{N}_k = \{x \in \mathbb{N} \mid x < k\}$ . 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 простые свойства конечных множеств, считая их очевидными: например то, что подмножество конечного множества является конечным. Они могут быть доказаны через свойства натуральных чисел и индукцию.

## 21. Конечные, бесконечные, счетные, континуальные множества, описание не более чем счетных множеств.

**Определение** (Конечное множество). Множество  $A$  называется *конечным множеством мощности*  $k$ , если  $|A| = |\mathbb{N}_k|$ , где  $k \in \mathbb{N}$ ,

а  $\mathbb{N}_k = \{x \in \mathbb{N} | x < k\}$

**Определение** (Бесконечное множество). Множество *бесконечно*, если оно не является конечным.

**Определение** (Счётное множество). Множество  $A$  *счётно*, если  $|A| = |\mathbb{N}|$ .

**Определение** (Континуальное множество). Множество  $A$  *континуально*, если  $|A| = |\mathbb{R}|$ .

**Определение** (Не более чем счётное множество). Множество  $A$  *не более чем счётно*, если  $|A| \leq |\mathbb{N}|$

**Следствие** (Описание не более чем счётных множеств). Множество не более чем счётно тогда и только тогда, когда оно конечно или счётно.

*Доказательство.*  $\Leftarrow$ : счётное множество не более чем счётно. Если  $A$  конечно, то  $|A| = |\mathbb{N}_k| \leq |\mathbb{N}|$ .

$\Rightarrow$ : Пусть  $A$  не более чем счётно. Предположим, что оно бесконечно. Тогда в  $A$  есть счётное подмножество  $B$ . Получаем, что  $|\mathbb{N}| - |B| \leq |A| \leq |\mathbb{N}|$ . По теореме Кантора-Бернштейна  $|A| = |\mathbb{N}|$ .  $\square$

22. Лемма о сохранении мощностей, теорема о мощности объединения (без доказательства).

**Лемма** (Лемма о сохранении мощностей).

(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  $|A \cup B| = |A_1 \cup B_1|$

*Доказательство.*

(a) Пусть даны биекции

$$f : A \xrightarrow[\text{на}]{}^{1-1} A_1 \text{ и } g : B \xrightarrow[\text{на}]{}^{1-1} B_1.$$

Построим  $h : A \times B \xrightarrow[\text{на}]{}^{1-1} A_1 \times B_1$  так:  $h_1(< x; y >) = < f(x), g(y) >$ . Легко проверить, что  $h_1$  - нужная биекция.

(b) Построим  $h_2 : A \cup B \xrightarrow[\text{на}]{}^{1-1} A_1 \cup B_1$  так:  $h_2(x) = \begin{cases} f(x), & \text{если } x \in A \\ g(x), & \text{если } x \in B \end{cases}$

Условие  $A \cap B = \emptyset$  гарантирует, что определение корректно.

Вновь нетрудно доказать, что  $h_2$  - биекция. Проверим в качестве примера, что  $h_2$  инъективна. Пусть  $h_2(x) = h_2(y)$ . Если  $x, y \in A$ , то получаем  $f(x) = f(y)$  и  $x = y$ . Если  $x, y \in B$ , рассуждения аналогичны. Если же  $x \in A, y \in B$  (или наоборот), то  $h_2(x) \in A_1$  и  $h_2(y) \in B_1$ , что невозможно в силу  $A_1 \cap B_1 = \emptyset$ .

□

**Лемма** (о мощности объединения). *Если хотя бы одно из множеств  $A, B$  бесконечно, то  $|A \cup B| = \max\{|A|, |B|\}$ .*

23. Теорема о мощности квадрата бесконечного множества (доказательства для счетного и континуального), теорема о мощности произведения (без доказательства).

**Теорема** (о мощности квадрата бесконечного множества). *Если  $A$  - бесконечное множество, то  $|A \times A| = |A|$*

*Доказательство.*

- Докажем, что  $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$

Построим  $f : \mathbb{N} \times \mathbb{N} \xrightarrow{1-1} \mathbb{N}$  и  $g : \mathbb{N} \xrightarrow{1-1} \mathbb{N} \times \mathbb{N}$

$$f(x, y) = 2^x + 3^y$$

$$g(x) = < x, 0 >$$

Заметим, что обе функции инъективны, а значит  $\begin{cases} |\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}| \\ |\mathbb{N} \times \mathbb{N}| \geq |\mathbb{N}| \end{cases}$

тогда по теореме *Кантора-Бернштейна* получаем, что  $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$

- Докажем, что  $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$

По аналогии с  $\mathbb{N}$  построим две инъекции:

$$(a) f : \mathbb{R} \times \mathbb{R} \xrightarrow{\text{1-1}} \mathbb{R}$$

Для построения данной функции докажем, равномощность  $\mathbb{R}$  и  $(0, 1)$ :

Для этого построим биекцию  $h : (0, 1) \xrightarrow[\text{на}]{} \mathbb{R}$

$h(x) = ctg(x * \pi)$  - функция биекция из-за  $E(ctgx) = \mathbb{R}$

Значит  $|\mathbb{R}| = |(0, 1)|$

Докажем, что  $\mathbb{R} \times \mathbb{R}$  равномощно  $(0, 1) \times (0, 1)$ :

Для этого построим  $w : (0, 1) \times (0, 1) \xrightarrow[\text{на}]{} \mathbb{R} \times \mathbb{R}$

$w(x, y) = < h(x), h(y) >$

Значит  $|\mathbb{R} \times \mathbb{R}| = |(0, 1) \times (0, 1)|$

Построим инъекцию  $u : (0, 1) \times (0, 1) \xrightarrow{\text{1-1}} (0, 1)$

$u(x, y) = 0, \frac{10*a_1}{2} \frac{10*b_1}{2} \frac{10*a_2}{2} \frac{10*b_2}{2} \dots$

Где  $x = 0, a_1 a_2 \dots$ , а  $y = 0, b_1 b_2 \dots$

Т.к в формуле присутствует умножение на 10, то на каждое число из  $\frac{10*a_1}{2} \frac{10*b_1}{2} \frac{10*a_2}{2} \frac{10*b_2}{2} \dots$  отводится по две цифры, т.е  $\frac{10*4}{2} = 20$ , а  $\frac{10*9}{2} = 45$ , также  $\frac{10*0}{2} = 00$

$u$  - инъекция, тогда  $f(x, y) = h \circ u \circ w^{-1}(x, y)$

$$(b) g : \mathbb{R} \xrightarrow{\text{1-1}} \mathbb{R} \times \mathbb{R}$$

Построим  $g(x) = < x, 0 >$

Т.к  $f$  и  $g$  - инъекции, значит значит  $\begin{cases} |\mathbb{R} \times \mathbb{R}| \leq |\mathbb{R}| \\ |\mathbb{R} \times \mathbb{R}| \geq |\mathbb{R}| \end{cases}$  тогда по теореме *Кантора-Бернштейна* получаем, что  $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$

□

**Теорема** (о мощности произведения). *Если  $A, B$  - непустые множества и одно из них бесконечно, то:*

$$|A \times B| = \max\{|A|, |B|\}$$

24. Контигуум-гипотеза, теорема Гёделя-Коэна (без доказательства), обобщенная континуумгипотеза.

**Гипотеза** (Контигуум-гипотеза). Не существует множества  $A$  такого, что

$$|\mathbb{N}| < |A| < |\mathbb{R}|$$

**Теорема** (Теорема Гёделя-Коэна). *Если теория множеств ZFC непротиворечива, то континуум-гипотезу нельзя ни доказать, ни опровергнуть в рамках ZFC.*

**Гипотеза** (Обобщенная континуумгипотеза). Если множество  $B$  - бесконечно, то не существует множества  $A$  такого, что

$$|B| < |A| < |P(B)|$$

25. Ординалы, лемма об элементах ординала

**Определение** (Ординал). Ординалом называется транзитивное множество все элементы которого сравнимы относительно включения.

