

## Содержание

<b>1. Математическая логика .....</b>	<b>2</b>
1.1. Включение и равенство множеств. Основные способы задания множеств. Операции и основные тождества алгебры множеств. Упорядоченные пары и декартово произведение. ....	2
1.2. Бинарные отношения; композиция и обращение. Функции. Равномощность и вложение. Теорема Кантора; тождества в смысле равномощности для множеств $\mathbb{N} \times \mathbb{N}$ , $(A \times B)^C$ и $C^{B^A}$ . Теорема Кантора–Бернштейна–Шрёдера (без доказательства) с примером применения. ....	4
1.3. Частичные порядки. Связь строгих и нестрогих порядков. Максимальные и минимальные, наибольшие и наименьшие элементы, верхние и нижние грани, супремум и инфимум. Изоморфизм порядков. Отношения эквивалентности, фактор-множество. Разбиения и отношения эквивалентности. ....	7
1.4. Принципы математической индукции, «сильной» индукции и наименьшего числа. Их равносильность. Теорема о рекурсии в различных формах (без доказательства). Принцип Дирихле (с доказательством). Основные теоремы о мощностях конечных и счетных множеств (про подмножество, объединение, произведение, степень и пр.; доказательства как доп. вопросы). ....	10
1.5. Вполне упорядоченные множества (ВУМ). Теорема о строении элементов ВУМ. Начальные отрезки ВУМ и их свойства; теорема о сравнении ВУМ (доказательство как доп. вопрос). Сложение и умножение ВУМ; свойства этих операций..	14
1.6. Аксиома выбора (с любой мотивировочной задачей — например, о существовании правой обратной у сюръекции). Лемма Цорна и теорема Цермело (без доказательства). Любой пример применения. Теоремы о мощностях бесконечных множеств, вытекающие из них (доказательства как дополнительные вопросы) .	16

# ДМ Гос (ИВТ: Матлог + ДС)

**Disclaymer:** доверять этому конспекту или нет выбирайте сами

## 1. Математическая логика

### 1.1. Включение и равенство множеств. Основные способы задания множеств. Операции и основные тождества алгебры множеств. Упорядоченные пары и декартово произведение.

**Определение 1.1.1:** Множество  $A$  **включено**  $\subseteq$  в множество  $B \Leftrightarrow$   

$$x \in A \Rightarrow x \in B$$

**Определение 1.1.2:** Множество  $A$  **равно** множеству  $B \Leftrightarrow$   

$$x \in A \Leftrightarrow x \in B$$

**Лемма 1.1.1** (Свойства включения):

- $A \subseteq A$
- $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$
- $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

**Лемма 1.1.2** (Свойства равенства):

- $A = A$
- $A = B \wedge B = C \Rightarrow A = C$
- $A = B \Rightarrow B = A$

**Замечание 1.1.1** (Основные способы задания множеств):

- Назвать все его элементы, когда число этих элементов конечно и все они уже определены
- Выделение всех элементов какого-нибудь уже определённого множества  $A$ , обладающих некоторым точно определённым свойством  $\varphi$
- Рассмотреть **множество всех подмножеств** множества  $A$ . Такое множество обозначают выражением  $\mathcal{P}(A)$
- Располагая каким-нибудь множеством  $X$ , рассмотреть его объединение, обозначаемое  $\cup X$  и состоящее из всевозможных элементов множеств, принадлежащих  $X$

**Определение 1.1.3:** Объединением множеств  $A$  и  $B$  называется множество  $A \cup B$ :

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$

**Определение 1.1.4:** Пересечением множеств  $A$  и  $B$  называется множество  $A \cap B$ :

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$$

**Определение 1.1.5:** Разностью множеств  $A$  и  $B$  называется множество  $A \setminus B$ :

$$x \in A \setminus B \Leftrightarrow x \in A \wedge x \notin B$$

**Определение 1.1.6:** Нередко все рассматриваемые множества оказываются подмножествами какого-нибудь множества  $U$ .

Такое  $U$  называют тогда **универсумом**.

Для каждого подмножества  $A$  заданного универсума  $U$  определено **дополнение**

$$\bar{A} = U \setminus A$$

**Теорема 1.1.1** (Основные тождества алгебры множеств):  $\forall A, B, C$  и любого включающего их универсума  $U$  верно:

- $A \cap B = B \cap A; A \cup B = B \cup A$
- $(A \cap B) \cap C = A \cap (B \cap C); (A \cup B) \cup C = A \cup (B \cup C)$
- $A \cap A = A; A \cup A = A$
- $\overline{A \cap (A \cup B)} = A; A \cup (A \cap B) = A$
- $\overline{\bar{A}} = A$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C); A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $\overline{A \cap B} = \bar{A} \cup \bar{B}; \overline{A \cup B} = \bar{A} \cap \bar{B}$
- $A \cap \emptyset = \emptyset; A \cup \emptyset = A; A \cap U = A; A \cup U = U; \bar{\emptyset} = U; \bar{U} = \emptyset$
- $A \cap \bar{A} = \emptyset; A \cup \bar{A} = U$

**Определение 1.1.7:** Для произвольных множеств  $a$  и  $b$  символом  $(a, b)$  обозначают множество  $\{\{a\}, \{b, c\}\}$ , называемое **упорядоченной парой** множеств  $a$  и  $b$

**Определение 1.1.8:** Декартовым (или прямым) произведением множеств  $A$  и  $B$  называется множество

$$A \times B = \{z \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \exists a \in A : \exists b \in B : z = (a, b)\}$$

## 1.2. Бинарные отношения; композиция и обращение. Функции. Равномощность и вложение. Теорема Кантора; тождества в смысле равномощности для множеств $\mathbb{N} \times \mathbb{N}$ , $(A \times B)^C$ и $C^{B^A}$ . Теорема Кантора–Бернштейна–Шрёдера (без доказательства) с примером применения.

