Алгебра 7

Igor Engel

1

Теорема 1.1. Если $H \leq \mathbb{Z}/n$, то H - циклическая.

$$\forall d \quad n \vdots d \quad \exists! H \leq \mathbb{Z}/n \quad |H| = d.$$

Доказательство. Заметим, что существует эпиморфизм $\pi : \mathbb{Z} \mapsto \mathbb{Z}/n$. Так-как $H \leq \mathbb{Z}/n$, существует прообра $\pi^{-1}(H)$.
Докажем, что если $f : g_1 \mapsto g_2$, и $H \leq g_2$, то $f^{-1}(H) \leq g_1$.

$$f(e_{g_1}) = e_{g_2} \implies e_{g_1} \in f^{-1}(H).$$
$$f(a^{-1}) = f(a)^{-1} \implies \left(f(a) \in H \iff f(a)^{-1} \in H\right).$$
$$f(a \cdot b) = f(a) \times f(b) \implies f(a \cdot b) \in H.$$

Тогда мы знаем, что $\pi^{-1}(H) = \langle k \rangle$ - циклическая.
Тогда H тоже циклическая, и равна $\langle \pi(k) \rangle$:
Пусть $y \in \pi^{-1}(H)$. Тогда $y = sk$, а $\pi(y) = \overline{k}\overline{s}$, и $\pi(y) \in H$.
Для доказательство второго утверждения, построим подгруппу порядка d, где d - делитель n.
Возьмём $\frac{n}{d}$, и построим из него подгруппу.
Докажем единственность: любая другая подгруппа того-же порядка так-же циклическая, и порождена элементом порядка d. Назовём этот элемент x Тогда $\frac{n}{(n,x)} = d$, значит, $(n, x) = \frac{n}{d}$. Значит, $x \vdots \frac{n}{d}$, и $\langle x \rangle = \langle d \rangle$. □

Определение 1.1. Пусть $a_1 \dots a_k \in \{1, \dots, n\}$.
Тогда по этим элементом можно построить цикл:

$$C(x) = \begin{cases} x & x \notin \{a_1, \dots, a_k\} \\ a_{i+1} & x = a_i, i < k \\ a_1 & a_k = x \end{cases}$$

Цикл обозначается $(a_1, \dots, a_k)$

Теорема 1.2. Порядок цикла равен его размеру.

Доказательство. Рассмотрим перестановку $c^d(x)$ для каждого x:

1. Если $x \notin \{a_1, \ldots, a_k\}$, то $c^d(x) = x$
2. Если $x = a_1$, то $c^d = x \iff k$.
3. Для других аналогично.

□

Определение 1.2. x называется неподвижной относительно перестановки σ, если $\sigma(x) = x$.
Множество всех неподвижных точек обозначается $\operatorname{Fix}\sigma$.
Дополнение этого множества: $\operatorname{Supp}\sigma$

Определение 1.3. Перестановки σ_1 и σ_2 называются независимыми если $\operatorname{Supp}\sigma_1 \cap \operatorname{Supp}\sigma_2 = \emptyset$.

Лемма 1.3.1. Независимые перестаноки коммутируют.

Определение 1.4. x лежит в одной орбите с y относительно c, если $\exists k \in \mathbb{Z} \quad c^k(x) = y$.

Лемма 1.4.1. Это отношение эквивалентности.

Доказательство. Рефлексивность: $c^0(x) = x$
Симметричность: Если $c^k(x) = y$, то $c^{-k}(y) = x$.
Транзитивность: Если $c^{k_1}(x) = y$, $c^{k_2}(y) = z$, то $c^{k_2}(c^{k_1}(x)) = z \implies c^{k_1+k_2}(x) = z$ □

Теорема 1.3. Любую перестановку $\sigma \in S_n$ можно представить как произведение циклов $c_1, \ldots, c_k$, где циклы попарно независимы.

Доказательство. Разобьём σ на орбиты Ω_i.
Построем циклы:

$$C_i(x) = \begin{cases} x & x \notin \Omega_i \\ \sigma(x) & x \in \Omega_i \end{cases}$$

Докажем что C_i будет циклом:
Возьмём какой-нибудь $x \in \Omega_i$, тогда $\Omega_i = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{k-1}(x)\}$.
Где $k = |\Omega_i|$.
Елси хотя-бы один из элементов вида $\sigma^m(x)$ повторялся с любой из меньших степеней, $m \neq k$, то в $|\Omega_i|$ было-бы m, а не k. Строгое доказательство аналогично докательству про эквивалентность определений порядка элемента.

$$\operatorname{Supp} C_i = \begin{cases} \Omega_i & |\Omega_i| \neq 1 \\ \emptyset & |\Omega_i| = 1 \end{cases}$$

Значит, циклы независимы.
Пусть $x \in \Omega_i$, тогда все циклы кроме i-го ничего с ним не делают, а i-ый переводит в $\sigma(x)$. Значит, композиция (произведение) циклов равно σ. □

Теорема 1.4. Порядок перестановки равен НОК порядков циклов в её разложении.