**Определение** (Транзитивное множество). Множество  $\alpha$  называется транзитивным, если из  $x \in \alpha$  и  $y \in x$  следует, что  $y \in \alpha$ .

**Лемма** (Лемма об элементах ординала). *Если  $\alpha$  - ординал и  $\beta \in \alpha$ , то  $\beta$  - ординал.*

*Доказательство.* Пусть  $x, y \in \beta$ . Тогда  $x, y \in \alpha$ . Следовательно,  $x$  и  $y$  равны или сравнимы относительно  $\in$ . Докажем, что  $\beta$  транзитивно. Пусть  $y \in x \in \beta$ . Тогда  $x \in \alpha$  и  $y \in \alpha$ . Возможны три случая:

- (a)  $\beta \in y$  Тогда получаем, что  $\beta \in y \in x \in \beta$  - противоречие.
- (b)  $\beta = y$  Получаем, что  $\beta \in x \in \beta$  - противоречие.
- (c)  $y \in \beta$ . Следовательно,  $\beta$  - ординал.

□

26. Лемма о порядке на ординалах, теорема о свойствах ординалов.

**Лемма** (о порядке на ординалах). Для любых ординалов  $\alpha, \beta$  равносильно:

- (a)  $\alpha \leq \beta$ ;
- (b)  $\alpha \subseteq \beta$ .

*Доказательство.* (a  $\Rightarrow$  b): если  $\alpha = \beta$ , то  $\alpha \subseteq \beta$ . Если же  $\alpha \in \beta$  и  $x \in \alpha$ , то  $x \in \beta$

(b  $\Rightarrow$  a): если  $\alpha = \beta$ , то  $\alpha \leq \beta$ . Предположим, что  $\alpha \subset \beta$ . Тогда  $\beta \setminus \alpha \neq \emptyset$ . По аксиоме регулярности  $\exists \gamma \in \beta \setminus \alpha$  т. ч.  $\gamma \cap (\beta \setminus \alpha) \neq \emptyset$ . Покажем, что  $\alpha = \gamma$ .

Если  $x \in \gamma$ , то  $x \in \beta$  и  $x \notin \beta \setminus \alpha$ , следовательно,  $x \in \alpha$ .

Если  $x \in \alpha$ , то  $x \in \beta$  и возможны три случая:

- (a)  $\gamma \in x$ . Тогда  $\gamma \in \alpha$ , противоречие.
- (b)  $\gamma = x$ . Вновь  $\gamma \in \alpha$ , противоречие.
- (c)  $x \in \gamma$ .

Получаем, что  $\alpha \in \beta$  и  $\alpha \leq \beta$ . □

**Теорема** (о свойствах ординалов). Класс ординалов с порядком  $\leq$  обладает свойствами в.у.м. - для любых ординалов  $\alpha, \beta, \gamma$  верно:

- (a)  $\alpha \leq \alpha$ ;
- (b)  $\alpha \leq \beta$  и  $\beta \leq \alpha \Rightarrow \alpha = \beta$ ;
- (c)  $\alpha \leq \beta$  и  $\beta \leq \gamma \Rightarrow \alpha \leq \gamma$ ;
- (d)  $\alpha \leq \beta$  или  $\beta \leq \alpha$ ;
- (e) в любом непустом множестве ординалов есть минимальный элемент.

*Доказательство.* (a) очевидно.

- (b) если  $\alpha \subseteq \beta$  и  $\beta \subseteq \alpha$ , то  $\alpha = \beta$ .
- (c) если  $\alpha \subseteq \beta$  и  $\beta \subseteq \gamma$ , то  $\alpha \subseteq \gamma$ .
- (d) пусть  $\delta = \alpha \cap \beta$ . Легко проверить, что  $\delta$  является ординалом.  
По лемме о порядке на ординалах  $\delta \leq \alpha$  и  $\delta \leq \beta$ . Если  $\delta = \alpha$  или  $\delta = \beta$ , утверждение доказано. Допустим, что  $\delta \neq \alpha, \beta$ . Тогда  $\delta \in \alpha, \delta \in \beta$  и  $\delta \in \alpha \cap \beta = \delta$ , противоречие.
- (e) пусть  $S$  - непустое множество ординалов. По аксиоме регулярности  $\exists \alpha \in S$ , т.ч.  $\alpha \cap S = \emptyset$ . Если  $\beta < \alpha$ , то  $\beta \in \alpha$  и  $\beta \notin S$ . Ясно, что  $\alpha$  - минимальный элемент в  $S$ .

□

27. Предложение о супремуме множества ординалов (без доказательства), теорема о связи в.у.м. и ординалов (без доказательства), предложение о принципе трансфинитной индукции (без доказательства).

**Предложение** (о супремуме множества ординалов). Пусть  $A$  - некоторое множество ординалов. Тогда  $\cup A$  - ординал, являющийся супремумом множества  $A$ .

**Теорема** (о связи в.у.м. и ординалов). Для любого в.у.м. существует единственный изоморфный ему ординал.

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

28. Сумма и произведение ординалов, кардинал, мощность множества.

**Предложение** (принцип трансфинитной рекурсии). Пусть существует условие, которое для каждого ординала  $\alpha$  однозначно задаёт некоторое множество  $f_\alpha$  в предположении, что при  $\beta < \alpha$

множества  $f_\beta$  уже определены. Тогда каждому ординалу  $\alpha$  действительно можно сопоставить множество  $f_\alpha$  так, чтобы указанная связь между  $f_\alpha$  и  $f_\beta$ ,  $\beta < \alpha$  выполнялась. При этом  $f_\alpha$  определено однозначно.

**Пример.** На классе ординалов можно задать операции  $+$  и  $\cdot$  так, что для любых ординалов  $\alpha, \beta$  будет верно:

- (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)  $\alpha + \lambda = \sup\{\alpha + \beta | \beta < \lambda\}$  и  $\alpha \cdot \lambda = \sup\{\alpha \cdot \beta | \beta < \lambda\}$ , если  $\lambda$  - предельный ординал.

*Доказательство.* Зафиксируем  $\gamma$  и определим  $\gamma + \alpha$  трансфинитной рекурсией по  $\alpha$ . Предположим, что при  $\beta < \alpha$  ординал  $\gamma + \beta$  уже определён. Определим  $\gamma + \alpha$ , просто повторив формулировку для трёх случаев:

- (a)  $\alpha = 0$ , тогда  $\gamma + \alpha = \gamma$ ;
- (b)  $\alpha = \beta + 1$ , тогда  $\gamma + \alpha = (\gamma + \beta) + 1$ ;
- (c)  $\alpha$  - предельный, тогда  $\gamma + \alpha = \sup\{\gamma + \beta | \beta < \alpha\}$ .

Произведение  $\gamma \cdot \alpha$  определяется аналогично.  $\square$

**Определение** (Кардинал). Ординал  $\mu$  называется *кардиналом*, если он не равномощен никакому строго меньшему ординалу.

**Определение** (Мощность множества). *Мощность* множества  $A$  - это единственный кардинал, равномощный  $A$ , т.е.  $|\mu_A| = |A|$ .

29. Алфавит ИВ, формула ИВ, подформула, представление формул ИВ.

