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 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 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) $\{\mathrm{id},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}$. 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 S_4, которая обозначается 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 φ – изоморфизм, то обратное отображение φ^{-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* φ *– 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* φ *– 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 φ 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 φ 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 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 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 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 φ_g является автоморфизмом группы G.*

Доказательство. Проверим, что φ_g – гомоморфизм:

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

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

Автоморфизм называются *внутренним*, если он имеет вид φ_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 ψ – гомоморфизм. Так как все элементы G имеют вид g^k, ψ – сюръекция, а так как при $k \neq m$ выполнено $g^k \neq g^m$, ψ – инъекция. Итак, ψ – 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 ψ – 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 ψ – 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 ψ 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 ψ_k не лежит 1, а значит, ψ_k не сюръективно. Если же k обратим, то для любого вычета l имеем $\psi_k(k^{-1}l) = l$. Следовательно, ψ_k сюръективно, а значит, так как множество $\mathbb{Z}_n$ конечно, гомоморфизм ψ_k – биекция.

Итак, $\text{Aut}(\mathbb{Z}_n)$ состоит из ψ_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 ζ – 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 φ – это полный прообраз единицы $\{g \in G \mid \varphi(g) = e\}$. Обозначается ядро через $\operatorname{Ker}\varphi$.

Образ гомоморфизма φ – 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 π_H – гомоморфизм. Легко видеть, что он сюръективен. Гомоморфизм π_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 Ψ, 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 Ψопределено корректно.

Докажем, что Ψ – изоморфизм. То, что Ψ –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 Ψ 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 Ψ 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, φ – гомоморфизм, $\operatorname{Ker}\varphi = n\mathbb{Z}$ и φ – 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 σ, то f_i переставятся между собой по перестановке $\tau(\sigma)$. Ясно, что $\tau(\sigma \circ \delta) = \tau(\sigma) \circ \tau(\delta)$, то есть τ – 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 τ. Поскольку S_3 порождается транспозициями, гомоморфизм τ 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 Ψ – сюръекция. Действительно, пусть $khH \in (KH)/H$. Тогда $khH = kH = \Psi(k)$. Легко видеть, что Ψ – гомоморфизм. Найдем ядро Ψ. 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 Ω и Θ – 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 φ 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 φ и $\pi_{H'}$ – сюръекции, Ψ – 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 Ψ сюръективен. Ядро Ψ 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 φ сюръективен.*

Доказательство. Пусть φ 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 φ – 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 φ – 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 φ 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 φ не инъективен.

Пусть теперь φ 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 φ – изоморфизм. Из определения видно, что φ 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 φ инъективен. Но поскольку $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \oplus \mathbb{Z}_n|$ из инъективности φ следует его биективность. Итак, φ – 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 $\mathbb{Z}_{mn}$. □

Лекция 7

Для абелевых групп будем использовать аддитивную терминологию. Операцию будем обозначать "+"и называть сложением. Нейтральный элемент называем нулем. При этом степень g^k элемента g, будет обозначатся kg.

Замечание 9. То, что абелева группа A порождается подмножеством $S \subset A$ означает, что каждый элемент $a \in A$ представляется в виде $a = k_1 s_1 + \ldots + k_n s_n$, где $s_i \in S$, $k_i \in \mathbb{Z}$.

Мы почти всегда будем ограничиваться рассмотрением только конечно порожденных абелевых групп, то есть таких групп A, для которых множество S может быть выбрано конечным.

Определение 25. Система элементов S абелевой группы A называется *линейно независимой* (над $\mathbb{Z}$), если из того, что $k_1 s_1 + \ldots + k_n s_n = 0$ для некоторых $k_i \in \mathbb{Z}$, $s_i \in S$, следует что все k_i равны нулю.

Определение 26. *Базис* абелевой группы – это линейно независимая система порождающих этой группы.

Заметим, что не у всякой группы есть базис. Например, у группы $\mathbb{Z}_n$ базиса нет, так как для любой системы $\{s_1, \ldots, s_k\}$ выполнено $ns_1 = 0$, что противоречит линейной независимости этой системы.

