

## ЛЕКЦИЯ 1

**Определение 1.** Пусть  $G$  – некоторое множество.  $n$ -арной операцией на множестве  $G$  называется отображение

$$G \times \dots \times G \rightarrow G$$

из  $n$ -ой декартовой степени множества  $G$  в множество  $G$ .

Рассмотрим бинарную операцию  $*$  на множестве  $G$ :

$$G \times G \rightarrow G, \quad (g_1, g_2) \rightarrow g_1 * g_2.$$

**Определение 2.** Непустое множество  $G$  с фиксированной бинарной операцией  $*$  называется  *группоидом*.

Рассмотрим следующие условия (аксиомы) на операцию  $*$ .

A1. Ассоциативность. Для любых элементов  $a, b, c \in G$  выполнено  $(a * b) * c = a * (b * c)$ .

A2. Существование нейтрального элемента. Существует такой элемент  $e \in G$ , что для любого  $g \in G$  выполняется  $eg = ge = g$ .

A3. Существование обратного элемента. Для каждого элемента  $g \in G$  существует элемент  $g^{-1} \in G$  такой, что  $g * g^{-1} = g^{-1} * g = e$ .

A4. Коммутативность. Для любых элементов  $a, b \in G$  выполнено  $a * b = b * a$ .

Накладывая на операцию  $*$  различные множества условий, мы будем получать различные алгебраические структуры.

**Определение 3.** Если  $*$  удовлетворяет условию A1, то  $G$  называется *полугруппой*.

Если  $*$  удовлетворяет условиям A1 и A2, то  $G$  называется *моноидом*.

Если  $*$  удовлетворяет условиям A1 и A2 и A3, то  $G$  называется *группой*.

Условие A4 добавляет к названию структуры слово абелев (или, что то же самое, коммутативный). Так условия A1 и A4 задают *абелеву (коммутативную) полугруппу*, условия A1, A2 и A4 задают *абелев (коммутативный) моноид*, условия A1, A2, A3 и A4 задают *абелеву (коммутативную) группу*.

**Обозначение 1.** Если не очевидно, какая операция на множестве  $G$  имеется в виду, то будем использовать обозначение  $(G, *)$  для множества  $G$  с операцией  $*$ .

**Упражнение 1.** Рассмотрим аксиому, являющуюся "половиной" аксиомы A2.

A2': Существует такой элемент  $e \in G$ , что для любого  $g \in G$  выполняется  $eg = g$ . Докажите, что если структура  $(G, *)$  удовлетворяет условиям A1, A2' и A3, то  $G$  является группой.

**Задача 1.** Рассмотрим аксиому, являющуюся "половиной" аксиомы A3.

A3': Для каждого элемента  $g \in G$  существует элемент  $g^\vee \in G$  такой, что  $g * g^\vee = e$ .

Существует ли структура  $(G, *)$ , удовлетворяющая условиям A1, A2 и A3', но не являющаяся группой.

Рассмотрим некоторые элементарные следствия из аксиом.

**Лемма 1. Простые следствия из аксиом.**

1) (Обобщенная ассоциативность) Пусть  $(G, *)$  – полугруппа. И пусть  $g_1, \dots, g_k \in G$ . Тогда как бы ни были расставлены скобки в выражении  $g_1 * g_2 * \dots * g_k$  результат будет одинаковым.

- 2) В моноиде есть единственная единица.  
 3) В группе для каждого элемента есть единственный обратный.  
 4) Пусть  $(G, *)$  – группа. Пусть  $a, b \in G$ . Тогда если  $a * b = e$ , то  $b = a^{-1}$ . Аналогично если  $b * a = e$ , то  $b = a^{-1}$ .  
 5) Пусть  $(G, *)$  – группа,  $a, b \in G$ . Тогда  $(a * b)^{-1} = b^{-1} * a^{-1}$ .  
 6) Пусть  $(G, *)$  – группа,  $g \in G$ . Тогда  $(g^{-1})^{-1} = g$ .

*Доказательство.* 1) Докажем это утверждение индукцией по  $k$ .

*База индукции*  $k = 3$ . В этом случае обобщенная ассоциативность совпадает с ассоциативностью, то есть с аксиомой A1.

*Шаг индукции.* Предположим, что для  $k < n$  данное утверждение уже доказано. Докажем его для  $k = n$ . Среди всех расстановок скобок есть стандартная (при ней действия выполняются справа-налево):

$$(\dots (g_1 * g_2) * g_3) * \dots * g_{n-1} * g_n = g.$$

Достаточно доказать, что результат, который получается при произвольной расстановке скобок, совпадает с  $g$ . Фиксируем некоторую расстановку скобок. Для этой расстановки скобок есть последнее действие, которое даст операцию от двух скобок. Длиной скобки назовем количество  $g_i$ , входящих в нее. Докажем, что результат совпадает с  $g$  индукцией по длине правой скобки (обозначим эту длину  $s$ ).

*База второй индукции*  $s = 1$ . Наша расстановка скобок имеет вид  $(\dots) * g_n$ . По предположению первой индукции в левой скобке можно расставить скобки произвольным образом. В том числе стандартным образом. Но тогда в целом мы получим стандартную расстановку скобок. Значит, результат при нашей расстановке скобок совпадает с результатом при стандартной расстановке скобок.

*Шаг второй индукции.* Пусть при  $s < t$  утверждение доказано ( $t \geq 2$ ). Докажем при  $s = t$ . Последнее действие при нашей фиксированной расстановке скобок имеет вид  $(a) * (b)$ . Поскольку длина скобки  $(b)$  равна  $t \geq 2$ , то  $b = (c) * (d)$ . Тогда  $(a) * (b) = (a) * ((c) * (d))$ . Применяя аксиому A1, получаем

$$(a) * ((c) * (d)) = ((a) * (c)) * (d).$$

Но длина скобки  $(d)$  строго меньше, чем длина скобки  $(b) = ((c) * (d))$ . Значит, по предположению второй индукции результат получающийся при расстановке скобок  $((a) * (c)) * (d)$  совпадает с  $g$ .

