# Лекция 1

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

$$G \times \ldots \times G \to G$$

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

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

$$G \times G \to G, \qquad (g_1, g_2) \to g_1 * g_2.$$

**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 $g_1, \ldots, g_k \in G$. Тогда как бы ни были расставлены скобки в выражении $g_1 * g_2 * \ldots * g_k$ 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 дачт операцию от двух скобок. Длиной скобки назовчм 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 рассановку скобок. Значит, результат при нашей расстановке скобок совпадает с результатом при стандартной расстановке скобок.

*Шаг второй индукции.* Пусть при $s < m$ утверждение доказано ($m \geq 2$). Докажем при $s = m$. Последнее действие при нашей фиксированной расстановке скобок имеет вид $(a) * (b)$. Поскольку длина скобки $(b)$ равна $m \geq 2$, 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 каждго $g \in H$ есть обратный элемент $g^{-1}$ в группе $G$ и есть обратный элемент 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. Возьмчм 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. □

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 нулчм, 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 мощьность 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 $g^n = g \cdot \ldots \cdot g$ – 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 $\mathrm{ord}g$.

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

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

*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.

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

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

Отсюда

$$\frac{n}{\mathrm{НОД}(m,n)} = p_1^{\alpha_1 - \min\{\alpha_1,\beta_1\}} \dots p_l^{\alpha_l - \min\{\alpha_l,\beta_l\}} =$$

$$= p_1^{\max\{\alpha_1-\beta_1,0\}} \dots p_l^{\max\{\alpha_l-\beta_l,0\}}$$

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

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, соответствующео 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 $\mathrm{S}_n$ 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 $\varphi\colon X \to Y$, $\psi\colon Y \to Z$ и $\zeta\colon Z \to T$. 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 $X = Y = Z = T = \{1, 2, \ldots, n\}$ получаем ассоциативность $\mathrm{S}_n$. Порядок группы $\mathrm{S}_n$ равен $n!$. При $n > 3$ группа $\mathrm{S}_n$ не коммутативна.

б) Множество $\mathrm{A}_n$ четных перестановок из $\mathrm{S}_n$ с операцией композиции образует *группу четных перестановок*. Докажем, что $\mathrm{A}_n$ – подгруппа $\mathrm{S}_n$. 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) $\{\mathrm{id},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}$. 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 $\mathrm{S}_4$, которая обозначается $\mathrm{V}_4$. Эта группа коммутативна.

6') (Обобщение примера 6а) Пусть $X$ – некоторое множество (возможно бесконечное). Рассмотрим множество $\mathrm{S}(X)$ биекций $X \to X$ с операцией композиции. Если $|X| < \infty$, то получаем группу перестановок. В общем случае получаем *группу симметий множества* $X$. Нейтральный элемент – тождественное преобразование. Обратный – обратное преобразование. Ассоциативность следует из леммы 3.

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

а) $\mathrm{GL}_n(\mathbb{K})$ – 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, $(\mathrm{GL}(\mathbb{K}), \cdot)$ – группа.

б) $\mathrm{SL}_n(\mathbb{K})$ – 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 $\varphi\colon G \to H$ называется *гомоморфизмом*, если $\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2)$.

Докажем следующие элементарные свойства гомоморфизма.

**Лемма 4.** *Пусть $\varphi\colon (G, *) \to (H, \circ)$ – 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, $\varphi(g^{-1}) = \varphi(g)^{-1}$. □

.

**Задача 3.** Пусть $(G, *)$ и $(H, \circ)$ – моноиды с единицами $e_G$ и $e_H$ соответственно. И пусть $\psi\colon G \to H$ – 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 $\varphi\colon G \to H$ 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* $\varphi\colon \mathbb{R} \to \mathbb{R}_{>0}$, $\varphi(x) = 2^x$. *Легко видеть, что* $\varphi$ *– изоморфизм.*

**Пример 3.** *Группа* $\mathbb{Z}_n$ *изоморфна группе* $\mathcal{C}_n$. *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* $\mathrm{GL}_n(\mathbb{C})$ *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 $\overline{Q}_8$.

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

Здесь i – это мнимая единица (комплексное число).

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

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

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 $\mathrm{GL}_2(\mathbb{C})$. Значит, $\overline{Q}_8$ – подгруппа. Тогда $Q_8$ – группа, изоморфная $\overline{Q}_8$.

Ещч один важный пример группы дачт следующая конструкция.

**Группа диэдра** $\mathrm{D}_n$. Рассмотрим правильный $n$-угольник. Группа диэдра $\mathrm{D}_n$ – это группа всех движений плоскости, сохраняющих этот $n$-угольник.

**Упражнение 3.** а) Докажите, что в группе $\mathrm{D}_n$ ровно $2n$ элементов. Среди них $n$ поворотов и $n$ осевых симметрий. Все оси симметрий проходят через центр $n$- угольника. Если $n$ ччтно, то половина симметрий проходит через 2 вершины, а половина – через две серидины противоположных сторон. Если же $n$ неччтно, то все симметрии проходят через одну вершину и середину противоположной стороны.

б) Найдите, как устроена операция в группе $\mathrm{D}_n$, 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* 'nb[ 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 $\varphi\colon G \to G$ называется *эндоморфизмом*. Изомомрфизм $\varphi\colon G \to G$ называется *автоморфизмом*.

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

Пусть $g$ – элемент группы $G$. Рассмотрим отображение $\varphi_g\colon G \to G$, определчнное 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 $\varphi_{g^{-1}}$. □

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

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

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

*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 $\mathrm{Inn}(G)$ относительно композиции. Осталось проверить, что $\mathrm{Inn}(G)$ замкнуто относительно взятия обратного. Для этого заметим, что $\varphi_g \circ \varphi_{g^{-1}} = \varphi_e = \mathrm{id}$. □

**Определение 12.** Группа $G$ называется *циклической*, если найдётся 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 $\mathbb{Z}_2 \times \mathbb{Z}_2$, $(Q, +)$ и $\mathbb{Q}^\times$ не являются циклическими.

**Лемма 6.** *Пусть* $\mathrm{ord}(g) = n$. *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: $k = nm + r$, где $0 \leq k < n$. Тогда $g^k = (g^n)^m g^r = g^r \in S$.

