Лекция 3

Циклические группы

Порождающее множество группы

Пусть H подгруппа группы G: $H \subseteq G$; и множество $S \subseteq G, S \subseteq H$.

Определение 1. Подгруппа H, порожденная множеством S – это минимальная подгруппа, содержащая S.

Обозначается $H =< S >$.

Такая подгруппа единственная: $H' \subseteq H \subseteq H'$.

Утверждение 1. Пусть H_1 и H_2 – подгруппы группы G. Тогда $H_1 \cap H_2$ – так же подгруппа G.

Доказательство.

1. $e \in H_1$ и $e \in H_2 \Rightarrow e \in H_1 \cap H_2$.
2. $\forall a \in H_1 \cap H_2 \Rightarrow a \in H_1$ и $a \in H_2 \Rightarrow a^{-1} \in H_1$ и $a^{-1} \in H_2 \Rightarrow a^{-1} \in H_1 \cap H_2$.
3. Замкнутость: $a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow a * b \in H_1 \cap H_2$.
   $a \in H_1$ и $a \in H_2$, $b \in H_1$и $b \in H_2 \Rightarrow a * b \in H_1$ и $a * b \in H_2 \Rightarrow a * b \in H_1 \cap H_2$.

Минимальная подгруппа H, содержащая множество S, образована пересечением всех подгрупп, содержащих S.

Подгруппа, порожденная множеством S — это минимальная подгруппа, содержащая множество S. Она состоит из произведений элементов из S и обратных элементов.

Циклические группы

Определение 2. Если множество S состоит из одного элемента a, то порожденная им подгруппа $< a >$ называется *циклической подгруппой*, порожденной единственным элементом a.

Утверждение 2. Циклическая подгруппа $G =< a >$, порожденная элементом a, состоит из всех степеней элемента a.

$$G = \{\ldots a^{-2}, a^{-1}, a^0, a^1, a^2 \ldots\}.$$

Доказательство.

1. Ассоциативность выполняется.

2. $e = a^0$
3. $(a^n)^{-1} = a^{-n}$
4. Замкнутость. Докажем, что $a^n \cdot a^m = a^{n+m}$.

Рассмотрим следующие четыре случая:

1) $m \geq 0, n \geq 0$ – равенство $a^n \cdot a^m = a^{n+m}$ следует из ассоциативности операции.
2) $m < 0, n < 0$: $a^n \cdot a^m = a^{(-1)(-n)} \cdot a^{(-1)(-m)} = a^{(-1)(-(n+m))} = a^{n+m}$
3) $m < 0, n > 0$:

$$a^n \cdot a^m = a^n \cdot (a^{-1})^{-m} = \begin{cases} (aa^{-1})^n (a^{-1})^{-m-n} = (a^{-1})^{-m-n} = a^{n+m}, \text{если} -m \geq n \\ (aa^{-1})^{-m} a^{n-(-m)} = a^{n+m}, \text{если} -m < n \end{cases}$$

4) $m > 0, n < 0$: $a^n \cdot a^m = a^{n+m}$ – аналогично.

Группа, совпадающая с одной из своих циклических подгрупп называется *циклической*, а элемент – её образующим.

Циклическая группа может быть конечной или бесконечной.

Определение 3. Если все степени элемента a различны, то элемент a – бесконечного порядка.

Пусть $\exists i, j$: $a^i = a^j$. Домножим на a^{-j}, получим $a^{i-j} = e$, (для определенности $i > j$) $\Rightarrow a^p = e$.

a – элемент конечного порядка p, причем порядок a равен наименьшему $p > 0$: $a^p = e$.

Все циклические группы коммутативны (абелевы). Очевидно: $a^n \cdot a^m = a^m \cdot a^n$

Примеры 1 - 2.

1. Группа бесконечно порядка: $G =< \mathbb{Z}, +, 1 >$, $G =< 1 >=< -1 >$.
2. Группа конечного порядка: повороты треугольника

$$G_{\varphi_0} =< \varphi_1 >= \{\varphi_1^{\frac{2\pi}{3}}, \varphi_1^2 = \varphi_2^{\frac{4\pi}{3}}, \varphi_1^3 = \varphi_0 = e\} =< \varphi_2 > \quad p = 3$$

Если в циклической группе элемент a образующий, то a^{-1} также образующий элемент.