Алфавит ИВ состоит из трёх частей:

- (а) Пророзициональные символы (Заглавные буквы латинского алфавита, возможно, с индексами);

(b) Логические связки:

- $\neg$  - отрицание
- $\wedge$  - конъюнкция
- $\vee$  - дизъюнкция
- $\rightarrow$  - импликация

(c) Вспомогательные символы (запятая „,”);

Формула исчисления высказываний:

- (a) Пропозициональная переменная (Она же - атомарная формула);
- (b) Если  $A$  и  $B$  - формулы, то  $\neg A$ ,  $(A \wedge B)$ ,  $(A \vee B)$ ,  $(A \Rightarrow B)$  - формулы.
- (c) Других формул нет.

**Определение** (Подформула формулы  $A$ ). Подформула формулы  $A$  - любое подслово слова  $A$ , которое само является формулой.

Пусть  $\Delta(n)$  - некоторое высказывание, которое для любого  $n$  принимает значение истина или ложь.

**Предложение** (о представлении формул исчисления высказываний). Всякая неатомарная формула исчисления высказываний единственным образом представима в одном из следующих видов:

- $\neg \Phi$ ;
- $(\Phi \wedge \Psi)$ ;
- $(\Phi \vee \Psi)$ ;
- $(\Phi \Rightarrow \Psi)$

Для некоторых  $\Phi$  и  $\Psi$ .

30. Принцип математической индукции и возвратной индукции.

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

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

*Доказательство.* Оба принципа индукции легко вытекают из следующего факта: в любом непустом множестве натуральных числе есть минимальный элемент. Покажем, как отсюда выводится возвратная индукция.

Допустим, что  $\Delta(n)$  ложно при некотором  $n$ . Рассмотрим множество  $A = \{n | \Delta(n) \text{ ложно}\}$ . Оно не пусто, следовательно, в нём есть минимальный элемент  $n_0$ . Тогда  $\Delta(n_0)$  ложно, а если  $n < n_0$ , то  $n \notin A$  и  $\Delta(n)$  истинно. Получаем, что  $\Delta(n_0)$  тоже истинно, противоречие.  $\square$

31. Алфавит ИС, секвенция, аксиома, правило вывода, дерево вывода, доказуемость, пример вывода.

### 1.3. Исчисление секвенций (ИС)

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

$$\begin{aligned}\Phi_1, \dots, \Phi_n \vdash \Psi & \quad (\text{«из } \Phi_1, \dots, \Phi_n \text{ выводится } \Psi\text{»}), \\ \Phi_1, \dots, \Phi_n & \vdash \quad (\text{«набор } \Phi_1, \dots, \Phi_n \text{ противоречив»}), \\ \vdash \Psi & \quad (\text{«}\Psi\text{ выводима»}),\end{aligned}$$

где  $\Phi_1, \dots, \Phi_n, \Psi$  — формулы,  $n \geq 1$ . При этом  $\Phi_1, \dots, \Phi_n$  называются *посылками* секвенции, а  $\Psi$  — её *заключением*.

*Исчисление секвенций* ИС задаётся аксиомами и правилами вывода. В приведённом ниже списке правила  $\Phi, \Psi, \Delta$  обозначают некоторые формулы,  $\Gamma, \Gamma_1, \Gamma_2$  — конечные наборы формул (может быть, пустые).

*Аксиомы ИС:* все секвенции вида  $\Phi \vdash \Phi$

*Правила вывода ИС:*

$$\frac{\Gamma \vdash \Phi; \quad \Gamma \vdash \Psi}{\Gamma \vdash (\Phi \& \Psi)} \text{ (введение \&),}$$

$$\frac{\Gamma \vdash (\Phi \& \Psi)}{\Gamma \vdash \Phi} \text{ (удаление \&),} \quad \frac{\Gamma \vdash (\Phi \& \Psi)}{\Gamma \vdash \Psi} \text{ (удаление \&),}$$

$$\frac{\Gamma \vdash \Phi}{\Gamma \vdash (\Phi \vee \Psi)} \text{ (введение \vee),} \quad \frac{\Gamma \vdash \Psi}{\Gamma \vdash (\Phi \vee \Psi)} \text{ (введение \vee),}$$

$$\frac{\Gamma \vdash (\Phi \vee \Psi); \quad \Gamma, \Phi \vdash \Delta; \quad \Gamma, \Psi \vdash \Delta}{\Gamma \vdash \Delta} \text{ (удаление \vee),}$$

$$\begin{array}{c}
\frac{\Gamma, \Phi \vdash \Psi}{\Gamma \vdash (\Phi \rightarrow \Psi)} \text{ (введение } \rightarrow), \quad \frac{\Gamma \vdash \Phi; \quad \Gamma \vdash (\Phi \rightarrow \Psi)}{\Gamma \vdash \Psi} \text{ (удаление } \rightarrow), \\
\frac{\Gamma, \Phi \vdash}{\Gamma \vdash \neg \Phi} \text{ (введение } \neg), \quad \frac{\Gamma \vdash}{\Gamma \vdash \Phi} \text{ (добавление заключения),} \\
\frac{\Gamma, \neg \Phi \vdash}{\Gamma \vdash \Phi} \text{ (удален. } \neg), \quad \frac{\Gamma \vdash \Phi; \quad \Gamma \vdash \neg \Phi}{\Gamma \vdash} \text{ (сведение к противоречию),} \\
\frac{\Gamma_1, \Phi, \Psi, \Gamma_2 \vdash \Delta}{\Gamma_1, \Psi, \Phi, \Gamma_2 \vdash \Delta} \text{ (перестановка),} \quad \frac{\Gamma \vdash \Phi}{\Gamma, \Psi \vdash \Phi} \text{ (добавление посылки).}
\end{array}$$

Определим теперь понятие *дерева вывода секвенции* в ИС:

1) аксиома является деревом вывода этой аксиомы;

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

Секвенция  $S$  доказуема в ИС, если существует дерево вывода этой секвенции.

**Пример.** Секвенции  $\Phi \vdash \neg \neg \Phi$  и  $\neg \neg \Phi \vdash \Phi$  доказуемы в ИС.

Построим два дерева вывода:			
$\Phi \vdash \Phi$	$\frac{\neg \Phi \vdash \neg \Phi}{\neg \Phi, \Phi \vdash \neg \Phi}$	$\frac{\neg \Phi \vdash \neg \Phi}{\neg \Phi, \neg \neg \Phi \vdash \neg \Phi}$	$\frac{\neg \neg \Phi \vdash \neg \neg \Phi}{\neg \neg \Phi, \neg \Phi \vdash}$
$\Phi, \neg \Phi \vdash \Phi;$	$\Phi, \neg \Phi \vdash \neg \Phi$	$\neg \neg \Phi, \neg \Phi \vdash \neg \Phi;$	$\neg \neg \Phi, \neg \Phi \vdash \neg \neg \Phi$
$\frac{\Phi, \neg \Phi \vdash}{\Phi \vdash \neg \neg \Phi}$	$\frac{\neg \neg \Phi, \neg \Phi \vdash}{\neg \neg \Phi \vdash \Phi}$		

32. Семантика ИВ: означивание, значение формулы при означивании, выполнимые, опровергимые, тождественно истинные, тождественно ложные формулы, примеры.

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

$P$	$Q$	$(P \& Q)$	$(P \vee Q)$	$(P \rightarrow Q)$
<b>и</b>	<b>и</b>	<b>и</b>	<b>и</b>	<b>и</b>
<b>и</b>	<b>л</b>	<b>л</b>	<b>и</b>	<b>л</b>
<b>л</b>	<b>и</b>	<b>л</b>	<b>и</b>	<b>и</b>
<b>л</b>	<b>л</b>	<b>л</b>	<b>л</b>	<b>и</b>

$P$	$\neg P$
<b>и</b>	<b>л</b>
<b>л</b>	<b>и</b>

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

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

- 1) если  $\Phi$  — переменная  $P$ , то  $\Phi[\gamma] = \gamma(P)$ ;
- 2) если  $\Phi = (\Phi_1 \circ \Phi_2)$ , где  $\circ \in \{\&, \vee, \rightarrow\}$ , то  $\Phi[\gamma] = \Phi_1[\gamma] \circ \Phi_2[\gamma]$  (см. таблицу выше);
- 3) если  $\Phi = \neg\Phi_1$ , то  $\Phi[\gamma] = \neg\Phi_1[\gamma]$ .

