Лекция 7. Группы. Симметрическая группа перестановок S_n. Подгруппы. Теорема Кэли. Цикловой индекс группы перестановок.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.ru

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Нейтральный элемент

Пусть S — произвольное множество.
Алгебраической операцией $*$ на множестве S называется отображение $* : S \times S \to S$.

Элемент $e \in S$ называется **нейтральным элементом** относительно операции $*$, если для каждого элемента $a \in S$ верно

$$a * e = e * a = a.$$

Утверждение 1. *Нейтральный элемент (если он существует) единственен.*
Доказательство проведем от обратного: пусть найдутся два нейтральных элемента $e' \in S$ и $e'' \in S$, $e' \neq e''$.
Тогда

$$e' = \overset{e' * e''}{e' * e''} = e''$$

Симметричный элемент

Для элемента $a \in S$ элемент $a' \in S$ называется **симметричным**, если

$$a * a' = a' * a = e,$$

где $e \in S$ — нейтральный элемент относительно операции $*$.

Утверждение 2. *Симметричный элемент относительно ассоциативной операции (если он существует) единственен.*
Доказательство проведем от обратного: пусть для некоторого элемента $a \in S$ найдутся два симметричных элемента $a' \in S$ и $a'' \in S$, $a' \neq a''$.
Тогда

$$\begin{array}{ccccccc} & & & a' * a * a'' & & & \\ a' = & a' * e = a' * (a * a'') & = & (a' * a) * a'' & = & e * a'' & = a'' \end{array}$$

Группа

Множество S с одной или несколькими введенными на нем операциями называется *алгебраической структурой*.
Структура $G = (S; *)$ (т. е. множество S с введенной на нем алгебраической операцией $*$) называется **группой**, если
1) операция $*$ ассоциативна, т. е. для любых элементов $a, b, c \in S$ верно

$$(a * b) * c = a * (b * c);$$

2) существует нейтральный элемент относительно операции $*$, т. е. найдется такой элемент $e \in S$, что для каждого элемента $a \in S$ верно

$$a * e = e * a = a;$$

3) для каждого элемента $a \in S$ найдется симметричный к нему элемент $a' \in S$, т. е. такой что

$$a * a' = a' * a = e.$$

Группа

Если для группы $G = (S; *)$ дополнительно выполнено, что
4) операция $*$ коммутативна, т. е. для любых элементов $a, b \in S$ верно

$$a * b = b * a,$$

то такая группа называется **коммутативной**, или **абелевой**.

Группы

Утверждение 3 (правило сокращения).
Пусть $G = (S; *)$ — группа. Тогда если для некоторых элементов $a, b, c \in G$ верно

$$a * b = a * c \ (\text{или } b * a = c * a),$$

то $b = c$.

Доказательство. Пусть элемент $a' \in G$ симметричен относительно операции $*$ к элементу $a \in G$. Элемент $a' \in G$ найдется, т. к. G – группа. Тогда

$$\begin{gathered} a * b = a * c \\ a' * a * b = a' * a * c \\ b = e * b = \quad (a' * a) * b = (a' * a) * c \quad = e * c = c \end{gathered}$$

□

Примеры групп

1. $S = \{e\}$; $e * e = e$ — тривиальная группа.

Примеры групп

1. $S = \{e\}$; $e * e = e$ — тривиальная группа.

2. $S = \{e, a\}$; $x * e = e * x = x$, где $x = e, a$;
Чему равно $a * a =$?
Если $a * a = a$, то $a * a = a * e$ и $a = e$ — противоречие.
Значит, $a * a = e$.

Примеры групп

1. $S = \{e\}$; $e * e = e$ — тривиальная группа.

2. $S = \{e, a\}$; $x * e = e * x = x$, где $x = e, a$;
Чему равно $a * a =$?
Если $a * a = a$, то $a * a = a * e$ и $a = e$ — противоречие.
Значит, $a * a = e$.