2) Предположим, что в моноиде  $(G, *)$  есть две единицы:  $e$  и  $s$ . Рассмотрим  $e * s$ . Поскольку  $e$  – единица, получаем  $e * s = s$ . С другой стороны так как  $s$  – единица, то  $e * s = e$ . Таким образом,  $e = s$ .

3) Пусть  $(G, *)$  – группа. Предположим, что  $g \in G$  – элемент, у которого есть хотя бы два обратных:  $f$  и  $h$ . Тогда  $f = f * (g * h) = (f * g) * h = h$ .

4) Пусть  $a * b = e$ . Рассмотрим операцию элемента  $a^{-1}$  и левой части и приравняем к операции элемента  $a^{-1}$  и правой части. (Домножим на  $a^{-1}$  слева.) Получим  $a^{-1} * a * b = a^{-1} * e$ . То есть  $b = a^{-1}$ .

Если  $b * a = e$ , то аналогично домножая слева на  $a^{-1}$ , получаем  $b = a^{-1}$ .

5) Обозначим  $b^{-1} * a^{-1} = c$ . Рассмотрим  $(a * b) * c = (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e$ . Значит,  $c = (a * b)^{-1}$ .

6)  $g^{-1} * g = e$ , значит  $g = (g^{-1})^{-1}$ . □

**Определение 4.** Подмножество  $H$  группы  $(G, *)$  называется *подгруппой*, если  $(H, *)$  является группой.

Подмножество  $S$  группы  $(G, *)$  называется *замкнутым относительно операции  $*$* , если для любых  $a, b \in S$  выполнено  $a * b \in S$ . Подмножество  $S$  группы  $(G, *)$  называется *замкнутым относительно взятия обратного*, если для любого  $s \in S$  элемент  $s^{-1}$  также принадлежит  $S$ .

**Предложение 1.** *Непустое подмножество  $H$  группы  $(G, *)$  является подгруппой тогда и только тогда, когда оно замкнуто относительно операции и замкнуто относительно взятия обратного.*

*Доказательство.* Если  $(H, *)$  – группа, то операция  $*$  корректно определена на  $H$ . Значит,  $H$  замкнуто относительно операции  $*$ . Пусть  $e$  – нейтральный элемент группы  $G$ , а  $s$  – нейтральный элемент группы  $H$ . Получаем  $s * s = s$ . В группе  $G$  есть обратный к  $s$  элемент  $s^{-1}$ . Умножая на него слева предыдущее равенство, получаем  $s = e$ . То есть единицы у групп  $G$  и  $H$  совпадают. Для каждого  $g \in H$  есть обратный элемент  $g^{-1}$  в группе  $G$  и есть обратный элемент  $g^{\vee}$  в группе  $H$ . Тогда  $g * g^{-1} = e = g * g^{\vee}$ . Умножив слева на  $g^{-1}$ , получаем  $g^{-1} = g^{\vee}$ . Поскольку для группы  $(H, *)$  выполнена аксиома А3, то  $H$  замкнуто относительно взятия обратного.

Пусть теперь подмножество  $H$  замкнуто относительно операции и взятия обратного. Так как  $H$  замкнуто относительно операции,  $(H, *)$  – группоид. Поскольку ассоциативность выполнена в  $G$ , то она выполнена и в  $H$ . Подмножество не пусто. Возьмем элемент  $h \in H$ . Так как  $H$  замкнуто относительно взятия обратного,  $h^{-1} \in H$ . Пользуясь замкнутостью  $H$  относительно операции, получаем  $h * h^{-1} = e \in H$ . Таким образом, в  $H$  выполнена аксиома А2. Поскольку  $H$  замкнуто относительно взятия обратного, в  $H$  выполнена и аксиома А3.  $\square$

Зачастую вместо слова "операция" используют слово "умножение". Суть от этого не меняется и имеется в виду некоторая операция в группе. При этом на письме так же как и в случае обычного умножения чисел знак умножения можно опускать. Нейтральный элемент группы в этом случае зачастую называют "единицей группы". Такие обозначения называются *мультипликативными*.

Если заранее известно, что группа абелева, то часто используют *аддитивные* обозначения. Операция называется сложением и обозначается знаком  $+$  нейтральный элемент называется нулем, а обратный элемент называется "противоположным элементом".

Соберем эти обозначения в таблице.

общие обозначения	мультипликативные обозначения	аддитивные обозначения
произвольная группа	произвольная группа	абелева группа
операция $*$	умножение $\cdot$	сложение $+$
нейтральный элемент $e$	единица $e$	ноль $0$
обратный элемент $g^{-1}$	обратный элемент $g^{-1}$	противоположный элемент $-g$

**Определение 5.** Порядок группы  $G$  – это количество элементов в этой группе. (То есть мощность множества  $G$ .) Порядок группы  $G$  обозначается  $|G|$ .

**Определение 6.** Пусть  $g$  – элемент группы  $G$ , а  $n$  – целое число. Определим  $n$ -ю степень элемента  $g$  следующим образом. Если  $n$  положительное, то  $g^n =$

$g \cdot \dots \cdot g$  – произведение  $n$  элементов  $g$ . Если  $n$  отрицательное, то  $g^n = (g^{-1})^n$ . Нулевая степень любого элемента равна нейтральному элементу  $e$ .

**Упражнение 2.** Выполнены следующие свойства степеней элемента группы:

- 1)  $g^m g^n = g^{m+n}$ ,
- 2)  $(g^m)^n = g^{mn}$

*Указание.* Рассмотреть все случаи знаков  $m$  и  $n$ .

**Определение 7.** Пусть  $g$  – элемент группы  $G$ . Порядок  $g$  – это минимальное натуральное число  $n$  такое, что  $g^n = e$ . Если такого числа не существует, то порядок элемента  $g$  равен бесконечности. Порядок элемента  $g$  обозначается  $\text{ord}g$ .

**Лемма 2.** Пусть  $g$  – элемент группы  $G$  такой, что  $\text{ord}g = n$ , а  $m$  – целое число. Тогда

$$\text{ord}g^m = \frac{n}{\text{НОД}(m, n)}.$$

*Доказательство.* По свойству степеней  $(g^m)^k = g^{mk}$ . Следовательно порядок  $g^m$  – это минимальное натуральное  $k$  такое, что  $mk$  делится на  $n$ .

