Теория групп (полное собрание конспектов)

#вшпи #дискретная_математика

Автор всех нижеследующих конспектов: Гридчин Михаил

Алгебраические структуры. Таблица Кэли

Алгебраические структуры

Пусть дано множество M и операция $\times$, определённая на нём. Будем работать только с такими операциями, которые не выводят за пределы множества, то есть $\forall a, b : a \in M, b \in M \implies a \times b \in M$.

Def. Пусть задано множество M и операция $\circ$, заданная на нём. Если выполнена ассоциативность, т.е.

$$a \circ (b \circ c) = (a \circ b) \circ c$$

То эту структуру назовём **полугруппой**.
Пример: слова из алфавита $\{0, 1\}$ и операция конкатенации, определённая на этом множестве.

Def. Полугруппу, у которой существует единственный нейтральный элемент, то есть

$$\exists! e : a \circ e = e \circ a = a$$

Назовём **моноидом**.
Пример: слова из алфавита $\{0, 1\} \cup \{\epsilon\}$ (пустое слово) и операцией конкатенации слов, определённой на этом множестве.
Свойство: можно записать уравнение вида $a \circ x = b$, но не всегда можно решить.

Def. Моноид, для каждого элемента которого существует единственный обратный элемент, то есть

$$\forall x \exists! y : x \circ y = y \circ x = e$$

Назовём **группой**.

Про группы будем говорить всю следующую часть семестра.

Пример решения уравнения:

$$x \circ a = b$$
$$x \circ a \circ a^{-1} = b \circ a^{-1}$$
$$x \circ e = b \circ a^{-1}$$
$$\boxed{x = b \circ a^{-1}}$$

Пример: повороты пространства вокруг центра координат
Пример: пусть $m \in \mathbb{Z}$. $M := \{0, 1, \ldots, m-1\}$ с операцией $+_m$ (сложение по модулю m) образует группу. Стандартное обозначение $(\mathbb{Z}_m, +)$.
Пример: пусть $p \in \mathbb{N}$, p - простое. Тогда $M := \{1, 2, \ldots, p-1\}$ с операцией $\times_p$ (умножение по модулю p) образует группу. Стандартное обозначение $(\mathbb{Z}_p \backslash \{0\}, \times)$. Действительно, по малой теореме Ферма $a^{p-1} \equiv 1 \pmod p \iff a^{p-2} \equiv a^{-1} \pmod p$. Следовательно, для каждого элемента множества есть существует обратный элемент. (нейтральный элемент - 1)
Пример: рассмотрим M - множество перестановок (биекций) длины n. Обозначение перестановки:

$$\pi := \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}, \quad \pi(j) = i_j$$

Определим операцию "композиция перестановок" на M ($\circ$) следующим образом:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}, \quad \pi' = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ j_1 & j_2 & j_3 & \ldots & j_n \end{pmatrix}$$
$$\pi \circ \pi' = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(\pi'(1)) & \pi(\pi'(2)) & \pi(\pi'(3)) & \ldots & \pi(\pi'(n)) \end{pmatrix}$$

Нейтральный элемент

$$e =: id := \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$$

Обратный элемент

$$y = x^{-1} \iff y(x(i)) = i$$

Заметим, что поскольку функция $x(i)$ биективна, то она обратима, то есть $\forall x \exists ! y = x^{-1} \implies$ это группа.
Свойство: можно решить уравнение вида $a \circ x = b$.

Def. Кольцо $(M, +, \times)$ - это

1. коммутативная группа по сложению (то есть $+$ также коммутативен).
2. ассоциативна по $\times$
3. дистрибутивна $a \times (a + c) = a \times b + a \times c$.
   Пример: $(\mathbb{Z}_m, +, \times)$ - кольцо.

Пример: $(\mathbb{Z}_2, \oplus, \wedge)$. Коммутативно по $\oplus$, нейтральный элемент - 0, обратный элемент - само число. Ассоциативна по $\wedge$. Также $(a \oplus b) \wedge c = a \wedge c \oplus b \wedge c \implies$ кольцо.
Свойство: можно записать уравнение вида $a \times x + b = c$, но не всегда можно решить. Чтобы уравнение можно было решить, нужно определение поля.

Def. Поле $(M, +, \times)$ - это

1. коммутативная группа по $+$
2. $M \backslash \{0\}$ - коммутативная группа по $\times$
3. $a \times (b + c) = a \times b + a \times c$
   Пример: множества $\mathbb{Q}, \mathbb{R}, \mathbb{C}, (\mathbb{Z}_p, +, \times)$ - поля.

Конечные группы и таблицы Кэли

Def. *порядок группы* - количество элементов в ней.
Def. *мультипликативная запись*:

$$(a \circ b) \circ c = a \circ (b \circ c)$$
$$\exists! e := 1$$
$$a \circ 1 = 1 \circ a = a$$
$$\forall x \exists! x^{-1}$$
$$x \circ x^{-1} = x^{-1} x = 1$$

Def. *аддитивная запись*:

$$(a + b) + c = a + (b + c)$$
$$\exists! e := 0$$
$$a + 0 = 0 + a = a$$
$$\forall x \exists! (-x)$$
$$x + (-x) = (-x) + x = 0$$

Пример группы порядка k: $(\mathbb{Z}_k, +)$.

Def. Таблица Кэли - таблица для записи результатов применения операции ко всем парам элементов

Пример: таблица Кэли для группы порядка 2. В ней обязательно должен быть нейтральный элемент e и оставшийся элемент $a \neq e$. Заметим, что вариант может быть всего один, поскольку $ae = a, ea = a, ee = e$, остаётся только aa, значит, a - обратный элемент для $a \implies aa = e$

$\circ$	e	a
e	e	a
a	a	e

Значит, любые группы порядка 2 изоморфны (см. далее).

Пусть теперь $n = 3$. По аналогии заполним:

$$\begin{array}{c|ccc} \circ & e & a & b \\ \hline e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{array}$$

Гомоморфизм и изоморфизм. Циклические группы. Смежные классы

Аккуратнее про группы

Вспомним определение группы
Def. Множество M и операцию $\circ$ на нём ("$\circ$": $M \times M \to M$) называют группой G и пишут $G = (M, \circ)$, если:
0) "$\circ$" - алгебраическая операция, то есть $\forall a, b \in G(M) \implies a \circ b \in G$.

1. ассоциативность: $\forall a, b, c \in G \implies a \circ (b \circ c) = (a \circ b) \circ c$.
2. нейтральный элемент $\exists! e \in G : \forall a \in G \implies e \circ a = a \circ e = a$. Нетрудно показать, что нейтральный элемент единственный. Действительно, $e_1 \circ e_2 = e_1 = e_2 \circ e_1 = e_2 \implies e_1 = e_2$.
3. обратный элемент. $\forall a \in G \exists! b \in G : a \circ b = b \circ a = e$. Нетрудно показать, что обратный элемент может единственный. Действительно,

$$\begin{aligned} & a \circ b = a \circ c = e \quad \text{домножим на b слева} \\ & (b \circ a) \circ b = b = (b \circ a) \circ c = c \\ & b = c \end{aligned}$$

Свойство 1. $(a^n)^m = a^{nm}$ - по определению и по ассоциативности.
Свойство 2. $(a^{-1})^m \circ a^m = e$ по ассоциативности $\implies (a^{-1})^m = (a^m)^{-1} =: a^{-m}$.
Def. $a^0 := e$.
Def. *Порядок конечной группы* - количество элементов $:= |G|$.
Def. *Порядок элемента* $a \in G =: ord(a)$ - это такое наименьшее $m \in \mathbb{N} : a^m = e$.
Свойство 3. В конечных группах существуют порядки всех элементов (они конечны).
$\square$ Операция $(\circ)$ алгебраическая $\implies$ все степени элемента $a \in G$ также лежат в G. Рассмотрим ряд:

$$a^1 \quad a^2 \quad a^3 \quad \dots \quad a^N, \quad N > |G|$$

Тогда $\exists i, j \in \{1, 2, 3, \dots, N\} : a^i = a^j$ По принципу Дирихле. Тогда $a^{|i-j|} = e$. $\blacksquare$

Гомоморфизм и изоморфизм

Def. *Гомоморфизм групп* из группы G в группу G' - это такое отображение ϕ

$$\phi : G \to G', \quad G = (M, \circ), \quad G' = (M', *)$$

Что $\boxed{\forall a, b \in G : \phi(a \circ b) = \phi(a) * \phi(b)}$

Свойство гомоморфизма 1. $\phi(a^{-1}) = (\phi(a))^{-1}$, $\phi(e) = e'$.
□

1. $\phi(a \circ e) = \phi(a) * \phi(e) = \phi(a) = \phi(e \circ a) = \phi(e) * \phi(a) \implies \phi(e \circ a) = \phi(a \circ e) = \phi(a)$.
2. $\phi(a \circ a^{-1}) = \phi(a^{-1} \circ a) = \phi(e) = e' = \phi(a) * \phi(a^{-1}) = \phi(a^{-1}) * \phi(a)$. ■

Свойство гомоморфизма 2. $a^m = e \implies \phi(a^m) = e'$ (из свойства гомоморфизма 1) $\phi(a)^m = e'$ (по определению гомоморфизма) $\implies$ *порядок элемента $\phi(a)$ является делителем порядка элемента a.*

Def. *Сюръективный гомоморфизм* из G на G' - гомоморфизм, такой, что

$$\forall b \in G' \exists a \in G : \phi(a) = b \iff Im(\phi) = \phi(G) = G'$$

Def. *Изоморфизм* - гомоморфизм, являющийся биекцией. Обозначается: "$\cong$".

Свойство Изоморфизма. Изоморфизм - это гомоморфизм из G на G' и одновременно гомоморфизм из G' на G.

Таблицы Кэли.

Построим таблицу Кэли для множества на 4 элементах.

$$A : \begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array} \qquad B : \begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & c & e \\ b & b & c & e & a \\ c & c & e & a & b \end{array}$$

В таблице A порядок каждого элемента кроме нейтрального равен 2.
В таблице B порядок каждого элемента равен 3.

Для таблицы A например можно взять множество пар по модулю 2 с поэлементным xor-ом ($\oplus$) ($M = \{(0,0), (0,1), (1,0), (1,1)\}$). Нейтральный - $(0,0)$, обратный к $a \in M$ это сам a.
Для таблицы B подойдёт например $G(\mathbb{Z}_4, +)$.

Утверждение: группы, задающиеся таблицами Кэли для множества на 4 элементах неизоморфны.

□ По *второму свойству гомоморфизма* порядок элемента $\phi(a)$ должен быть делителем порядка элемента a, $\forall a \in G'$. Но порядки элементов $\phi(a)$ все кроме нейтрального равны 2, а у a порядки все кроме нейтрального равны 3. Как видим, 2 - не делитель 3. ■

Note. Группа порядка 5 всего одна.

Свойства групп

Свойство 4. Если $a^m = e$, то порядок a - делитель m, $m \in \mathbb{N}$.
☐ Мы точно знаем, что $ord(a) \leq m$. Обозначим $n := ord(a)$. Разделим m на n с остатком:

$$m = nq + r \implies a^m = e = \underbrace{(a^n)^q}_{=e} \circ a^r = a^r$$

Но при этом $0 \leq r < n$ и при этом n - наименьшее натуральное число, при котором $a^n = e \implies r = 0$. ■

Def. Группа G называется *циклической*, если $\exists a \in G$ (порождающий элемент):

$$\forall b \in G \exists m \in \mathbb{Z} : a^m = b$$

Замечание. m в определении именно *целое*, не натуральное, что важно в следующем утверждении.
Утверждение. Группа $(\mathbb{Z}, +)$ - циклическая группа . Действительно, порождающий элемент - 1 или -1.
Следствие. Порождающий элемент не обязательно единственный.

Пример. Группа $(\mathbb{Z}_m, +)$ - циклическая группа. Порождающий элемент - 1.

Def. Если группа G циклическая и $|G| = m$, то её обозначают C_m.
Теорема. Все циклические группы из m элементов изоморфны между собой.
☐ Пусть есть циклические группа C_m и C'_m, неизоморфные между собой:

$$\begin{array}{llllll} C_m: & e & a & a^2 & \ldots & a^{m-1} \\ C'_m: & e & b & b^2 & \ldots & b^{m-1} \end{array}$$

Все элементы первой и второй групп различны, иначе бы порядки групп были меньше. То есть *порядок порождающего элемента совпадает с порядком группы*. Изоморфизм тривиальный. Сопоставим $\phi(a^i) = b^i$. ■
Следствие. Всякая циклическая группа $C_m \cong (\mathbb{Z}_m, +)$.

Def. Будем говорить, что H - подгруппа группы $G(M, \circ)$ и записывать $H < G$, если

$$\begin{cases} H \subseteq G \\ H \text{ - группа относитаельно } (\circ) \end{cases}$$

Def (эквивалентное определение подгруппы). H - подгруппа G, если:

$$\begin{cases} H \subseteq G \\ \forall a, b \in H \implies a \circ b \in H \\ \forall a \in H \implies a^{-1} \in H \end{cases}$$

Теорема. Приведённые определения подгруппы эквивалентны.
$\square$
Пусть выполнено первое. Тогда второе следует из аксиоматики группы напрямую.
Пусть выполнено второе. Тогда H замкнуто относительно групповой операции ($\circ$), а также взятие обратного элемента также не выводит за пределы H из аксиоматики группы.
Отдельно доказывается, что нейтральный элемент также лежит в H. Это следует из единственности e также из аксиоматики группы и из того, что $a \circ a^{-1} = e$.
$\blacksquare$

Теорема (критерий подгруппы). H является подгруппой G тогда и только тогда, когда $\forall a, b \in H \implies a \circ b^{-1} \in H$ и $H \subseteq G$.
$\square$ В одну сторону очевидно и в другую тоже очевидно.
Слева направо. Если $b \in H$, то и $b^{-1} \in H$, значит $a \circ b^{-1} \in H$.
Справа налево. Если $\forall a, b \in H$ верно, что $a \circ b^{-1} \in H$, тогда

1. возьмём $b = a$. Тогда $e \in H$.
2. возьмём $a = e$. Тогда $b^{-1} \in H$.
3. возьмём $b = b^{-1}$. Тогда $a \circ b^{-1^{-1}} = a \circ b \in H$. И получили первый пункт эквивалентного определения подгруппы $\blacksquare$

Теорема. Пусть дана произвольная группа G и элемент $a \in G : ord(a) = n, n \in \mathbb{N}$. Тогда

$$H := \{a^0, a^1, \ldots, a^{n-1}\} < G$$

$\square$ Заметим, что $H \subseteq G$. Тогда применим критерий подгруппы и получим требуемое. $\blacksquare$

Пример. Пример бесконечной группы, у которой есть конечные циклические подгруппы. Рассмотрим множество всех многочленов с коэффициентами по модулю m. Обозначается $\mathbb{Z}_m[x]$. Причём порядок каждого элемента - делитель m.

Def. Пусть $H < G$. Возьмём $g \in G$. Будем говорить, что gH - *левый смежный класс по подгруппе H с представителем g*, если

$$gH := \{g \circ h \mid h \in H\}$$

Утверждение. Смежные классы не пересекаются или совпадают.
$\square$ Пусть $\exists z \in aH \cap bH \implies \exists h_1 \in H, h_2 \in H : z = a \circ h_1 = b \circ h_2 \implies a = b \circ h_2 \circ h_1^{-1}$, также $\implies \forall t \in aH \to t = a\tilde{h} = b \circ \underbrace{h_2 \circ h_1^{-1} \circ \tilde{h}}_{\in H} \implies t \in bH$. $\blacksquare$

Нормальные подгруппы. Факторгруппы.

Теорема Лагранжа

На прошлой лекции было доказано, что левые (правые) смежные классы не пересекаются или совпадают.

Теорема (Лагранжа). Количество элементов в группе делится на количество элементов в подгруппе. Записывается:

$$\boxed{|G| = (G : H)|H|}$$

Где $(G : H)$ - индекс подгруппы H.

$\square$
Докажем для левых смежных классов, для правых доказательство аналогично.

ШАГ 1. Докажем сначала, что количество элементов в $|gH| = |H|$. То есть, другими словами $\forall h_1, h_2 \in H, h_1 \neq h_2 \implies g \circ h_1 \neq g \circ h_2$. Действительно, если это не так и выполнено $g \circ h_1 = g \circ h_2$, то умножим обе части на $g^{-1} \in G$ слева. Получим:

$$g^{-1} \circ (g \circ h_1) = g^{-1} \circ (g \circ h_2)$$
$$e \circ h_1 = e \circ h_2$$
$$h_1 = h_2$$

Противоречие, значит, количество элементов в $|gH|$ действительно равно количеству элементов в $|H|$.

ШАГ 2. Докажем, что $\forall g \in G \implies g \in gH$. Действительно, поскольку H - подгруппа, то $e \in H$. Но тогда $g \circ e = g \in gH$.

ШАГ 3. Смежные классы не пересекаются или совпадают. Тогда группа G разбита на непересекающиеся подмножества $aH, bH, \ldots$, в каждом из которых ровно по $|H|$ элементов. Также каждый элемент G принадлежит какому-то смежному классу. Значит, количество элементов в G делится на количество элементов в H. Получили требуемое. А индекс подгруппы H - это количество различных смежных классов (левых)
$\blacksquare$

Def. *Правый смежный класс по подгруппе H группы G с представителем $g \in G$*:

$$Hg := \{h \circ g \mid h \in H\}$$

Нормальные подгруппы

Def. Подгруппа $H < G$ называется *нормальной* (и обозначается $H \lhd G$), если $\forall g \in G \implies gH = Hg$.

Размышления. $gH = Hg \iff \{g \circ h \mid h \in H\} = \{h \circ g \mid h \in H\}$. Умножим на g^{-1} справа. Но тогда получим:

$$gHg^{-1} = H$$

Тогда можно ввести эквивалентное определение нормальной подгруппы.

Def (эквивалентное определение нормальной подгруппы).

$$H \lhd G \iff \forall g \in G, \forall h \in H \implies g \circ h \circ g^{-1} \in H$$

Теорема: Приведённые определения эквивалентны.
□
$1 \Rightarrow 2$: $H \lhd G \implies gH = Hg \implies \forall h_1 \in H \exists h_2 \in H : g \circ h_1 = h_2 \circ g \implies g \circ h_1 \circ g^{-1} = h_2 \in H$.
$1 \Leftarrow 2$: $\forall g \in G, \forall h \in H \implies g \circ h \circ g^{-1} \in H$. Тогда рассмотрим $gHg^{-1} = \{g \circ h \circ g^{-1} \mid h \in H\}$. Но это множество содержит столько же элементов, сколько и H. Почему меньше быть не может? Смотрите первый шаг доказательства теоремы Лагранжа. Тогда поскольку также все элементы $g \circ h \circ g^{-1} \in H \forall h \in H \forall g \in G$, то выполнено $gHg^{-1} = H$. Умножим на g справа, получим $gH = Hg$, это и требовалось показать.
■

Факторгруппы

"Нормальные подгруппы - это достаточно ценная вещь. С её помощью мы можем делать так называемые факторгруппы. Пусть есть множество каких-то объектов, которые вместе с операцией образуют группу. Элементов в ней может быть достаточно много, но иногда для наших прикладных целей столько элементов рассматривать не надо. Надо рассматривать какие-то более группы. Факторизация - это возможность объединять некоторые группы в подмножества и делать групповую операцию над укрупнёнными подгруппами".

Def. Пусть $H \lhd G$. Рассмотрим смежные классы. Для определённости левые по H. Введём операцию $(aH) * (bH) := (a \circ b)H, a \in G, b \in G$. То есть это операция на множестве смежных классов, которая двум смежным классам сопоставляет третий.

Утверждение + Def. Множество смежных классов относительно данной операции образует группу (называемую *факторгруппой группы G по нормальной подгруппе H и обозначаемую G/H*).
□
ШАГ 1. Докажем ассоциативность $(*)$.

$$\forall a, b, c \in G \implies \begin{cases} ((aH) * (bH)) * (cH) = ((a \circ b)H) * (cH) = ((a \circ b) \circ c)H = (a \circ b \circ c)H \\ (aH) * ((bH) * (cH)) = (aH) * ((b \circ c)H) = (a \circ (b \circ c))H = (a \circ b \circ c)H \end{cases}$$

Получили требуемое.

ШАГ 2. Докажем существование нейтрального элемента. Докажем, что $eH = H$ - искомый нейтральный элемент. Действительно,

$$\forall a \in G \implies (aH) * (eH) = (a \circ e)H = (e \circ a)H = (eH) * (aH)$$

Теперь докажем единственность нейтрального элемента. Доказательство от противного. Пусть существуют nH и eH - нейтральные элементы относительно операции $(*)$. Заметим, что e - нейтральный элемент относительно операции $(\circ)$, а n - нет. Тогда:

$$(nH) * (eH) = (eH) = (nH)$$

Первое равенство из того, что nH - нейтральный, второе равенство из того, что eH - нейтральный. Получили, что $eH = nH$. Противоречие. Значит, нейтральный элемент единственный. Получили требуемое.

ШАГ 3. Докажем существование обратного элемента. Действительно,
$\forall a \in G \implies (aH) * (a^{-1}H) = (a^{-1}H) * (aH) = eH = H$.
Единственность доказывается аналогично шагу 2.

Значит, множество смежных классов относительно введённой операции $(*)$ образует группу.
■

Вопрос. Зачем нам нужна была нормальность подгруппы, если мы её нигде не использовали? Ответ: мы воспользовались нормальностью подгруппы H в тот момент, когда ввели операцию $(*)$. Оказывается, что её можно определить для нормальной подгруппы и нельзя для ненормальной. Действительно, корректности (независимости от представителя) должно быть выполнено:

$$\begin{cases} \forall a_1 \in aH \implies a_1H = aH \\ \forall b_1 \in bH \implies b_1H = bH \end{cases}$$

□
$(a_1H) * (b_1H) = (a_1 \circ b_1)H$. Покажем, что $(a_1 \circ b_1)H = (a \circ b)H$. Для этого нам достаточно найти хотя бы один общий элемент, чтобы они были равны (поскольку смежные классы не пересекаются или совпадают). Покажем, что $(a_1 \circ b_1) \in (a \circ b)H$. Действительно,

$$\begin{aligned} &a_1 \in aH \implies \exists h_a \in H : a_1 = a \circ h_a \\ &b_1 \in bH \implies \exists h_b \in H : b_1 = b \circ h_b \\ &a_1 \circ b_1 = a \circ \boxed{h_a \circ b} \circ h_b \end{aligned}$$

Но у нас нет коммутативности, чтобы поменять h_a и b местами, чтобы получить требуемое. В этот момент нам и приходит на помощь нормальность подгруппы. Мы знаем, что

$$bH = Hb \implies \forall h \in H \exists \tilde{h} \in H : h \circ b = b \circ \tilde{h}$$

Но тогда и для $\boxed{h_a \circ b}$ найдётся такой элемент $\tilde{h}_a : b \circ \tilde{h}_a = h_a \circ b$. Итого получаем:

$$a_1 \circ b_1 = a \circ b \circ \underbrace{\tilde{h}_a \circ h_b}_{=:\tilde{h} \in H} = a \circ b \circ \tilde{h}$$

Но так как $\tilde{h} \in H$, то и $(a_1 \circ b_1) \in (a \circ b)H$.
■

Вопрос. Сколько элементов в факторгруппе? Ответ: индекс H. Действительно, вся факторгруппа состоит из всех смежных классов, количество которых равно индексу H.

Гомоморфизм групп

Из прошлой лекции *гомоморфизм* - это такое отображение $\phi : G(M, (\circ)) \to G'(M', (*))$, что $\forall a, b \in G \implies \phi(a \circ b) = \phi(a) * \phi(b)$.
Уже доказанные свойства:

- $\phi(e) = e'$
- $\phi(a^{-1}) = (\phi(a))^{-1}$. Следствие: $\phi(a^m) = (\phi(a))^m$
- порядок элемента $\phi(a)$ является делителем порядка элемента a.

Def. *Образ гомоморфизма* - $Im\phi = \phi(G) = \{\phi(a) \mid a \in G\}$.
Теорема. Образ гомоморфизма - это подгруппа G'.
□
Из определения $Im\phi \subseteq G'$. Применим *критерий подгруппы* для доказательства, что это подгруппа. Рассмотрим произвольные элементы $c, d \in Im\phi$. По определению образа $\exists a, b \in G : \phi(a) = c, \phi(b) = d$. Рассмотрим $(c * d^{-1})$:

$$c * d^{-1} = \phi(a) * \phi(b^{-1}) = \phi(a \circ b^{-1}) \in Im\phi$$

Следовательно, $Im\phi < G'$ по критерию подгруппы.
■

Def. *Ядро гомоморфизма* - $Ker\phi = \{g \mid g \in G, \phi(g) = e'\}$.
Теорема. Ядро гомоморфизма - это подгруппа G.
□
Из определения $Ker\phi \subseteq G$. Применим *критерий подгруппы* для доказательства, что это подгруппа. Возьмём произвольные $a, b \in Ker\phi$. Тогда:

$$\phi(a \circ b^{-1}) = \phi(a) * \phi(b) = e' * (e')^{-1} = e' \implies a \circ b^{-1} \in Ker\phi$$

Следовательно, $Ker\phi < G$ по критерию подгруппы.
■

Теорема. $Ker\phi \lhd G$.
□
Рассмотрим произвольный элемент $g \in G$. Рассмотрим $gKer\phi$. Поскольку $Ker\phi < G$, то $|gKer\phi| = |(Ker\phi)g| = |Ker\phi|$. Рассмотрим произвольное $\boxed{t \in gKer\phi}$. Для него

$\exists h \in Ker\phi : t = g \circ h$. Рассмотрим $g \circ h \circ g^{-1}$. Для него выполнено $\phi(g \circ h \circ g^{-1}) = \phi(g) * \phi(h) * \phi(g^{-1})$. Заметим, что $\phi(h) = e'$, так как $h \in Ker\phi$. Тогда $\phi(g \circ h \circ g^{-1}) = e' \implies (g \circ h \circ g^{-1}) \in Ker\phi \implies \underbrace{g \circ h}_{=t} \in (Ker\phi)g \implies \boxed{t \in (Ker\phi)g}$. Но t и g были выбраны произвольно. Тогда по определению нормальной подгруппы $Ker\phi \triangleleft G$.

■

Факторгруппа по ядру гомоморфизма

Рассмотрим $G/Ker\phi$ (факторгруппа G по подгруппе $Ker\phi$).

Утверждение. Два элемента группы G содержатся в одном смежном классе по $Ker\phi \iff$ их образы совпадают. То есть $a, b \in gKer\phi \iff \phi(a) = \phi(b)$. То есть между элементами $Im\phi$ и смежными классами биекция $\phi(g) \iff gKer\phi$.

□

$\Rightarrow$

Рассмотрим произвольные $a, b \in gKer\phi \implies \exists h_a, h_b \in Ker\phi : a = g \circ h_a, b = g \circ h_b$.
Рассмотрим $\phi(a) = \phi(g \circ h_a) = \phi(g) * \underbrace{\phi(h_a)}_{=e'} = \phi(g)$. Аналогично, $\phi(b) = \phi(g)$. Тогда

$\phi(a) = \phi(b)$.

$\Leftarrow$

Пусть $\phi(a) = \phi(b) \implies \phi(a \circ b^{-1}) = \phi(a) * (\phi(b))^{-1} = e' \implies (a \circ b^{-1}) \in Ker\phi$. Тогда поскольку $a = (a \circ b^{-1}) \circ b \in (Ker\phi)b = b(Ker\phi)$. А также $a \in aKer\phi$. А значит смежные классы совпадают, поскольку имеют общий элемент.

■

Теорема. $Im\phi \cong G/Ker\phi$ (гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма).

□

В предыдущем утверждении мы доказали биекцию между $Im\phi$ и $G/Ker\phi(\times)$
$f : \phi(g) \iff gKer\phi$.

$$f(\phi(g)) = gKer\phi$$

$$f(\phi(a) * \phi(b)) = f(\phi(a \circ b)) = (a \circ b)Ker\phi$$

$$f(\phi(a)) \times f(\phi(b)) = aKer\phi \times bKer\phi = (a \circ b)Ker\phi$$

Следовательно, $f(\phi(a) * \phi(b)) = f(\phi(a)) \times f(\phi(b))$. Значит, f - гомоморфизм. Но f - биекция. Следовательно, f - изоморфизм.

■

Теорема Кэли. Группа перестановок. Порядок элементов. Транспозиции.

Замечание. В этом конспекте будем считать, что знак $(\circ)$ обозначает композицию и вычисляется *справа налево*, а произведение с опусканием знака или $(\cdot)$ обозначает групповую операцию.

Теорема Кэли

Теорема Кэли. Пусть G - конечная группа. $|G| =: n$. Тогда $\exists H < S_n : G \cong H$. То есть всякая конечная группа изоморфна некоторой подгруппе группы перестановок из n элементов. Другими словами $G \cong L_G < S_n$.

□

Так как G - конечная группа, пронумеруем все элементы этой группы, как $g_2, g_2, \dots g_n$. Рассмотрим левые сдвиги $L_a, a \in G$:

$$\begin{aligned} &g_1 \to ag_1 \\ &g_2 \to ag_2 \\ &\dots \\ &g_n \to ag_n \end{aligned}$$

Поскольку все получившиеся элементы лежат в G, а также они все различны (иначе умножим на a^{-1} слева и получим равенство, см. предыдущие лекции), получаем, что L_a - это какая-то перестановка исходных элементов $g_1, g_2, \dots, g_n$ (взаимно однозначное соответствие). Рассмотрим L_a для всех $a \in G$. Заметим, что они образуют группу. Действительно, $L_e = e'$ (тождественная перестановка, $\forall g_i \in G \implies eg = g$).
$L_a \circ L_{a^{-1}} = L_{a^{-1}} \circ L_a = L_e$. Действительно, $\forall g_i \in G \implies g_i = a^{-1}ag_i$. Также по определению $L_a \circ L_b = L_{ab} \implies L_a \circ (L_b \circ L_c) = (L_a \circ L_b) \circ L_c = L_{abc}$. Таким образом, доказали существование нейтрального элемента, обратного элемента и ассоциативность. Докажем теперь, что эта группа изоморфна группе G. Действительно, во первых мы доказали, что L_a - биекция $\forall a \in G$. А также мы показали, что $L_a \circ L_b = L_{ab} \implies$ по определению $G \cong L_G$. Поскольку $|L_G| = n$ и $L_G < S_n$, а также L_G - группа относительно той же групповой операции, что и S_n (композиция), то доказали альтернативную формулировку теоремы.

■

Группа перестановок

Def. *Перестановкой* назовём биекцию конечного множества на себя.

Def. *Перестановка в канонической записи* длины n обозначается следующим образом:

$$\pi := \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

Note. Перестановка - это также таблично заданная функция.

Def. *Произведение перестановок* длины n определим следующим образом:

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

$$\sigma \circ \pi := \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ \sigma(\pi(1)) & \sigma(\pi(2)) & \dots & \sigma(\pi(i)) & \dots & \sigma(\pi(n)) \end{pmatrix}$$

Def. *Неканонической записью перестановки* длины n назовём такую перестановку, в которой аргументы могут быть перемешаны. При этом если $\pi(i) = i$, то этот столбец можно опустить.
Пример.

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

Def. *Обратной перестановкой* π^{-1} к перестановке π длины n назовём перестановку:

$$\pi^{-1} := \begin{pmatrix} \pi(1) & \pi(2) & \dots & \pi(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

Def. *Циклом* длины k перестановки длины n назовём последовательность элементов, где каждый элемент переходит в следующий, а последний - в первый и будем обозначать:

$$(i_1 \quad i_2 \quad \dots \quad i_k) = \begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k \\ i_2 & i_3 & \dots & i_k & i_1 \end{pmatrix}$$

Note. Цикл - это биекция k-элементного множества на себя.
Note. Из предыдущего замечания следует, что цикл - это элемент группы перестановок.

Def. *Цикловой записью перестановки* длины n

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

Определяется представление перестановки в виде произведения непересекающихся циклов.

Пример. Рассмотрим перестановку

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

У неё есть следующие циклы:

$$1 \to 3 \to 5 \to 1$$
$$2 \to 4 \to 2$$

Значит

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

Утверждение. Любую перестановку можно разложить в непересекающиеся циклы.
Утверждение. Циклы перестановки коммутируют, то есть, если a и b - циклы, то

$a \cdot b = b \cdot a$ и они задают одну и ту же перестановку. Доказательство по определению.
Утверждение. Любая перестановка раскладывается в произведение (композицию) **непересекающихся** циклов единственным образом с точностью до записи цикла и порядка циклов.

Утверждение. Порядок цикла длины k равен k, то есть $ord(i_1, i_2, \ldots, i_k) = k$
□
Действительно, по определению цикла элемент i_1 переходит в элемент i_2 и так далее, то есть

$$i_1 \to i_2 \to \ldots \to i_k \to i_1$$

Количество переходов равно k, а значит порядок каждого элемента равен k, значит и порядок всего цикла равен k. То есть $(i_1, i_2, \ldots, i_k)^k = (i_1, i_2, \ldots, i_k)$.
■

Def + теорема. Если перестановка записана в виде непересекающихся циклов длины $c_1, c_2, \ldots, c_m$, то *порядком данной перестановки* равен $НОК(c_1, c_2, \ldots, c_m)$.
□
Действительно, поскольку порядок перестановки должен делиться на порядок каждого цикла (чтобы элемент i перешёл сам в себя), а циклы не пересекаются, то $ord(\pi) = НОК(c_1, c_2, \ldots, c_m)$.
■

Транспозиции

Def. *Транспозиция* - это цикл длины 2. То есть цикл (i_1, i_2).
Note. Транспозиция - это элемент группы перестановок
Note. Для транспозиции (a_i, a_j) обратная транспозиция - (a_i, a_j), то есть $(a_i, a_j)^2 = e = \mathrm{id}$.

Теорема. Любая перестановка представима в виде произведения транспозиций.
□
Нестрогое доказательство: из курса алгоритмов или из детского сада известно, что существуют сортировки сравнением. А значит, перестановка - это какое-то количество применённых операций $swap(a_i, a_j)$, что и задаёт транспозицию.

Строгое доказательство: Докажем сначала, что любой цикл можно разложить в произведение транспозиций. Действительно, рассмотрим цикл длины m:

$$(a_1 \quad a_2 \quad \ldots \quad a_m)$$

Такой цикл можно представить в виде произведения транспозиций следующим образом:

$$(a_1 \quad a_2 \quad \ldots \quad a_m) = (a_1 \quad a_m)\,(a_1 \quad a_{m-1}) \cdots (a_1 \quad a_3)\,(a_1 \quad a_2)$$

В данной записи умножение выполняется справа налево, как композиция функций. Действительно, элемент a_i, где $i \in \{2, 3, \ldots, m-1\}$ сначала перейдёт в a_1, а на следующем шаге перейдёт в a_{i+1}, а далее к нему не будет выполнено никаких операций.