3. $S = \{e, a, b\}$;

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Перечисленные группы коммутативны.

Изоморфизм групп

Две группы $G_1 = (S_1; *)$ и $G_2 = (S_2; \times)$ называются **изоморфными**, если найдется взаимно однозначное отображение

$$\varphi : S_1 \to S_2,$$

сохраняющее операцию, т. е. для любых элементов $a, b \in S_1$ верно

$$\varphi(a * b) = \varphi(a) \times \varphi(b).$$

При этом взаимно однозначное отображение φ называется **изоморфизмом** групп G_1 и G_2.

Отметим, что перечисленные в п.п. 1–3 группы единственные с точностью до изоморфизма группы соответственно из одного, двух и трех элементов.

Свойства изоморфизма групп

Пусть $\varphi : S_1 \to S_2$ — изоморфизм групп $G_1 = (S_1; *)$ и $G_2 = (S_2; \times)$. Тогда

1) $\varphi(e_1) = e_2$, где e_1, e_2 — соответственно нейтральные элементы групп G_1, G_2. В самом деле, если $a \in S_1$, то

$$\varphi(a) = \varphi(a * e_1) = \varphi(a) \times \varphi(e_1),$$

откуда $\varphi(e_1) = e_2$.

2) $\varphi(a') = \varphi(a)'$, где $a' \in S_1, \varphi(a)' \in S_2$ — соответственно симметричные элементы к элементам $a \in S_1, \varphi(a) \in S_2$ групп G_1, G_2. В самом деле,

$$e_2 = \varphi(e_1) = \varphi(a * a') = \varphi(a) \times \varphi(a'),$$

откуда $\varphi(a') = \varphi(a)'$.

Порядок группы

Группа $G = (S; *)$ называется **конечной**, если в множестве S конечное число элементов.
Если группа $G = (S; *)$ конечна, то число элементов в множестве S называется ее **порядком** и обозначается $|G|$.

Пусть $G = (S; *)$ — группа с нейтральным элементом e.
Для элемента $a \in G$ наименьшее натуральное число n (если оно существует), такое что

$$\underbrace{a * a * \ldots * a}_{n} = e,$$

называется его **порядком**.

Конечные коммутативные группы

Утверждение 4. *Пусть $G = (S; *)$ — конечная коммутативная группа и $e \in S$ — ее нейтральный элемент. Тогда для любого элемента $a \in S$ верно $\underbrace{a * \ldots * a}_{|G|} = a^{|G|} = e$.*

Доказательство. Пусть $S = \{a_1, \ldots, a_n\}$, и $a \in S$. Рассмотрим элементы группы

$$a * a_1, \ a * a_2, \ \ldots, \ a * a_n.$$

Все эти элементы различны (почему?). И их ровно n. Значит, здесь перечислены все элементы группы.
Поэтому, с учетом коммутативности и ассоциативности операции $*$, получаем:

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} (a * a_i) = a^{|G|} \prod_{i=1}^{n} a_i.$$

По правилу сокращения получаем $a^{|G|} = e$. $\square$

Малая теорема Ферма

Следствие 4.1 (малая теорема Ферма). *Если p — простое число, то для каждого натурального числа a, $1 \leqslant a \leqslant p-1$, верно $a^{p-1} = 1 (\mathrm{mod}\ p)$.*

Доказательство. Пусть $S = \{1, 2, \ldots, p-1\}$ и $\cdot (\mathrm{mod}\ p)$ — операция умножения по модулю p чисел из S.

Несложно проверить, что $G = (S, \cdot (\mathrm{mod}\ p))$ — коммутативная группа порядка $(p-1)$ с нейтральным элементом $e = 1$.

Поэтому получаем, что $a^{p-1} = 1 (\mathrm{mod}\ p)$ для каждого $a \in S$.