Утверждение 3. Пусть a – элемент конечного порядка p, тогда порожденная им группа $G =< a >$ имеет порядок p (содержит p элементов).

Доказательство.

Покажем, что группа состоит из p элементов: $\{a^0, a^1, \dots, a^{p-1}\}$.

1. Покажем, что все p элементов $\{a^0, a^1, \dots, a^{p-1}\}$ различны. От противного. Пусть $\exists i, j: a^i = a^j, i, j = 0, \dots, p-1;\ i > j$ для определенности. Домножим на $a^{-j}: a^i \cdot a^{-j} = e \Rightarrow a^{i-j} = e$, причем $i - j = 1 \dots p-1$, а это противоречит тому, что p – наименьшее натуральное число такое, что $a^p = e \Rightarrow$ все p элементов различны.
2. Покажем, что $a^l, \forall l \in \mathbb{Z}$ совпадет с одним из элементов множества $\{a^0, a^1, \dots, a^{p-1}\}$. Представим $l = kp + r$, остаток $0 \le r \le p-1 \Rightarrow a^l = a^{kp+r} = a^{kp} \cdot a^r = (a^p)^k \cdot a^r = e^k \cdot a^r = e \cdot a^r = a^r \Rightarrow a^r = a^l$.

Теорема 1. Каждая подгруппа циклической группы циклическая.

Доказательство.

Пусть $G = < a >$ циклическая группа и H ее подгруппа, отличная от единичной. Выберем в H элемент с наименьшей положительной степенью: $a^p \in H$, тогда очевидно, что $\forall a^{kp} \in H, k \in \mathbb{Z}$. Докажем, что $H = \{a^{kp}\}, k \in \mathbb{Z}$. Предположим, что это не так, т.е. $\exists a^l \in H$ такое, что l не делится нацело на p. Разделим с остатком:

$$l = kp + r, \quad 0 < r \le p-1 \quad \Rightarrow \quad r = l - kp \Rightarrow$$

$\Rightarrow a^r = a^{l-kp} = a^l \cdot a^{-kp} \Rightarrow a^r \in H$, т.к. a^l и $a^{-kp} \in H$. Это противоречит тому, что p наименьшая положительная степень: $a^p \in H \ \ (r < p)$.

Примеры 3 - 4.

1. Группа бесконечно порядка: $G = < \mathbb{Z}, +, 1 > -$ циклическая: $G = < 1 > = < -1 >$, подгруппа – четные числа: $H = < 2 > = < -2 >$.
2. Группа вращений квадрата: $G = \left\{\varphi_0,\ \varphi_{\frac{\pi}{2}},\ \varphi_\pi,\ \varphi_{\frac{3\pi}{2}}\right\} = < \varphi_{\frac{\pi}{2}} > = < \varphi_{\frac{3\pi}{2}} >$.

   Подгруппа $H = < \varphi_\pi >$.

Симметрические группы

Рассмотрим множество всех биекций множества X в себя: $f: X \to X$. Операция – $\circ$ (композиция).

Покажем, что $< M, \circ, e_x > -$ некоммутативная группа.

1. Композиция ассоциативна:

$$\big(f(x) \circ g(x)\big) \circ h(x) = f(x) \circ \big(g(x) \circ h(x)\big)$$

2. e_x – единичный элемент.
3. Существует обратная функция и она тоже биекция (было доказано в прошлом семестре).
4. Композиция не коммутативна:

$$f(x) \circ g(x) \neq g(x) \circ f(x)$$

Рассмотрим множество $\boldsymbol{X = \{1, \ldots, n\}}$.

Определение 4. Симметрическая группа — это группа всех биекций множества X в себя.

$$f: X \to X.$$

В общем случае множество X может содержать любые n элементов $g_1,\ g_2, \ldots, g_n$.