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 $\mathrm{ord}(g) = n$. □

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, порождённую 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 $\mathrm{ord}(g) = \infty$. Из этого следует, что при $k \neq m$ выполнено $g^k \neq g^m$. Рассмотрим отображение

$$\psi \colon \mathbb{Z} \to G, \qquad k \mapsto g^k.$$

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

$$\psi \colon \mathbb{Z}_n \to G, \qquad k \mapsto g^k, \qquad k \in \{0, 1, \dots, n-1\}.$$

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 $\langle m \rangle = \langle НОД(m, n) \rangle$.*

*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 $G = \langle g^s \rangle$.

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 $\psi\colon \mathbb{Z}_n \to \mathbb{Z}_n$ имеет вид

$$\psi_k\colon m \mapsto km.$$

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

$$\zeta\colon \text{Aut}(\mathbb{Z}_n) \to \mathbb{Z}_n^\times, \qquad \zeta(\psi_k) = k$$

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

**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:

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

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

*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. □

**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 $\mathrm{ord}(g) = |H|$, порядок $G$ делится на $\mathrm{ord}(g)$.

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

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

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

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

□

**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

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

Найдчм мощность $S$. Элементы $g_1, \ldots, g_{p-1}$ можно выбрать любыми, а элемент $g_p$ равен $(g_1 \cdot \ldots \cdot g_{p-1})^{-1}$. 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: $U = \{g, \ldots, g \mid g^p = e\}$ и

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

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

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

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 НОД$(k, p) = 1$, существуют целые $u$ и $v$ такие, что $uk + vp = 1$. Сделав $u$ раз по $k$ циклическихс двигов 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 $(e, e, \ldots, e) \in U$. Так как $|U|$ не равно 1, есть другой элемент $(g, \ldots, g) \in U$. Тогда $g^p = e$, а значит (так как $p$ – простое число) $\mathrm{ord}(g) = p$. □

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

$2 \Longrightarrow 3$ Очевидно.

$3 \Longrightarrow 1$. Для каждых $g \in G$ и $h \in H$ выполнено $ghg^{-1} = \tilde{h} \in H$. Тогда $gh = ghg^{-1}g = \tilde{h}g$. Отсюда $gH \subset Hg$. Аналогично $hg = gg^{-1}hg = g\widehat{h}$ для $\widehat{h} = g^{-1}hg \in H$. Значит, $gH \supset Hg$. В итоге $gH = Hg$. □

## Лекция 4

**Определение 16.** Пусть $H$ – нормальная подгруппа в группе $G$. Факторгруппа $G/H$ – это множество (левых, они же правые) смежных классов по подгруппе $H$ с операцией

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

Определение умножения в факторгруппе требует проверки корректности, то есть проверки того, что результат умножения не зависит от выбора представителей в смежных классах. Потенциальная проблема содержится в том, что $g_1H = g_1'H$, $g_2H = g_2'H$, но при этом смежный класс $g_1g_2H$ может не совпадать с $g_1'g_2'H$. Тогда умножение называется некорректным.

**Предложение 3.** *Пусть $G$ – группа, $H$ – подгруппа. Тогда умножение на множестве левых смежных классов корректно тогда и только тогда, когда $H$ нормальна.*

*Доказательство.* Пусть $H$ нормальна и $g_1H = g_1'H$, $g_2H = g_2'H$. Получаем, что $g_1'^{-1}g_1 \in H$ и $g_2'^{-1}g_2 \in H$. Обозначим $g_1'^{-1}g_1$ через $h$. Имеем

$$(g_1'g_2')^{-1}(g_1g_2) = g_2'^{-1}g_1'^{-1}g_1g_2 = g_2'^{-1}hg_2 \in H$$

Это означает, что $g_1g_2H$ совпадает с $g_1'g_2'H$. Значит, умножение корректно.

Пусть теперь $H$ не нормальна. Тогда найдутся $g \in G$ и $h \in H$ такие, что $ghg^{-1} \notin H$. Тогда $gH = (gh)H$. Рассмотрим следующие смежные классы: $gH = (gh)H$ и $g^{-1}H$. Имеем $gH \cdot g^{-1}H = H$, но $(gh)H \cdot g^{-1}H = (ghg^{-1})H \neq H$. Значит, умножение не корректно. □

Легко видеть, что $G/H$ действительно группа. Ассоциативность произведения следует из ассоциативности произведения в $G$, единичный элемент – это $eH = H$, обратный к $gH$ элемент – это $g^{-1}H$. Из теоремы Лагранжа следует, что если $G$ – конечная группа, то $|G/H| = \frac{|G|}{|H|}$.

Пусть $\varphi\colon G \to G'$ – гомоморфизм групп.

**Определение 17.** Ядро гомоморфизма $\varphi$ – это полный прообраз единицы $\{g \in G \mid \varphi(g) = e\}$. Обозначается ядро через $\operatorname{Ker}\varphi$.

Образ гомоморфизма $\varphi$ – это множество $\operatorname{Im}\varphi = \{\varphi(g) \mid g \in G\}$.

**Лемма 9.** *1) Ядро $\operatorname{Ker}\varphi$ – нормальная подгруппа в группе $G$.*

*2) Образ $\operatorname{Im}\varphi$ – подгруппа в группе $G'$.*

*Доказательство.* 1) Пусть $g_1, g_2 \in \operatorname{Ker}\varphi$, тогда $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = e$. Значит, $g_1g_2 \in \operatorname{Ker}\varphi$. То есть $\operatorname{Ker}\varphi$ замкнуто относительно произведения. Аналогично, если $g \in G$, то $\varphi(g^{-1}) = \varphi(g)^{-1} = e$. То есть $\operatorname{Ker}\varphi$ замкнуто относительно взятия обратного. Поскольку $e \in \operatorname{Ker}\varphi$, ядро не пусто. По предложению 1 ядро является подгруппой.

Пусть $g \in G$, $h \in \operatorname{Ker}\varphi$. Тогда

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e.$$

Значит, $ghg^{-1} \in \operatorname{Ker}\varphi$, то есть $\operatorname{Ker}\varphi$ – нормальная подгруппа.