Рассмотрим разложения на простые множители чисел  $n$  и  $m$ . Можем считать, что простые множители входящие в  $m$  и  $n$  одинаковы, но при этом степени вхождения могут быть равны нулю.

$$n = p_1^{\alpha_1} \dots p_l^{\alpha_l}, \quad m = p_1^{\beta_1} \dots p_l^{\beta_l}.$$

Имеем:  $\text{НОД}(m, n) = p_1^{\min\{\alpha_1, \beta_1\}} \dots p_l^{\min\{\alpha_l, \beta_l\}}$ .

Отсюда

$$\begin{aligned} \frac{n}{\text{НОД}(m, n)} &= p_1^{\alpha_1 - \min\{\alpha_1, \beta_1\}} \dots p_l^{\alpha_l - \min\{\alpha_l, \beta_l\}} = \\ &= p_1^{\max\{\alpha_1 - \beta_1, 0\}} \dots p_l^{\max\{\alpha_l - \beta_l, 0\}} \end{aligned}$$

Легко видеть, что это минимальное число  $k$  такое, что  $km$  делится на  $p_i^{\alpha_i}$  для каждого  $i$ .  $\square$

Конечную группу можно задавать с помощью таблицы умножения. Таблица умножения – это квадратная таблица, строки и столбцы которой соответствуют элементам группы. А на пересечении строки и столбца стоит произведение элемента, соответствующее строки и элемента, соответствующего столбцу.

**Пример 1.** Построим таблицу сложения для группы  $(\mathbb{Z}_2, +) = \{0, 1\}$

+	0	1
0	0	1
1	1	0

**Примеры групп.**

1) Числовые аддитивные группы:

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +).$$

Нейтральный элемент 0, обратный к элементу  $x$  – это  $-x$ . Выполнение аксиом следуют из свойств сложения чисел. Все данные группы бесконечны и коммутативны.

2) Группа вычетов (остатков) по модулю  $n$ :  $(\mathbb{Z}_n, +)$ . Сложение происходит по модулю  $n$ . Нейтральный элемент  $0$ , обратный к элементу  $x$  – это  $n - x$ . Выполнение аксиом следуют из свойств остатков. Данная группа коммутативна и имеет порядок  $n$ .

3) Числовые мультипликативные группы:

$$\mathbb{Q}^\times = (\mathbb{Q} \setminus \{0\}, \cdot), \mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \cdot), \mathbb{C}^\times = (\mathbb{C} \setminus \{0\}, \cdot).$$

Нейтральный элемент  $1$ , обратный к элементу  $x$  – это  $\frac{1}{x}$ . Выполнение аксиом следуют из свойств умножения чисел. Данные группы бесконечны и коммутативны.

4) (Обобщение примера 3) Пусть  $R$  – кольцо с единицей. Обозначим множество обратимых элементов через  $R^\times$ . Рассмотрим группу обратимых элементов  $(R^\times, \cdot)$ . Нейтральный элемент – единица кольца. Обратные элементы существуют так как  $R^\times$  состоит из обратимых элементов. Если  $R$  – коммутативное кольцо, то  $R^\times$  – коммутативная группа.

**Задача 2.** Приведите пример некоммутативного кольца  $R$  такого, что  $R^\times$  – коммутативная группа порядка больше 1.

5) Группа комплексных корней из единицы  $n$ -ой степени. Пусть  $\mathcal{C}_n$  – множество всех комплексных корней степени  $n$  из 1. Тогда  $(\mathcal{C}_n, \cdot)$  – абелева группа порядка  $n$ . Докажем это. Для того, чтобы доказать, что  $\mathcal{C}_n$  – группа мы воспользуемся, тем, что это подмножество в известной нам группе  $\mathbb{C}^\times$ . Нам надо лишь проверить, что  $\mathcal{C}_n$  замкнуто относительно умножения и взятия обратного. Пусть  $a, b \in \mathcal{C}_n$ , то есть  $a^n = b^n = 1$ . Тогда  $(ab)^n = a^n b^n = 1$ , значит,  $ab \in \mathcal{C}_n$ . Мы доказали, что  $\mathcal{C}_n$  замкнуто относительно умножения. С другой стороны  $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$ , следовательно,  $\mathcal{C}_n$  замкнуто относительно взятия обратного. То, что группа  $\mathcal{C}_n$  абелева следует из того, что она является подгруппой в абелевой группе  $\mathbb{C}^\times$ .

Единица этой группы – это 1, обратный к элементу  $x$  – это  $\frac{1}{x}$ .

6) Группы перестановок.

а) Множество  $S_n$  всех перестановок  $n$  элементов с операцией композиции  $\circ$  является группой. Докажем это. Нейтральный элемент этой группы – это тождественная перестановка, обратный элемент – обратная перестановка. Ассоциативность следует из следующей важной леммы.

**Лемма 3.** Пусть есть четыре множества:  $X, Y, Z$  и  $T$ . И пусть фиксированы отображения между этими множествами  $\varphi: X \rightarrow Y, \psi: Y \rightarrow Z$  и  $\zeta: Z \rightarrow T$ . Тогда  $(\zeta \circ \psi) \circ \varphi = \zeta \circ (\psi \circ \varphi)$ .

*Доказательство.* Возьмем элемент  $x \in X$ . Тогда

$$(\zeta \circ \psi) \circ \varphi(x) = (\zeta \circ \psi)(\varphi(x)) = (\zeta(\psi(\varphi(x)))).$$

С другой стороны

$$\zeta \circ (\psi \circ \varphi)(x) = \zeta(\psi \circ \varphi)(x) = (\zeta(\psi(\varphi(x)))).$$

□

Применяя данную лемму к случаю  $X = Y = Z = T = \{1, 2, \dots, n\}$  получаем ассоциативность  $S_n$ . Порядок группы  $S_n$  равен  $n!$ . При  $n > 3$  группа  $S_n$  не коммутативна.