**Определение 1.2.1:** Множество  $R$  называется **бинарным отношением**, если каждый его элемент является упорядоченной парой множеств.

**Определение 1.2.2:** Назовём **областью определения** отношения  $R$  множество

$$\text{dom } R = \{a \in \cup \cup R \mid \exists b : (a, b) \in R\}$$

и **областью значений** отношения  $R$  – множество

$$\text{rng } R = \{b \in \cup \cup R \mid \exists a : (a, b) \in R\}$$

**Определение 1.2.3:** Для любых отношений  $P$  и  $Q$  определена **композиция** отношений  $P$  и  $Q$ :

$$Q \circ P = \{(a, c) \in \text{dom } P \times \text{rng } Q \mid \exists b : (a, b) \in P \wedge (b, c) \in Q\}$$

**Определение 1.2.4:** Пусть  $R$  – бинарное отношение. **Обратным отношением** к  $R$  называется отношение

$$R^{-1} = \{(b, a) \in \text{rng } R \times \text{dom } R \mid (a, b) \in R\}$$

**Определение 1.2.5:** Пусть  $R$  – бинарное отношение и  $X$  – некоторое множество.

Мы называем **образом под действием отношения  $R$  множества  $X$**  множество

$$R[X] = \{b \in \text{rng } R \mid \exists a \in X : aRb\}$$

**Определение 1.2.6:** Бинарное отношение  $R$  называется:

- **Функциональным**, если  $\forall x : \forall y : \forall z : xRy \wedge xRz \Rightarrow y = z$
- **Инъективным**, если  $\forall x : \forall y : \forall z : xRy \wedge zRy \Rightarrow x = z$
- **Тотальным** для множества  $Z$ , если  $\forall x \in Z : \exists y : (x, y) \in R$
- **Сюръективным** для множества  $Z$ , если  $\forall y \in Z : \exists x : (x, y) \in R$

**Определение 1.2.7:** Функциональное отношение  $f \subseteq A \times B$  называется **частичной функцией на множестве  $A$  во множество  $B$** . В таком случае пишем  $f : A \xrightarrow{p} B$ .

Если, помимо того, отношение является тотальным для множества  $A$ , то оно называется **функцией на множестве  $A$  во множество  $B$** . В таком случае пишем  $f : A \rightarrow B$ .

**Определение 1.2.8:** Множество

$$\{f \in \mathcal{P}(A \times B) \mid f : A \rightarrow B\}$$

всех функций из  $A$  в  $B$  обозначается символом  $B^A$

**Определение 1.2.9:** Если функция  $f : A \rightarrow B$  инъективна, она называется **инъекцией из  $A$  в  $B$** .

**Определение 1.2.10:** Если функция  $f : A \rightarrow B$  сюръективна, она называется **сюръекцией из  $A$  в  $B$** .

**Определение 1.2.11:** Если функция  $f : A \rightarrow B$  инъективна и сюръективна, она называется **биекцией из  $A$  в  $B$** .

**Определение 1.2.12:** Будем писать  $A \stackrel{p}{\sim} B$ , если  $f : A \rightarrow B$  есть биекция.

Скажем, что множество  $A$  **равномощно** множеству  $B$ , если существует  $f$ , такая что  $A \stackrel{f}{\sim} B$ . Тогда пишем  $A \sim B$ .

**Определение 1.2.13:** Множество  $A$  **не превосходит по мощности (вкладывается во)** множество  $B$ , если существует инъекция  $f : A \rightarrow B$ . Тогда пишем  $A \stackrel{f}{\lesssim} B$  и  $A \lesssim B$

**Теорема 1.2.1 (Кантора):** Ни для какого множества  $A$  невозможно  $\mathcal{P}(A) \lesssim A$

*Доказательство:* Пусть не так. Рассмотрим произвольную инъекцию  $f : \mathcal{P}(A) \rightarrow A$ . Положим

$$Y = \{a \in A \mid \forall X \in \mathcal{P}(A) : a = f(X) \Rightarrow a \notin X\}$$

Очевидно,  $Y \in \mathcal{P}(A)$ . По определению  $Y$  следует, что  $f(Y) \notin Y$ .

Рассмотрим произвольное  $X \in \mathcal{P}(A) : f(Y) = f(X)$ . В силу инъективности  $f$  имеем  $X = Y$ . Но тогда  $f(Y) \notin X$  для всех таких  $X$ .

