Лекция 1. Определение группы. Группа перестановок

Мы будем использовать язык теории множеств: множества, декартово произведение множеств, отображения, сюръекции, иньекции, биекции.

Определение 1. *Группой* называется множество G с бинарной операцией умножение $G \times G \to G$ если выполнены следующие аксиомы:
1) (Ассоциативность) $\forall a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
2) (Существование единицы) $\exists e \in G : \forall a \in G$, $a \cdot e = e \cdot a = a$
3) (Обратный элемент) $\forall a \in G$, $\exists b$ такой что $a \cdot b = e$. (Такой элемент называется обратным и обозначается a^{-1}).

Замечание. Из аксиом группы следует, что а) единичный элемент единственный, б) обратный элемент удовлетворяет также свойству $a^{-1} \cdot a = e$.

Примеры групп
1 Группа целых чисел $\mathbb{Z}$ операцией сложения. Аналогично группа вещественных $\mathbb{R}$ или комплексных $\mathbb{C}$ чисел с операцией сложения.
Все ненулевые вещественные (или комплексные) числа с операцией умножения.
2 Группа матриц $n \times n$ с действительными коэффициентами и ненулевым определителем. Обозначение $GL(n, \mathbb{R})$. Аналогично $GL(n, \mathbb{C})$.
3. Циклическая группа из n элементов $C_n = \{e, r, \ldots, r^{n-1}\}$, где $r^n = e$. Элементы группы можно представлять как повороты на угол $\frac{2\pi k}{n}$ вокруг начала координат.
4. Группа перестановок S_n.

Определение 2. *Перестановкой* n элементов (или *подстановкой* из n элементов) называется биекция n-элементного множества на себя. Множество всех перестановок множества $\{1, 2, \ldots, n\}$ обозначается S_n.

Произведение перестановок определяется как композиция биекций. То есть обозначение $\alpha\beta$ означает, что сначала действует β, а потом α.

Упражнение 1. Перемножьте перестановки $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ и $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

Упражнение 2. Вычислите $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}^{100}$

Через $(i_1, i_2, \ldots, i_n)$ обозначается цикл который переводит $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_n \mapsto i_1$.

Предложение 1. Любая перестановка разбивается в произведение непересекающихся циклов.

Например, для написанной выше перестановки мы имеем

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} = (1, 4)(2, 5, 3).$$

Определение 3. *Порядком элемента* $g \in G$ называют наименьшее натуральное n такое, что $g^n = e$. Если такого n не существует, то говорят что порядок равен бесконечности.
Количеством элементов в группе называется *порядком группы*. Обозначение: $|G|$.

Предложение 2. Если перестановка равна произведению независимых циклов длины $d_1, \ldots, d_k$, то ее порядок равен НОК$(d_1, d_2, \ldots, d_k)$

Упражнение 3. Найдите порядки всех элементов в группе C_6.

Теорема 3. Если $|G| < \infty$, то любой элемент $g \in G$ имеет конечный порядок не превышающий $|G|$.
Доказательство: Рассмотрим элементы $e, g, g^2, \ldots g^{|G|}$. Так как всего в группе $|G|$ элементов, значит найдутся $0 \leqslant i < j \leqslant |G|$ такие, что $g^i = g^j$. Значит, $g^{j-i} = e$. ■

Определение 4. *Транспозицией* называется цикл длины 2. Обозначение:

$$(a, b) = \begin{pmatrix} 1 & \ldots & a & \ldots & b & \ldots & n \\ 1 & \ldots & b & \ldots & a & \ldots & n \end{pmatrix}$$

Упражнение 4. Что получится если перестановку $\begin{pmatrix} 1\,2 & \ldots & n \\ i_1\,i_2 & \ldots & i_n \end{pmatrix}$ умножить на транспозицию (a, b) а) слева, б) справа?

Предложение 4. а) Любая перестановка может быть представлена как произведение транспозиций. б) Любая перестановка может быть представлена как произведение транспозиций соседних элементов $(i, i+1)$ (такие транспозиции называются элементарными).