**Замечание.** Значение формулы  $\Phi$  при означивании  $\gamma$  зависит от значений только тех переменных, которые входят в  $\Phi$ .

Ясно, что, если не все переменные формулы  $\Phi$  получают значения при означивании  $\gamma$ , говорить о  $\Phi[\gamma]$ , вообще говоря, бессмысленно. Договоримся, что всякий раз, когда речь идёт о значении формулы при означивании  $\gamma$ , неявно подразумевается условие, что все её переменные обязательно получают какие-то значения.

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

Пусть фиксировано некоторое означивание. Секвенция вида  $\Phi_1, \dots, \Phi_n \vdash \Psi$  *истинна* при этом означивании, если  $\Psi$  истинна или хотя бы одна из  $\Phi_i$  ложна. Секвенция вида  $\Phi_1, \dots, \Phi_n \vdash$  *истинна*, если хотя бы одна из  $\Phi_i$  ложна. Секвенция  $\vdash \Psi$  *истинна*, если формула  $\Psi$  истинна.

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

**Теорема (о корректности ИС).** Любая доказуемая в ИС секвенция тождественно истинна.

Пусть  $S$  — доказуемая секвенция,  $\mathcal{D}$  — её дерево вывода. Индукцией по числу секвенций в  $\mathcal{D}$  докажем, что  $S$  тождественно истинна.

Предположим, что в  $\mathcal{D}$  одна секвенция. Тогда она совпадает с  $S$  и является аксиомой вида  $\Phi \vdash \Phi$ . Ясно, что она тождественно истинна.

Предположим, что в  $\mathcal{D}$   $n$  секвенций,  $n > 1$ , и для меньшего числа секвенций утверждение уже доказано. Дерево  $\mathcal{D}$  имеет вид  $\frac{\mathcal{D}_1; \dots; \mathcal{D}_k}{S}$ , где  $\mathcal{D}_i$  — деревья вывода секвенций  $S_i$ , а  $\frac{S_1; \dots; S_k}{S}$  — правило вывода. По предположению индукции все  $S_i$ ,  $i \leq k$ , тождественно истинны. Чтобы доказать, что  $S$  тождественно истинна, нужно перебрать все возможные правила вывода.

Рассмотрим случай, когда последнее правило в  $\mathcal{D}$  имеет вид  $\frac{\Gamma \vdash \Phi; \Gamma \vdash (\Phi \rightarrow \Psi)}{\Gamma \vdash \Psi}$ . Рассмотрим произвольное означивание и

покажем, что секвенция  $\Gamma \vdash \Psi$  истинна при этом означивании. Если одна из формул в  $\Gamma$  ложна, секвенция истинна. Предположим, что все формулы в  $\Gamma$  истинны. Тогда истинны формулы  $\Phi$  и  $(\Phi \rightarrow \Psi)$ . Ясно, что  $\Psi$  тоже истинна.

Остальные правила разбираются аналогично.

### 33. Тождественно истинные секвенции, теорема о корректности ИС.

**Определение** (Тождественно истинные секвенции). Секвенция называется тождественно истинной, если она истинна при любом означивании входящих в неё переменных.

**Теорема** (о корректности ИС). *Любая доказуемая в ИС секвенция тождественно истинна.*

*Доказательство.* Пусть  $S$  — доказуемая секвенция,  $D$  — её дерево вывода. Индукцией по числу секвенций в  $D$  докажем, что  $S$

тождественно истинна.

Предположим, что в  $D$  одна секвенция. Тогда она совпадает с  $S$  и является аксиомой вида  $\Phi \vdash \Phi$ . Ясно, что она тождественно истинна.

Предположим, что в  $D$   $n$  секвенций,  $n > 1$ , и для меньшего числа секвенций утверждение уже доказано. Дерево  $D$  имеет вид  $\frac{D_1; \dots; D_k}{S}$ , где  $D_i$  - деревья вывода секвенций  $S_i$ , а  $\frac{S_1; \dots; S_k}{S}$  - правило вывода. По предположению индукции все  $S_i$ ,  $i \leq k$ , тождественно истинны. Чтобы доказать, что  $S$  тождественно истинна, нужно перебрать все возможные правила вывода.

Рассмотрим случай, когда последнее правило в  $D$  имеет вид  $\frac{\Gamma \vdash \Phi; \Gamma \vdash (\Phi \rightarrow \Psi)}{\Gamma \vdash \Psi}$ . Рассмотрим произвольное означивание и покажем, что секвенция  $\Gamma \vdash \Psi$  истинна при этом означивании. Если одна из формул в  $\Gamma$  ложна, секвенция истинна. Предположим, все формулы в  $\Gamma$  истинны. Тогда истинны формулы  $\Phi$  и  $(\Phi \rightarrow \Psi)$ . Ясно, что  $\Psi$  тоже истинна.

Остальные правила разбираются аналогично.  $\square$

#### 34. Допустимые правила вывода, примеры.

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

$$\frac{\Gamma \vdash \Phi; \Gamma, \Phi \vdash \Psi}{\Gamma \vdash \Psi} \text{ (сечение), } \frac{\Gamma, \Phi \vdash \Delta; \Gamma, \Psi \vdash \Delta}{\Gamma, (\Phi \vee \Psi) \vdash \Delta} \text{ (разбор случаев),}$$

$$\frac{\Gamma \vdash (\Phi \rightarrow \Psi)}{\Gamma, \Phi \vdash \Psi} \text{ (удаление } \rightarrow\text{), } \frac{\Gamma, \Phi, \Psi \vdash \Delta}{\Gamma, (\Phi \& \Psi) \vdash \Delta} \text{ (соединение посылок),}$$

$$\frac{\Gamma, (\Phi \& \Psi) \vdash \Delta}{\Gamma, \Phi, \Psi \vdash \Delta} \text{ (разделение посылок), } \frac{\Gamma, \neg \Phi \vdash \neg \Psi}{\Gamma, \Psi \vdash \Phi}$$

$$\frac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg \Psi \vdash \neg \Phi} \text{ (контрапозиция), } \frac{\Gamma, \Phi \vdash \neg \Psi}{\Gamma, \Psi \vdash \neg \Phi} \text{ и } \frac{\Gamma, \neg \Phi \vdash \Psi}{\Gamma, \neg \Psi \vdash \Phi}$$

$$\frac{\Phi_1, \dots, \Phi_n \vdash \Psi}{\Delta_1, \dots, \Delta_m \vdash \Psi} \text{ и } \frac{\Phi_1, \dots, \Phi_n \vdash \Delta}{\Delta_1, \dots, \Delta_m \vdash \Delta} \text{ (структурные), где } \{\Phi_1, \dots, \Phi_n\} \subseteq \{\Delta_1, \dots, \Delta_m\}.$$

Докажем допустимость правила  $\frac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg\Psi \vdash \neg\Phi}$ , построив следующее дерево:

$$\frac{\frac{\frac{\Gamma, \Phi \vdash \Psi}{\Gamma, \Phi, \neg\Psi \vdash \Psi} \quad \frac{\neg\Psi \vdash \neg\Psi}{\vdots}}{\Gamma, \neg\Psi, \Phi \vdash \Psi; \quad \frac{\Gamma, \neg\Psi, \Phi \vdash \neg\Psi}{\Gamma, \neg\Psi, \Phi \vdash}}{\Gamma, \neg\Psi \vdash \neg\Phi}.$$