По определению множества  $Y$  получаем  $f(Y) \in Y$ . Противоречие.  $\square$

**Утверждение 1.2.1:** Убедимся, что

$$\mathbb{N}^2 \sim \mathbb{N}$$

*Доказательство:* Положим

$$\forall (m, n) \in \mathbb{N}^2 : f(m, n) = 2^m(2n + 1) - 1$$

Докажем инъективность, если  $f(m, n) = f(m', n')$ , то

$$2^m(2n + 1) = 2^{m'}(2n' + 1)$$

Допустим, что  $m \neq m'$  и БОО  $m < m'$ . Тогда

$$2n + 1 = 2^{m'-m}(2n' + 1)$$

Причём второе число чётно, а первое – нет. Противоречие показывает, что  $m = m'$ , но тогда  $2n + 1 = 2n' + 1 \Rightarrow n' = n$ . Инъективность доказана.

Докажем сюръективность. Пусть некоторое положительное натуральное число не имеет вида  $2^m(2n + 1)$ . Тогда найдётся наименьшее такое число  $k$ .

Это число чётно (иначе оно имело бы вид  $2^0(2n + 1)$ ). Следовательно  $k = 2k'$ . Но  $k' < k$ , а, значит,

$$k' = 2^{m'}(2n' + 1) \text{ для некоторых } m', n' \in \mathbb{N}.$$

Но тогда  $k = 2^{m'+1}(2n' + 1)$  – противоречие. Сюръективность, а значит и биективность доказана  $\square$

**Утверждение 1.2.2:**

$$(A \times B)^C \sim A^C \times B^C$$

*Доказательство:* Рассмотрим функции-проекторы  $\pi_1 : A \times B \rightarrow A$  и  $\pi_2 : A \times B \rightarrow B$ .

Положим теперь  $\psi : f \mapsto (\pi_1 \circ f, \pi_2 \circ f)$  для всех  $f \in (A \times B)^C$ .

Это отображения является биекцией, доказывается очевидной проверкой инъективности и сюръективности.  $\square$

**Утверждение 1.2.3:**

$$C^{B^A} \sim C^{A \times B}$$

*Доказательство:* Для всех  $f \in C^{B^A}$  и  $z \in A \times B$  положим

$$\psi(f) : z \mapsto (f(\pi_1(z)))(\pi_2(z))$$

Это отображения является биекцией, доказывается очевидной проверкой инъективности и сюръективности.  $\square$

**Теорема 1.2.2** (Кантора-Шрёдера-Бернштейна): Для любых множеств  $A$  и  $B$ , если  $A \lesssim B$  и  $B \lesssim A$ , то  $A \sim B$ .

*Пример:* Очевидно, что  $\mathbb{N} \lesssim \mathbb{Q}$ .

С другой стороны,  $\mathbb{Q} \lesssim \mathbb{N}^3$ : каждое положительное рациональное число  $q$  однозначно представляется несократимой дробью  $\frac{m}{n}$ , где  $m, n \in \mathbb{N}$ . Тогда отображение

$$f(q) = \begin{cases} (0,1,0), & q=0 \\ (m,n,0), & q>0 \\ (m,n,1), & q<0 \end{cases}$$

является искомой инъекцией. Осталось вспомнить, что  $\mathbb{N}^3 = \mathbb{N}^2 \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ .

Показали инъекцию в обе стороны, а значит по КШБ  $\mathbb{Q} \sim \mathbb{N}$ .

### 1.3. Частичные порядки. Связь строгих и нестрогих порядков. Максимальные и минимальные, наибольшие и наименьшие элементы, верхние и нижние грани, супремум и инфимум. Изоморфизм порядков. Отношения эквивалентности, фактор-множество. Разбиения и отношения эквивалентности.

**Определение 1.3.1:** Бинарное отношение  $R$  называется

- **Рефлексивным** для множества  $Z$ , если  $\forall x \in Z : (x, x) \in R$
- **Иррефлексивным**, если  $\forall x : (x, x) \notin R$
- **Симметричным**, если  $\forall x : \forall y : xRy \Rightarrow yRx$
- **Антисимметричным**, если  $\forall x : \forall y : xRy \wedge yRx \Rightarrow x = y$
- **Транзитивным**, если  $\forall x : \forall y : \forall z : xRy \wedge yRz \Rightarrow xRz$

**Лемма 1.3.1:** Отношение  $R \subseteq A^2$ :

- Рефлексивно  $\Leftrightarrow \text{id}_A \subseteq R$
- Иррефлексивно  $\Leftrightarrow \text{id}_A \cap R = \emptyset$
- Симметрично  $\Leftrightarrow R \subseteq R^{-1} \Leftrightarrow R = R^{-1} \Leftrightarrow R^{-1} \subseteq R$
- Антисимметрично  $\Leftrightarrow R \cap R^{-1} \subseteq \text{id}_A$
- Транзитивно  $\Leftrightarrow R \circ R \subseteq R$

**Определение 1.3.2:** Отношение  $R$  на каком-либо множестве называется **строгим частичным порядком** на этом множестве, если  $R$  иррефлексивно и транзитивно.

**Определение 1.3.3:** Отношение  $R$  на каком-либо множестве называется **нестрогим частичным порядком** на этом множестве, если  $R$  рефлексивно, транзитивно и антисимметрично.