2) Пусть $\varphi(g)$ и $\varphi(h)$ – два элемента из $\operatorname{Im}\varphi$. Тогда $\varphi(g)\varphi(h) = \varphi(gh) \in \operatorname{Im}\varphi$. Значит, $\operatorname{Im}\varphi$ замкнуто относительно умножения. Кроме того $\varphi(g)^{-1} = \varphi(g^{-1})$, то есть $\operatorname{Im}\varphi$ замкнуто относительно взятия обратного. Поскольку $\operatorname{Im}\varphi$ не пусто, это подгруппа. □

**Определение 18.** Рассмотрим следующее отображение $\pi_H \colon G \to G/H$, $g \mapsto gH$. Из определения операции в факторгруппе следует, что $\pi_H$ – гомоморфизм. Легко видеть, что он сюръективен. Гомоморфизм $\pi_H$ называется *каноническим гомоморфизмом.*

Для канонического гомоморфизма ядро – это нормальная подгруппа $H$, а образ – факторгруппа $G/H$. Следующая теорема показывает, что ситуация аналогична для любого гомоморфизма.

**Теорема 6.** *(Теорема о гомоморфизме) Пусть $\varphi \colon G \to G'$ – гомоморфизм групп. Тогда $G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.*

*Доказательство.* Рассмотрим отображение

$$\Psi \colon G/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi, \qquad \Psi(g\operatorname{Ker}\varphi) = \varphi(g).$$

Сперва нам надо проверить корректность отображения $\Psi$, то есть то, что оно не зависит от выбора представителя $g$ из смежного класса. Для этого заметим, что если $g\operatorname{Ker}\varphi = g'\operatorname{Ker}\varphi$, то $g'^{-1}g = h \in \operatorname{Ker}\varphi$. Тогда $g = g'h$. Получаем $\varphi(g) = \varphi(g'h) = \varphi(g')\varphi(h) = \varphi(g')e = \varphi(g')$. Таким образом, отображение $\Psi$определено корректно.

Докажем, что $\Psi$ – изоморфизм. То, что $\Psi$ –гомоморфизм следует из равенства:

$$\Psi((g\operatorname{Ker}\varphi)(f\operatorname{Ker}\varphi)) = \Psi(gf\operatorname{Ker}\varphi) = \varphi(gf) = \varphi(g)\varphi(f) = \Psi(g\operatorname{Ker}\varphi)\Psi(f\operatorname{Ker}\varphi).$$

Инъективность $\Psi$ следует из того, что если $\varphi(g) = \varphi(f)$, то $\varphi(f^{-1}g) = e$, то есть $f^{-1}g \in \operatorname{Ker}\varphi$, а значит, $g\operatorname{Ker}\varphi = f\operatorname{Ker}\varphi$. Сюръективность $\Psi$ очевидна, так как для любого элемента $\varphi(g)$ в $\operatorname{Im}\varphi$ в него отображается смежный класс $g\operatorname{Ker}\varphi$. □

**Следствие 2.** *Если $|G| < \infty$ и $\varphi \colon G \to G'$ – гомоморфизм, то*

$$|\operatorname{Ker}\varphi| \cdot |\operatorname{Im}\varphi| = |G|.$$

**Пример 6.** *Найдем, чему изоморфна факторгруппа $\mathbb{Z}/n\mathbb{Z}$. Для того, чтобы применить теорему о гомоморфизме, нам нужно построить гомоморфизм $\varphi \colon Z \to G'$ для некторой группы $G'$ такой, что $\operatorname{Ker}\varphi = n\mathbb{Z}$. Легко видеть, что подходит следующий гомоморфизм*

$$\varphi \colon \mathbb{Z} \to \mathbb{Z}_n, \qquad k \mapsto k \,(\mathrm{mod}\, n)$$

*Действительно, $\varphi$ – гомоморфизм, $\operatorname{Ker}\varphi = n\mathbb{Z}$ и $\varphi$ – сюръекция, то есть $\operatorname{Im}\varphi = \mathbb{Z}_n$. По теореме о гомоморфизме $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.*

**Определение 19.** Пусть группа $G$ содержит подмножество $S$. *Подгруппой, порождённой подмножеством $S$*, называется минимальная подгруппа, содержащая $S$. Обозначается эта подгруппа $\langle S\rangle$. Если $G = \langle S\rangle$, то $S$ называется *множеством порождающих группы $G$.*

**Лемма 10.** *Пусть $G = \langle S\rangle$, тогда $G$ совпадает с множеством конечных произведений элементов из $S$ и обратных к ним, то есть*

$$\{s_1^{\pm 1} \dots s_n^{\pm 1} \mid s_i \in S, n \in \mathbb{N}\}.$$

*Доказательство.* Легко видеть, что множество конечных произведений элементов из $S$ и обратных к ним замкнуто относительно произведения и взятия обратного. Кроме того в нчм лежит $ss^{-1} = e$. Значит, это подгруппа, содержащая $S$, и следовательно, совпадает с $G$. □

**Упражнение 5.** Докажите, что
а) $\mathbb{Z} = \langle 1 \rangle$,
б) $S_n = \langle (1,2), (2,3) \ldots, (n-1,n) \rangle = \langle (1,2), (1,2,\ldots,n) \rangle$,
в) $A_n = \langle (1,2,3), (1,2,4), \ldots, (1,2,n) \rangle$.

**Пример 7.** *Напомним конструкцию сюръективного гомоморфизма $S_4 \to S_3$. Рассмотрим 4 переменные $x_1, x_2, x_3, x_4$ и три многочлена от этих переменных:*

$$f_1 = x_1x_2 + x_3x_4, \qquad f_2 = x_1x_3 + x_2x_4, \qquad f_3 = x_1x_4 + x_2x_3.$$

*Если применить к $x_1, x_2, x_3, x_4$ перестановку $\sigma$, то $f_i$ переставятся между собой по перестановке $\tau(\sigma)$. Ясно, что $\tau(\sigma \circ \delta) = \tau(\sigma) \circ \tau(\delta)$, то есть $\tau$ – гомоморфизм $S_4 \to S_3$.*