□

Терминология

Общая	Аддитивная	Мультипликативная
$*$ операция	$+$ сложение	$\cdot$ умножение
e нейтральный	0 ноль	1 единица
a' симметричный	$-a$ противоположный	a^{-1} обратный
$\underbrace{a * a * \ldots * a}_{n}$	na	a^n степень

Перестановки

Пусть $N = \{1, 2, \ldots, n\}$, где $n \geqslant 1$.

Перестановкой (n элементов) π называется взаимно однозначное отображение

$$\pi : N \to N.$$

Множество всех перестановок n элементов обозначим как S_n.

Задавать перестановки можно

1) таблицей: $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ — в каждом столбце элемент в первой строке перестановкой переводится в элемент во второй строке;

2) строкой: $\pi = [2143]$ — в строке на i-м месте стоит элемент $\pi(i)$;

3) произведением циклов: $\pi = (12)(34)$ — каждая скобка является отдельным циклом, в каждой скобке следующий элемент получен из предыдущего применением перестановки, первый элемент получен из последнего применением перестановки.

Перестановки

Длиной цикла перестановки называется число элементов в нем.

Типом перестановки $\pi \in S_n$ называется набор

$$\lambda(\pi) = (\lambda_1(\pi), \ldots, \lambda_n(\pi)),$$

где $\lambda_i(\pi)$ — число циклов длины i в перестановке π.

Заметим, что для любой перестановки $\pi \in S_n$ верно $\sum_{i=1}^{n} i \cdot \lambda_i(\pi) = n$, т. к. каждый элемент принадлежит ровно одному циклу.

Например, для перестановки $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ ее тип $\lambda(\pi) = (0, 2, 0, 0)$, т. е. в ней два цикла, каждый из которых содержит по два элемента.

Перестановки

Введем операцию **композиции** $\circ$ на множестве перестановок.

Композицией (или **произведением**) перестановок π и ρ называется такая перестановка $\pi \circ \rho$, что для любого элемента $x \in N$ верно

$$(\pi \circ \rho)(x) = \pi(\rho(x)).$$

Перестановки

Утверждение 5. При $n \geqslant 3$ операция композиции перестановок n элементов не является коммутативной.

Доказательство. Рассмотрим перестановки

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \text{ и } \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}.$$

Тогда

$$(\pi \circ \rho)(1) = 1,$$

а

$$(\rho \circ \pi)(1) = 3.$$

$\square$

Группа перестановок

Утверждение 6. *Множество перестановок n элементов S_n с операцией композиции $\circ$ является группой.*

Доказательство. Проверим свойства группы.
1) Ассоциативность операции $\circ$.
Пусть $\pi, \rho, \tau \in S_n$. Тогда для любого элемента $x \in N$

$$((\pi \circ \rho) \circ \tau)(x) = (\pi \circ \rho)(\tau(x)) = \pi(\rho(\tau(x)))$$

и

$$(\pi \circ (\rho \circ \tau))(x) = \pi((\rho \circ \tau)(x)) = \pi(\rho(\tau(x))).$$

Группа перестановок

Доказательство.

2) Существование нейтрального элемента e.

Нейтральным элементом является перестановка

$$\pi_e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix},$$

оставляющая каждый элемент на месте.

3) Для каждого элемента π существование симметричного элемента π'.

Для перестановки

$$\pi = \begin{pmatrix} 1 & \dots & i & \dots & n \\ \pi(1) & \dots & \pi(i) & \dots & \pi(n) \end{pmatrix}$$

обратным (симметричным) элементом является перестановка

$$\pi^{-1} = \begin{pmatrix} \pi(1) & \dots & \pi(i) & \dots & \pi(n) \\ 1 & \dots & i & \dots & n \end{pmatrix}.$$

Группа перестановок

Доказательство.
Следовательно, $(S_n, \circ)$ — группа.

Кроме того, при $n \geqslant 3$ эта группа не коммутативна.

□

Группа всех перестановок n элементов с операцией композиции $\circ$ называется **симметрической группой перестановок** и обозначается как S_n.

Утверждение 7. *Порядок симметрической группы перестановок S_n равен $n!$, т. е.*

$$|S_n| = n!$$

Группа S_3

Рассмотрим симметрическую группу перестановок S_3.

$\pi_1 = e = [123] = (1)(2)(3)$ — нейтральный элемент (единица группы);
$\pi_2 = [132] = (1)(23)$ — элемент 1 остается на месте, элементы 2 и 3 меняются местами;
$\pi_3 = [321] = (13)(2)$ — элемент 2 остается на месте, элементы 1 и 3 меняются местами;
$\pi_4 = [213] = (12)(3)$ — элемент 3 остается на месте, элементы 1 и 2 меняются местами;
$\pi_5 = [231] = (123)$ — элементы 1, 2 и 3 сдвигаются по циклу по часовой стрелке;
$\pi_6 = [321] = (132)$ — элементы 1, 2 и 3 сдвигаются по циклу против часовой стрелки.

Порядок группы $|S_3| = 3! = 6$.

Подгруппы

Пусть $G = (S; *)$ — группа, и $T \subseteq S$.

Если $H = (T; *)$ является группой, то она называется **подгруппой** группы $G = (S; *)$.

Если при этом $T \neq \{e\}$ и $T \neq S$, то подгруппа называется **собственной**.

Подгруппы

Утверждение 8 (критерий подгруппы). *Пусть $G = (S; *)$ — группа и $T \subseteq S$. Тогда $H = (T; *)$ является группой в том и только в том случае, когда для любых элементов $a, b \in T$ верно $a * b' \in T$.*

Доказательство.

$\Leftarrow$. Проверим свойства группы.

1) ассоциативность операции $*$: т. к. G — группа;

2) существование нейтрального элемента e: если $a \in T$, то $a * a' = e \in T$;

3) для каждого элемента существование симметричного элемента: если $a \in T$, то $e * a' = a' \in T$;

4) алгебраичность операции $*$ для множества T: если $a, b \in T$, то по п. 3) $b' \in T$, и $a * (b')' = a * b \in T$.

□

Подгруппы

Примеры подгрупп в группах.
1. Если $G = (S, \cdot)$ — мультипликативная группа, и $a \in G$ — элемент порядка n в ней, то множество

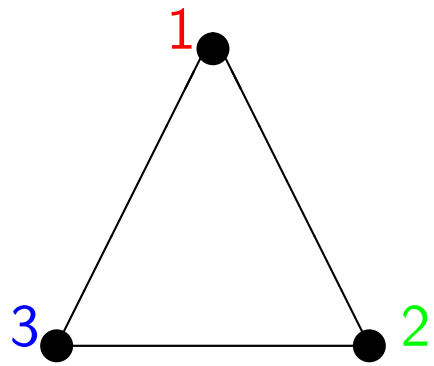
$$T = \{a, a^2, \ldots, a^{n-1}, a^n = 1\}$$

с операцией $\cdot$ образует мультипликативную подгруппу $H = (T; \cdot)$ порядка n группы $G = (S; \cdot)$.
Мультипликативная группа называется **циклической**, если каждый из ее элементов является некоторой степенью выделенного элемента группы, который называется **образующим** элементом группы.
Группа с образующим элементом a обозначается как $\langle a \rangle$.
Группа $H = (T; \cdot)$ из п. 1 является циклической подгруппой группы $G = (S; \cdot)$ с образующим элементом $a \in T$, т. е. $H = \langle a \rangle$.

Подгруппы

2. Найдем группу H перестановок вершин правильного треугольника при его вращениях в плоскости, переводящих его в себя.

