

# АЛГЕБРА

для потока «Прикладная математика и информатика»

*Четвёртый модуль 2020 – 2021 уч. года*

## ЛЕКЦИИ

### Я 3

*Г.М. Полотовский*  
([polotovsky@gmail.com](mailto:polotovsky@gmail.com)  
)

18 апреля 2022 г.

**Теорема 2.5.** Пусть  $G$  – группа,  $g \in G$ . Множество  $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$  всех степеней элемента  $g$  является подгруппой в  $G$ .

Это утверждение непосредственно следует из определения 6 и теоремы 2.3.

**Определение 7.** Подгруппа  $\langle g \rangle$  называется *циклической подгруппой*, порождённой элементом  $g$ , а элемент  $g$  – *порождающим элементом* подгруппы  $\langle g \rangle$ .

**Замечания:** в аддитивной записи  $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$ ; образующий элемент циклической подгруппы, вообще говоря, может быть выбран не единственным способом.

## Примеры.

1.  $G = \mathbf{C} \setminus \{0\} \equiv \mathbf{C}^*$  относительно операции умножения комплексных чисел.

$i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1; \langle i \rangle = \{1, i, -1, -i\}$  – подгруппа порядка 4.

$$2. \quad GL_2(\mathbf{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \middle| a_{ij} \in \mathbf{R}, \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0 \right\}.$$

Пусть  $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ , тогда  $\langle A \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ , поскольку

$$A^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

Таким образом, циклическая группа, порождённая матрицей  $A$ , имеет порядок 2.

$$\text{Если } A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \text{ то } A^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix};$$

$$A^3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}; \dots; A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Таким образом, теперь подгруппа, порождённая матрицей  $A$ , имеет бесконечный порядок.

Пусть  $G$  – произвольная группа,  $g \in G$ . Рассмотрим циклическую подгруппу, порожденную элементом  $g$ . Возможны следующие два случая:

1). Все степени элемента  $g$  различны между собой. Тогда группа  $\langle g \rangle$

бесконечна и не существует такого целого ненулевого числа  $n$ , что  $g^n = e$ .

2). Существуют различные  $s < t$ , такие что  $g^s = g^t$ . Умножим это равенство на  $g^{-s}$ , получим  $g^{t-s} = e$ . Следовательно, существует такое целое положительное число  $n$ , что  $g^n = e$ . Среди таких чисел  $n$  можно выбрать наименьшее.

**Определение 8.** *Порядком элемента  $g$  называется наименьшее целое положительное число  $n$ , такое что  $g^n = e$ . Обозначение:  $\text{ord } g = n$ . Если такого числа не существует, то говорят, что  $g$  имеет бесконечный порядок.*

### Примеры.

1)  $G = \mathbb{Z}$ ,  $\text{ord } 0 = 1$ , порядки остальных элементов  $G$  бесконечны, так как если кратное  $nm = 0$  при  $n \neq 0$ , то  $m = 0$ .

**Теорема 3.1.** Пусть  $G$  – группа,  $e$  – её нейтральный элемент,  $g \in G$ . Тогда

(1)  $g^k = e \Leftrightarrow \text{ord } g \mid k$  ( $a \mid b$  означает, что  $a$  является делителем числа  $b$ );

(2)  $\text{ord } g^k = \frac{\text{ord } g}{(k, \text{ord } g)}$  ( $(a, b)$  обозначен НОД  $(a, b)$ ).

Доказательство. Пусть  $\text{ord } g = n$ .

(1) Разделим с остатком  $k$  на  $n$ :  $k = nt + r$ ,  $0 \leq r < n$ .

$$g^k = g^{nt+r} = (g^n)^t g^r = e g^r = g^r;$$

$$g^k = e \Leftrightarrow g^r = e \Leftrightarrow r = 0 \text{ (т.к. } r < n \text{)}.$$

(2) Пусть  $(k, n) = d$  и  $n = n_1 d, k = k_1 d$ , т.е.  $(n_1, k_1) = 1$ .

$$\forall m: (g^k)^m = e \Leftrightarrow g^{km} = e \xleftrightarrow[\text{в силу (1)}]{} n \mid km \Leftrightarrow n_1 \mid k_1 m \Leftrightarrow n_1 \mid m$$

$$\text{Итак, } (g^k)^m = e \Leftrightarrow \frac{\text{ord } g}{(k, \text{ord } g)} \mid m. \text{ В силу (1) } \text{ord } g^k = \frac{\text{ord } g}{(k, \text{ord } g)}. \quad \blacksquare$$

**Теорема 3.2.** *Порядок циклической подгруппы, порождённой элементом  $g$  группы  $G$ , совпадает с порядком элемента  $g$ .*

Доказательство.

Если порядок элемента  $g$  бесконечен, то все его степени различны, поэтому циклическая группа  $\langle g \rangle$  бесконечна.

Пусть  $\text{ord } g = n$ . Рассмотрим любой элемент  $g^k \in \langle g \rangle$ .

Разделим с остатком  $k$  на  $n$ :  $k = nt + r$ ,  $0 \leq r < n$ .

Имеем  $g^k = g^{nt+r} = (g^n)^t g^r = e g^r = g^r$ ;

Следовательно,  $\langle g \rangle = \{g^0, g^1, g^2, \dots, g^{n-1}\}$ , так как  $0 \leq r < n$ .

Все элементы в фигурных скобках различны:

если бы было  $g^p = g^q$  при  $0 \leq p < q < n$ , то получили бы  $g^{q-p} = e$  при  $0 < q - p < n$ , что противоречит тому, что  $\text{ord } g = n$ .

Итак,  $\langle g \rangle = \{g^0, g^1, g^2, \dots, g^{n-1}\}$  и  $|\langle g \rangle| = n = \text{ord } g$ . ■

**Определение 9.** Группа  $G$  называется *циклической*, если существует элемент  $g \in G$  такой, что  $G = \langle g \rangle$ .

Следует отметить, что любая циклическая группа абелева, так как любые две степени элемента перестановочны между собой:  $g^m g^n = g^n g^m \quad \forall m, n \in \mathbb{Z}$ . Также отметим, что циклические группы могут быть как конечными, так и бесконечными.

### Примеры.

1. Группа  $G = (\mathbb{Z}, +)$  – бесконечная циклическая группа.

В качестве порождающего элемента можно выбрать число 1 или число  $-1$ .

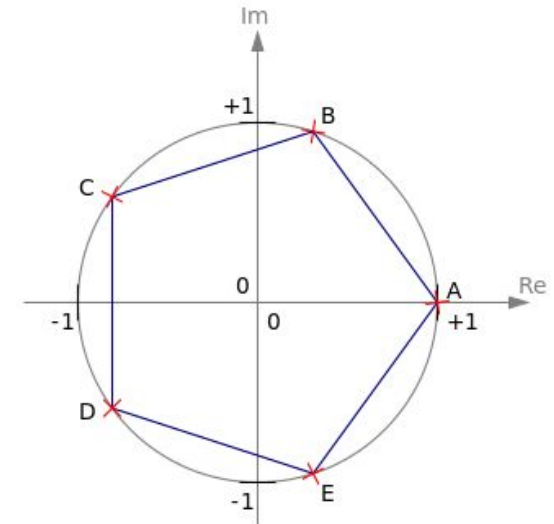
Других порождающих элементов у этой группы нет.

2. Пусть  $U_n = \left\{ \varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \mid k \in \{0, 1, 2, \dots, n-1\} \right\}$  – множество комплексных корней степени  $n$  из единицы.

Очевидно,  $(U_n, \cdot)$  – группа порядка  $n$ , и эта группа циклическая – её образующим элементом будет

$$\varepsilon_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n},$$

поскольку  $\varepsilon_1^k = \varepsilon_k \quad \forall k \in \{0, 1, \dots, n-1\}$





**Теорема 3.3.** (1) Конечная группа  $G$  циклическая  $\Leftrightarrow$  в  $G$  есть элемент порядка  $|G|$ .

(2) Элемент  $g^k$  является образующим в конечной группе  $\langle g \rangle \Leftrightarrow$   
 $(k, \text{ord } g) = 1$ .

(3) Количество образующих в циклической группе порядка  $n$  равно  $\varphi(n)$ .  
 Доказательство.

(1) очевидно (группа циклическая  $\Leftrightarrow$  есть порождающий элемент  $\Leftrightarrow$  порядок этого элемента равен порядку группы (теорема 3.2));

(2) следует из (1) и из утверждения (2) теоремы 3.1.

(3). Напомню, что через  $\varphi(n)$  обозначается функция Эйлера, которая по определению есть количество чисел, не превосходящих  $n$  и взаимно простых с  $n$ , поэтому (3) следует из (2).

**Пример.**  $Z_6 = \{0, 1, 2, 3, 4, 5\}$ .  $|Z_6|=6$ .  $\varphi(6) = 2$ . Образующие: 1 и 5.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

2 не является образующим.

$\{0, 2, 4\}$  – подгруппа, порождённая элементом 2.

### Теорема 3.4. (о подгруппах циклической группы)

(1) Любая подгруппа циклической группы сама является циклической.

(2) Имеется взаимно однозначное соответствие между делителями порядка конечной циклической группы и её подгруппами.

Доказательство. (1) Пусть  $G = \langle g \rangle$  и  $H \subset G$  – подгруппа в  $G$ .

Если  $H = \{e\}$  или  $H = G$ , то  $H$  циклическая.

Пусть  $H \neq \{e\}$ . Так как в  $G$  все элементы являются степенями элемента  $g \in G$ , то элементы из  $H$  тоже являются степенями элемента  $g$ , где  $g \neq e$ .

Если  $g^k \in H$  то  $g^{-k} = (g^k)^{-1} \in H$ , поскольку  $H$  – подгруппа.

Таким образом, в  $H$  найдётся элемент  $g$  в положительной степени. Среди всех таких положительных степеней выберем элемент  $g^m$  с **наименьшим показателем**  $m$ , т. е. если  $g^t \in H$  и  $0 \leq t < m$ , то  $t = 0$ .

Покажем, что  $H = \langle g^m \rangle$ .

Так как  $g^m \in H$ , то  $\langle g^m \rangle \subset H$ .

Чтобы показать обратное включение, надо показать, что любой элемент из  $H$  является некоторой степенью элемента  $g^m$ .

Как уже отмечалось, все элементы из  $H$  являются степенями элемента  $g^m$ .

Пусть  $g^k \in H$ . Поделим с остатком  $k$  на  $m$ :  $k = mq + r$  и  $0 \leq r < m$ .

$g^r = g^{k-mq} = g^k (g^m)^{-q} \in H$ , т. к.  $g^k \in H$  и  $g^m \in H$ .

$r = 0$  в силу выбора числа  $m$ , поэтому  $k = mq$ , т. е.  $g^k = (g^m)^q$ , ч. т. д.

(2) Пусть  $G$  – циклическая группа порядка  $n$ , и  $g$  – её порождающий элемент, т. е.  $G = \{e, g, g^2, g^3, \dots, g^{n-1}\}$ .

Пусть  $k|n$ , т. е.  $n = kq$ , где  $q \in \mathbb{Z}$ . Тогда  $\{e = (g^k)^0, g^k, (g^k)^2, \dots, (g^k)^{q-1}\}$  – циклическая подгруппа порядка  $q$ : замкнутость операции очевидна из свойств степени, а  $(g^k)^q = g^n = e$ .

Таким образом, имеем инъекцию из множества делителей порядка группы  $G$  в множество её циклических подгрупп.

Обратно, пусть  $H$  – подгруппа конечной циклической группы  $G = \langle g \rangle$  и  $|G| = n$ , т. е.  $g^n = e$  и  $n$  – **наименьшее из таких положительных чисел**.

В доказательстве части (1) мы доказали, что неединичная подгруппа  $H$  однозначно определяется числом  $m = \min_{g^k \in H} \{k > 0\}$ , причём если  $|H| = q$ , то  $(g^m)^q = e$ , т. е.  $g^{mq} = e$  и  $mq$  – **наименьший из таких показателей**.

Следовательно,  $n = mq$ , т. е. каждой подгруппе конечной циклической группы отвечает делитель  $q$  её порядка  $n$ , и это соответствие – инъекция. ■

Итак, если  $G = \langle g \rangle$ ,  $|G| = n$  и  $H = \langle g^m \rangle \subset G$ , то  $m = \min_{g^k \in H} \{k > 0\}$ ,

$$q = |H| \text{ – делитель числа } n \text{ и } m = \frac{n}{q} = \frac{|G|}{|H|}.$$

## Пример.

$Z_6$ .      6 :    1,        2,        3,        6.

Подгруппы:       $\{Z_6\}$      $\{0, 2, 4\}$      $\{0, 3\}$      $\{0\}$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

**Упражнение.** Перечислите все подгруппы группы  $Z_{15}$ , выбрав в качестве образующей в  $Z_{15}$  класс вычетов числа 2.