**Пример.** Доказуема секвенция  $\vdash \Phi \vee \neg\Phi$ .

Построим допустимое дерево вывода, используя новые правила:

$$\frac{\frac{\frac{\neg\Phi \vdash \neg\Phi}{\neg\Phi \vdash \Phi \vee \neg\Phi} \quad \frac{\Phi \vdash \Phi}{\Phi \vdash \Phi \vee \neg\Phi}}{\neg(\Phi \vee \neg\Phi) \vdash \Phi; \quad \frac{\neg(\Phi \vee \neg\Phi) \vdash \neg\Phi}{\neg(\Phi \vee \neg\Phi) \vdash}}{\neg(\Phi \vee \neg\Phi) \vdash}}{\vdash \Phi \vee \neg\Phi}.$$

### 35. Лемма об основных эквивалентностях, теорема о замене для ИВ.

**Лемма** (об основных эквивалентностях). Для любых формул  $\Phi, \Psi, \Phi', \Psi'$  и  $\Delta$  верно:

- (a)  $\Phi \equiv \Phi$ ;
- (b)  $\Phi \equiv \Psi \Rightarrow \Psi \equiv \Phi$ ;
- (c)  $\Phi \equiv \Psi, \Psi \equiv \Delta \Rightarrow \Phi \equiv \Delta$ ;
- (d)  $\Phi \equiv \Phi' \Rightarrow \neg\Phi \equiv \neg\Phi'$ ;
- (e)  $\Phi \equiv \Phi', \Psi \equiv \Psi' \Rightarrow (\Phi' \circ \Psi) \equiv (\Phi' \circ \Psi')$ , где  $\circ \in \{ \&, \vee, \rightarrow \}$ .

*Доказательство.* Пункты a), b) очевидны; c): предположим, что доказуемы секвенции  $\Phi \vdash \Psi, \Psi \vdash \Phi, \Psi \vdash \Delta, \Delta \vdash \Psi$ . Покажем доказуемость секвенции  $\Phi \vdash \Delta$ , построив допустимое дерево:

$$\frac{\Phi \vdash \Delta}{\Phi \vdash \Psi \quad \frac{\Phi, \Psi \vdash \Delta}{\Phi \vdash \Delta}}$$

Дерево для  $\Delta \vdash \Phi$  строится симметрично. Далее будем указывать только деревья.

d) :

$$\frac{\Phi' \vdash \Phi}{\neg \Phi \vdash \neg \Phi'}$$

e) : построим три дерева для случаев  $\circ = \rightarrow$ ,  $\circ = \&$  и  $\circ = \vee$ . Далее мы иногда будем пропускать структурные правила, соединяя несколько структурных правил с одним основным или допустимым в один переход дерева.

$$\frac{\Phi' \vdash \Phi; (\Phi \rightarrow \Psi) \vdash (\Phi \rightarrow \Psi)}{(\Phi \rightarrow \Psi), \Phi' \vdash \Psi} \quad \frac{\Psi \vdash \Psi'}{(\Phi \rightarrow \Psi), \Phi', \Psi \vdash \Psi'} \\ \frac{(\Phi \rightarrow \Psi), \Phi' \vdash \Psi'}{(\Phi \rightarrow \Psi) \vdash (\Phi' \rightarrow \Psi')}$$

$$\frac{\Phi \vdash \Phi'}{\Phi, \Psi \vdash \Phi'} \quad \frac{\Psi \vdash \Psi'}{\Phi, \Psi \vdash \Psi'} \quad \frac{\Phi \vdash \Phi'}{\Phi \vdash (\Phi' \vee \Psi')} \quad \frac{\Psi \vdash \Psi'}{\Psi \vdash (\Phi' \vee \Psi')} \\ \frac{(\Phi \& \Psi) \vdash \Phi'; (\Phi \& \Psi) \vdash \Psi'}{(\Phi \& \Psi) \vdash (\Phi' \& \Psi')} \quad \frac{(\Phi \vee \Psi) \vdash (\Phi' \vee \Psi')}{(\Phi \vee \Psi) \vdash (\Phi' \vee \Psi')}$$

□

**Теорема** (о замене для ИВ). *Пусть  $\Psi$  - подформула формулы  $\Phi$ . Обозначим через  $\Phi'$  результат замены  $\Psi$  на  $\Psi'$ . Если  $\Psi \equiv \Psi'$ , то и  $\Phi \equiv \Phi'$ .*

*Доказательство.* Индукцией по  $|\Phi|$  докажем, что  $\Phi'$  - формула, эквивалентная  $\Phi$ . Если  $\Phi = \Psi$ , то  $\Phi' = \Psi'$  и  $\Phi \equiv \Phi'$ . Поэтому будем рассматривать только случай  $\Phi \neq \Psi$ .

Пусть  $|\Phi| = 1$ . Тогда  $\Phi = \Psi$ , и этот случай уже рассмотрен.

Пусть  $|\Phi| > 1$ , и для формул меньшей длины утверждение уже доказано. Если  $\Phi = \neg\Phi_1$ , то  $\Psi$  - подформула  $\Phi_1$ , и по предположению индукции  $\Phi_1 \equiv \Phi'_1$ . Тогда  $\Phi = \neg\Phi_1 \equiv \neg\Phi'_1 = \Phi'$

Если  $\Phi = (\Phi_1 \circ \Phi_2)$ , где  $\circ \in \{\&, \vee, \rightarrow\}$ , то  $\Psi$  - подформула  $\Phi_1$  или  $\Phi_2$ . Предположим, что  $\Psi$  - подформула  $\Phi_1$ . По предположению индукции  $\Phi_1 \equiv \Phi'_1$ , отсюда  $\Phi = (\Phi_1 \circ \Phi_2) \equiv (\Phi'_1 \circ \Phi_2) = \Phi'$ .  $\square$

### 36. Д.н.ф., к.н.ф., теорема о приведении к д.н.ф. и к.н.ф.

*Элементарная конъюнкция* — формула вида  $(\Phi_1 \& \dots \& \Phi_n)$ ,  $n \geq 1$ , где каждая  $\Phi_i$  — переменная или отрицание переменной.

*Дизъюнктивная нормальная форма* (д.н.ф.) — формула вида  $(\Psi_1 \vee \dots \vee \Psi_k)$ ,  $k \geq 1$ , где каждая  $\Psi_i$  — элементарная конъюнкция.

*Элементарная дизъюнкция* — формула вида  $(\Phi_1 \vee \dots \vee \Phi_n)$ ,  $n \geq 1$ , где каждая  $\Phi_i$  — переменная или отрицание переменной.

*Конъюнктивная нормальная форма* (к.н.ф.) — формула вида  $(\Psi_1 \& \dots \& \Psi_k)$ ,  $k \geq 1$ , где каждая  $\Psi_i$  — элементарная дизъюнкция.

Формулы  $\Phi_i$  из этих определений назовём компонентами соответствующей элементарной конъюнкции или дизъюнкции.

**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.

Чтобы доказать теорему, укажем алгоритм приведения формулы к д.н.ф. и к.н.ф., состоящий из трёх шагов. На первом удалим из формул  $\rightarrow$ , на втором внесём  $\neg$  под скобки так, чтобы они стояли только перед переменными, и на третьем получим д.н.ф. (или к.н.ф.).