б) Множество  $A_n$  четных перестановок из  $S_n$  с операцией композиции образует *группу четных перестановок*. Докажем, что  $A_n$  – подгруппа  $S_n$ . Это следует из того, что произведение четных перестановок – четная перестановка и обратная к четной перестановке четная. Группа  $A_n$  не коммутативна при  $n \geq 4$ .

в) Группа Клейна. Рассмотрим множество перестановок (в виде произведения независимых циклов)  $\{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ . Несложно проверить, что это множество замкнуто относительно композиции и что каждая перестановка из этого множества обратна самой себе. Получаем, что данные перестановки образуют подгруппу в  $S_4$ , которая обозначается  $V_4$ . Эта группа коммутативна.

б') (Обобщение примера ба) Пусть  $X$  – некоторое множество (возможно бесконечное). Рассмотрим множество  $S(X)$  биекций  $X \rightarrow X$  с операцией композиции. Если  $|X| < \infty$ , то получаем группу перестановок. В общем случае получаем *группу симметрий множества  $X$* . Нейтральный элемент – тождественное преобразование. Обратный – обратное преобразование. Ассоциативность следует из леммы 3.

7) Матричные группы. Пусть  $\mathbb{K}$  – поле.

а)  $GL_n(\mathbb{K})$  – множество невырожденных матриц  $n \times n$  с элементами из  $\mathbb{K}$ . Легко видеть, что это множество замкнуто относительно умножения матриц. Умножение матриц ассоциативно, единичная матрица – нейтральный элемент и все невырожденные матрицы обратимы (обратная также невырождена). Следовательно,  $(GL(\mathbb{K}), \cdot)$  – группа.

б)  $SL_n(\mathbb{K})$  – множество  $n \times n$  матриц с определителем 1 с элементами из  $\mathbb{K}$ . Это подмножество замкнуто относительно умножения и взятия обратного.

Эти группы конечны тогда и только тогда, когда поле  $\mathbb{K}$  конечно.

8) Группы преобразований векторного пространства. (Подгруппы в группе  $S(V)$ , где  $V$  – векторное пространство.)

а) Группа обратимых линейных преобразований  $V$ .

б) Группа ортогональных линейных преобразований  $V$ .

в) Группа обратимых аффинных преобразований  $V$ .

г) Группа движений  $V$ .

Во всех этих группах нейтральный элемент – тождественное преобразование, а обратный элемент – обратное преобразование. Эти группы конечны тогда и только тогда, когда поле, над которым  $V$  – векторное пространство конечно и размерность  $V$  конечна.

## ЛЕКЦИЯ 2

**Определение 8.** Пусть  $(G, *)$  и  $(H, \circ)$  – две группы. Отображение  $\varphi: G \rightarrow H$  называется *гомоморфизмом*, если  $\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2)$ .

Докажем следующие элементарные свойства гомоморфизма.

**Лемма 4.** Пусть  $\varphi: (G, *) \rightarrow (H, \circ)$  – гомоморфизм. Обозначим через  $e_G$  и  $e_H$  единицы группы  $G$  и  $H$  соответственно. Тогда

1)  $\varphi(e_G) = e_H$ ,

2)  $\varphi(g^{-1}) = \varphi(g)^{-1}$ . (В левой части обратный берется в группе  $G$ , а в правой – в  $H$ .)

*Доказательство.* 1) Поскольку  $e_G$  – единица группы  $G$ . Тогда  $e_G * e_G = e_G$ , а значит,

$$\varphi(e_G) \circ \varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G).$$

В группе  $H$  есть обратный к  $\varphi(e_G)$  элемент. Умножим на него обе части. Получим

$$\varphi(e_G) = e_H.$$

2)  $e_H = \varphi(e_G) = \varphi(g * g^{-1}) = \varphi(g) \circ \varphi(g^{-1})$ . Следовательно,  $\varphi(g^{-1}) = \varphi(g)^{-1}$ .  $\square$

**Задача 3.** Пусть  $(G, *)$  и  $(H, \circ)$  – моноиды с единицами  $e_G$  и  $e_H$  соответственно. И пусть  $\psi: G \rightarrow H$  – отображение такое, что  $\psi(g_1 * g_2) = \psi(g_1) \circ \psi(g_2)$ . Может ли так быть, что  $\psi(e_G) \neq \psi(e_H)$ ?

**Определение 9.** Биективный гомоморфизм  $\varphi: G \rightarrow H$  называется *изоморфизмом*, а группы  $G$  и  $H$  при наличии изоморфизма между ними называются *изоморфными*.

Легко видеть, что если  $\varphi$  – изоморфизм, то обратное отображение  $\varphi^{-1}$  также является изоморфизмом. Кроме того композиция двух изоморфизмов – изоморфизм. Из этого следует, что классы изоморфности групп – это классы эквивалентности.

**Пример 2.** Рассмотрим две группы:  $(\mathbb{R}, +)$  и  $(\mathbb{R}_{>0}, \cdot)$ . Вторая группа состоит из всех положительных вещественных чисел с операцией умножения. Рассмотрим отображение  $\varphi: \mathbb{R} \rightarrow \mathbb{R}_{>0}$ ,  $\varphi(x) = 2^x$ . Легко видеть, что  $\varphi$  – изоморфизм.

**Пример 3.** Группа  $\mathbb{Z}_n$  изоморфна группе  $\mathbb{C}_n$ . Один из возможных автоморфизмов переводит  $k \in \mathbb{Z}_n$  в  $\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$ . То, что  $\varphi$  – гомоморфизм обеспечивается тем, что при умножении комплексных чисел их аргументы складываются.

**Пример 4.** Группа  $GL_n(\mathbb{C})$  изоморфна группе невырожденных линейных преобразований векторного пространства  $\mathbb{C}^n$  с операцией композиции. Чтобы получить изоморфизм между этими группами нужно выбрать некоторый базис в  $\mathbb{C}^n$  и отобразить линейное преобразование в его матрицу в этом базисе.

Изоморфные группы имеют одинаковую алгебраическую структуру. Более строго любой алгебраический факт (то есть формулирующийся только в терминах операции) верный в одной из них, верен и в другой. Поэтому в дальнейшем мы будем отождествлять изоморфные группы и будем изучать группы с точностью до изоморфизма.