*Заметим, что $\tau(2,3) = (1,2)$, значит, $(1,2) \in \operatorname{Im} \tau$. Аналогично можно проверить, что все транспозиции лежат в образе $\tau$. Поскольку $S_3$ порождается транспозициями, гомоморфизм $\tau$ сюръективен. Легко видеть, что $V_4 \subset \operatorname{Ker} \varphi$. С другой стороны $|\operatorname{Ker} \varphi| = \frac{|S_4|}{|S_3|} = 4$. Следовательно, $\operatorname{Ker} \varphi = V_4$.*

*По теореме о гомоморфизме получаем следующий изоморфизм:*

$$S_4/V_4 \cong S_3.$$

**Лемма 11.** *Пусть $G$ – группа, $H \lhd G$ – нормальная подгруппа, $K \subset G$ – подгруппа. Тогда $\langle K \cup H \rangle = KH = \{kh \mid k \in K, h \in H\}$.*

*Доказательство.* Докажем, что $KH$ замкнуто относительно умножения. Действительно,

$$(k_1h_1)(k_2h_2) = k_1k_2k_2^{-1}h_1k_2h_2 = k_1k_2(k_2^{-1}h_1k_2)h_2 = k_1k_2\widehat{h}h_2 \in KH.$$

Теперь докажем, что $KH$ замкнуто относительно взятия обратного:

$$(kh)^{-1} = h^{-1}k^{-1} = k^{-1}kh^{-1}k^{-1} = k^{-1}(kh^{-1}k^{-1}) = k^{-1}\widetilde{h} \in KH.$$

Поскольку $KH$ не пусто, это группа. Очевидно, что $KH$ – наименьшая подгруппа, содержащая $K$ и $H$. □

**Теорема 7.** *(Вторая теорема о гомоморфизме) Пусть $G$ – группа, $H \lhd G$ – нормальная подгруппа, $K \subset G$ – подгруппа.*
*1) $H \cap K$ – нормальная подгруппа в $K$ и $H$ – нормальная подгруппа в $KH$,*
*2) $KH/H \cong K/(H \cap K)$.*

*Доказательство.* 1) Пусть $a \in H \cap K$, $k \in K$. Тогда $a \in H \Rightarrow kak^{-1} \in H$. С другой стороны $a \in K \Rightarrow kak^{-1} \in K$. То есть $kak^{-1} \in H \cap K$. То есть $(H \cap K) \lhd K$.

Пусть $h \in H, g \in KH$, тогда, так как $g \in G$, $ghg^{-1} \in H$. Значит, $H \lhd KH$.

2) Рассмотрим $\Psi\colon K \to (KH)/H$, $k \mapsto kH$. Докажем, что $\Psi$ – сюръекция. Действительно, пусть $khH \in (KH)/H$. Тогда $khH = kH = \Psi(k)$. Легко видеть, что $\Psi$ – гомоморфизм. Найдем ядро $\Psi$. Пусть $k \in \operatorname{Ker} \Psi$, тогда $kH = H$. Это значит, что $k \in H$. С другой стороны $k \in K$. То есть $k \in (H \cap K)$. Итак, $\operatorname{Ker} \Psi = H \cap K$. По теореме о гомоморфизме $K/(H \cap K) \cong KH/H$. □

**Теорема 8.** *(Третья теорема о гомоморфизме) Пусть $\varphi\colon G \to G'$ – сюръективный гомоморфизм, $K = \operatorname{Ker}\varphi$, $H' \subset G'$ –подгруппа. Пусть $H = \varphi^{-1}(H')$ – полный прообраз. Тогда*

*1) $H' \leftrightarrow H$ – биекция между подгруппами в $G'$ и подгруппами в $G$, содержащими $K$.*

*2) Подгруппа $H$ нормальна в $G$ тогда и только тогда, когда $H'$ нормальна в $G'$.*

*3) Если $H$ и $H'$ нормальны, то $G/H \cong G'/H'$.*

*Доказательство.* 1) Для подгруппы $H' \subset G'$ обозначим через $\Omega(H') = H$ подгруппу $\varphi^{-1}(H') \subset G$. Легко видеть, что $\Omega(H')$ содержит $K = \varphi^{-1}(e)$. Пусть $H$ – подгруппа $G$, содержащая $K$, обозначим через $\Theta(H)$ образ $\varphi(H)$, это подгруппа в $G'$. Докажем, что $\Omega$ и $\Theta$ – взаимно обратные отображения. Для этого надо проверить, что $\Omega \circ \Theta = \mathrm{id}$ и $\Theta \circ \Omega = \mathrm{id}$. Действительно, $\Theta \circ \Omega(H')$ – это образ от полного прообраза $H'$, то есть $H'$. Теперь рассмотрим $\Omega \circ \Theta(H)$ – полный прообраз от образа $H$. Очевидно, что $H \subset \Omega \circ \Theta(H)$. Пусть $g \in \Omega \circ \Theta(H)$, тогда $\varphi(g) \in \Theta(H)$. Следовательно, есть $h \in H$ такое, что $\varphi(h) = \varphi(g)$. Тогда $\varphi(h^{-1}g) = e$, то есть $h^{-1}g \in K$. Значит $g = hk \in H$. Итак, $\Omega \circ \Theta(H) = H$.

2) Пусть $G \triangleright H$. Рассмотрим $h' \in H'$, $g' \in G'$. Так как гомоморфизм $\varphi$ сюръективный, найдутся $h \in H$ и $g \in G$ такие, что $\varphi(h) = h'$, $\varphi(g) = g'$. Тогда $ghg^{-1} \in H$, а значит, $g'h'g'^{-1} = \varphi(ghg^{-1}) \in H'$. Таким образом, $H' \triangleleft G'$.

Пусть теперь $H' \triangleleft G'$. Рассмотрим $g \in G$, $h \in H$. Тогда $\varphi(g) \in G'$, $\varphi(h) \in H'$, а значит, $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in H'$. Тогда $ghg^{-1} \in H$, то есть $G \triangleright H$.