**Утверждение 1.3.1:** Пусть  $P \subseteq A \times B, Q, R$  – бинарные отношения, тогда

- $(P^{-1})^{-1} = P$
- $(P \cup Q)^{-1} = P^{-1} \cup Q^{-1}$
- $\overline{P^{-1}} = \overline{P}^{-1}$
- $(P \cup Q) \circ R = (P \circ R) \cup (Q \circ R)$
- $(P \cap Q) \circ R \subseteq (P \circ R) \cap (Q \circ R)$

**Теорема 1.3.1** (Связь строгих и нестрогих порядков): Положим

$$S(A) = \{R \in \mathcal{P}(A^2) \mid R \text{ строгий порядок}\}$$

и аналогично выделим множество  $N(A)$  всех нестрогих порядков на  $A$ .

Рассмотрим функции  $\varphi : S(A) \rightarrow \mathcal{P}(A^2)$  и  $\psi : N(A) \rightarrow \mathcal{P}(A^2)$ :

$$\varphi(P) = P \cup \text{id}_A \quad \psi(Q) = Q \setminus \text{id}_A$$

Тогда утверждается, что

- $\varphi(P) \in N(A) \wedge \psi(\varphi(P)) = P$
- $\psi(Q) \in S(A) \wedge \varphi(\psi(Q)) = Q$

*Доказательство:* Проверим нестрогость  $\varphi(P)$ :

- Рефлексивно, так как  $\text{id}_A \subseteq \varphi(P)$
- Транзитивно, так как

$$\begin{aligned} \varphi(P) \circ \varphi(P) &= (P \cup \text{id}_A) \circ (P \cup \text{id}_A) = \\ &= (P \circ P) \cup (P \circ \text{id}_A) \cup (\text{id}_A \circ P) \cup (\text{id}_A \circ \text{id}_A) = \\ &= (P \circ P) \cup P \cup \text{id}_A \subseteq P \cup \text{id}_A = \varphi(P) \end{aligned}$$

- Антисимметрично, так как

$$\begin{aligned} \varphi(P) \cap (\varphi(P))^{-1} &= (P \cup \text{id}_A) \cap (P \cup \text{id}_A)^{-1} = \\ &= (P \cup \text{id}_A) \cap (P^{-1} \cup \text{id}_A) = (P \cap P^{-1}) \cup \text{id}_A = \text{id}_A \end{aligned}$$

Итак,  $\varphi(P) \in N(A)$ . Далее,

$$\begin{aligned} \psi(\varphi(P)) &= (P \cup \text{id}_A) \cap \overline{\text{id}_A} = \\ &= (P \cap \overline{\text{id}_A}) \cup \emptyset = (P \cap \overline{\text{id}_A}) \cup (P \cap \text{id}_A) = P \cap (\text{id}_A \cup \overline{\text{id}_A}) = P \cap A^2 = P \end{aligned}$$

Проверим нестрогость  $\psi(Q)$ :

- Ирефлексивно, так как  $\text{id}_A \cap \psi(Q) = \emptyset$
- Транзитивно, так как пусть  $xQy \wedge yQz$ , где  $x \neq y \wedge y \neq z$ . Если  $x = z$ , то  $zQy \wedge yQz \Rightarrow z = y$  – противоречие.

Итак,  $\psi(Q) \in S(A)$ . Далее,

$$\varphi(\psi(Q)) = (Q \cap \overline{\text{id}_A}) \cup \text{id}_A = (Q \cup \text{id}_A) \cap (\text{id}_A \cup \overline{\text{id}_A}) = Q \cap A^2 = Q$$



□

**Определение 1.3.4:** Если на множестве  $A$  задан строгий частичный порядок  $P$ , элемент  $x \in A$  называется **максимальным**, если

$$\forall y \in A : \neg(xPy)$$

В случае нестрогого порядка  $Q$  определяется, как

$$\forall y \in A : xQy \Rightarrow y = x$$

**Определение 1.3.5:** Если на множестве  $A$  задан строгий частичный порядок  $P$ , элемент  $x \in A$  называется **минимальным**, если

$$\forall y \in A : \neg(yPx)$$

В случае нестрогого порядка  $Q$  определяется, как

$$\forall y \in A : yQx \Rightarrow y = x$$

**Определение 1.3.6:** Если  $R$  есть строгий или нестрогий частичный порядок на множестве  $A$ , пара  $(A, R)$  называется **частично упорядоченным множеством (ч.у.м.)**

**Определение 1.3.7:** Элемент  $x \in B$  называется **наибольшим** в подмножестве  $B$  ч.у.м.  $(A, <)$ , если

$$\forall y \in B : y < x$$

и **наименьшим**, если

$$\forall y \in B : x < y$$

**Определение 1.3.8:** Пусть  $(A, <)$  ч.у.м. и  $B \subseteq A$ . Элемент  $x \in A$  назовём **верхней гранью** множества  $B$ , если

$$\forall y \in B : y \leq x$$

Аналогично определяются **нижние грани**.

Определим  $B^\Delta$  – множество всех верхних граней, а также  $B^\nabla$  – нижних граней.

**Определение 1.3.9:** Мы говорим, что  $x \in A$  есть **точная верхняя грань (супремум)** множества  $B$ , если  $x$  есть наименьший элемент множества  $B^\Delta$ .

Аналогично определяется **точная нижняя грань (инфимум)**.