Определение 27. Пусть в абелевой группе A есть базис $\{e_1, \ldots, e_n, \ldots$. Тогда группа A называется *свободной абелевой группой*. Будем обозначать эту группу

$$\langle e_1, \ldots, e_n, \ldots \rangle_a$$

Если базис конечен и имеет мощность n, то будем говорить, что A – свободная абелева группа ранга n и обозначать $\operatorname{rk} A = n$.

Задача 6. Докажите, что

$$\langle e_1, \ldots, e_n \rangle_a = \langle e_1, \ldots, e_n \mid e_i e_j e_i^{-1} e_j^{-1}, 1 \le i < j \le n \rangle.$$

Лемма 17. *Ранг свободной абелевой группы определен однозначно.*

Доказательство. Пусть в некоторой группе A есть два базиса $\{e_1, \ldots, e_m\}$ и $\{e'_1, \ldots, e'_n\}$, причем $n > m$. Так как $\{e_1, \ldots, e_m\}$ – базис, каждый элемент e'_j выражается через $\{e_1, \ldots, e_m\}$ с целыми коэффициентами: $e'_j = c_{1j} e_1 + \ldots + c_{mj} e_m$. Можно собрать все коэффициенты c_{ij} в целочисленную матрицу C размера $m \times n$ такую, что

$$(e'_1, \ldots, e'_n) = (e_1, \ldots, e_m) C.$$

Интерпретируем столбцы $C^{(1)}, \ldots, C^{(n)}$ матрицы C как векторы из пространства $\mathbb{Q}^m$ строк с рациональными коэффициентами длины m. Тогда столбцы – это n векторов в m-мерном векторном пространстве. По основной лемме о линейной зависимости

столбцы C линейно зависимы, то есть есть рациональные числа $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ не все равные нулю такие, что

$$\frac{p_1}{q_1}C^{(1)} \ldots + \frac{p_n}{q_n}C^{(n)} = 0.$$

Домножим это равенство на произведение знаменателей и получим

$$k_1C^{(1)} \ldots + k_nC^{(n)} = 0$$

для некоторых $k_i \in \mathbb{Z}$ не всех равных нулю. Но тогда $k_1e'_1 + \ldots + k_ne'_n = 0$, что противоречит линейной независимости $\{e'_1, \ldots, e'_n\}$. □

Замечание 10. Пусть $F = \langle e_1, \ldots, e_n \rangle_a$. Тогда $F = \langle e_1 \rangle \oplus \ldots \oplus \langle e_n \rangle \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$.

Предложение 6. *Подгруппа L свободной абелевой группы F ранга n – это свободная абелева группа ранга $m \leq n$.*

Доказательство. Докажем это утверждение индукцией по n.

База индукции $n = 1$. $F \cong \mathbb{Z}$. По теореме 2(2) подгруппа в $\mathbb{Z}$ имеет вид $k\mathbb{Z}$. При $k \neq 0$ это свободная абелева группа ранга 1. Если же $k = 0$ получаем свободную абелеву группу ранга ноль.

Шаг индукции. Пусть для $n < k$ утверждение доказано. Рассмотрим

$$P = \langle e_1, \ldots, e_{n-1} \rangle_a \subset F.$$

Обозначим $B = P \cap L$. Так как P – свободная группа ранга $n-1$, по предположению индукции $B \subset P$ – свободная абелева группа ранга не более $n-1$. Если $L \subset P$, то $L = B$ – свободная абелева группа ранга не более $n-1$. Пусть $L \neq B$. Тогда найдется $l \in L$ такой, что $l = k_1e_1 + \ldots + k_ne_n$, где $k_n \neq 0$. Будем считать, что l – элемент из L с минимальным модулем последней координаты k_n. Пусть $s = t_1e_1 + \ldots t_ne_n \in L$. Поделим t_n на k_n с остатком: $t_n = qk_n + r$, где $|r| < |k_n|$. Получаем

$$s - ql = (t_1 - qk_1)e_1 + \ldots + re_n \in L.$$

Так как l – элемент L с минимальной по модулю последней координатой, получаем $r = 0$. Значит, $s - ql \in B$. То есть $s \in B \oplus \langle l \rangle$. Получаем $L = B \oplus \langle l \rangle$ – свободная абелева группа ранга $\operatorname{rk} B + 1 \leq n$. □

Теорема 13 (Универсальное свойство свободной абелевой группы)**.** *Пусть A – абелева группа с образующими $a_1, \ldots, a_n$. Тогда существует сюръективный гомоморфизм*

$$\varphi\colon \langle x_1, \ldots, x_n \rangle_a \to A,$$

причем $\varphi(x_i) = a_i$.

Доказательство. Подходит гомоморфизм определенный по правилу

$$\varphi(k_1x_1 + \ldots + k_nx_n) = k_1a_1 + \ldots + k_na_n.$$

□

Применяя теорему о гомоморфизме, получаем следствие.

Следствие 4. *Каждая конечно порожденная абелева группа изоморфна факторгруппе свободной абелевой группы по некоторой подгруппе (ядру гомоморфизму φ).*

Опишем все базисы данной свободной абелевой группы через один фиксированный базис.

Определение 28. Обозначим через $\mathrm{GL}_n(\mathbb{Z})$ множество целочисленных матриц $n \times n$ с определителем ± 1.

Легко проверить, что $\mathrm{GL}_n(\mathbb{Z})$ – подгруппа в $\mathrm{GL}(\mathbb{Q})$.

Предложение 7. *Пусть $\{e_1, \dots, e_n\}$ базис свободной абелевой группы F. Тогда следующие условия эквивалентны:*
1) $\{e'_1, \dots, e'_n\}$ – базис F;
2) $(e'_1, \dots, e'_n) = (e_1, \dots, e_n)C$, где $C \in \mathrm{GL}_n(\mathbb{Z})$.

Доказательство. $1 \Rightarrow 2$. Поскольку $\{e_1, \dots, e_n\}$ – базис F, каждый вектор выражается через $\{e_1, \dots, e_n\}$. Значит, $(e'_1, \dots, e'_n) = (e_1, \dots, e_n)C$, где C – некоторая целочисленная матрица $n \times n$. Аналогично $(e_1, \dots, e_n) = (e'_1, \dots, e'_n)D$ для некоторой целочисленной матрицы D. Тогда $(e_1, \dots, e_n) = (e_1, \dots, e_n)CD$. Так как $\{e_1, \dots, e_n\}$ – базис, получаем $CD = E$. Тогда $\det C \det D = 1$ и при этом $\det C, \det D \in \mathbb{Z}$. Значит, $\det C = \pm 1$.

$2 \Rightarrow 1$. Применяя формулу через алгебраические дополнения, получаем, что обратная матрица C^{-1} также является целочисленной. Для любого $f \in F$ выполняется

$$f = \begin{pmatrix} e_1 & \dots & e_n \end{pmatrix} \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} = \begin{pmatrix} e'_1 & \dots & e'_n \end{pmatrix} C^{-1} \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}.$$

Таким образом любой элемент f выражается через $\{e'_1, \dots, e'_n\}$. Так как матрица C невырожденная, система $\{e'_1, \dots, e'_n\}$ линейно независима над $\mathbb{Z}$. Значит, это базис F. □

Примерами матриц из $\mathrm{GL}_n(\mathbb{Z})$ являются матрицы следующих элементарных преобразований:
1) прибавление одной строки к другой с целым коэффициентом,
2) смена двух строк местами
3) умножение строки на -1.

Таким образом, переходя от базиса $(e_1, \dots, e_n)$ к базису $(e_1, \dots, e_n)C$ мы можем делать данные элементарные преобразования с данным базисом. Назовчм данные элементарные преобразования базиса *допустимыми*.

Рассмотрим пару состоящую из свободной абелевой группы $F = \langle x_1, \dots, x_n \rangle_a$ и ее подгруппы $L = \langle y_1, \dots, y_m \rangle_a$, $m \leq n$. Тогда

$$(y_1, \dots, y_m) = (x_1, \dots, x_n)P,$$

где P – целочисленная матрица размера $n \times m$.

Теорема 14 (Теорема о согласованных базисах)**.** *Существует такой базис $\{e_1, \dots, e_n\}$ группы F и такие натуральные числа $u_1, \dots u_m$, что u_i делится на u_j при $i > j$, и система $\{u_1 e_1, \dots, u_m e_m\}$ является базисом L.*

Доказательство. Будем делать элементарные преобразования с базисами группы F и подгруппы L. Пусть $(x'_1, \dots, x'_n) = (x_1, \dots, x_n)C$, $(y'_1, \dots, y'_m) = (y_1, \dots, y_m)D$, тогда равенство $(y_1, \dots, y_m) = (x_1, \dots, x_n)P$ дает $(y'_1, \dots, y'_m) = (x'_1, \dots, x'_n)C^{-1}PD$. При умножении P слева на матрицу C^{-1} и справа на матрицу D происходят допустимые элементарные преобразования со строками и столбцами P. Далее утверждение теоремы следует из следующей леммы.

Лемма 18. *Пусть P – целочисленная матрица $n \times m$. Делая допустимые элементарные преобразования со строками и столбцами P можно привести P к виду*

$$\begin{pmatrix} u_1 & 0 & 0 & \dots & 0 \\ 0 & u_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & 0 & 0 & u_m \\ 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Причем если $i > j$, то u_i делится на u_j.

Доказательство леммы. Если не все коэффициенты матрицы равны нулю, то перестановкой строк и столбцов можно поставить на место p_{11} ненулевой элемент с минимальным модулем. Далее будем уменьшать минимальный модуль ненулевого элемента пока это будет возможно.

Случай 1. В первой строке матрицы P есть элемент p_{1i} не делящийся на p_{11}. Поделим p_{1i} на p_{11} с остатком: $p_{1i} = qp_{11} + r$, $0 < |r| < |p_{11}|$. Прибавим первый столбец к i- му с коэффициентом $-q$. На месте p_{1i} получим r. Таким образом мы уменьшили модуль минимального по модулю ненулевого элемента.

Случай 2. В первом столбце матрицы P есть элемент p_{i1} не делящийся на p_{11}. Прибавляя 1-ю строку к i-ой с нужным коэффициентом получаем элемент с модулем меньше $|p_{11}|$ в первом столбце.

Случай 3. Все элементы первой строки и первого столбца делятся на p_{11}, но есть p_{ij}, не делящийся на p_{11}. Прибавим первую строку и первый столбец к остальным так, чтобы все элементы, кроме p_{11} стали равны нулю. При этом p_{ij} всч равно не будет делиться на p_{11} (к нему прибавилось нечто делящееся на p_{11}). Прибавим i-ю строку к первой и попадем в случай 1.

Так как бесконечно уменьшать модуль минимального ненулевого элемента мы не можем, рано или поздно получится ситуация, когда все элементы p_{ij} делятся на p_{11}. Тогда можно сделать все элементы первой строки и первого столбца нулевыми. Получим матрицу

$$\begin{pmatrix} u_1 & 0 & 0 & \dots & 0 \\ 0 & p_{22} & p_{23} & \dots & p_{2m} \\ 0 & p_{32} & p_{33} & \dots & p_{3m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & p_{n2} & p_{n3} & \dots & p_{nm} \end{pmatrix}$$

Далее работаем аналогичным образом с матрицей без первой строки и первого столбца. При этом элементарные преобразования строк со 2 по n-ю и столбцов со 2-го по m-ый не меняет того, что все элементы p_{ij} делятся на u_1. В итоге получаем нужный вид матрицы. □

Замечание 11. Легко доказать, что при допустимых элементарных преобразованиях НОД всех элементов матрицы не меняется. Поэтому u_1 равен НОД всех элементов матрицы.