3) Рассмотрим композицию гомоморфизмов $\Psi = \pi_{H'} \circ \varphi\colon G \to G'/H'$. Так как $\varphi$ и $\pi_{H'}$ – сюръекции, $\Psi$ – также сюръекция. Заметим, что $\Psi(g) = eH'$ тогда и только тогда, когда $\varphi(g) \in H'$, то есть $g \in H$. Получаем, что $\operatorname{Ker}\Psi = H$. По теореме о гомоморфизме получаем $G/H \cong G'/H'$. □

## Лекция 5

**Следствие 3** (Следствие из третьей теоремы о гомоморфизме)**.** *Пусть $H$ и $N$ – две нормальные подгруппы группы $G$, причем $N \subset H$. Пусть $\pi_N\colon G \to G/N$ – канонический гомоморфизм. Тогда $\pi_N(H) \cong H/N$ – нормальная подгруппа в $G/N$ и*

$$(G/N)/(H/N) \cong G/H.$$

*Доказательство.* Гомоморфизм $\pi_N\colon G \to G/N = G'$ сюръективен. Значит, мы находимся в условиях третьей теоремы о гомоморфизме. Поскольку $H$ – нормальная подгруппа в $G$, $\pi_N(H)$ – также нормальная подгруппа в $G/N$. Так как $\operatorname{Ker}\pi_N = N$, $\pi_N(H) \cong H/N$. По пункту 3) третьей теоремы о гомоморфизме

$$G/H \cong (G/N)/\pi_N(H).$$

□

**Пример 8.** *Рассмотрим нормальные подгруппы $V_4 \subset A_4$ в $S_4$. По предыдущему следствию получаем $S_4/A_4 \cong (S_4/V_4)(A_4/V_4)$. В самом деле, $S_4/A_4 \cong \mathbb{Z}_2$, $S_4/V_4 \cong S_3$ (см. пример 7), $|A_4/V_4| = 3$, а значит, $A_4/V_4 \cong \mathbb{Z}_3$. При этом $\pi_{V_4}(A_4) \cong \mathbb{Z}_3$ – подгруппа в $S_3$, следовательно, $\pi_{V_4}(A_4) = A_3$. И мы получаем, что $(S_4/V_4)(A_4/V_4) \cong S_3/A_3 \cong \mathbb{Z}_2$.*

**Определение 20.** Центр группы $G$ – это множество $Z(G)$ элементов, коммутирующих со всеми элементами группы. $Z(G) = \{z \in G \mid \forall g \in G : gz = zg\}$.

**Лемма 12.** *Центр – это нормальная подгруппа $G$.*

*Доказательство.* Пусть $z_1, z_2 \in Z(G)$. Тогда для любого $g \in G$ выполнено

$$z_1 z_2 g = z_1 g z_2 = g z_1 z_2.$$

Значит, $Z(G)$ – замкнутое относительно операции подмножество. Для доказательства замкнутости относительно взятия обратного заметим, что если $z \in Z(G)$, то для любого $g \in G$ выполнено $zg^{-1} = g^{-1}z$. Тогда

$$z^{-1}g = (g^{-1}z)^{-1} = (zg^{-1})^{-1} = gz^{-1}.$$

Кроме того $Z(G) \neq \varnothing$, так как $e \in Z(G)$.

То, что подгруппа $Z(G)$ нормальна следует из равенства $gzg^{-1} = z \in Z(G)$. □

**Предложение 4.** *Факторгруппа группы $G$ по центру изоморфна группе внутренних атоморфизмов* $\mathrm{Inn}(G)$.

*Доказательство.* По предложению 2(б) отображение $\Psi\colon G \to \mathrm{Inn}(G)$, $g \mapsto \varphi_g$ является гомоморфизмом. По определению внутренних автоморфизмов гомоморфизм $\Psi$ сюръективен. Ядро $\Psi$ состоит из тех элементов $g \in G$, для которых $\varphi_g = \mathrm{id}$, то есть $\forall h \in G$ выполнено $ghg^{-1} = h$. Это означает $g \in Z(G)$. Итак, $\operatorname{Ker}\varphi = Z(G)$, $\operatorname{Im}\varphi = \mathrm{Inn}(G)$. По теореме о гомоморфизме $G/Z(G) \cong \mathrm{Inn}(G)$. □

**Предложение 5.** *Если группа $G$ не коммутативна, то группа $G/Z(G)$ не является циклической.*

*Доказательство.* Предположим, что $G/Z(G) = \langle aZ(G)\rangle$, $a \in G$. Тогда для любого $g \in G$ выполнено $g \in a^k Z(G)$, то есть $g = a^k z$, где $z \in Z(G)$. Возьмем $g_1, g_2 \in G$, тогда $g_1 = a^k z_1$, $g_2 = a^m z_2$. Имеем

$$g_1 g_2 = a^k z_1 a^m z_2 = a^{k+m} z_1 z_2 = a^{k+m} z_2 z_1 = a^m z_2 a^k z_1 = g_2 g_1.$$

Таким образом, $G$ коммутативна. (И следовательно, $G/Z(G) \cong \{e\}$.) □

Пусть $S$ – некоторое множество. Рассмотрим множество конечных слов от букв $s \in S$ и $s^{-1}$, где $s \in S$. (Так как на множестве $S$ нет никакой операции, то $s^{-1}$ – некий формальный символ.) Также мы рассматриваем пустое слово $\varnothing$. Два слова назовем *эквивалентными*, если одно переводится в другое некой конечной цепочкой следующих элементарных преобразований:

1) Если в некотором месте есть пара подряд идущих букв $ss^{-1}$ или $s^{-1}s$, то их можно убрать.

2) В любое место можно вписать пару $ss^{-1}$ или $s^{-1}s$.

Конкатенацией двух слов называется операция приписывания одного слова к другому. Например, $(xyx^{-1})(xzzx) = xyx^{-1}xzzx$.

**Лемма 13.** *Класс эквивалентности конкатенации слов из двух классов эквивалентности не зависит от выбора представителей в этих классах.*

*Доказательство.* Пусть слово $A$ эквивалентно слову $B$, а слово $C$ эквивалентно слову $D$. Наша задача доказать, что слова $AC$ и $BD$ эквивалентны. Заметим, что мы можем делать с левой частью слова $AC$ те же элементарные преобразования, что и со словом $A$ и получим слово $BC$. Затем будем делать с правой частью $BC$ те же элементарные преобразования, что и с $C$. Получим $CD$. □

**Определение 21.** *Свободной группой с множеством порождающих $S$* называется множество классов эквивалентности конечных слов от букв $s \in S$ и $s^{-1}$, где $s \in S$ с операцией конкатенации. Обозначать эту группу мы будем $\langle S\rangle$.

Если множество $S$ конечно, то $|S|$ называется *рангом* свободной группы $\langle S\rangle$.

*Замечание* 5. Легко видеть, что свободная группа действительно является группой. Ассоциативность конкатенации очевидна. Нейтральный элемент – класс пустого слова. Обратный элемент к каждому слову легко выписать.

**Теорема 9.** *Пусть $G$ группа с порождающими $g_1, \dots, g_k$. Существует единственный гомоморфизм из свободной группы $\langle x_1, \dots, x_k\rangle$ ранга $k$ в группу $G$ такой, что $\varphi(x_i) = g_i$. Гомоморфизм $\varphi$ сюръективен.*

*Доказательство.* Пусть $\varphi$ переводит класс слова $x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_m}^{\varepsilon_m}$, $\varepsilon_j = \pm 1$, в

$$g = g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \dots g_{i_m}^{\varepsilon_m} \in G.$$

Чтобы проверить корректность определения, нужно доказать, что $g$ не зависит от выбора представителя в классе. Если два слова отличаются элементарным преобразованием, то в одном из них есть "дополнительное"$x_i x_i^{-1}$, которое переходит в $g_i g_i^{-1} = e$. Это не меняет образ. То, что $\varphi$ – гомоморфизм и $\varphi(x_i) = g_i$ очевидно. Сюръективность следует из того, что $G$ порождается $g_1, \dots, g_k$. □

**Определение 22.** Пусть $M$ – некоторое подмножество группы $G$. Нормальное замыкание $M$ – это наименьшая по включению нормальная $N(M)$ в $G$ подгруппа, содержащая $M$.

Легко видеть, что пересечение нормальных подгрупп – это нормальная подгруппа. Из этого следует, что наименьшая нормальная подгруппа, содержащая $M$ существует.

**Лемма 14.** *Подгруппа $N(M)$ совпадает с подгруппой, порожденной элементами $gmg^{-1}$ для всех $m \in M, g \in G$.*

*Доказательство.* Поскольку $N(M)$ – нормальная подгруппа и $M \subset N(M)$, получаем $gmg^{-1} \in N(M)$, а значит, $\langle gmg^{-1} \mid g \in G, m \in M\rangle \subset N(M)$. С другой стороны $\langle gmg^{-1} \mid g \in G, m \in M\rangle$ – это нормальная подгруппа. В самом деле, $(gmg^{-1})^{-1} = gm^{-1}g^{-1}$. А значит, любой элемент $\langle gmg^{-1} \mid g \in G, m \in M\rangle$ имеет вид

$$(g_1 m_1^{\varepsilon_1} g_1^{-1}) \dots (g_k m_k^{\varepsilon_k} g_k^{-1}) \qquad \varepsilon_j = \pm 1.$$

При этом

$$g(g_1 m_1^{\varepsilon_1} g_1^{-1}) \dots (g_k m_k^{\varepsilon_k} g_k^{-1}) g^{-1} = \\ = (gg_1 m_1^{\varepsilon_1} g_1^{-1} g^{-1})(gg_2 m_2^{\varepsilon_2} g_2^{-1} g^{-1}) \dots (gg_k m_k^{\varepsilon_k} g_k^{-1} g^{-1}) \in \langle gmg^{-1} \mid g \in G, m \in M\rangle.$$

□

**Определение 23.** Говорят, что группа $G$ задана образующими $g_1, \dots, g_k$ и соотношениями $g_1^{\alpha_1} \dots g_k^{\alpha_k}, \dots, g_1^{\beta_1} \dots g_k^{\beta_k}$, если для гомоморфизма $\varphi\colon \langle x_1, \dots, x_k\rangle \to G$, $x_i \mapsto g_i$ ядро совпадает с $N(x_1^{\alpha_1} \dots x_k^{\alpha_k}, \dots, x_1^{\beta_1} \dots x_k^{\beta_k})$. Тогда

$$G \cong \langle x_1, \dots, x_k\rangle / N(x_1^{\alpha_1} \dots x_k^{\alpha_k}, \dots, x_1^{\beta_1} \dots x_k^{\beta_k}).$$

В таком случае пишут

$$G = \langle g_1, \dots, g_k \mid g_1^{\alpha_1} \dots g_k^{\alpha_k}, \dots, g_1^{\beta_1} \dots g_k^{\beta_k}\rangle.$$

**Пример 9.** *Докажем, что $D_n = \langle a, b \mid a^2, b^2, (ab)^n\rangle$.*

*Ясно, что $D_n$ порождается двумя симметриями с минимальным углом между ними. Их композиция – это поворот на $\frac{2\pi}{n}$. Если обозначить эти симметрии $a$ и $b$, то ясно, что $a^2 = b^2 = (ab)^n = e$. То есть для $\varphi\colon \langle x_1, x_2\rangle \to D_n$, $x_1 \mapsto a, x_2 \mapsto b$ ядро*

*содержит* $N(x_1^2, x_2^2, (x_1x_2)^n)$. *Наша цель – доказать, что* $\operatorname{Ker}\varphi = N(x_1^2, x_2^2, (x_1x_2)^n)$. *Если это не так, то по следствию 3 имеем:*

$$G \cong \langle x_1, x_2\rangle/\operatorname{Ker}\varphi \cong (\langle x_1, x_2\rangle/N(x_1^2, x_2^2, (x_1x_2)^n))/(\operatorname{Ker}\varphi/N(x_1^2, x_2^2, (x_1x_2)^n)).$$