Рассмотрим правильный треугольник и будем поворачивать его по часовой стрелке:



поворот на угол 0: $\pi_1 = e = (1)(2)(3)$;

поворот на угол $\frac{2\pi}{3}$: $\pi_2 = (123)$;

поворот на угол $\frac{4\pi}{3}$: $\pi_3 = (132)$.

Подгруппы

Получаем группу вращений вершин правильного треугольника в плоскости $H = (\{\pi_1, \pi_2, \pi_3\}; \circ)$, $|H| = 3$.

Она является подгруппой группы перестановок S_3.

Теорема Кэли

Теорема 1 (Кэли). *Каждая конечная группа изоморфна некоторой подходящей подгруппе симметрической группы перестановок S_n.*

Доказательство. Пусть $G = (S; *)$ — заданная конечная группа, $|G| = n$ и $S = \{g_1 = e, g_2, \ldots, g_n\}$.
Для каждого элемента $g_i \in G$ построим соответствующую ему перестановку $\pi_{g_i} \in S_n$ по правилу

$$\pi_{g_i} = \begin{pmatrix} g_1 & g_2 & \ldots & g_n \\ g_i * g_1 & g_i * g_2 & \ldots & g_i * g_n \end{pmatrix},$$

или

$$\pi_{g_i} = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi_{g_i}(1) & \pi_{g_i}(2) & \ldots & \pi_{g_i}(n) \end{pmatrix},$$

где $\pi_{g_i}(j) = k$, если $g_i * g_j = g_k$.

Теорема Кэли

Доказательство.
1. Сначала покажем, что такое определение задает перестановки.
От обратного: пусть это не так, т. е. для некоторого $g_i \in G$ найдутся такие элементы $g_j \in G$ и $g_l \in G$, $g_j \neq g_l$, что

$$g_i * g_j = g_i * g_l.$$

Но тогда по правилу сокращения верно $g_j = g_l$ — противоречие.

Обозначим полученное множество перестановок как T, $T \subseteq S_n$.

Теорема Кэли

Доказательство. Рассмотрим перестановку π_{g_i}, где $g_i \in G$,

$$\pi_{g_i} = \begin{pmatrix} g_1 & g_2 & \dots & g_n \\ g_i * g_1 & g_i * g_2 & \dots & g_i * g_n \end{pmatrix}.$$

Пусть $g_i' \in G$ — симметричный к g_i элемент. Тогда

$$\pi_{g_i}^{-1} = \begin{pmatrix} g_1 & g_2 & \dots & g_n \\ g_i' * g_1 & g_i' * g_2 & \dots & g_i' * g_n \end{pmatrix}.$$

Значит, $\pi_{g_i}^{-1} = \pi_{g_i'}$.

Теорема Кэли

Доказательство. 2. Теперь по критерию подгруппы покажем, что множество перестановок T с операцией композиции образует подгруппу симметрической группы перестановок S_n.

Выберем любые элементы $g_i, g_j \in G$ и рассмотрим перестановку $\pi_{g_i} \circ \pi_{g_j}^{-1}$.

Т. к. G — группа, верно $g_j' \in G$.
Тогда для любого элемента $x \in N$ получаем

$$(\pi_{g_i} \circ \pi_{g_j}^{-1})(x) = (\pi_{g_i} \circ \pi_{g_j'})(x) = \pi_{g_i}(\pi_{g_j'}(x)) = \pi_{g_i * g_j'}(x).$$

Т. к. G — группа, верно $g_i * g_j' = g_k \in G$, откуда $\pi_{g_i * g_j'} = \pi_{g_k}$.
Значит, $\pi_{g_i} \circ \pi_{g_j}^{-1} \in T$.

Следовательно, $H = (T; \circ)$ — подгруппа группы S_n.