Определение 5. Множество элементов $\{s_1, s_2 \ldots\} \in G$ называется образующими группы G, если любой элемент $g \in G$ может быть представлен в виде $g = s_{i_1}^{\pm 1} \cdot \ldots \cdot s_{i_l}^{\pm 1}$. Здесь среди индексов $i_1, \ldots, i_l$ могут быть одинаковые. Множество образующих может быть как конечным так и бесконечным.

Пример.а) Возьмем $G = \mathbb{Q}_{>0}$ — положительные рациональные числа, с операцией умножения. Тогда простые числа $2, 3, 5, \ldots$ являются образующими группы $\mathbb{Q}_{>0}$.
б) Как следует из предыдущего предложения в качестве образующих группы S_n можно взять элементарные транспозиции $s_i = (i, i+1)$, где $1 \leqslant i \leqslant n-1$.
в) Циклическая группа C_n порождена всего одной образующей r.

Представление элемента группы в виде произведения образующих не единственно. Например для S_n всегда можно вставить произведение $(i, i+1)(i, i+1) = e$. Или воспользоваться соотношением

$$(1, 3) = (1, 2)(2, 3)(1, 2) = (2, 3)(1, 2)(2, 3).$$

Однако, хотя само разложение не однозначно, оказывается, что четность числа сомножителей всегда будет одна и та же.

Определение 6. Инверсией (беспорядком) перестановки σ называется такая пара чисел i, j, что $i < j$, но $\sigma(i) > \sigma(j)$. Количество инверсий обозначается $|\sigma|$.

Перестановка называется четной, если число инверсий четное, в противном случае перестановка называется нечетной.

Предложение 5. Умножение на элементарную транспозицию либо увеличивает либо уменьшает число беспорядков на 1.

Теорема 6. Пусть σ разложено в произведение элементарных транспозиций $\tau_1\tau_2\dots\tau_k$. Тогда k больше либо равно $|\sigma|$. Кроме того $k \equiv |\sigma| \pmod 2$

Предложение 7. Произведение четных перестановок — четное.
Произведение нечетной и четной перестановок — нечетное.
Произведение нечетных перестановок — четное.

Определение 7. Подмножество $H \subset G$ называется *подгруппой*, если $\forall a, b \in H$ $a \cdot b \in H$ и $a^{-1} \in H$.

Так как аксиомы группы выполняются в G, то они выполняются и в H, т.е. любая подгруппа является группой.

Предложение 8. Четные перестановки образуют подгруппу в группе S_n (эта подгруппа обычно называется A_n). Нечетные перестановки подгруппу не образуют.

Домашнее задание

Решения надо прислать или принести до начала лекции 13 февраля. Помимо письменной сдачи надо быть готовым ответить на вопросы по решениям.

Упражнение 1. а) Пусть $\alpha = (1,3,5)(2,4,7)$, $\beta = (1,4,7)(2,3,5,6)$ (перестановки даны в разложении по непересекающимся циклам). Найдите произведение $\alpha\beta$.
б) Найдите порядок перестановки $\begin{pmatrix} 1&2&3&4&5&6&7\\ 5&6&4&7&2&1&3 \end{pmatrix}$.

Задача 2. а) Докажите, что любая транспозиция (не только элементарная) является нечетной перестановкой.
Указание: найдите число инверсий.
б) Пусть перестановка разложена в произведение транспозиций. Тогда ее четность равна четности количества этих транспозиций.
в) Перестановка σ является циклом длины d. Разложите ее в произведение транспозиций. Найдите четность σ.

Задача 3. Поставим каждой перестановке σ в соответствие матрицу $n \times n$ $R(\sigma)$, так что $R(\sigma)_{ij} = 1$ если $j = \sigma(i)$ и нулю иначе. Найдите собственные значения матрицы $R(\sigma)$ (дайте ответ в терминах циклического типа перестановки σ).

Задача 4 (*). Каких перестановок в S_n больше — четных или нечетных?

Материалы, а также полезная информация есть на сайте:
[qft.itp.ac.ru/mbersht/Group.html]