# Семинар №4 по курсу «Основы высшей алгебры и теории кодирования»

Репеев Роман, Шиманогов Игорь



## Порождающие соотношения

**Определение 1 (Порожденная группа)**
Группа $G$ называется *порождённой* множеством $M$, если она является *наименьшей по включению* группой, содержащей $M$, то есть пересечением всех таких групп.
Обозначение: $G = \langle M \rangle$. Множество $M$ называется *множеством порождающих*.

Конструктивно это означает, что группа (или подгруппа), порожденная некоторым множеством, содержит единицу, обратные к элементам множества, а также всевозможные произведения этих элементов.

Идея задания группы в том, чтобы указать некоторое множество порождающих и указать дополнительные *порождающие соотношения*.

**Пример 1 (Циклическая группа)**
*Группа $C_n$ порождается множеством $\{a\}$ и соотношением $a^n = e$.*

**Задача 1**
Группа $G$ порождена множеством $\{a, b\}$ и задана соотношениями (в аддитивной записи):

$$ab = ba, \quad 12a + 7b = 0, \quad 10a + 9b = 0$$

Доказать, что $G$ конечна. Является ли она циклической?

**Решение** Из первого соотношения ясно, что $G$ абелева. Тогда

$$(12a + 7b) - (10a + 9b) = (12a - 10a) + (7b - 9b) = 2a - 2b = 0 \Rightarrow 2a = 2b$$

$$12a + 7b = 6(2a) + 7b = 12b + 7b = 19b = 0$$

$$20a = 20b = 19b + b = 0 + b = b \Rightarrow b = 20a$$

Из последнего ясно, что группа является циклической с порождающим $a$.
Также из $19b = 0$ получаем, что $38b = 38a = 0$, то есть порядок $a$ не больше 38, значит, группа конечна.

## Диэдральная группа

**Определение 2 (Группа диэдра)**
Диэдральной группой (диэдр — «двугранник») $D_n$ называют группу симметрий правильного $n$-угольника, то есть группу преобразований, переводящих многогранник в него же.

Группа диэдра содержит $2n$ элементов: тождественное преобразование, $n-1$ поворот вокруг оси $C_n$, проходящей через центр, и по одной симметрии (или же повороту на $\pi$) относительно $n$ осей $C_2$.

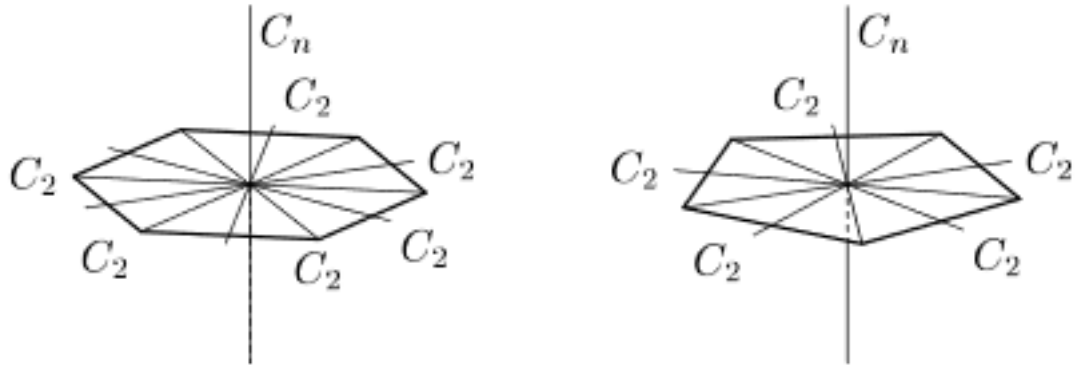


Рис. 1: Схемы для $C_6$ (четный случай) и $C_5$ (нечетный случай)

### Задание диэдральной группы порождающими

Возьмем ось $C_n$ и выберем ось $C_2$. Обозначим поворот на $2\pi/n$ вокруг $C_n$ за $r$, а симметрию относительно $C_2$ за $p$.
Из циклической структуры поворотов вокруг осей ясны два соотношения:

$$r^n = 1 \qquad p^2 = 1$$

При повороте $r$ одна ось $C_2$ переходит в другую, поэтому

$$(pr)^2 = 1$$

Полученные три соотношения порождают $D_n$. Покажем это.

Из третьего соотношения имеем $prp = r^{-1}$. Поэтому:

$$pr^k p = pr^{k-1}pprp = pr^{k-1}pr^{-1} = \cdots = r^{-k}$$

То есть если в выражении встречаются два элемента $p$, они уходят. Поэтому любое произведение элементов равно произведению, где $p$ встречается не более одного раза.

Значит, все элементы выглядят так: $1 = p^0 = r^0$, $r^k$, $pr^k$, $r^k p$.
Учитывая первое соотношение, $0 \leqslant k < n$
Вспомним третье соотношение: $(pr)^2 = 1 \Leftrightarrow rp = pr^{-1}$. Тогда

$$r^k p = r^{k-1} p r^{-1} = \cdots = p r^{-k} = p r^{n-k}$$

Значит, остается три вида элементов. Всего их не более $1 + (n-1) + n = 2n$.
Поэтому группа совпадает с $D_n$.

# Гомоморфизмы

**Определение 3 (Гомоморфизм)**
Говорят, что группа $\langle G', \circ \rangle$ *гомоморфна* группе $\langle G, * \rangle$, если существует отображение $\varphi: \ G \mapsto G'$, называемое *гомоморфизмом*, такое, что $\varphi(a * b) = \varphi(a) \circ \varphi(b)$.

То есть определение то же, что для изоморфизма, но не требующее биективности. В этом смысле, изоморфизм — это биективный гомоморфизм.

**Замечание 1**
*В общем случае говорят, что определён гомоморфизм из группы $G$ **в** группу $G'$. Он не обязан быть биективным, а также полный образ группы $G$ может быть собственным подмножеством $G'$.*
*Если гомоморфизм **сюръективный** (то есть $G'$ совпадает с полным образом гомоморфизма), то иногда говорят, что это гомоморфизм $G$ **на** $G'$.*

Приведём некоторые свойства гомоморфизмов:

**Теорема 1 (Свойства гомоморфизма)**
1) $\varphi(e) = e'$
2) $\varphi(a^{-1}) = (\varphi(a))^{-1}$
3) Композиция гомоморфизмов — гомоморфизм
4) $\varphi(G) = H' < G'$, то есть гомоморфный образ группы есть группа
5) Если $H < G$, то $\varphi(H) < \varphi(G)$, то есть гомоморфный образ подгруппы есть подгруппа образа группы

**Определение 4 (Образ, ядро)**
*Полным образом* отображения называется

$$\mathrm{Im}\varphi = \left\{ x \in G' \mid \exists y \in G: \ \varphi(y) = x \right\}$$

*Ядром* отображения называется

$$\mathrm{Ker}\varphi = \left\{ x \in G \mid \varphi(x) = e' \right\}$$

**Пример 2**
*Рассмотрим группу $G = \mathbb{Z}$ по сложению. Отображение $\varphi: \mathbb{Z} \mapsto \mathbb{Z}_n^+$, заданное $\varphi(x) = x \mod n$, является сюръективным гомоморфизмом.*
*$ImG = \mathbb{Z}_n$. $Ker\varphi = n\mathbb{Z}$.*

# Факторгруппы

Здесь разбирается частный случай более общего приема, называемого *факторизацией*. Факторизация — это разбиение множества на *классы эквивалентности* по некоторому отношению эквивалентности. Множество этих классов называется *фактормножеством*.

Мы будем рассматривать отношение «лежать в одном смежном классе». Из рассуждений, сделанных о смежных классах ранее, ясно, что это действительно отношение эквивалентности.

**Определение 5 (Факторгруппа)**
Пусть $H$ — **нормальная** подгруппа $G$ (обозначается $H \lhd G$).
*Факторгруппой* $G$ по $H$ называется группа

$$G/H = \{xH = Hx \mid x \in G\}$$

с определенной на ней операцией

$$(xH) \circ (yH) = (xyH)$$

То есть мы как бы «делим» группу на подгруппу $H$. Исходя из этих соображений, нормальные подгруппы также называют *нормальными делителями*.

**Замечание 2**
*Стоит обратить внимание, что факторгруппа берется исключительно по **нормальной** подгруппе.*
*Вдумчивый читатель может проверить, что определение операции на фактормножествах будет некорректной, если $H$ не будет нормальной, на примере некоммутативной группы $S_3$ и ее подгруппы $H = \{e, (12)\}$.*

Заметим, что если группа конечна, то

$$|G/H| = \frac{|G|}{|H|} = (G : H)$$

**Пример 3**
*$G = \mathbb{Z}$, $H = n\mathbb{Z} \lhd G$. Тогда $G/H = \mathbb{Z}/n\mathbb{Z}$ — группа смежных классов, они представляют множества чисел с различными остатками от деления на $n$.*
*Раньше мы уже использовали обозначение $\mathbb{Z}/n\mathbb{Z}$, теперь оно имеет смысл ☺.*

## Теорема о гомоморфизме групп

Вынесем следующее утверждение в отдельную теорему

**Теорема 2**
Ядро комоморфизма является нормальной подгруппой.

Это значит, что, имея гомоморфизм, по его ядру можно взять факторгруппу. Это приводит нас к важной теореме

**Теорема 3 (Теорема о гомоморфизме групп)**
Пусть $\varphi: G \mapsto G'$ — гомоморфизм. Тогда $G/\mathrm{Ker}\varphi \cong \varphi(G)$.

Обратно, пусть $K \lhd G$. Тогда существует группа $G'$ (а именно $G/K$) и гомоморфизм $\pi: G \mapsto G'$ такие, что $\mathrm{Ker}\pi = K$.

То есть **гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма**.
Стоит обратить внимание, что теорема действует в две стороны.

**Пример 4**
*Вернемся к нашему примеру с $\mathbb{Z}$. Вспомним, что $Ker\varphi = n\mathbb{Z}$, и убедимся, что $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n^+$.*