Теорема Кэли

Доказательство. 3. Теперь покажем, что группы $G = (S; *)$ и $H = (T; \circ)$ — изоморфны.
Рассмотрим отображение

$$\varphi : S \to T, \ g \mapsto \pi_g,$$

которое элемент $g \in S$ переводит в элемент $\varphi(g) = \pi_g \in T$.
1) Отображение φ взаимно однозначно.
2) Если $g_i, g_j \in G$, то

$$\varphi(g_i * g_j) = \pi_{g_i * g_j} = \pi_{g_i} \circ \pi_{g_j} = \varphi(g_i) \circ \varphi(g_j).$$

Т. е. отображение φ сохраняет операцию.
Значит, оно является изоморфизмом групп $G = (S; *)$ и $H = (T; \circ)$.

□

Теорема Кэли

Для конечной группы $G = (S; *)$ построенная в доказательстве изоморфная ей подгруппа $H = (T; \circ)$ называется **левым регулярным представлением Кэли**.

Найдем левое регулярное представление Кэли для группы из трех элементов из рассмотренного ранее примера.

Пусть $S = \{e, a, b\}$;

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

, или

$*$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Тогда

$$\pi_e = (1)(2)(3); \quad \pi_a = (123); \quad \pi_b = (132).$$

Получаем группу вращений H правильного треугольника в плоскости, являющуюся подгруппой группы S_3.

Цикловой индекс

Пусть $G = (S; \circ)$ — подгруппа симметрической группы перестановок S_n.

Цикловым индексом группы перестановок G называется многочлен n переменных

$$Z_G(t_1, \ldots, t_n) = \frac{1}{|G|} \sum_{\pi \in G} t_1^{\lambda_1(\pi)} \cdot \ldots \cdot t_n^{\lambda_n(\pi)},$$

где $\lambda(\pi) = (\lambda_1(\pi), \ldots, \lambda_n(\pi))$ — тип перестановки π.

Цикловой индекс

1. Найдем цикловой индекс группы H вращений правильного треугольника в плоскости.
Для каждой перестановки ищем ее тип:
$\pi_1 = e = (1)(2)(3), \ \ \lambda(\pi_1) = (3, 0, 0);$
$\pi_2 = (123), \ \ \lambda(\pi_2) = (0, 0, 1);$
$\pi_3 = (132), \ \ \lambda(\pi_3) = (0, 0, 1).$

Замечая, что $|H| = 3$, получаем цикловой индекс

$$Z_H(t_1, t_2, t_3) = \frac{1}{3}(t_1^3 + 2t_3).$$

Цикловой индекс

2. Найдем цикловой индекс симметрической группы перестановок S_3.

Аналогично находим типы всех ее перестановок:

$\pi_1 = e = (1)(2)(3)$, $\lambda(\pi_1) = (3, 0, 0)$;

$\pi_2 = (1)(23)$, $\pi_3 = (13)(2)$, $\pi_4 = (12)(3)$,

$\lambda(\pi_2) = \lambda(\pi_3) = \lambda(\pi_4) = (1, 1, 0)$;

$\pi_5 = (123)$, $\pi_6 = (132)$, $\lambda(\pi_5) = \lambda(\pi_6) = (0, 0, 1)$.

Порядок группы $|S_3| = 3! = 6$.

Поэтому ее цикловой индекс

$$Z_{S_3}(t_1, t_2, t_3) = \frac{1}{6}(t_1^3 + 3t_1t_2 + 2t_3).$$

Задачи для самостоятельного решения

1. Найти группу G перестановок вершин квадрата при его вращениях в плоскости, являющуюся подгруппой группы S_4.

2. Найти левое регулярное представление Кэли группы $G = (S; *)$, где $S = \{0, 1, 2, 3\}$, операция $*$ — сложение по модулю 4.

3. Найти левое регулярное представление Кэли группы $G = (S; *)$, где $S = \{1, 2, 3, 4\}$, операция $*$ — умножение по модулю 5.

4. Найти цикловой индекс группу G перестановок сторон квадрата при его вращениях в плоскости.

Литература к лекции

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. Т. 1. С. 12–23.

Конец лекции