На самом деле изоморфизм (биективное соответствие, переводящее умножение одной группы в умножение другой) можно задать в случае, когда про одну из структур не известно, группа это или нет. Тогда вторая структура будет автоматически группой. Воспользуемся этой идеей в следующем примере.

**Группа кватернионов  $Q_8$ .** Рассмотрим множество из 8 элементов:

$$\{1, -1, i, -i, j, -j, k, -k\}.$$

Умножение устроено следующим образом: знаки умножаются отдельно,

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k, ji = -k, ik = -j, ki = j, jk = i, kj = -i.$$

Легко видеть, что 1 – нейтральный элемент, и каждый элемент обратим. Для того, чтобы утверждать, что  $Q_8$  – группа, необходимо проверить ассоциативность. Сделаем это опосредованно.

Рассмотрим следующее множество из 8 комплексных матриц, которое мы обозначим  $\overline{Q}_8$ .

$$\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}.$$

Здесь  $i$  – это мнимая единица (комплексное число).

Рассмотрим биекцию  $\varphi$  между  $Q_8$  и  $\overline{Q}_8$ .

$$\pm 1 \mapsto \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i \mapsto \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j \mapsto \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k \mapsto \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Легко убедиться, что  $\varphi$  переводит умножение в  $Q_8$  в матричное умножение. Следовательно,  $(\overline{Q}_8, \cdot)$  – это замкнутое относительно умножения и взятия обратной матрицы подмножество в  $GL_2(\mathbb{C})$ . Значит,  $\overline{Q}_8$  – подгруппа. Тогда  $Q_8$  – группа, изоморфная  $\overline{Q}_8$ .

Ещё один важный пример группы дадут следующая конструкция.

**Группа диэдра  $D_n$ .** Рассмотрим правильный  $n$ -угольник. Группа диэдра  $D_n$  – это группа всех движений плоскости, сохраняющих этот  $n$ -угольник.

**Упражнение 3.** а) Докажите, что в группе  $D_n$  ровно  $2n$  элементов. Среди них  $n$  поворотов и  $n$  осевых симметрий. Все оси симметрий проходят через центр  $n$ -угольника. Если  $n$  чётно, то половина симметрий проходит через 2 вершины, а половина – через две середины противоположных сторон. Если же  $n$  нечётно, то все симметрии проходят через одну вершину и середину противоположной стороны.

б) Найдите, как устроена операция в группе  $D_n$ , то есть чему равна композиция двух поворотов, двух симметрий и поворота с симметрией.

Можно конструировать группу из уже известных с помощью следующей конструкции.

**Определение 10.** Пусть  $G$  и  $H$  – две группы. *Прямым произведением*  $n$  групп называется группа  $G \times H$ , состоящая из пар  $(g, h)$ , где  $g \in G$ ,  $h \in H$ . Операция устроена следующим образом:  $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$ . Ассоциативность следует из ассоциативности операций в  $G$  и  $H$ . Нейтральный элемент – это  $(e_G, e_H)$ , обратный элемент к элементу  $(g, h)$  – это  $(g^{-1}, h^{-1})$ . Порядок прямого произведения групп – это произведение их порядков.

Особый интерес представляют гомоморфизмы и изоморфизмы из группы в себя.

**Определение 11.** Гомоморфизм  $\varphi: G \rightarrow G$  называется *эндоморфизмом*. Изоморфизм  $\varphi: G \rightarrow G$  называется *автоморфизмом*.

Легко видеть, что композиция двух эндоморфизмов – это эндоморфизм, а композиция двух автоморфизмов – автоморфизм. Множество эндоморфизмов группы  $G$  с операцией композиции образует моноид  $\text{End}(G)$  с нейтральным элементом  $\text{id}$ . Множество автоморфизмов группы  $G$  с операцией композиции образует группу  $\text{Aut}(G)$ .

Пусть  $g$  – элемент группы  $G$ . Рассмотрим отображение  $\varphi_g: G \rightarrow G$ , определенное по правилу  $\varphi_g(h) = ghg^{-1}$ .

**Лемма 5.** *Отображение  $\varphi_g$  является автоморфизмом группы  $G$ .*

*Доказательство.* Проверим, что  $\varphi_g$  – гомоморфизм:

$$\varphi_g(hf) = ghfg^{-1} = ghg^{-1}gfg^{-1} = \varphi_g(h)\varphi_g(f).$$

То, что  $\varphi_g$  – биекция следует из того, что существует обратное отображение. А именно, обратное к  $\varphi_g$  отображение – это  $\varphi_{g^{-1}}$ .  $\square$

Автоморфизмы называются *внутренними*, если он имеет вид  $\varphi_g$  для некоторого  $g \in G$ .

**Предложение 2.** *а) Множество внутренних автоморфизмов с операцией композиции образует подгруппу  $\text{Inn}(G)$  в  $\text{Aut}(G)$ .*

*б) Отображение  $g \rightarrow \varphi_g$  – это гомоморфизм из  $G$  в  $\text{Inn}(G)$ .*

*Доказательство.* Докажем равенство  $\varphi_g \circ \varphi_h = \varphi_{gh}$ . Для этого применим этот гомоморфизм к элементу  $s \in G$ :

$$\varphi_g \circ \varphi_h(s) = \varphi_g(\varphi_h(s)) = \varphi_g(hsh^{-1}) = ghsh^{-1}g^{-1} = (gh)s(gh)^{-1} = \varphi_{gh}(s).$$

Из доказанного равенства следует пункт б) и замкнутость  $\text{Inn}(G)$  относительно композиции. Осталось проверить, что  $\text{Inn}(G)$  замкнуто относительно взятия обратного. Для этого заметим, что  $\varphi_g \circ \varphi_{g^{-1}} = \varphi_e = \text{id}$ .  $\square$

**Определение 12.** Группа  $G$  называется *циклической*, если найдется элемент  $g \in G$  такой, что каждый элемент  $G$  имеет вид  $g^k$  для некоторого целого числа  $k$ .

Элемент  $g$  называется *порождающим элементом группы  $G$* , при этом группа  $G$  обозначается  $\langle g \rangle$ .