Элементы симметрической группы называются подстановками.

$$\pi = \begin{pmatrix} 1 & 2 & 3 \ldots \mathrm{n} \\ i_1 & i_2 & i_3 \ldots i_{\mathrm{n}} \end{pmatrix}$$

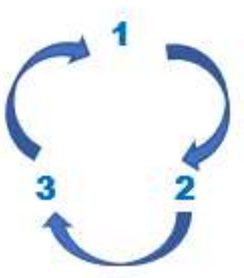
$$i_j \neq i_k, j \neq k \qquad i_j, i_k \in \{1, \ldots, n\}$$

$i_1\ \ i_2\ \ i_3 \ldots i_{\mathrm{n}}$ – перестановка элементов $1\ \ 2\ \ 3 \ldots \mathrm{n}$. Симметрическая группа S_n содержит n! элементов (подстановок) – всевозможных перестановок множества X: $|S_n| = n!$

Пример. $|S_3| = 3! = 6$ элементов

$$\pi_0 = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 2\ 3 \end{pmatrix} = e$$

$$\pi_1 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix} = (123) = (231) = (312)$$



$$\pi_2 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 1\ 2 \end{pmatrix} = (132)$$

$$\pi_3 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix} = (12)$$

$$\pi_4 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 2\ 1 \end{pmatrix} = (13)$$

$$\pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$$

Определение 5. Цикл – это подстановка $\pi = (i_1\, i_2 \dots i_p)$ такая, что

$$\pi(i_1) = i_2,\ \pi(i_2) = i_3, \dots, \pi(i_{p-1}) = i_p,\ \pi(i_p) = i_1.$$

$$\boldsymbol{i_1 \to i_2 \to i_3 \to \dots \to i_p \to i_1.}$$

Определение 6. Циклы π_1 и π_2 – независимые, если они не содержат общих элементов.

Пример 5.

(1 2 4) (3 5) – независимые циклы.

(1 2 4) (3 4 5) – не являются независимыми циклами, т.к. содержат общий элемент 4.

Введем на множестве подстановок операцию умножение (композиция) подстановок: $(\pi_1 \cdot \pi_2)(i) = \pi_1(\pi_2(i))$ – последовательное применение подстановок к каждому элементу.

Пример 6.

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5) \qquad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix} = (1\ 3\ 2\ 4)$$

$$\pi_1 \cdot \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} =$$

$$= (1\ 2\ 3\ 4\ 5)(1\ 3\ 2\ 4) = (1\ 4\ 2\ 5)$$

$$\pi_2 \cdot \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix} = (1\ 4\ 5\ 3)$$

$$\Rightarrow \pi_1 \cdot \pi_2 \neq \pi_2 \cdot \pi_1$$

$\pi_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} = (5\ 4\ 3\ 2\ 1) = (1\ 5\ 4\ 3\ 2)$. В двухэтажной записи – переход снизу вверх. В независимом цикле – переход справа налево:

$$(1 \curvearrowleft 2 \curvearrowleft 3 \curvearrowleft 4 \curvearrowleft 5)^{-1} = (5\ 4\ 3\ 21) = (1\ 5\ 4\ 3\ 2).$$

$\pi_1^2 = (1\ 2\ 3\ 4\ 5) = (1\ 3\ 5\ 2\ 4)$ –переход через одно число.

$$\pi_1^5 = (1)(2)(3)(4)(5) = \pi_0$$

Порядок независимого цикла равен числу элементов в цикле:

$p\,(\pi_1) = 5$, т.к. $\pi_1^5 = (1\ 2\ 3\ 4\ 5)^5 = \pi_0$.

$\pi_1^{-2} = \pi_1^3$ (т.к. $-2 = 3 - 5$). $\pi_1^{-122} = \pi_1^{-2}$ (остаток от деления на порядок – 5).

Порядок подстановки – наименьшее натуральное число p такое, что $\pi^{\mathrm{p}} = e$. Пусть

$$\pi = \pi_1\pi_2\ldots\pi_k$$

Тогда порядок p подстановки π равен

$$p = \text{НОК}(\#\pi_1, \#\pi_2, \ldots, \#\pi_{\mathrm{k}}) = \text{НОК}(p_1, p_2, \ldots, p_{\mathrm{k}})$$

$\#$ – число элементов. p_{i} – порядок цикла $\pi_{\mathrm{i}}, i = 1, \ldots, k$.

Утверждение 4. Порядок подстановки равен наименьшему общему кратному длин независимых циклов (порядков независимых циклов), входящих в разложение этой подстановки: $\pi = \pi_1\pi_2\ldots\pi_k$

Доказательство.

