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) $x \sim t \to x - y \equiv 0 \pmod m \to y - x \equiv 0 \pmod m \to y \sim x$
3) $x - y \equiv 0 \pmod m, y - z \equiv 0 \pmod m \to (x - y) + (y - z) = x - z \equiv 0 \pmod m$

Заданное нами отношение действительно является отношением эквивалентности.
$[0] \coloneqq \{0, m, -m, 2m, -2m, ...\}$
$[1] \coloneqq \{1, m + 1, -m + 1, ...\}$
$\vdots$
$[a] \coloneqq \{a, m + a, -m + a, 2m + a, -2m + a, ...\}$
$a = 0, ..., m - 1$
[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) $x \in X, X_i \coloneqq \{y \in X | x \sim y\}$

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) $\{X\}_{i \in I}$ - 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) $x, y \in X_i \wedge y, z \in X_i \Rightarrow x \in X_i \wedge z \in X_i \Rightarrow x \sim z$ $\square$

Перестановки и определение группы

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

Записать перестановку можно следующим образом:

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

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:

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

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

Заметим, что с таким умножением перестановки образуют группу, называющуюся 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 $\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ i_1 & i_2 & i_3 & ... & i_n \end{pmatrix}$, тогда $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 & ... & i_n \\ 1 & 2 & 3 & ... & n \end{pmatrix}$, можно легко проверить, что $\sigma^{-1} \circ \sigma = e$.

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

Доказательство: остается читателю как несложное упражнение. $\square$

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

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

Теорема. $\sigma \in \mathrm{S}_n \Longrightarrow \sigma$ раскладывается в пр-е независимых циклов:

$$\sigma = \sigma_1\sigma_2\sigma_3...$$

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

Введём отношение эквивалетности:

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

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

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

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

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

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

$\sigma\Big|_{X_i} = \sigma_i$ - цикл $\Longrightarrow \sigma$ 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: