Лекция 7. Гомоморфизм и изоморфизм. Циклические группы. Смежные классы

#вшпи #дискретная_математика #теория

Автор конспекта: Гридчин Михаил

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).
□ 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 $a^{|i-j|} = e$. ■

Гомоморфизм и изоморфизм

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

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

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

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

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

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

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

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

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:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

B:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

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 хог-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 $\varphi(a)$ должен быть делителем порядка элемента a, $\forall a \in G'$. Но порядки элементов $\varphi(a)$ 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:

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

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 $\varphi(a^i) = b^i$. ■
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.
□
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 $a \circ a^{-1} = e$.
■

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 $H \subseteq G$.
□ 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 ■

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

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

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

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.
□ 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 $\implies \forall t \in aH \to t = a\tilde{h} = \underbrace{b \circ h_2 \circ h_1^{-1} \circ \tilde{h}}_{\in H} \implies t \in bH$. ■