Пусть p – порядок подстановки π, обозначим $q = \text{НОК}(p_1, p_2, \ldots, p_{\mathrm{k}})$. Покажем, что q нацело делится на p, а p нацело делится на q. В этом случае получим, $p = q$.

1. $\pi^q = (\pi_1\pi_2\ldots\pi_k)^q = {\pi_1}^q{\pi_2}^q \ldots {\pi_{\mathrm{k}}}^q$, т. к. циклы независимые. ${\pi_1}^q = e, \ldots, {\pi_{\mathrm{k}}}^q = e$, т.к. $q = \text{НОК}(p_1, p_2, \ldots, p_{\mathrm{k}})$, т.е. q нацело делится на $p_1, p_2, \ldots, p_{\mathrm{k}}$. Следовательно, $\pi^q = e \ldots e = e$ и q нацело делится на p: $q = lp, l \in N$.
2. $\pi^p = (\pi_1\pi_2 \ldots \pi_k)^p = {\pi_1}^p{\pi_2}^p \ldots {\pi_{\mathrm{k}}}^p$, $\pi^p = e$, т.к. p – порядок подстановки π: $\pi^p = e$. Тогда, ${\pi_1}^p{\pi_2}^p \ldots {\pi_{\mathrm{k}}}^p = e$ и, следовательно, ${\pi_1}^p = e, \ldots, {\pi_{\mathrm{k}}}^p = e$, т.к. циклы независимые. Следовательно, p нацело делится на порядки $p_1, p_2, \ldots, p_{\mathrm{k}}$ и p нацело делится на q.

Утверждение доказано.

Пример 7.

$((1\ 2\ 5\ 7)(3\ 4\ 6))^{111} = (1\ 2\ 5\ 7)^{111=4\cdot 28-1}(3\ 4\ 6)^{111=3\cdot 37+0} = (1\ 2\ 5\ 7)^{-1}\pi_0 = (1\ 7\ 5\ 2)$.

Теорема 2. Каждую подстановку можно представить произведением независимых циклов, причем единственным образом с точностью до перестановки циклов.

$$\pi = \pi_1\pi_2\ldots\pi_k$$

Как представить, показано выше – перемножить подстановки.

Доказательство единственности. От противного. Пусть $\pi = \pi_1\pi_2\ldots\pi_k$ – независимые циклы и пусть существует другое представление: $\pi = \sigma_1\sigma_2\ldots\sigma_l$. Выбираем произвольно элемент $i \in \{1, \ldots, n\}$, не остающийся на месте при действии подстановки. Он находится только в одном из независимых циклов каждого представления подстановки π, пусть это будут циклы π_q и σ_r:

$$\pi(i) = \pi_q(i) \quad \text{и} \quad \pi(i) = \sigma_r(i).$$

Будем возводить подстановку π в степени:

$$\pi^s(i) = \pi_q^s(i) = \sigma_r^s(i), \quad (s = 1,2 \ldots).$$

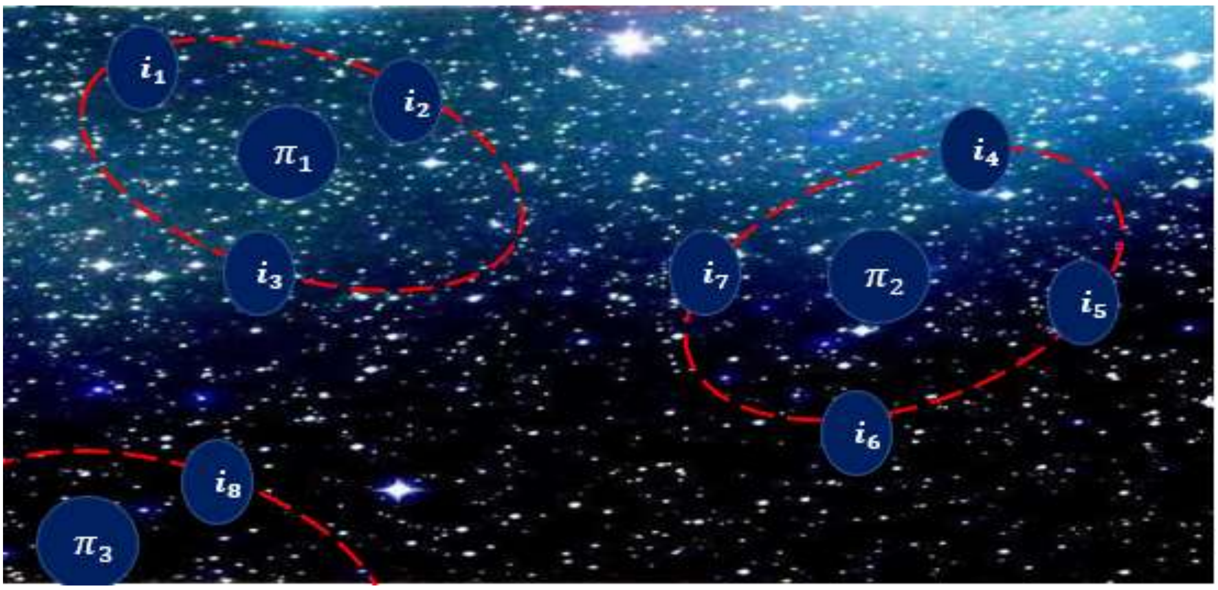
Получаем, что $\pi_q = \sigma_r$, так как цикл однозначно определяется действием подстановки на элемент i. Выбираем элемент, который не входит в полученный независимый цикл. Также возводим подстановку π в степени и получим совпадение следующей пары циклов. Таким образом, выбирая все элементы из π, получим попарное совпадение всех независимых циклов. Следовательно, у подстановки π только одно представление произведением независимых циклов.

Определение 6. Два элемента множества X: $i, j \in X$ – эквивалентные относительно подстановки π, если $\exists s \in \{1, \ldots, n\}: \pi^s(i) = j$.

Это определение порождает отношение эквивалентности на множестве *X*. Это отношение порождает разбиение множества *X* на классы эквивалентности $X_1, X_2, \ldots, X_k$:

$$X = X_1 \cup X_2 \cup \ldots \cup X_k .$$

$X_i \cap X_j = \emptyset, i \neq j$. Каждое из подмножеств разбиения содержит элементы соответствующего независимого цикла $\pi_1, \pi_2, \ldots, \pi_k$ (π-орбиты).



Транспозиции

Определение 7. Транспозиция — это цикл длины два.

Любую перестановку можно разложить в произведение транспозиций. Разложений может быть несколько.

Например, независимый цикл можно разложить в произведение транспозиций по следующим формулам:

$$(i_1\, i_2\, i_3 \ldots i_{n-1}\, i_n) = (i_1\, i_n)(i_1\, i_{n-1})\ldots(i_1\, i_3)(i_1\, i_2)$$

и

$$(i_1\, i_2\, i_3 \ldots i_{n-1}\, i_n) = (i_\mathrm{n}\, i_{n-1})(i_\mathrm{n}\, i_{n-2})\ldots(i_\mathrm{n}\, i_2)(i_\mathrm{n}\, i_1).$$

В правильности разложения легко убедиться перемножив транспозиции.

Пример 8. Два способа разложения подстановки в произведение суперпозиций.

(1 2 3) = (1 3) (1 2) = (3 2) (3 1). Согласно вышеприведенным формулам, число транспозиций для заданной подстановки всегда одно и то же.

Подстановки делятся на четные и нечетные (с четным и нечетным числом транспозиций).

Покажем, что четные подстановки образуют группу:

1) $e = \pi_0$ – четная.
2) π^{-1} – четная перестановка, если π четная.
3) Если π_1 и π_2 – четные подстановки, то и $\pi_1 \cdot \pi_2$ – четная перестановка (замкнутость).

Пример 9. РГР №2.

$(\pi_1 \cdot \pi_2 \cdot \pi_3)^{213} = ((1\,3\,5\,8\,6)(2\,6\,4\,5\,3)(1\,4\,7\,3\,6))^{213} = (1\,8\,6\,3\,4\,7\,2)^{213} =$

$= (1\,8\,6\,3\,4\,7\,2)^3 = (1\,3\,2\,6\,7\,8\,4)$, порядок подстановки $p(\pi) = 7$.

Разложение в транспозиции:

$$(1\,3\,2\,6\,7\,8\,4) = (1\,4)(1\,8)(1\,7)(1\,6)(1\,2)(1\,3)$$

Число транспозиций – 6, подстановка четная.