

Алгебра

Конспект лекций В. В. Нестерова, 2024

Пётр живёт в пунке
 И вот пошел первый год,
 Пётр ушёл от людей,
 Он ушёл от мирских хлопот,
 Он просто устал от жизни
 И не держит зла на людей,
 Но было время –
 Он был носителем великих идей
 Теперь матмех стал его домом,
 Он здесь может спокойно
 ботать,
 Он компилирует Си в голове
 И его решения никак не
 взломать
 А по ночам он приходит ко мне,
 Он зовёт меня в коворк,
 Он идёт к луне,
 Он видит ночь, как никто
 другой...

раз два три четыре пять,
 с рифмой с детства я дружу

Отношение эквивалентности и разбиения

Начнем с примера. Работаем с \mathbb{Z} , зафиксируем $m \in \mathbb{Z}, m > 0, x \sim y \iff x - y \equiv 0 \pmod{m}$.

Проверка:

- 1) $x \sim x$, поскольку $x - x \equiv 0 \pmod{m}$
- 2) $x \sim t \rightarrow x - y \equiv 0 \pmod{m} \rightarrow y - x \equiv 0 \pmod{m} \rightarrow y \sim x$
- 3) $x - y \equiv 0 \pmod{m}, y - z \equiv 0 \pmod{m} \rightarrow (x - y) + (y - z) = x - z \equiv 0 \pmod{m}$

Заданное нами отношение действительно является отношением эквивалентности.

$$[0] := \{0, m, -m, 2m, -2m, \dots\}$$

$$[1] := \{1, m + 1, -m + 1, \dots\}$$

\vdots

$$[a] := \{a, m + a, -m + a, 2m + a, -2m + a, \dots\}$$

$$a = 0, \dots, m - 1$$

$[a]$ называется классом эквивалентности

Теорема.

- 1) \sim задает на X разбиение на классы эквивалентности
- 2) Разбиение множества X задаёт на X отношение эквивалентности

Доказательство:

1) $x \in X, X_i := \{y \in X | x \sim y\}$

Покажем, что $\{X_i\}_{i \in I}$ является разбиением X . Очевидно, что объединение этого семейства равно X . Проверим, что классы эквивалентности не могут пересекаться.

Действительно, предположим противное: пусть $x \in X, x \in X_i = [y], x \in X_j = [z], i, j \in I, i \neq j$. Воспользуемся транзитивностью эквивалентности: $x \sim y, x \sim z \Rightarrow y \sim z \Rightarrow [y]$ и $[z]$ совпадают \Rightarrow противоречие - мы брали два разных класса эквивалентности.

2) $\{X_i\}_{i \in I}$ - разбиение X . Введем следующее отношение - $x \sim y \iff \exists i \in I : x \in X_i \wedge y \in X_i$.

Проверим:

1) рефлексивность очевидна

2) $x, y \in X_i \Rightarrow y, x \in X_i \Rightarrow y \sim x$

3) $x, y \in X_i \wedge y, z \in X_i \Rightarrow x \in X_i \wedge z \in X_i \Rightarrow x \sim z$ □

Перестановки и определение группы

Опр. Биективное отображение конечного множества $\sigma : X \rightarrow X$ называется **перестановкой**.

Записать перестановку можно следующим образом:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$$

Опр. Группой называется множество G с заданной на нем бинарной операцией \circ со следующими свойствами:

1) ассоциативность операции: $\forall x, y, z \in G : (x \circ y) \circ z = x \circ (y \circ z)$

2) существование нейтрального элемента $e \in G$ такого, что: $\forall x \in G$
 $x \circ e = e \circ x = x$. Легко заметить, что нейтральный элемент единственен.