*Замечание 1.* В предыдущем определении не требуется, чтобы все степени  $g$  были различны.

**Пример 5.** *а) Группа  $\mathbb{Z}$  является циклической. В самом деле,  $\mathbb{Z} = \langle 1 \rangle$ .*

*б) Аналогично  $\mathbb{Z}_n = \langle 1 \rangle$ .*

**Упражнение 4.** Проверьте, что группы  $\mathbb{Z}_2 \times \mathbb{Z}_2$ ,  $(\mathbb{Q}, +)$  и  $\mathbb{Q}^\times$  не являются циклическими.

**Лемма 6.** *Пусть  $\text{ord}(g) = n$ . Тогда порядок группы  $\langle g \rangle$  также равен  $n$ .*

*Доказательство.* Рассмотрим множество элементов  $S = \{g^0 = e, g, g^2, \dots, g^{n-1}\}$ . Докажем, что все элементы группы  $\langle g \rangle$  лежат в  $S$  и что все элементы  $S$  различны.

В самом деле, пусть  $g^k$  – некоторый элемент  $\langle g \rangle$ . Разделим  $k$  на  $n$  с остатком:  $k = nt + r$ , где  $0 \leq r < n$ . Тогда  $g^k = (g^n)^t g^r = g^r \in S$ .

С другой стороны. Пусть  $0 \leq a < b < n$  и  $g^a = g^b$ . Умножая последнее равенство на  $g^{-a}$ , получаем  $e = g^{b-a}$ . Поскольку  $0 < b-a < n$ , это противоречит тому, что  $\text{ord}(g) = n$ .  $\square$

Если известно, что порядок  $g$  равен  $n$ , то группу  $\langle g \rangle$  обозначают  $\langle g \rangle_n$ .

*Замечание 2.* Для каждого элемента  $g$  некоторой группы  $G$  можно рассмотреть циклическую подгруппу, порожденную этим элементом:  $\langle g \rangle \subset G$ .

**Теорема 1.** а) Любая циклическая группа бесконечного порядка изоморфна  $\mathbb{Z}$ .  
б) Любая циклическая группа порядка  $n$  изоморфна  $\mathbb{Z}_n$ .

*Доказательство.* а) Пусть  $G = \langle g \rangle$  и  $|G| = \infty$ . Тогда  $\text{ord}(g) = \infty$ . Из этого следует, что при  $k \neq m$  выполнено  $g^k \neq g^m$ . Рассмотрим отображение

$$\psi: \mathbb{Z} \rightarrow G, \quad k \mapsto g^k.$$

Легко видеть, что  $\psi$  – гомоморфизм. Так как все элементы  $G$  имеют вид  $g^k$ ,  $\psi$  – сюръекция, а так как при  $k \neq m$  выполнено  $g^k \neq g^m$ ,  $\psi$  – инъекция. Итак,  $\psi$  – изоморфизм.

б) В предыдущей лемме мы доказали, что  $G = \{g^0, \dots, g^{n-1}\}$ . Рассмотрим отображение

$$\psi: \mathbb{Z}_n \rightarrow G, \quad k \mapsto g^k, \quad k \in \{0, 1, \dots, n-1\}.$$

Легко видеть, что  $\psi$  – изоморфизм. □

**Теорема 2.** 1) Подгруппа циклической группы циклическая.

2) Все подгруппы в  $\mathbb{Z}$  имеют вид  $k\mathbb{Z}$ .

3) Все подгруппы в  $\mathbb{Z}_n$  имеют вид  $\langle d \rangle = d\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{d}}$ , где  $d$  делитель числа  $n$ . В частности, для каждого делителя  $q$  числа  $n$  есть ровно одна подгруппа в  $\mathbb{Z}_n$ , изоморфная  $\mathbb{Z}_q$ , а именно,  $\langle \frac{n}{q} \rangle$ .

4) Пусть  $m \in \mathbb{Z}_n$ , тогда  $\langle m \rangle = \langle \text{НОД}(m, n) \rangle$ .

*Доказательство.* 1) Пусть  $G = \langle g \rangle$  и пусть  $H$  – некоторая подгруппа в  $G$ . Если  $H = \{e\}$ , то утверждение доказано. Пусть  $H \neq \{e\}$ . Если  $g^k \in H$ , то  $g^{-k} \in H$ . Значит существует положительное число  $k$  такое, что  $g^k \in H$ . Пусть  $l$  – наименьшее положительное число такое, что  $g^l \in H$ . Рассмотрим некоторое  $m$  такое, что  $g^m \in H$ . Разделим  $m$  на  $l$  с остатком:  $m = ls + r$ , где  $0 \leq r < l$ . Получаем  $g^r = g^m (g^l)^{-s} \in H$ . Поскольку  $l$  минимальное положительное число такое, что  $g^l \in H$ , получаем  $r = 0$ . То есть в  $G$  все элементы имеют вид  $(g^l)^s$ , значит  $G = \langle g^l \rangle$ .

2) По пункту 1 любая подгруппа в циклической группе  $\mathbb{Z}$  имеет вид  $\langle k \rangle = k\mathbb{Z}$ .

3) По доказательству пункта 1 подгруппа  $H \subset \langle g \rangle$  циклическая и порождается элементом  $g^l$  для минимального положительного  $l$  такого, что  $g^l \in H$ . Значит если  $H$  – подгруппа  $\mathbb{Z}_n$ , то  $H = \langle d \rangle$ , где  $d$  – минимальное положительное число такое, что его вычет лежит в  $H$ . Допустим, что  $n$  не делится на  $d$ . Тогда  $n = dq + r$ , где  $0 < r < d$ . Однако тогда  $r$  – положительное число меньше  $d$  такое, что его вычет лежит в  $H$ . Это противоречие с выбором  $d$ . Значит,  $n$  делится на  $d$ . Легко видеть, что  $\langle d \rangle = d\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{d}}$ .

4) По лемме 2 порядок элемента  $m \in \mathbb{Z}_n$  равен  $\frac{n}{\text{НОД}(m, n)}$ . А значит,

$$\langle m \rangle \cong \mathbb{Z}_{\frac{n}{\text{НОД}(m, n)}}.$$

Но по пункту 3 есть ровно одна подгруппа в  $\mathbb{Z}_n$ , изоморфная  $\mathbb{Z}_{\frac{n}{\text{НОД}(m, n)}}$  и это  $\langle \text{НОД}(m, n) \rangle$ . Следовательно,  $\langle m \rangle = \langle \text{НОД}(m, n) \rangle$ . □

## ЛЕКЦИЯ 3

**Теорема 3.** 1)  $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$ ,  
 2)  $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$ .

*Замечание 3.* Напомним, что  $\mathbb{Z}_n^\times$  – это группа обратимых по умножению элементов кольца вычетов  $\mathbb{Z}_n$ . Группа  $\mathbb{Z}_n^\times$  состоит из вычетов взаимно простых с  $n$ . В частности,  $|\mathbb{Z}_n^\times| = \varphi(n)$ , где  $\varphi(\cdot)$  – функция Эйлера.

*Доказательство теоремы 3.* 1) Пусть  $\psi$  – автоморфизм  $\mathbb{Z}$ . Тогда  $\psi(0) = 0$ . Пусть  $\psi(1) = k$ . Тогда

$$\psi(2) = \psi(1 + 1) = \psi(1) + \psi(1) = 2k,$$

$$\psi(3) = \psi(1 + 1 + 1) = \psi(1) + \psi(1) + \psi(1) = 3k,$$

и т.д. Аналогично  $\psi(-1) = -k$ ,  $\psi(-2) = \psi((-1) + (-1)) = -2k$ . Получаем

$$\psi(m) = mk.$$

Однако при  $k \neq \pm 1$  гомоморфизм  $\psi$  не будет сюръективен. При  $k = 1$  и  $k = -1$  получаем тождественное отображение и отображение  $\{x \mapsto -x\}$ . Легко видеть, что эти два автоморфизма с операцией композиции образуют группу, изоморфную  $\mathbb{Z}_2$ .

2) Аналогично случаю 1 любой гомоморфизм  $\psi: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  имеет вид

$$\psi_k: m \mapsto km.$$

Если  $k$  не обратим, то в образе  $\psi_k$  не лежит 1, а значит,  $\psi_k$  не сюръективно. Если же  $k$  обратим, то для любого вычета  $l$  имеем  $\psi_k(k^{-1}l) = l$ . Следовательно,  $\psi_k$  сюръективно, а значит, так как множество  $\mathbb{Z}_n$  конечно, гомоморфизм  $\psi_k$  – биекция.

Итак,  $\text{Aut}(\mathbb{Z}_n)$  состоит из  $\psi_k$  для  $k \in \mathbb{Z}_n^\times$ . Докажем, что отображение

$$\zeta: \text{Aut}(\mathbb{Z}_n) \rightarrow \mathbb{Z}_n^\times, \quad \zeta(\psi_k) = k$$

является изоморфизмом. Это очевидно биекция, осталось проверить, что  $\zeta$  – гомоморфизм. Это следует из равенства  $\psi_k \circ \psi_m = \psi_{km}$ , которое легко проверить.  $\square$

**Определение 13.** Пусть  $H$  – подгруппа группы  $G$ . Рассмотрим элемент  $g \in G$ . *Левым смежным классом элемента  $g$  по подгруппе  $H$*  называется множество

$$gH = \{gh \mid h \in H\}.$$

*Правым смежным классом элемента  $g$  по подгруппе  $H$*  называется множество

$$Hg = \{hg \mid h \in H\}.$$

**Лемма 7.** 1)  $g \in fH$  тогда и только тогда, когда  $f^{-1}g \in H$ ,

1')  $g \in Hf$  тогда и только тогда, когда  $gf^{-1} \in H$ ,

2) Левые (правые) смежные классы – это классы эквивалентности. (Более точно, отношение  $g \sim f$ , если  $g \in fH$  является отношением эквивалентности.)

3) Следующие мощности одинаковы  $|gH| = |Hg| = |H|$ .

*Доказательство.* 1)  $g \in fH \iff g = fh \iff f^{-1}g = h$ .

1')  $g \in Hf \iff g = hf \iff gf^{-1} = h$ .

2) Докажем только для левых смежных классов. Для правых аналогично.

Рефлексивность:  $g \in gH$  так как  $e \in H$ ,

Симметричность:

$$g \in fH \iff f^{-1}g \in H \iff (f^{-1}g)^{-1} = g^{-1}f \in H \iff f \in gH.$$

Транзитивность:

$$g \in fH, f \in sH \implies f^{-1}g \in H, s^{-1}f \in H \implies s^{-1}ff^{-1}g = s^{-1}g \in H.$$

3) Следует из того, что  $gh_1 = gh_2$  тогда и только тогда, когда  $h_1 = h_2$ .  $\square$

*Замечание 4.* Из пункта 2 следует, что левые (правые) смежные классы либо не пересекаются, либо совпадают.

**Определение 14.** Индекс подгруппы  $H$  группы  $G$  – это мощность множества левых смежных классов. Обозначается индекс  $[G : H]$

**Задача 4.** Докажите, что  $gH \leftrightarrow Hg^{-1}$  – биекция между левыми и правыми смежными классами, и следовательно мощность правых смежных классов также равна индексу подгруппы.

**Теорема 4.** (Лагранж) Пусть  $G$  – конечная группа и  $H$  – подгруппа  $G$ . Тогда

$$|G| = |H| \cdot [G : H].$$

*Доказательство.* Поскольку каждый элемент группы  $G$  лежит в некотором левом смежном классе и левые смежные классы либо совпадают, либо не пересекаются, вся группа  $G$  разбивается на непересекающиеся левые смежные классы. Так как мощность каждого смежного класса равна  $|H|$ , мощность всей группы равна  $|H|$  умножить на количество смежных классов.  $\square$

**Следствие 1.** (Следствия из теоремы Лагранжа)

1) Порядок конечной группы делится на порядок ее подгруппы.

2) Порядок конечной группы делится на порядок ее элемента.

3) Для любого элемента  $g$  конечной группы  $G$  выполнено  $g^{|G|} = e$ .