*Тогда порядок группы* $G$ *будет строго меньше, чем* $H = \langle a, b \mid a^2, b^2, (ab)^n\rangle = \langle x_1, x_2\rangle/N(x_1^2, x_2^2, (x_1x_2)^n)$. *Докажем, что в* $H$ *не более* $2n$ *элементов. Легко видеть, что любой элемент* $H$ *может быть записан либо в виде конечного слова* $abab\ldots$, *либо в виде* $baba\ldots$. *Действительно,* $a^{-1} = a$, $b^{-1} = b$, *значит, любое слово от* $a, b, a^{-1}, b^{-1}$ *– это слово от* $a$ *и* $b$. *При этом если есть сочетание* $aa$ *или* $bb$, *то его можно сократить. Поскольку* $(ab)^n = e$, *среди слов* $abab\ldots$ *различными являются слова длины* $0, 1, 2\ldots, 2n-1$. *С другой стороны* $ba = b^{-1}a^{-1} = (ab)^{-1}$. *Значит,* $(ba)^n = e$ *и среди слов* $baba\ldots$ *также различными являются слова длины* $0, 1, 2\ldots, 2n-1$. *Осталось заметить, что*

$$b = (ab)^n b = (ab)^{n-1}a;$$
$$ba = (ab)^n ba = (ab)^{n-1};$$
$$\vdots$$
$$(ba)^{n-1}b = (ab)^n(ba)^{n-1}b = a.$$

*Таким образом, все слова вида* $baba\ldots$ *представляются словами вида* $abab\ldots$. *Значит,* $|H| \le 2n$. *Отсюда следует, что* $D_n = H$.

## Лекция 6

**Проблема равенства слов.** Пусть $S$ – некоторое множество. И пусть даны два конечных слова от букв $s_i \in S$ и $s_i^{-1}$. Возникает вопрос: эквивалентны ли эти два слова, то есть дают ли они один и тот же элемент свободной группы $\langle S\rangle$? Этот вопрос называется проблеммой равенства слов.

Один из способов решить проблему равенства слов – это определить некий канонический вид, к которому можно привести каждое слово, причцм этот вид должен быть единственным. Если этот подход будет реализован, то для проверки эквивалентности двух слов нужно оба слова привести к каноническому виду и сравнить результаты.

Напомним, что слова называются эквивалентными, если от одного до другого можно добраться следующими элементарными преобразованиями: можно сокращать подряд идущие пары символов типа $xx^{-1}$ или $x^{-1}x$, а также можно приписывать в любое место слова пары символов $xx^{-1}$ или $x^{-1}x$. Преобразования первого типа назовем *сокращениями*, а второго – *приписываниями*. Любое слово можно сокращениями привести к *несократимому виду*, то есть к виду, в котором нет подряд идущих сочетаний вида $xx^{-1}$ и $x^{-1}x$.

**Теорема 10.** *В каждом классе эквивалентности есть только одно несократимое слово.*

*Доказательство.* Пусть есть два различных несократимых слова $u$ и $v$, которые эквивалентны. Рассмотрим цепочку элементарных преобразований, переводящих $u$ в $v$. Пусть в этой цепочке есть сокращение, идущее после приписывания. Докажем, что эту пару можно заменить либо на пару сокращение, а затем приписывание, либо убрать. В самом деле если ни один из сокращцнных символов не совпадает с только что приписанными, то можно поменять эти две операции. Остацтся случай, когда было приписывание $xx^{-1}$, а затем сокращение, использующее один или оба из приписанных символов. Но тогда в результате этих двух операций слово не поменялось и можно

эту пару убрать. Назовчм такую замену одной пары другой (или убирание пары) перестройкой.

Для цепочки элементарных преобразований рассмотрим сумму позиций, на которых стоят сокращения. (То есть в цепочке "сокращение, приписывание, приписывание, сокращение, сокращение"сокращения стоят на 1, 4 и 5 местах и сумма равна 10.) При перестройке данная сумма уменьшается. Следовательно, не возможно бесконечное число перестроек и за конечное число перестроек мы достигнем цепочки, в которой сначала идут несколько сокращений, а затем несколько приписываний. Однако слово $u$ несократимо. Значит, цепочка не могла начинаться с сокращений. Тогда она состоит только из приписываний. Но это противоречит несократимости слова $v$. □

*Замечание* 6. Можно поставить аналогичный вопрос равенства слов не только в свободной группе, но и в группе с соотношениями. В этом случае слова эквивалентны не только, когда они различаются цепочкой сокращений и приписываний, но также можно вставлять в любое место или убирать любые элементы из $N(r_1, \ldots, r_k)$, где $r_i$ – соотношения. Оказывается, что проблема равенства слов может стать гораздо сложнее, более того она не всегда резрешима. Более точно, существует конечно порожденная группа с конечным числом соотношений, в которой проблема равенства слов алгоритмически не разрешима.

**Внутреннее прямое произведение подгрупп.**

Напомним, что прямым произведением групп $K$ и $H$ мы называли множество пар $(k, H) \mid k \in K, h \in H$ с покомпонентным умножением. Назовчм такое прямое произведение *внешним*.

**Определение 24.** Пусть $K$ и $H$ – нормальные подгруппы в группе $G$ такие, что $K \cap H = \{e\}$ и $G$ порождается подгруппами $K$ и $H$. Тогда $G$ называется *внутренним прямым произведением* подгрупп $H$ и $K$.

**Лемма 15.** *Пусть $K$ и $H$ – подгруппы в $G$. Следующие условия эквивалентны:*

*1) Группа $G$ – это внутреннее прямое произведение подгрупп $K$ и $H$.*

*2) Каждый элемент $g \in G$ единственным образом представляется в виде произведения $g = kh$, $k \in K$, $h \in H$. При этом если $g_1 = k_1h_1$ и $g_2 = k_2h_2$, то $g_1g_2 = k_1k_2h_1h_2$.*

*Доказательство.* $1 \Rightarrow 2$. Так как группа $G$ порождена подгруппами $K$ и $H$ и подгруппа $H$ нормальна, то по лемме 11 любой элемент $g \in G$ представляется в виде $g = kh$. Предположим, что $k_1h_1 = k_2h_2$. Тогда, умножая слева на $k_2^{-1}$, а справа – на $h_1^{-1}$, получаем $k_2^{-1}k_1 = h_2h_1^{-1} \in K \cap H$. Следовательно, $k_2^{-1}k_1 = h_2h_1^{-1} = e$, то есть $k_1 = k_2$ и $h_1 = h_2$. Итак, представление $g = kh$ единственно.