3) существование обратного элемента: $\forall x \in G \exists x^{-1} \in G : x \circ x^{-1} = x^{-1} \circ x = e$

Теперь вернемся к перестановкам. Заметим, что мы можем перемножить две перестановки одного множества X - это просто композиция двух отображений. Продемонстрируем на примере:

$$\sigma : X \rightarrow X, \tau : X \rightarrow X, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$
$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Заметим, что с таким умножением перестановки образуют группу, называемуюся S_n . Действительно, ассоциативность следует из ассоциативности композиции отображений, нейтральным элементом выступает тождественная перестановка id (или e), и для каждой перестановки можем явно указать обратную ей. Пусть $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$, тогда $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$, можно легко проверить, что $\sigma^{-1} \circ \sigma = e$.

Лемма. (вспомогательное утверждение, полезное не само по себе, а для доказательства других утверждений) $f : X \rightarrow X$, f - биекция $\iff \exists f^{-1}$.

Доказательство: остается читателю как несложное упражнение. \square

Опр. Перестановка σ , действующая на k элементов, называется **циклом длины k** , если:

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_k \\ i_2 & i_3 & \dots & i_1 \end{pmatrix}$$

Теорема. $\sigma \in S_n \implies \sigma$ раскладывается в пр-е независимых циклов:

$$\sigma = \sigma_1 \sigma_2 \sigma_3 \dots$$

Доказательство: $\sqsubset X = \{1, 2, \dots, n\} \quad i, j \in X$

Введём отношение эквивалентности:

$$i \sim j \iff \exists k \geq 0 \quad \sigma^k(i) = j$$

1) В набора: $\{i, \sigma(i), \sigma^2(i), \dots\} \quad \exists k : \sigma^k(i) = i$.

$\sqsubset \sigma^s(i) = \sigma^{s+1}(i) \implies \sigma^{-s}(i) = \sigma^{s+1}(i) = \sigma^{-s}\sigma^s(i) \implies \sigma^k(i) = i$. Если это не так, значит все последовательные степени различны. Однако множество конечное, поэтому в некоторый момент $\sigma^k(i) = i$

2) Если $i \sim j \implies \sigma^k(i) = j \implies i = \sigma^{-k}(j)$

Очевидно, что если мощность нашего множества n , то $\sigma^n = \text{id} \implies i = \sigma^{n-k}(j)$

3) $i \sim j, j \sim e$, то есть $j = \sigma^s(i), e = \sigma^t(j) \implies e = \sigma^{s+t}(i) \implies \implies \sim$ - эквивалентность $\implies X = \bigcup_i X_i$

$\sigma \Big|_{X_i} = \sigma_i$ - цикл $\implies \sigma$ можно записать в виде произведения. \square

Опр. Циклы длины 2 называются **транспозициями**:

$$\sigma_{ij} = \begin{pmatrix} i & j \\ j & i \end{pmatrix}$$

Следствие. $\forall \sigma \in S_n$ раскладывается в произведения транспозиций.

Доказательство:

Возьмём цикл длины k :

$$\begin{pmatrix} i_1 & i_2 & \dots & i_k \\ i_2 & i_3 & \dots & i_1 \end{pmatrix} = \begin{pmatrix} i_1 & i_k \\ i_k & i_1 \end{pmatrix} = \begin{pmatrix} i_1 & i_{k-1} \\ i_{k-1} & i_1 \end{pmatrix} \dots \begin{pmatrix} i_1 & i_2 \\ i_2 & i_1 \end{pmatrix} \quad \square$$

Опр. Пусть $\sigma = \tau_1 \dots \tau_k$, где τ_i - транспозиция. Тогда **знак перестановки** определяется как:

$$\sigma := (-1)^k$$

Теорема.

$\sigma \in S_n$, тогда:

- 1) ε_σ не зависит от способа разложения σ на транспозиции
- 2) $\varepsilon_{\sigma_1\sigma_2} = \varepsilon_{\sigma_1} \cdot \varepsilon_{\sigma_2}$, где $\sigma_1, \sigma_2 \in S_n$

Опр. σ называется **четной перестановкой**, если ее знак равен $+1$, **нечетной**, если знак равен -1 .

Опр. Множество всех четных перестановок есть A_n .