4) Группа простого порядка циклическая.

5) (Теорема Эйлера) Пусть  $m$  и  $n$  – взаимно простые натуральные числа. Тогда  $n^{\varphi(m)}$  имеет остаток 1 при делении на  $m$ .

*Доказательство.* 1) Очевидно следует из теоремы Лагранжа.

2) Пусть  $g$  – элемент конечной группы  $G$ . Рассмотрим циклическую подгруппу  $H = \langle g \rangle$ . Поскольку  $\text{ord}(g) = |H|$ , порядок  $G$  делится на  $\text{ord}(g)$ .

3) Пусть  $|G| = \text{ord}(g) \cdot k$ . Тогда  $g^{|G|} = (g^{\text{ord}(g)})^k = e^k = e$ .

4) Пусть  $|G| = p$  – простое число. Рассмотрим  $g \neq e \in G$ . Поскольку порядок  $g$  делит  $p$  и не равен 1, получаем  $\text{ord}(g) = p$ . А значит,  $G = \langle g \rangle$ .

5) Применим пункт 3 к группе  $\mathbb{Z}_m^\times$  и ее элементу  $n$ . Получаем

$$n^{|\mathbb{Z}_m^\times|} = n^{\varphi(m)} = 1.$$

$\square$

**Задача 5.** Приведите пример конечной группы и делителя ее порядка такого, что в группе нет подгруппы такого порядка.

**Теорема 5.** (Коши) Пусть  $p$  – простой делитель порядка конечной группы  $G$ . Тогда в  $G$  есть элемент  $g$  порядка  $p$ .

*Доказательство.* Рассмотрим множество

$$S = \{(g_1, \dots, g_p) \mid g_i \in G, g_1 \cdot \dots \cdot g_p = e\}.$$

Найдем мощность  $S$ . Элементы  $g_1, \dots, g_{p-1}$  можно выбрать любыми, а элемент  $g_p$  равен  $(g_1 \cdot \dots \cdot g_{p-1})^{-1}$ . Таким образом  $|S| = |G|^{p-1}$ . Так как  $|G|$  делится на  $p$ , то и  $|S|$  делится на  $p$ . Множество  $S$  есть объединение двух непересекающихся множеств:  $U = \{g, \dots, g \mid g^p = e\}$  и

$$T = \{(g_1, \dots, g_p) \mid \exists g_i \neq g_j\}.$$

Рассмотрим  $(g_1, \dots, g_p) \in T$ . Так как  $g_1 \cdot \dots \cdot g_p = e$ , получаем  $g_1 \cdot \dots \cdot g_{p-1} = g_p^{-1}$ . Умножая на  $g_p$  слева, имеем  $g_p \cdot g_1 \cdot \dots \cdot g_{p-1} = e$ . Аналогично

$$(g_1, \dots, g_p) \in T, (g_p, g_1, \dots, g_{p-1}) \in T, \dots, (g_2, \dots, g_p, g_1) \in T.$$

Докажем, что все эти элементы  $T$ , получающиеся друг из друга циклическими сдвигами, различны. Допустим, что совершив  $k < p$  сдвигов мы получим тот же элемент. Так как  $\text{НОД}(k, p) = 1$ , существуют целые  $u$  и  $v$  такие, что  $uk + vp = 1$ . Сделаем  $u$  раз по  $k$  циклических сдвигов получим тот же элемент. (Если  $u$  меньше нуля, то циклические сдвиги делаем в другую сторону.) Затем сделаем  $v$  раз по  $p$  сдвигов. Снова получим тот же элемент. Но в итоге мы сделали ровно один циклический сдвиг. Значит, все элементы  $g_i$  одинаковы. Это противоречит определению  $T$ .

Итак, мы доказали, что все  $p$  элементов, полученных из элемента  $T$  циклическими сдвигами, различны. А значит,  $|T|$  делится на  $p$ . Но тогда  $|U| = |S| - |T|$  также делится на  $p$ . Очевидно, что  $(e, e, \dots, e) \in U$ . Так как  $|U|$  не равно 1, есть другой элемент  $(g, \dots, g) \in U$ . Тогда  $g^p = e$ , а значит (так как  $p$  – простое число)  $\text{ord}(g) = p$ .  $\square$

**Определение 15.** Подгруппа  $H$  группы  $G$  называется нормальной, если для любого  $g \in G$  выполнено  $gH = Hg$ . То, что  $H$  – нормальная подгруппа  $G$  обозначается так:  $G \triangleright H$ .

Обозначим через  $gHg^{-1}$  множество  $\{ghg^{-1} \mid h \in H\}$ .

**Лемма 8.** Следующие условия равносильны:

- 1)  $G \triangleright H$ ,
- 2) для каждого  $g \in G$  выполнено  $gHg^{-1} = H$ ,
- 3) для каждого  $g \in G$  выполнено  $gHg^{-1} \subset H$ ,

*Доказательство.*  $1 \implies 2$  В множестве  $gH = Hg$  каждый элемент имеет вид  $gh_1 = h_2g$ . При этом  $h_1$  и  $h_2$  пробегают всю группу  $H$ . Домножим каждый элемент справа на  $g^{-1}$ , получим  $gh_1g^{-1} = h_2$ . То есть  $gHg^{-1} = H$ .

$2 \implies 3$  Очевидно.

$3 \implies 1$ . Для каждого  $g \in G$  и  $h \in H$  выполнено  $ghg^{-1} = \tilde{h} \in H$ . Тогда  $g\tilde{h} = ghg^{-1}g = \tilde{h}g$ . Отсюда  $gH \subset Hg$ . Аналогично  $hg = gg^{-1}hg = \hat{h}$  для  $\hat{h} = g^{-1}hg \in H$ . Значит,  $gH \supset Hg$ . В итоге  $gH = Hg$ .  $\square$

**Определение 16.** Пусть  $H$  – нормальная подгруппа в группе  $G$ . Фактор-группа  $G/H$  – это множество (левых, они же правые) смежных классов по

подгруппе  $H$  с операцией

$$(g_1H) \cdot (g_2H) = (g_1g_2)H.$$