Доказательство. Пусть $\sigma = c_1 c_2 \dots c_k$
Так-как независимые перестановки коммутируют, $\sigma^d = c_1^d c_2^d \dots c_k^d$.
Эти циклы всё ещё независимы, значит чтобы σ была тождественной, надо чтобы все циклы были тождественными перестановками.
Наименьшее такое d - НОК порядков циклов. □

Теорема 1.5. Обратная перестановка получается переворотом элементов в циклах разложения.

Теорема 1.6. Пусть $\overline{C}_n$ - множество всех циклов в S_n.
Тогда $S_n = \langle \overline{C}_n \rangle$

Определение 1.5. Транспозиция - цикл длины 2.

Теорема 1.7. S_n порождена транспозициями.

Доказательство. Выразим цикл $(a_1, \dots, a_k)$ как произведение транспозицией.

$$(a_1, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_2)\,.$$
$$(a_1, \dots, a_k) = (a_1, a_2)\,(a_2, a_3) \dots (a_{k-1}, a_k).$$ □

Определение 1.6. Перестановка $\sigma \in S_n$, то пара $i < j$ задаёт инверсию для σ, если $\sigma(i) > \sigma(j)$

Определение 1.7. Чётность σ - чётность число инверсий.

Определение 1.8. Знак $\operatorname{sgn}\sigma$ - $-1^{\text{число инверсий}}$

Лемма 1.8.1. Знак перестановки равен 1 если она чётная, и -1 если нечётная.

Лемма 1.8.2.

$$\operatorname{sgn}\sigma = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Доказательство. $j - i$ положительное, $\sigma(j) - \sigma(i)$ отрицательно тогда и только тогда, когда i, j задают инверсию.
Заметим, для каждого множителя в числителе найдётся равный ему по модулю множитель в знаменателе (так-как σ - биекция, в числителе тоже встретится разность любых двух элементов, но возможно в другом порядке). □

Лемма 1.8.3.

$$\operatorname{sgn}\sigma = \prod_{\{i,j\}} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Лемма 1.8.4. $\operatorname{sgn}\sigma$ - гомоморфизм из S_n в $\{\pm 1\}$

Доказательство.

$$\operatorname{sgn}\sigma\tau = \operatorname{sgn}\sigma\operatorname{sgn}\tau = \prod_{\{i,j\}}\frac{\sigma(j)-\sigma(i)}{j-i}\prod_{\{e,k\}}\frac{\tau(k)-\tau(e)}{k-e}.$$

$$i,j = \{\tau(k),\tau(e)\}.$$

$$\prod_{\{k,e\}}\frac{\sigma(\tau(k))-\sigma(\tau(e)}{\tau(k)-\tau(e)}\prod_{\{k,e\}}\frac{\tau(k)-\tau(e)}{k-e} = \prod_{\{k,e\}}\frac{\sigma(\tau(k))-\sigma(\tau(e))}{k-e} = \operatorname{sgn}\sigma\tau. \qquad \square$$

Лемма 1.8.5. $g \in S_n$.

$$g(1,2)g^{-1} = (g(1),g(2)).$$

Лемма 1.8.6. $\operatorname{sgn}(a_1,a_2) = -1$

Доказательство.

$$\operatorname{sgn}(1,2) = -1.$$

Возьмём $g \in S_n$, такое, что $g(1) = a_i$, $g(2) = a_j$.
Тогда $\operatorname{sgn}(a_i,a_j) = \operatorname{sgn} g(1,2)g^{-1} = \operatorname{sgn} g\operatorname{sgn} g^{-1}\operatorname{sgn}(1,2) = -1$ $\square$

Лемма 1.8.7. Если σ - произведение k транспозиций, то $\operatorname{sgn}\sigma = (-1)^k$

Определение 1.9 (Игра в 15)**.** Возьмём квадрат 4×4, поставим в него 15 квадратов, слева-направа, сверху-вниз, помяв местами квадраты 14 и 15.
Можно-ли поменять квадраты обртано?

Лемма 1.9.1. Нет.

Доказательство. Добавим «фантомный» 16-й квадарт. Тогда квадрат эквивалентен перестановке из S_{16}.
Начальная перестаовка эквивалентна $(14,15)$.
Любое действие с квадратом эквивалентно домножению слева на $(16,x)$.
Надо получить тождественную перестановку.
Количество шагов должно быть нечётно, так-как начальная перестановка нечётна, а тождественная - чётна. Заметим, что квадрат 16 является фиксированной точкой и в начальной и в тождественной перестановке.
На каждом ходу квадрат сдвигается на одну клетку, значит движений вверх столько-же, сколько вниз и движений влево столько-же, сколько вправо, иначе квадрат не вернётся в начальную точку.
Значит, шагов должно быть чётно. Противоречие. $\square$