**Определение 1.3.10:** Структуры  $\mathcal{A} = (A, R); \mathcal{B} = (B, Q)$  **изоморфны**, если существует функция  $\alpha : A \rightarrow B$ , т.ч.  $A \simeq B$  и

$$xRy \Leftrightarrow \alpha(x)Q\alpha(y)$$

**Определение 1.3.11:** Отношение  $R \subseteq A^2$  называется **отношением эквивалентности (эквивалентностью)** на  $A$ , если  $R$  рефлексивно, симметрично и транзитивно.

**Определение 1.3.12:** Пусть  $E$  есть эквивалентность на множестве  $A$  и  $x \in A$ . Назовём множество

$$[x]_E = \{z \in A \mid xEz\}$$

**классом эквивалентности** элемента  $x$  по отношению  $E$ .

**Определение 1.3.13:** Множество

$$A/E = \{\sigma \in \mathcal{P}(A) \mid \exists x \in A : [x]_E = \sigma\} = \{[x]_E \mid x \in A\}$$

называется **фактор-множеством** множества  $A$  по отношению  $E$ .

**Определение 1.3.14:** Назовём множество  $\Sigma \subseteq \mathcal{P}(A)$  **разбиением** множества  $A$ , если

$$\emptyset \notin \Sigma \wedge \bigcup \Sigma = A \wedge (\forall \sigma, \tau \in \Sigma : \sigma \cap \tau \neq \emptyset \Leftrightarrow \sigma = \tau)$$

#### 1.4. Принципы математической индукции, «сильной» индукции и наименьшего числа. Их равносильность. Теорема о рекурсии в различных формах (без доказательства). Принцип Дирихле (с доказательством). Основные теоремы о мощностях конечных и счетных множеств (про подмножество, объединение, произведение, степень и пр.; доказательства как доп. вопросы).

**Определение 1.4.1:** Принцип математической индукции:

$$\forall X \subseteq \mathbb{N} : (0 \in X \wedge (\forall n \in \mathbb{N} : n \in X \Rightarrow n + 1 \in X)) \Rightarrow X = \mathbb{N}$$

**Определение 1.4.2:** Назовём множество  $X \subseteq \mathbb{N}$  **прогрессивным**, если

$$\forall n \in \mathbb{N} : \forall m < n : (m \in X \Rightarrow n \in X)$$

**Принцип порядковой индукции:**

$$\forall X \subseteq \mathbb{N} : X \text{ — прогрессивное} \Rightarrow X = \mathbb{N}$$

**Определение 1.4.3:** Принцип наименьшего числа:

$$\forall X \subseteq \mathbb{N} : X \neq \emptyset \Rightarrow \exists \min X$$

**Теорема 1.4.1:** Следующие утверждения равносильны:

1. Принцип порядковой индукции
2. Принцип наименьшего числа
3. Принцип математической индукции

*Доказательство:*  $(1 \Rightarrow 2)$ . Предположим, что в некотором  $X$  нет наименьшего элемента. Покажем, что  $\bar{X}$  прогрессивно:

$$\forall m < n : m \notin X \Rightarrow n \notin X$$

ибо иначе  $n = \min X$ , что невозможно.

По принципу порядковой индукции  $\bar{X} = \mathbb{N} \Rightarrow X = \emptyset$ .

$(2 \Rightarrow 3)$ . Рассмотрим множество  $\bar{X}$ . Допустим, что  $\bar{X} \neq \emptyset$ . Тогда  $\exists n = \min \bar{X}$ .

По предположению,  $n \neq 0$  (так как  $0 \in X$ ). Значит,  $n = m + 1$  для некоторого  $m \in \mathbb{N}$ . Поскольку  $m < n$ , имеем  $m \in X$ , но по предположению должно было быть, что  $m + 1 = n \in X$ , что не так. Следовательно  $\bar{X} = \emptyset, X = \mathbb{N}$ .  $(3 \Rightarrow 1)$ . Рассмотрим множество

$$Y = \{n \in \mathbb{N} \mid \forall m < n : m \in X\}$$

Очевидно,  $0 \in Y$ .

Допустим, что  $n \in Y$ . Тогда  $\forall m < n : m \in X$ , что, в силу прогрессивности, влечёт  $n \in X$ , а значит и  $n + 1 \in Y$ .

Для множества  $Y$  мы проверили базу и шаг индукции, а значит  $Y = \mathbb{N}$ .

Наконец, для всякого  $n \in \mathbb{N}$  имеем  $n < n + 1 \in Y \Rightarrow n \in X$ . Следовательно, и  $X = \mathbb{N}$ .  $\square$

**Теорема 1.4.2** (О рекурсии): Пусть  $U$  – некоторое множество,  $u_0 \in U$  и  $h : U \rightarrow U$ .

Тогда существует единственная функция  $f : \mathbb{N} \rightarrow U$ :

$$f(0) = u_0 \wedge \forall n \in \mathbb{N} : f(n + 1) = h(f(n))$$

**Теорема 1.4.3** (О рекурсии, знающей шаг): Пусть  $U$  – некоторое множество,  $u_0 \in U$  и  $h : \mathbb{N} \times U \rightarrow U$ .

Тогда существует единственная функция  $f : \mathbb{N} \rightarrow U$ :

$$f(0) = u_0 \wedge \forall n \in \mathbb{N} : f(n + 1) = h(n, f(n))$$

**Теорема 1.4.4** (О примитивной рекурсии): Пусть  $U, V$  – некоторые множества,  $g : V \rightarrow U$  и  $h : \mathbb{N} \times V \times U \rightarrow U$ .