Примеры:

- 1) $id \in A_n$
- 2) транспозиции нечетны. Также заметим, что $\tau^{(-1)} = \tau$, а тогда A_n - группа.

NB. $|S_n| = n!$, $|A_n| = \frac{n!}{2}$

Основы теории чисел. Делимость

Опр. Говорят, что $b \neq 0$ **делит** a , если $\exists q : a = b \cdot q$

$(b|a - b \text{ делит } a, a:b - a \text{ делится на } b)$

Свойства:

- 1) рефлексивность
- 2) на \mathbb{N} антисимметрично
- 3) транзитивно
- 4) $a|b, a|c \implies a|(b \pm c)$
- 5) $a|b, a|(b+c) \implies a|c$
- 6) $a|b \implies \forall c \quad a \cdot c|b$
- 7) $a|b \implies \forall k \neq 0 \quad k \cdot a|k \cdot b$

Теорема. (деление с остатком)

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}_+ \quad \exists! q, r : 0 \leq r < b$$

Доказательство:

- 1) Сначала покажем существование. Рассмотрим $a - b \cdot q$ ($a > 0$). Выберем такое q , что $a - b \cdot q \geq 0$, тогда это будет наименьшее возможное отрицательное по нашему выбору. Получим, что $r = a - b \cdot q \geq 0$. Кроме этого, $r \leq b$ в силу выбора q . Тогда $a - b(q+1) < 0 \implies b(q+1) > a \implies r = a - b \cdot q \leq b(q+1) - b \cdot q \leq b \implies 0 \leq r < b$

2) Покажем единственность. Предположим, что есть $a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2$, $0 \leq r_1, r_2 < b \implies |r_1 - r_2| < b$. Также, приравняв a , получим $r_1 - r_2 = b(q_2 - q_1)$. Если q_1, q_2 различны $\implies |r_1 - r_2| \geq b \implies$ противоречие $\implies q_1 = q_2 \implies r_1 = r_2$

□

Простые числа

Опр. p - простое, если $p > 1$ и делится только на 1 и на p .

Опр. a - составное, если $a > 1$ и $a = b \cdot c$, где $1 < b, c < a$.

НБ: $\mathbb{N} = \{1\} \cup \{\text{простые}\} \cup \{\text{составные}\}$

Теорема.

$p|a$, $p \neq 1$ и p - наименьший делитель $a \implies p$ - простое.

Доказательство:

$M = \{d \in \mathbb{N} \mid d \neq 1 \wedge d|a\}$, $M \neq \emptyset$, так как $a \in M$. Очевидно M ограничено снизу, тогда выберем $p := \min(M)$. \square p составное $\implies p = b \cdot c$

$$\begin{cases} b < p \\ c < p \end{cases} \implies c|a \wedge b|a, \text{ противоречие, так как } p \neq \min(M)$$

□

Теорема.

\square p - наименьший делитель n и $p \neq 1 \implies p \leq \sqrt{n}$

Доказательство:

$n = p \cdot m$, $p \leq m \implies n \cdot p \leq n \cdot m \implies p^2 \cdot m \leq n \cdot m \implies p^2 \leq n$

□

Теорема(Евклида, о бесконечности простых чисел)

Доказательство:

От противного: \square множество простых чисел конечно (n штук).

\square $m = p_1 \cdot \dots \cdot p_n + 1$ не делится ни на одно простое число $\implies m$ - простое, это противоречие.

□

Наибольший общий делитель (gcd)

Опр. Наибольшим общим делителем a_1, a_2, \dots, a_n называется такое число $d > 0$:

- 1) $d|a_i \quad \forall i$
- 2) $d'|a_i \implies d'|d$

Опр. Числа a_1, a_2, \dots, a_n называются **взаимно простыми**, если:

$$\gcd(a_1, \dots, a_n) = 1$$

Свойства:

- 1) $b|a \implies \gcd(a, b) = b$

Доказательство:

Рассмотрим множества делителей a и b . Очевидно, что их пересечение равно b , то есть

$$\{\text{делители } a \text{ и } b\} = \{\text{делители } b\}$$

- 2) $a = b \cdot q + c \implies \gcd(a, b) = \gcd(b, c)$

- 3) Алгоритм Евклида

$$\begin{aligned} & \gcd(a, b) = ?, \quad a \geq b \\ & a = b \cdot q_1 + r_1, 0 \leq r_1 < b \\ & b = r_1 \cdot q_2 + r_2, 0 \leq r_2 < r_1 \\ & r_1 = r_2 \cdot q_3 + r_3, 0 \leq r_3 < r_2 \\ & \dots \\ & r_{n-2} = r_{n-1} \cdot q_n + r_n, 0 \leq r_n < r_{n-1} \\ & r_{n-1} = r_n \cdot q_{n+1} \\ & \gcd(a, b) = r_n \end{aligned}$$

Доказательство:

Дойдем до 0, так как $\sqsupset \{r_1, r_2, \dots, r_n\}$ строго убывает, а $r_i \in \mathbb{N}$

Кроме этого, по свойству (2) $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_n, 0) = r_n$

□

- 4) $\forall m \quad (m \cdot a, m \cdot b) = m \cdot (a, b)$

- 5) $d|a, d|b \implies \gcd(a/d, b/d) = \gcd(a, b)/d$

- 6) $\sqsupset \gcd(a, b) = 1 \implies \gcd(a, b \cdot c) = \gcd(a, c)$

Доказательство:

$$\begin{aligned} & \begin{cases} \gcd(a, c)|a \\ \gcd(a, c)|c \end{cases} \implies \gcd(a, c)|b \cdot c \implies \gcd(a, c)|\gcd(a, b \cdot c) \\ & \gcd(a, b \cdot c)|b \cdot c \implies \gcd(a, bc)|\gcd(a \cdot c, b \cdot c) \implies \gcd(a \cdot c, b \cdot c) = c \cdot \gcd(a, b) \\ & \implies \gcd(a, b)|\gcd(a, c) \end{aligned}$$

□

7) $\exists \gcd(a, b) = 1$ и $a|bc \implies a|\gcd(c \cdot a, c \cdot b)$

Теорема. (соотношение Безу)

$$\exists d = \gcd(a, b) \implies \exists u, v \in \mathbb{Z} : u \cdot a + v \cdot b = d$$

Доказательство:

$$\begin{aligned} r_{n-2} &= r_{n-1} \cdot q_n + d \\ d &= r_{n-2} - r_{n-1} \cdot q_n \\ r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1} \\ d &= r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1}) \cdot q_n \\ &\dots \end{aligned}$$

И так далее. Поднимаясь вверх к первым индексам, сможем выразить d уже через a, b с некоторыми коэффициентами. □

Наименьшее общее кратное

Опр. Общим кратным чисел $\{a_1, \dots, a_n\}$ называется число

$$M > 0 : \forall a_i | M \text{ и } \forall S \neq M : \forall a_i | M \text{ верно, что } M | S$$

NB. Наименьшее общее кратное обозначается так: $\text{lcm}(a_1, \dots, a_n)$

Теорема.

$$\text{lcm}(a, b) = a \cdot b \cdot \gcd(a, b)$$

Доказательство:

$\exists d = \gcd(a, b)$. $a = a_1 \cdot d$, $b = b_1 \cdot d$. Если M - общее кратное a и b , то $M = a \cdot k = b \cdot l$

$$\begin{aligned} l &= \frac{M}{b} = \frac{a \cdot k}{b} = \frac{a_1 \cdot d \cdot k}{b_1 \cdot d} = \frac{a_1 \cdot k}{b_1} \in \mathbb{Z} \implies b_1 | k, k = b_1 \cdot t \\ \implies M &= a \cdot b_1 \cdot t, t \in \mathbb{N} \end{aligned}$$

Если $t = 1$:

$$\text{lcm}(a, b) = a \cdot b_1 = a \cdot \frac{b}{\gcd(a, b)} = \frac{a \cdot b}{\gcd(a, b)}$$

□