Элемент a_1 перейдёт в a_2 на самом первом шаге, а далее к нему не будет выполнено никаких операций. Элемент a_m перейдёт в a_1 на последнем шаге. В результате получаем, что $\forall i \in \{1, 2, \dots, m\} : a_i \to a_{i+1 \pmod m}$. Значит, любой цикл представим в виде произведения транспозиций. Но любая перестановка представима в виде непересекающихся и коммутирующих циклов, а значит, что она представима и в виде произведения транспозиций.

■

Теорема. Пусть перестановка π задана произведением транспозиций:

$$\pi = t_1 t_2 \dots t_k$$

Тогда

$$\boxed{\pi^{-1} = t_k^{-1} t_{k-1}^{-1} \dots t_1^{-1} = t_k t_{k-1} \dots t_2 t_1}$$

□

Поскольку транспозиция - это элемент группы перестановок, то для транспозиций выполняется та же аксиоматика групп, что и для перестановок. Тогда если положим

$$\pi = t_1 t_2 \dots t_k$$

То для π^{-1} будет выполнено

$$\pi^{-1} = (t_1 t_2 \dots t_k)^{-1} = t_k^{-1} t_{k-1}^{-1} \dots t_1^{-1}$$

Докажем этот факт по индукции.

БАЗА. $k = 1$: $(t_1)^{-1} = t_1^{-1}$. Очевидно верно

ШАГ. Предположим, что предположение верно для k, докажем для $k+1$.

Пусть $\sigma = t_1 t_2 \dots t_k t_{k+1} = \sigma' t_{k+1}$, где $\sigma' = t_1 t_2 \dots t_k$. Тогда:

$$\sigma^{-1} = (\sigma' t_k)^{-1} = t_{k+1}^{-1} (\sigma')^{-1} = t_{k+1}^{-1} t_k^{-1} \dots t_1^{-1}$$

Получили требуемое.

Теперь, поскольку $t = t^{-1}$, получаем второе требуемое равенство.

■

Теорема. Для различных разложений перестановки в произведение транспозиций чётность количества транспозиций сохраняется.

□

Предположим противное, что для перестановки π существует разложение на чётное количество транспозиций и на нечётное количество транспозиций. Вспомним, что π^{-1} представляет обратное произведение транспозиций для π . Рассмотрим произведение $\pi \circ \pi^{-1}$, как произведение их транспозиций в одном и в другом случае.

$$\pi \circ \pi^{-1} = e = \underbrace{\sigma_1 \sigma_2 \dots \sigma_k}_{\text{нечётное количество}}$$

Докажем, что если e раскладывается в n транспозиций, то e раскладывается и в $n-2$ транспозиции. Рассмотрим в произведении такое $\sigma_p = (s,t)$, что элемент s правее ($\forall i > p$) не встречается. Рассмотрим σ_{p-1}. Есть несколько случаев.

1. $\sigma_{p-1} = (s,t)$, тогда $\sigma_{p-1}\sigma_p = e$.
2. $\sigma_{p-1} = (q,r)$, $\{q,r\} \cap \{s,t\} = \varnothing$. То есть они не пересекаются, следовательно, они коммутируют. Поменяем местами: $\sigma_{p-1}\sigma_p = \sigma_p\sigma_{p-1}$. То есть мы сместили выбранный s элемент левее
3. $\sigma_{p-1} = (s,r)$. Тогда $\sigma_{p-1}\sigma_p = \begin{pmatrix} s & r & t \\ t & s & r \end{pmatrix} = (s,t)(r,t)$. То есть мы опять сдвигаем s влево.
4. $\sigma_{p-1} = (t,r)$. Тогда $\sigma_{p-1}\sigma_p = \begin{pmatrix} s & t & r \\ r & s & t \end{pmatrix} = (s,r)(t,r)$. То есть мы опять сдвигаем s влево.

   Поймём, что произойдёт с s. Либо в какой-то момент подойдёт первый случай, и s сократится, либо получим, что s содержится в первой транспозиции, а правее не будет ни одной транспозиции, содержащей s (по построению). То есть

   $$e = (s,t')\underbrace{(\ldots)\cdots(\ldots)}_{\text{не содержат } s}$$

   Тогда s отображается в t'. Может ли быть такое, если $t' \neq s$? Нет, поскольку в итоге s должен перейти в s, чтобы перестановка была нейтральной. Значит, такого быть не может и в какой-то момент s сократится с какой-то ещё скобкой. То есть в какой-то момент выполнится критерий первого случая.
   Повторяя описанные выше действия, каждый раз сокращаются ровно 2 скобки, но поскольку изначально их было нечётное количество, то в конце концов останется одна скобка из двух разных элементов, а такого быть не может. Значит, наше предположение было неверным, и чётность количества транспозиций сохраняется.
   ■

Def. Чётность количества транспозиций в перестановке назовём *чётностью перестановки*.
Утверждение. В группе перестановок одинаковое количество чётных и нечётных перестановок. Доказательство почти тривиально (умножим на транспозицию (a_1, a_2))
Утверждение. Множество чётных перестановок образует подгруппу группы перестановок.
Утверждение. Подгруппа чётных перестановок является нормальной.