Тогда существует единственная функция  $f : \mathbb{N} \times V \rightarrow U$ :

$$\forall v \in V : f(0, v) = g(v) \wedge \forall n \in \mathbb{N} : f(n + 1, v) = h(n, v, f(n))$$

**Определение 1.4.4:** Пусть  $n \in \mathbb{N}$ , тогда определим множество

$$\underline{n} = \{m \in \mathbb{N} \mid m < n\} = \{0, \dots, n-1\}$$

**Определение 1.4.5:** Множество  $A$  **конечно**, если  $\exists n \in \mathbb{N} : A \sim \underline{n}$

**Определение 1.4.6:** Множество  $A$  **счётно**, если  $A \sim \mathbb{N}$

**Лемма 1.4.1:** Для каждого  $n \in \mathbb{N}$ , если  $f : \underline{n+1} \rightarrow \underline{n}$ , то  $f$  не инъекция

*Доказательство:* Предположим противное, пусть найдётся  $n \in \mathbb{N}$ , для которого есть инъекция  $f : \underline{n+1} \rightarrow \underline{n}$ .

Согласно принципу наименьшего числа, рассмотрим наименьшее такое  $n$ .

Заметим, что инъекция  $f : \underline{1} \rightarrow \underline{0} = \emptyset$  невозможна. Значит  $n \neq 0 \Rightarrow \exists m \in \mathbb{N} : n = m + 1$ .

Пусть  $f(n) = x \in \underline{n}$ . Рассмотрим функцию  $g$ , меняющую  $m < n$  и  $x < n$  местами.

Ясно, что  $g$  — биекция, а ограничение инъекции  $f|_{\underline{n}}$  также является инъекцией. Тогда и  $h = g \circ f|_{\underline{n}}$  также инъекция.

Заметим, если  $h(k) = m$ , то  $f|_{\underline{n}} = x$ , но  $f$  принимала  $x$  только на  $n$ , так что текущая ситуация невозможна из-за инъективности.

Значит  $\text{rng } h \subseteq \underline{m} \Rightarrow h : \underline{m+1} \rightarrow \underline{m}$  — инъекция для  $m < n$  — противоречие.  $\square$

**Теорема 1.4.5** (Принцип Дирихле): Если  $m > n$  и  $f : \underline{m} \rightarrow \underline{n}$ , то  $f$  не инъекция

*Доказательство:* Допустим,  $\exists m > n : f : \underline{m} \rightarrow \underline{n}$  — инъекция.

Но тогда  $f|_{\underline{n+1}} : \underline{n+1} \rightarrow \underline{n}$  — тоже инъекция, что противоречит предыдущей лемме.  $\square$

**Теорема 1.4.6** (Правило подмножеств): Если  $A \subseteq \mathbb{N}$ , то множество  $A$  конечно или счётно.

*Доказательство:* Согласно теореме о рекурсии, существует функция  $\alpha : \mathbb{N} \rightarrow \mathcal{P}(A)$

$$\alpha(0) := A \wedge \alpha(n+1) := \begin{cases} \alpha(n) \setminus \{\min \alpha(n)\}, & \alpha(n) \neq \emptyset \\ \emptyset, & \text{else} \end{cases}$$

Определим  $f(m) := \min \alpha(m)$ , тогда будут два случая

- $\exists n_0 : \alpha(n_0) = \emptyset$ , выберем из таких  $n_0$  наименьшее и докажем, что  $f : \overline{n_0} \rightarrow A$  – биекция
- Иначе  $f : \mathbb{N} \rightarrow A$ , также является биекцией.

□

**Теорема 1.4.7** (Правило суммы): Пусть множества  $A$  и  $B$  конечны и  $A \cap B = \emptyset$ .

Тогда множество  $A \cup B$  тоже конечно, причём

$$|A \cup B| = |A| + |B|$$

*Доказательство:* Допустим, что  $A \stackrel{f}{\sim} \underline{n}, B \stackrel{g}{\sim} \underline{m}$ . Определим функцию  $h : A \cup B \rightarrow \underline{n+m}$ :

$$h(x) = \begin{cases} f(x), x \in A \\ n+g(x), x \in B \end{cases}$$

Доказательство её биективности тривиально.

□

**Теорема 1.4.8** (Правило произведения): Пусть множества  $A$  и  $B$  конечны.

Тогда множество  $A \times B$  тоже конечно, причём

$$|A \times B| = |A| \cdot |B|$$

*Доказательство:* Допустим, что  $A \stackrel{f}{\sim} \underline{n}, B \stackrel{g}{\sim} \underline{m}$ . Если  $m = 0 \vee n = 0$ , то  $A \times B = \emptyset$  – тривиальный случай.

Определим функцию  $h : A \times B \rightarrow \underline{nm}$ :

$$h(x, y) = mf(x) + g(y)$$

Доказательство её биективности тривиально.

□

**Теорема 1.4.9** (Правило объединения): Пусть множества  $A$  и  $B$  конечны.

Тогда множество  $A \times B$  тоже конечно, причём

$$|A \times B| = |A| + |B| - |A \cap B|$$

*Доказательство:* Заметим, что  $A \cup B = (A \setminus B) \cup B$ , причём  $(A \setminus B) \cap B = \emptyset$ .