Пусть теперь $g_1 = k_1h_1$ и $g_2 = k_2h_2$. Докажем, что $h_1k_2h_1^{-1}k_2^{-1} = e$. В самом деле так как $K$ – нормальная подгруппа, $h_1k_2h_1^{-1} = \widehat{k} \in K$, с другой стороныб так как $H$ – нормальна подгруппа, $k_2h_1^{-1}k_2^{-1} = \widehat{h} \in H$. Тогда

$$h_1k_2h_1^{-1}k_2^{-1} = h_1\widehat{h} = \widehat{k}k_2^{-1} \in K \cap H = \{e\}.$$

Итак, $h_1k_2h_1^{-1}k_2^{-1} = e$. Значит, $h_1k_2 = k_2h_1$. Но тогда $g_1g_2 = k_1h_1k_2h_2 = k_1k_2h_1h_2$.

$2 \Rightarrow 1$. Рассмотрим $g \in G$, $k \in K$. Тогда $g = k_0h_0$, $k = ke$. Рассмотрим $\overline{g} = k_0^{-1}h_0^{-1}$. По правилу умножения $g\overline{g} = k_0k_0^{-1}h_0h_0^{-1} = e$, значит, $\overline{g} = g^{-1}$. Получаем $ghg^{-1} = (k_0h_0)(ke)(k_0^{-1}h_0^{-1})$. По правилу умножения это равно $(k_0kk_0^{-1})(h_0eh_0^{-1}) = k$. Значит, $K$ –нормальная подгруппа. Аналогично доказывается, что $H$ – нормальная подгруппа.

Пусть $s \in K \cap H$. Тогда $s = se = es$ – два представления $s$ в виде $kh$. Так как такое представление должно быть единственно, $s = e$. То есть $K \cap H = \{e\}$.

Осталось заметить, что раз любой элемент $g$ равен $kh$, то $G$ – группа, порожденная подгруппами $K$ и $H$. □

*Замечание* 7. Результат предыдущей леммы можно интерпретировать так: внутреннее прямое произведение подгрупп изоморфно внешнему произведению этих подгрупп. Для установления этого изоморфизма нужно отождествить $kh$ и $(k, h)$.

С другой стороны любое внешнее прямое произведение может быть интерпретировано как внутреннее. Действительно, рассмотрим во внешнем прямом произведении $K \times H$ подгруппы $K' = \{(k, e)\} \cong K$ и $H' = \{(e, h)\} \cong H$. Тогда $K \times H$ является внутренним прямым произведением подгрупп $K'$ и $H'$.

В дальнейшем мы не будем различать внутренннее и внешнее прямые произведения и будем использовать единый термин "прямое произведение".

**Теорема 11** (Теорема о факторизации прямого произведения)**.** *Пусть $G_1, \ldots, G_k$ – группы. В каждой группе $G_i$ фиксируем нормальную подгруппу $H_i$. Тогда $H_1 \times \ldots \times H_k$ является нормальной подгруппой $G_1 \times \ldots \times G_k$ и*

$$(G_1 \times \ldots \times G_k)/(H_1 \times \ldots \times H_k) \cong G_1/H_1 \times \ldots \times G_k/H_k.$$

*Доказательство.* Рассмотрим отображение

$$\varphi\colon G_1 \times \ldots \times G_k \to G_1/H_1 \times \ldots \times G_k/H_k,$$

$$\varphi\colon (g_1, \ldots, g_k) \mapsto (g_1H_1, \ldots, g_kH_k).$$

Легко видеть, что $\varphi$ – это сюръективный гомоморфизм, ядро которого совпадает с $H_1 \times \ldots \times H_k$. Это доказывает оба утверждения. □

**Лемма 16** (Критерий инъективности гомоморфизма)**.** *Пусть $\varphi\colon G \to G'$ – гомоморфизм групп. Тогда $\varphi$ инъективен если и только если* $\operatorname{Ker}\varphi = \{e\}$.

*Доказательство.* Пусть $g \neq e \in \operatorname{Ker}\varphi$. Тогда $\varphi(g) = e = \varphi(e)$, то есть гомоморфизм $\varphi$ не инъективен.

Пусть теперь $\varphi$ не инъективен. Тогда есть два элемента $x \neq y \in G$ такие, что $\varphi(x) = \varphi(y)$. Но тогда $\varphi(xy^{-1}) = e$. Следовательно, $xy^{-1} \neq e \in \operatorname{Ker}\varphi$. □

*Замечание* 8. Так же как в случае абелевой группы мы используем аддитивные обозначения, если группы $A$ и $B$ абелевы, то прямое произведение групп $A$ и $B$ мы будем называть *прямой суммой* и обозначать $A \oplus B$.

**Теорема 12** (Китайская теорема об остатках.)**.** *Пусть $m$ и $n$ – натуральные числа. Тогда следующие условия эквивалентны:*

*1) НОД$(m, n) = 1$;*

*2) $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$.*

*Доказательство.* $1 \Rightarrow 2$. Рассмотрим

$$\varphi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n, \qquad \varphi(u) = (u \bmod m, u \bmod n).$$

Докажем, что $\varphi$ – изоморфизм. Из определения видно, что $\varphi$ переводит сложение в сложение, то есть является гомоморфизмом.

Пусть $u \in \operatorname{Ker}\varphi$. Тогда $u$ делится и на $m$, и на $n$. Значит, так как $m$ и $n$ взаимно просты, $u$ делится на $mn$. То есть $u$ равен нулю по модулю $mn$. Следовательно, $\operatorname{Ker}\varphi = \{0\}$, а значит, по лемме 16 гомоморфизм $\varphi$ инъективен. Но поскольку $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \oplus \mathbb{Z}_n|$ из инъективности $\varphi$ следует его биективность. Итак, $\varphi$ – изоморфизм.

$2 \Rightarrow 1$. Пусть НОД$(m, n) = d > 1$. Тогда для любого элемента $(a, b) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$ выполнено

$$\frac{mn}{d}(a, b) = \text{НОК}(m, n)(a, b) = (0, 0).$$

Значит, любой элемент в $\mathbb{Z}_m \oplus \mathbb{Z}_n$ имеет порядок не больше $\frac{mn}{d}$, то есть нет элемента из $\mathbb{Z}_m \oplus \mathbb{Z}_n$, порядок которого равен $mn$. Значит, группа $\mathbb{Z}_m \oplus \mathbb{Z}_n$ не циклическая и не изоморфна $\mathbb{Z}_{mn}$. $\square$