Сначала мы забудем про условие на переменные и покажем, как привести формулу  $\Phi$  к д.н.ф. Затем заметим, что набор переменных не меняется на всех шагах алгоритма. Небольшая модификация алгоритма даст нам приведение к к.н.ф.

**Лемма 1.** Любая формула  $\Phi$  синтаксически эквивалентна формуле  $\Phi'$ , не содержащей  $\rightarrow$ .

▷ Для доказательства нужно просто заменить все подформулы вида  $\Phi_1 \rightarrow \Phi_2$  на  $\neg\Phi_1 \vee \Phi_2$ , пользуясь соответствующей эквивалентностью. Формально это рассуждение требует индукции по  $|\Phi|$ . Если  $|\Phi| = 1$ , то  $\Phi$  — переменная, и  $\Phi' = \Phi$ .

Предположим, что  $|\Phi| > 1$ , и для формул меньшей длины утверждение доказано. Если  $\Phi = (\Phi_1 \circ \Phi_2)$ , где  $\circ \in \{\&, \vee\}$ , то по предположению индукции  $\Phi_i \equiv \Phi'_i$ , где  $\Phi'_i$  не содержат  $\rightarrow$  при  $i = 1, 2$ . Тогда  $\Phi \equiv (\Phi'_1 \circ \Phi'_2)$ . Если  $\Phi = (\Phi_1 \rightarrow \Phi_2)$ , то  $\Phi \equiv \neg\Phi_1 \vee \Phi_2 \equiv \neg\Phi'_1 \vee \Phi'_2$  по теореме о замене. Рассуждения для случая  $\Phi = \neg\Phi_1$  аналогичны.  $\square$

**Лемма 2.** Любая формула  $\Phi$  синтаксически эквивалентна формуле  $\Phi'$ , не содержащей  $\rightarrow$ , в которой  $\neg$  стоят только перед переменными.

▷ В силу леммы 1 можно считать, что в  $\Phi$  уже нет  $\rightarrow$ . Далее рассуждаем индукцией по  $|\Phi|$ . Если  $|\Phi| = 1$ , то  $\Phi$  — переменная, и  $\Phi' = \Phi$ .

Предположим, что  $|\Phi| > 1$ , и для формул меньшей длины утверждение доказано. Если  $\Phi = (\Phi_1 \circ \Phi_2)$ , где  $\circ \in \{\&, \vee\}$ , то рассуждаем точно так же, как в лемме 1. Предположим,

что  $\Phi = \neg\Psi$ . Далее нужно рассмотреть варианты строения  $\Psi$ . Если  $\Psi$  — переменная  $P$ , то  $\Phi = \neg P = \Phi'$ . Если  $\Psi = \neg\Psi_1$ , то  $\Phi = \neg\neg\Psi_1 \equiv \Psi_1$ . По предположению индукции  $\Psi_1 \equiv \Psi'_1$ , где  $\Psi'_1$  удовлетворяет условию леммы. Тогда  $\Phi \equiv \Psi'_1$ .

Рассмотрим случай  $\Psi = \Psi_1 \& \Psi_2$ . Тогда  $\Phi = \neg(\Psi_1 \& \Psi_2) \equiv \neg\Psi_1 \vee \neg\Psi_2$ . По предположению индукции существуют формулы  $\Delta_1$  и  $\Delta_2$ , удовлетворяющие условию леммы, т. ч.  $\neg\Psi_i \equiv \Delta_i$  при  $i = 1, 2$ . Тогда  $\Phi \equiv \Delta_1 \vee \Delta_2$ .

Случай  $\Psi = \Psi_1 \vee \Psi_2$  аналогичен.  $\square$

**Лемма 3.** Любая формула  $\Phi$  синтаксически эквивалентна некоторой д.н.ф.  $\Phi'$ .

$\triangleright$  В силу леммы 2 считаем, что в  $\Phi$  нет  $\rightarrow$ , а все  $\neg$  стоят перед переменными. Вновь используем индукцию по  $|\Phi|$ . Если  $|\Phi| = 1$ , то  $\Phi$  — переменная  $P$ , и  $\Phi' = \Phi$ .

Предположим, что  $|\Phi| > 1$ , и для формул меньшей длины утверждение доказано. Если  $\Phi = \neg\Phi_1$ , то  $\Phi_1$  — переменная  $P$ , и вновь  $\Phi' = \Phi$ .

Пусть  $\Phi = \Phi_1 \circ \Phi_2$ , где  $\circ \in \{\&, \vee\}$ . Тогда  $\Phi_t \equiv \Phi'_t$ , где  $\Phi'_t$  — д.н.ф.,  $t = 1, 2$ . Пусть  $\Phi'_1 = \Psi_1 \vee \dots \vee \Psi_n$  и  $\Phi'_2 = \Delta_1 \vee \dots \vee \Delta_k$ , где  $\Psi_i, \Delta_j$  — элементарные конъюнкции. Если  $\Phi = \Phi_1 \vee \Phi_2$ , то  $\Phi \equiv (\Psi_1 \vee \dots \vee \Psi_n) \vee (\Delta_1 \vee \dots \vee \Delta_k) \equiv (\Psi_1 \vee \dots \vee \Psi_n \vee \Delta_1 \vee \dots \vee \Delta_k)$  — это д.н.ф.

Если же  $\Phi = \Phi_1 \& \Phi_2$ , то  $\Phi \equiv (\Psi_1 \vee \dots \vee \Psi_n) \& (\Delta_1 \vee \dots \vee \Delta_k) \equiv \bigvee_{j=1}^k [(\Psi_1 \vee \dots \vee \Psi_n) \& \Delta_j] \equiv \bigvee_{j=1}^k [\bigvee_{i=1}^n (\Psi_i \& \Delta_j)]$ .

Поскольку  $(\Psi_i \& \Delta_j)$  эквивалентны элементарным конъюнкциям, ясно, что вся формула эквивалентна д.н.ф.  $\square$

Осталось заметить, что в формулировку каждой из этих лемм можно вставить указание на то, что набор переменных в  $\Phi$  и  $\Phi'$  совпадает, и доказательство останется верным.

Если мы хотим привести формулу  $\Phi$  к к.н.ф., леммы 1 и 2 остаются теми же самыми, а в лемме 3 нужно просто поменять дизъюнкции на конъюнкции и наоборот. При этом случай  $\Phi = \Phi_1 \& \Phi_2$  становится простым, а  $\Phi = \Phi_1 \vee \Phi_2$  — сложным.

37. Предложение о тождественно истинных к.н.ф.

### Предложение (о тождественно истинных к.н.ф.).

К.н.ф.  $\Phi$  тождественно истинна тогда и только тогда, когда каждая её элементарная дизъюнкция содержит компоненты  $P$  и  $\neg P$  для некоторой переменной  $P$ .

Пусть  $\Phi$  — к.н.ф. и  $\Phi = (\Psi_1 \& \dots \& \Psi_n)$ , где  $\Psi_i$  — элементарные дизъюнкции. Если фиксировано означивание  $\gamma$ , то

$$\Phi[\gamma] = \text{и} \Leftrightarrow \forall i \leq n \quad \Psi_i[\gamma] = \text{и}.$$

Это почти очевидно и формально может быть доказано индукцией по  $n$ . Если, в свою очередь,  $\Psi_i = (\Delta_1 \vee \dots \vee \Delta_k)$ , то

$$\Psi_i[\gamma] = \text{и} \Leftrightarrow \exists j \leq k \quad \Delta_j[\gamma] = \text{и}.$$

Переход ( $\Leftarrow$ ) очевиден: если  $\Psi_i = (\dots \vee P \vee \dots \vee \neg P \vee \dots)$ , то  $\Psi_i$  истинна при любом означивании. Получаем, что  $\Phi$  тождественно истинна.

( $\Rightarrow$ ): если  $\Phi$  тождественно истинна, то все  $\Psi_i$ ,  $i \leq n$ , тоже тождественно истинны. Зафиксируем  $i \leq n$  и покажем, что  $\Psi_i$  содержит  $P$  и  $\neg P$ . Допустим, что это не так. Пусть в  $\Psi_i$  входят переменные  $P_1, \dots, P_m$ . Зададим их означивание: если  $j \leq m$  и  $P_j$  входит в  $\Psi_i$  без отрицания, положим  $P_j = \text{л}$ , а если входит с отрицанием, то  $P_j = \text{и}$ . Это можно сделать, так как мы предположили, что  $P_j$  не может входить одновременно с отрицанием и без него. Ясно, что при этом  $\Psi_i$  станет ложна,  $\uparrow\downarrow$ .

### 38. Теорема о полноте ИС.

**Теорема (о полноте ИС).** Секвенция доказуема в ИС тогда и только тогда, когда она тождественно истинна.

Переход ( $\Rightarrow$ ) был доказан в теореме о корректности ИС. Покажем, что любая тождественно истинная секвенция доказуема. Доказательство разбивается на несколько случаев.

**Случай 1.** Рассмотрим тождественно истинную секвенцию вида  $\vdash \Psi$ . Тогда формула  $\Psi$  тождественно истинна. По теореме о приведении к к.н.ф. существует к.н.ф.  $\Psi'$  т. ч.  $\Psi \equiv \Psi'$ .

Поскольку секвенция  $\Psi \vdash \Psi'$  доказуема, она тождественно истинна по теореме о корректности. Получаем, что  $\Psi'$  тоже тождественно истинна.

Пусть  $\Psi' = (\Psi_1 \& \dots \& \Psi_n)$ , где  $\Psi_i$  — элементарные дизъюнкции. По только что доказанному каждая  $\Psi_i$  содержит  $P$  и  $\neg P$ . Используя коммутативность и ассоциативность  $\vee$ , найдём формулу  $\Delta_i$  т. ч.  $\Psi_i \equiv (P \vee \neg P) \vee \Delta_i$ . Поскольку секвенция  $\vdash P \vee \neg P$  была доказана ранее, допустимое дерево

$$\frac{\vdash P \vee \neg P}{\frac{\vdash (P \vee \neg P) \vee \Delta_i; \quad (P \vee \neg P) \vee \Delta_i \vdash \Psi_i}{\vdash \Psi_i}}$$

показывает, что секвенция  $\vdash \Psi_i$  доказуема при  $i \leq n$ . Дерево

$$\frac{\begin{array}{c} \vdash \Psi_1; \quad \vdash \Psi_2 \\ \vdash (\Psi_1 \& \Psi_2); \quad \vdash \Psi_3 \\ \vdash (\Psi_1 \& \Psi_2) \& \Psi_3 \\ \vdots & \vdash \Psi_n \\ \hline \vdash \Psi' \end{array}}{\vdash \Psi'}$$

даёт доказуемость  $\vdash \Psi'$ , а дерево

$$\frac{\vdash \Psi'; \quad \Psi' \vdash \Psi}{\vdash \Psi}$$

даёт доказуемость  $\vdash \Psi$ .

**Случай 2.** Рассмотрим тождественно истинную секвенцию вида  $\Phi_1, \dots, \Phi_n \vdash \Psi$ . Тогда формула  $(\Phi_1 \& \dots \& \Phi_n) \rightarrow \Psi$  тождественно истинна, и секвенция  $\vdash (\Phi_1 \& \dots \& \Phi_n) \rightarrow \Psi$  доказуема по случаю 1. Допустимое дерево

$$\frac{\begin{array}{c} \vdash (\Phi_1 \& \dots \& \Phi_n) \rightarrow \Psi \\ \Phi_1 \& \dots \& \Phi_n \vdash \Psi \\ \vdots \\ \hline \Phi_1, \dots, \Phi_n \vdash \Psi \end{array}}{\vdash \Phi_1, \dots, \Phi_n \vdash \Psi}$$

завершает доказательство.

**Случай 3.** Рассмотрим теперь тождественно истинную секвенцию вида  $\Phi_1, \dots, \Phi_n \vdash$ . Ясно, что секвенции  $\Phi_1, \dots, \Phi_n \vdash P$  и  $\Phi_1, \dots, \Phi_n \vdash \neg P$  тоже тождественно истинны, следовательно, доказуемы. Строим допустимое дерево:

$$\frac{\Phi_1, \dots, \Phi_n \vdash P; \quad \Phi_1, \dots, \Phi_n \vdash \neg P}{\Phi_1, \dots, \Phi_n \vdash}.$$

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

**Следствие.**  $\Phi \equiv \Psi$  тогда и только тогда, когда  $\Phi \sim \Psi$ .

( $\Rightarrow$ ): если секвенции  $\Phi \vdash \Psi$  и  $\Psi \vdash \Phi$  доказуемы, то они тождественно истинны. Ясно, что если  $\Phi$  при некотором означивании истинна, то истинна и  $\Psi$ , и наоборот.

( $\Leftarrow$ ): если  $\Phi \sim \Psi$ , то секвенции  $\Phi \vdash \Psi$  и  $\Psi \vdash \Phi$  тождественно истинны, следовательно, доказуемы.

В силу этого далее будем говорить просто про *эквивалентные формулы*.

### 39. Совершенные нормальные формы, теорема о совершенных нормальных формах.

*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 один раз;
- 2) любые две её элементарные конъюнкции *существенно различаются*, т. е. одна из них содержит компоненту  $P$ , а другая  $\neg P$  для некоторой переменной  $P$ .

*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 один раз;
- 2) любые две элементарные дизъюнкции существенно различаются.

### Теорема (о совершенных нормальных формах).

- а) Любая не тождественно ложная формула эквивалентна некоторой с.д.н.ф., содержащей тот же набор переменных, что и она сама.
- б) Любая не тождественно истинная формула эквивалентна некоторой с.к.н.ф., содержащей тот же набор переменных, что и она сама.
- с) Нормальная форма в а) и б) единственна с точностью до перестановки элементарных конъюнкций (дизъюнкций) и их компонент.

Будем работать с семантической эквивалентностью. а): пусть  $\Phi$  — не тождественно ложная формула от переменных  $P_1, \dots, P_n$ . Рассмотрим множество всех значений переменных, при которых  $\Phi$  истинна, т. е. множество  $I =$

$$\{\langle \alpha_1, \dots, \alpha_n \rangle \mid \alpha_i \in \{\text{и}, \text{л}\} \text{ и } \Phi = \text{и} \text{ при } P_1 = \alpha_1, \dots, P_n = \alpha_n\}.$$

По условию оно непусто. Обозначим через  $P^{\text{и}}$  формулу  $P$ , а через  $P^{\text{л}}$  — формулу  $\neg P$ . Если  $\alpha \in \{\text{и}, \text{л}\}$  и  $\gamma$  — означивание, то ясно, что  $P^\alpha[\gamma] = \text{и} \Leftrightarrow \gamma(P) = \alpha$ . Положим

$$\Psi = \bigvee_{\langle \alpha_1, \dots, \alpha_n \rangle \in I} (P_1^{\alpha_1} \& P_2^{\alpha_2} \& \dots \& P_n^{\alpha_n}).$$

Легко проверить, что  $\Psi$  — с.д.н.ф. Покажем, что  $\Phi \sim \Psi$ . Зададим означивание  $\gamma$ . Тогда  $\Psi[\gamma] = \text{и} \Leftrightarrow$   
 существует  $\langle \alpha_1, \dots, \alpha_n \rangle \in I$  т. ч.  $(P_1^{\alpha_1} \& \dots \& P_n^{\alpha_n})[\gamma] = \text{и} \Leftrightarrow$   
 существует  $\langle \alpha_1, \dots, \alpha_n \rangle \in I$  т. ч.  $P_1^{\alpha_1}[\gamma] = \text{и}, \dots, P_n^{\alpha_n}[\gamma] = \text{и} \Leftrightarrow$   
 существует  $\langle \alpha_1, \dots, \alpha_n \rangle \in I$  т. ч.  $\gamma(P_1) = \alpha_1, \dots, \gamma(P_n) = \alpha_n \Leftrightarrow$   
 $\Phi[\gamma] = \text{и}$ .