Тогда по правилу суммы

$$|A \cup B| = |(A \setminus B) \cup B| = |A \setminus B| + |B| = |A| - |A \cap B| + |B|$$

□

**Теорема 1.4.10** (Правило степени): Если множество  $A$  конечно, то при любом  $n \in \mathbb{N}$  множество  $A^n$  тоже конечно, причём

$$|A^n| = |A|^n$$

*Доказательство:* Индукция по  $n$  с учётом  $A^{n+1} = A^n \times A$ .

□

## 1.5. Вполне упорядоченные множества (ВУМ). Теорема о строении элементов ВУМ. Начальные отрезки ВУМ и их свойства; теорема о сравнении ВУМ (доказательство как доп. вопрос). Сложение и умножение ВУМ; свойства этих операций.

**Определение 1.5.1:** Порядок  $<$  на множестве  $A$  называется **линейным**, если любые два элемента  $A$  сравнимы.

Мы говорим, что ч.у.м.  $(A, <)$  есть **линейно упорядоченное множество (л.у.м.)**, если порядок  $<$  линейный.

**Определение 1.5.2:** Порядок  $<$  на множестве  $X$  **фундирован**, если во всяком непустом  $Y \subseteq X$  существует минимальный элемент.

Множество **вполне упорядоченно (в.у.м.)**, если оно линейно и фундировано.

**Определение 1.5.3:** Для элемента  $x$  в.у.м.  $(X, <)$  введём обозначение

$$[0, x) := \{y \mid y < x\}$$

Элемент  $x$  называется **предельным**, если

$$x \in \lim \Leftrightarrow x = \sup[0, x) \wedge x \neq 0$$

Наименьший элемент в.у.м.  $0$  тоже иногда считают предельным, поскольку  $0 = \sup \emptyset = \sup[0, 0)$ , мы не станем этого делать, но обозначим

$$\lim^* = \lim \cup \{0\}$$

**Утверждение 1.5.1** (Свойства предельных элементов): Следующие условия эквивалентны:

- $x \in \lim^*$
- $\forall y : \neg(y + 1 = x)$
- $\forall y < x : y + 1 < x$

**Теорема 1.5.1** (О строении элементов в.у.м.): Всякий элемент  $x \in X$  однозначно однозначно представим в виде  $x = y + n$ , где  $y \in \lim^*$

*Доказательство:* Если  $x = 0$ , то всё доказано.

Пусть  $x > 0$ . Рассмотрим множество

$$C = \{z \in X \mid \exists k \in \mathbb{N}_+ : z + k = x\}$$

Если  $C = \emptyset$ , то  $\forall z \in X : z + 1 \neq x \Rightarrow x$  — предельный. (по свойствам выше)

Иначе  $C \neq \emptyset \Rightarrow \exists z' := \min C$  и для некоторого  $k' > 0 : x = z' + k'$ .

Если  $z' = 0$ , то  $y = 0, n = k'$ . Если же  $z' \notin \text{lim}$ , то по свойствам  $\exists z'' : z' = z'' + 1$ , что противоречит минимальности  $z' \Rightarrow z' \in \text{lim}$ . Значит можно брать  $y = z', n = k'$ .

Пусть  $x = y_1 + n_1 = y_2 + n_2$ . Если БОО  $n_1 < n_2$ , то  $y_1 = y_2 + (n_2 - n_1)$ , что противоречит предельности  $y_1 \Rightarrow n_1 = n_2 \Rightarrow y_1 = y_2$ , всё доказали.  $\square$

**Определение 1.5.4:** Подмножество  $I$  в.у.м.  $X$  называется **начальным отрезком**, если оно «замкнуто вниз»:

$$\forall x \in I : \forall y < x : y \in I$$

Если  $I \neq X$ , то это **собственный начальный отрезок**.

**Утверждение 1.5.2** (Свойства начальных отрезков в.у.м.): Пусть  $(X, <)$  в.у.м. Тогда

1.  $X$  есть свой начальный отрезок
2. Пусть  $I_a$  – н.о.  $X$  при всех  $a \in A$ . Тогда  $\cup_{a \in A} I_a$  тоже н.о.
3. Если  $x \in X$ , то  $[0, x)$  есть н.о.  $X$
4. Если  $I$  собственный н.о.  $X$ , то существует и единственен такой  $x \in X$  :  
 $I = [0, x)$
5. Пусть  $\mathcal{J} = \{I \mid I \text{ — начальный отрезок } X\}$ . Тогда  $(\mathcal{J}, \subseteq)$  есть в.у.м.
6.  $(\mathcal{J}, \subseteq) \simeq X + 1$ ;  $(\mathcal{J} \setminus X, \subseteq) \simeq X$

*Доказательство:*

2. Пусть  $x \in \cup_{a \in A} I_a \wedge y < x$ . Тогда найдётся  $I_a \ni x \Rightarrow y \in I_a \subseteq \cup_{a \in A} I_a$
4. Имеем  $X \setminus I \neq \emptyset$ . Возьмём наименьший  $x$  элемент этого множества. Очевидно  $y < x \Rightarrow y \in I$ . Причём если  $x \leq y \Rightarrow x \in I$  – не может быть.
5. Порядок  $(\mathcal{J}, \subseteq)$  линейен: все собственные н.о. вложены в  $X$  и сравнимы между собой по предыдущему пункту. Выделим в произвольном подмножестве  $\mathcal{J} \subseteq \mathcal{J}$  наименьший элемент. Если  $\mathcal{J} = \{X\}$ , то всё ясно. Иначе возьмём в непустом множестве  $\{x \mid [0, x) \in \mathcal{J} \setminus X\}$  наименьший элемент  $x'$ .
6. Изоморфизм строится как  $[0, x) \mapsto x$ , а  $X$  переходит в наибольший элемент множества  $X + 1$ .

$\square$

**Определение 1.5.5** (Сравнение в.у.м.):

$$A < B \Leftrightarrow A \text{ изоморфен собственному н.о. } B$$

**Лемма 1.5.1:** Пусть  $(X, <)$  – в.у.м. и функция  $f : X \rightarrow X$  монотонна. Тогда  
 $\forall x \in X : f(x) \geq x$

*Доказательство:* От противного. Тогда подмножество

$$C := \{x \mid f(x) < x\} \neq \emptyset$$

Пусть  $x'$  его наименьший элемент. Имеем  $f(x') < x'$  по монотонности, но тогда  $f(f(x')) < f(x') \Rightarrow f(x') \in C$ , т.е.  $x'$  не наименьший.  $\square$

**Теорема 1.5.2** (О сравнении в.у.м.): Пусть  $C$  – в.у.м. и  $B \subseteq C$ . Тогда  $B \leq C$ .

*Доказательство:* Допустим  $B > C$ . Тогда, по определению

$$\exists b \in B : C \stackrel{f}{\simeq} [0_B, b) \subset B$$

Поскольку  $b \in C$ , то  $f(b) < b$ , но  $f$  монотонна, как изоморфизм, а значит  $f(b) \geq b$  (по предыдущей лемме) – противоречие.  $\square$

**Определение 1.5.6:** Произведением  $AB$  в.у.м.  $(A, <_A)$  и  $(B, <_B)$  называется  $(A \times B, <)$ :

$$(a_1, b_1) < (a_2, b_2) := \left( b_1 <_B b_2 \right) \vee \left( (b_1 = b_2) \wedge \left( a_1 <_A a_2 \right) \right)$$

**Определение 1.5.7:** Сумма в.у.м.  $A + B$  есть  $(A \times \{0\} \cup B \times \{1\}, <)$ :

$$(x, \varepsilon) < (y, \delta) := (\varepsilon < \delta) \vee \left( (\varepsilon = \delta = 0) \wedge \left( x <_A y \right) \right) \vee \left( (\varepsilon = \delta = 1) \wedge \left( x <_B y \right) \right)$$

**Лемма 1.5.2** (Свойства операций над в.у.м.):

1.  $A + (B + C) \simeq (A + B) + C$
2.  $A(BC) \simeq (AB)C$
3.  $C(A + B) \simeq CA + CB$

**1.6. Аксиома выбора (с любой мотивировочной задачей — например, о существовании правой обратной у сюръекции). Лемма Цорна и теорема Цермело (без доказательства). Любой пример применения. Теоремы о мощностях бесконечных множеств, вытекающие из них (доказательства как дополнительные вопросы)**

**Определение 1.6.1** (Аксиома выбора): Пусть множество  $A$  таково, что  $\emptyset \notin A$ .

Тогда существует функция  $f : A \rightarrow \cup A$ , т.ч.  $f(a) \in a$  для всех  $a \in A$ .

*Пример:* Пусть  $f : A \rightarrow B$ . Правая обратная функция  $g : B \rightarrow A$  существует тогда и только тогда, когда  $f$  есть сюръекция.



$\Rightarrow$ . Тогда  $f \circ g = \text{id}_B \Rightarrow \forall b \in B : (b, b) \in f \circ g$ , а значит найдётся  $a \in A$ , для которого  $(a, b) \in f$ , что и есть сюръективность.

$\Leftarrow$ . Ясно теперь, что множества  $f^{-1}[\{b\}]$  непусты для все  $b \in B$ . Определим функцию  $g : B \rightarrow A$ , полагая

$$g(b) = \text{какой-либо элемент множества } f^{-1}[\{b\}]$$

Теперь очевидно, что  $f(g(b)) = b$ .

**Определение 1.6.2:** Пусть  $(A, <)$  – ч.у.м. Множество  $C \subseteq A$  называется **цепью** в  $A$ , если

$$\forall x, y \in C : x \leq y \vee y \leq x$$

Напротив, множество  $D \subseteq A$  называется **антицепью**, если никакие два его (различные) элемента несравнимы.

**Лемма 1.6.1** (Цорна): Пусть  $(X, <)$  – частично упорядоченное множество, в котором любая цепь  $C \subset X$  имеет верхнюю грань. Тогда в  $(X, <)$  найдётся максимальный элемент.

**Теорема 1.6.1** (Цермело): Для всякого множества  $X$  существует бинарное отношение  $<$  на  $X$  такое, что  $(X, <)$  – в.у.м.

**Теорема 1.6.2:** Любые два множества сравнимы по мощности, то есть для любых множеств  $A, B$  найдётся инъекция из  $A$  в  $B$  или из  $B$  в  $A$ .

*Доказательство:* Вполне упорядочим эти множества по теореме Цермело. Тогда одно из них вложено в другое, как начальный отрезок.  $\square$