Докажем теперь единственность. Пусть  $\Psi'$  — другая с.д.н.ф. от переменных  $P_1, \dots, P_n$  т. ч.  $\Psi' \sim \Phi$ . Легко понять, что с точностью до перестановки  $\Psi'$  имеет вид

$$\bigvee_{\langle \alpha_1, \dots, \alpha_n \rangle \in I'} (P_1^{\alpha_1} \& P_2^{\alpha_2} \& \dots \& P_n^{\alpha_n})$$

для некоторого множества  $I'$ . Пусть  $\gamma$  — произвольное означивание. Повторяя предыдущее рассуждение, получаем, что

$$\Psi'[\gamma] = \text{и} \Leftrightarrow \langle \gamma(P_1), \dots, \gamma(P_n) \rangle \in I'.$$

Кроме того,  $\Psi'[\gamma] = \text{и} \Leftrightarrow \Phi[\gamma] = \text{и} \Leftrightarrow \langle \gamma(P_1), \dots, \gamma(P_n) \rangle \in I$ . Поскольку значения  $\gamma(P_i)$  могут быть выбраны любыми, получаем, что  $I' = I$ .

b): пусть  $\Phi$  — не тождественно истинная формула от тех же переменных. Тогда  $\neg\Phi$  не тождественно ложна и по уже доказанному

$$\neg\Phi \sim \bigvee_{\langle \alpha_1, \dots, \alpha_n \rangle \in I} (P_1^{\alpha_1} \& P_2^{\alpha_2} \& \dots \& P_n^{\alpha_n}).$$

Пользуясь эквивалентностями, легко получить, что

$$\Phi \sim \neg\neg\Phi \sim \bigwedge_{\langle \alpha_1, \dots, \alpha_n \rangle \in I} (P_1^{\bar{\alpha}_1} \vee P_2^{\bar{\alpha}_2} \vee \dots \vee P_n^{\bar{\alpha}_n}),$$

где  $\bar{\text{и}} = \text{л}$  и  $\bar{\text{л}} = \text{и}$ . Это искомая с.к.н.ф.

Единственность: пусть  $\Psi'$  — другая с.к.н.ф. для  $\Phi$ . С точностью до перестановки  $\Psi'$  имеет вид

$$\bigwedge_{\langle \alpha_1, \dots, \alpha_n \rangle \in I'} (P_1^{\bar{\alpha}_1} \vee P_2^{\bar{\alpha}_2} \vee \dots \vee P_n^{\bar{\alpha}_n}).$$

Тогда

$$\neg\Phi \sim \neg\Psi' \sim \bigvee_{\langle \alpha_1, \dots, \alpha_n \rangle \in I'} (P_1^{\alpha_1} \& P_2^{\alpha_2} \& \dots \& P_n^{\alpha_n}).$$

По доказанному выше  $I = I'$ .

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

С.д.н.ф. не может быть тождественно ложной: она содержит хотя бы одну элементарную конъюнкцию  $(P_1^{\alpha_1} \& \dots \& P_n^{\alpha_n})$ , где  $\alpha_i \in \{\text{и}, \text{л}\}$ , и при означивании  $P_1 = \alpha_1, \dots, P_n = \alpha_n$  эта конъюнкция и вся с.д.н.ф. будут истинны. Аналогично можно показать, что с.к.н.ф. не может быть тождественно истинной.

40. Гильбертовское исчисление высказываний: аксиоматика, выводимость, примеры выводов.

## Гильбертовское исчисление высказываний

### Аксиоматика:

- 1)  $(\phi \rightarrow (\psi \rightarrow \phi))$
- 2)  $((\phi \rightarrow \psi) \rightarrow ((\phi \rightarrow (\psi \rightarrow \chi)) \rightarrow (\phi \rightarrow \chi)))$
- 3)  $((\phi \& \psi) \rightarrow \phi)$
- 4)  $((\phi \& \psi) \rightarrow \psi)$
- 5.1)  $(\phi \rightarrow (\psi \rightarrow (\phi \& \psi)))$

5.2)  $((\phi \rightarrow \psi) \rightarrow ((\phi \rightarrow \chi) \rightarrow (\phi \rightarrow (\psi \ \& \ \chi))))$

6)  $(\phi \rightarrow (\phi \vee \psi))$

7)  $(\psi \rightarrow (\phi \vee \psi))$

8)  $((\phi \rightarrow \psi) \rightarrow ((\chi \rightarrow \psi) \rightarrow ((\phi \vee \chi) \rightarrow \psi)))$

9.1)  $((\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \neg\phi))$

9.2)  $((\phi \rightarrow \psi) \rightarrow ((\phi \rightarrow \neg\psi) \rightarrow \neg\phi))$

10)  $\neg\neg\phi \rightarrow \phi$

**Правило modes ponens:**  $\frac{\phi, (\phi \rightarrow \psi)}{\psi}$

**Определение** (Вывод формулы в ГИВ). Выводом формулы  $\phi$  в ГИВ называется последовательностью формул, каждой из которых является либо аксиомой, либо получена из предыдущего по правилу modes ponens.

Последнее из вывода есть вывод  $\phi$

**Теорема.** Выводом  $\phi$  из  $\Gamma$ , называется последовательность формул, каждая из которых либо является аксиомой, либо принадлежащая  $\Gamma$ , либо следует из двух предыдущих по правилу modes ponens.

Последняя формула в последовательности это  $\phi$

#### 41. Теорема о дедукции.

**Теорема** (о дедукции). Если  $\Gamma, A \triangleright B$ , то  $\Gamma \triangleright A \rightarrow B$

*Доказательство.* Пусть  $B_1, \dots, B_n = B$  - вывод  $B$  из  $\Gamma, A$

По индукции докажем, что  $\forall i \Gamma \triangleright A \rightarrow B_i$

•  $B_i \in \Gamma$ :

1)  $B_i \in \Gamma$  2)  $(B_i \rightarrow (A \rightarrow B_i))$  - Аксиома №1 3)  $A \rightarrow B_i$  - mp  
1,2

•  $B_i$  - следствие из  $B_j$  и  $B_j \rightarrow B_i$  по mp:

По ИГ :  $\Gamma \triangleright (A \rightarrow B_j)$ ,  $\Gamma \triangleright (B_j \rightarrow B_i)$

.

.

.

n)  $(A \rightarrow B_j)$

m)  $(A \rightarrow (B_j \rightarrow B_i))$

m+1)  $((A \rightarrow B_j) \rightarrow ((A \rightarrow (B_j \rightarrow B_i)) \rightarrow (A \rightarrow B_i)))$  -

Аксиома №2

m+2)  $(((A \rightarrow (B_j \rightarrow B_i)) \rightarrow (A \rightarrow B_i)) \rightarrow (A \rightarrow B_i))$  - mp n,m+1

m+3)  $(A \rightarrow B_i)$  - mp m, m+2

□

42. Связь гильбертовского и секвенциального исчисления. ?????