□

Следствие 5. *Любая конечно порожденная абелева группа изоморфна*

$$\mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z},$$

где u_i делится на u_j, если $i > j$.

Доказательство. Пусть A – конечно порожденная абелева группа. По теореме 13 существует сюръективный гомоморфизм φ из свободной абелевой группы F конечного ранга n в группу A. Применим теорему о согласованных базисах к паре $\operatorname{Ker}\varphi \subset F$. Получаем

$$F = \langle e_1 \rangle \oplus \ldots \oplus \langle e_m \rangle \oplus \langle e_{m+1} \rangle \oplus \ldots \oplus \langle e_n \rangle,$$
$$\operatorname{Ker}\varphi = \langle u_1 e_1 \rangle \oplus \ldots \oplus \langle u_m e_m \rangle \oplus \{0\} \oplus \ldots \oplus \{0\}.$$

Применяя теорему о факторизации прямого произведения, получаем

$$A \cong F/\operatorname{Ker}\varphi \cong \langle e_1 \rangle / \langle u_1 e_1 \rangle \oplus \ldots \oplus \langle e_m \rangle / \langle u_m e_m \rangle \oplus \langle e_{m+1} \rangle / \{0\} \oplus \ldots \cong$$
$$\cong \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}.$$

□

Лекция 8

Докажем следующую полезную лемму.

Лемма 19. *Пусть $G_1, \ldots, G_l$ – группы. Рассмотрим $\overline{g} = (g_1, \ldots, g_l) \in G_1 \times \ldots \times G_l$. Тогда если среди g_i есть элемент бесконечного порядка, то $\overline{g}$ имеет бесконечный порядок. Если же все элементы g_i конечного порядка, то*

$$\operatorname{ord}\overline{g} = HOK(\operatorname{ord} g_1, \ldots, \operatorname{ord} g_l).$$

Доказательство. Заметим, что $k\overline{g} = (kg_1, \ldots, kg_l)$. А значит, $k\overline{g} = 0$ тогда и только тогда, когда $kg_i = 0$ для всех i, то есть k делится на $\operatorname{ord} g_i$ для всех i. Если существует j такое, что $\operatorname{ord} g_j = \infty$, то такого k не существует, и следовательно, $\operatorname{ord}\overline{g} = \infty$. Если же все порядки g_i конечны, то минимальное k равно наименьшему общему кратному этих порядков. □

По следствию 5 каждая конечно порожденная абелева группа A изоморфна

$$\mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z},$$

где u_i делится на u_j, если $i > j$. Назовем такую форму записи A *первой канонической формой абелевой группы.*

Определение 29. Абелева группа называется примарной, если она имеет порядок p^a, где p – простое число, $a \in \mathbb{N}$.

Применим китайскую теорему об остатках к группе $\mathbb{Z}_u$. Пусть $u = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Тогда

$$\mathbb{Z}_u \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_k}}.$$

Применив это к каждому слагаемому первой канонической формы абелевой группы A и переупорядочив слагаемые, получим *вторую каноническую форму группы A*

$$\mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_1^{a_2}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{a_{m_1}}} \oplus \mathbb{Z}_{p_2^{b_1}} \oplus \mathbb{Z}_{p_2^{b_2}} \oplus \ldots \oplus \mathbb{Z}_{p_2^{b_{m_2}}} \oplus \ldots \oplus$$
$$\oplus \mathbb{Z}_{p_k^{c_1}} \oplus \mathbb{Z}_{p_k^{c_2}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{c_{m_k}}} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}. \quad (1)$$

Здесь каждое простое число может несколько раз встречаться в одной и той же степени в качестве порядка циклического слагаемого.

Наша цель – доказать что первая и вторая канонические формы действительно канонические (то есть одну группу нельзя представить двумя различными способами в такой форме). Начнем со второй формы.

Теорема 15 (Теорема о строении конечно порожденных абелевых групп)**.** *Пусть A – конечно порожденная абелева группа. Тогда A изоморфна прямой сумме конечного числа циклических групп. Каждая из этих циклических групп либо является бесконечной циклической группой, либо примарной циклической группой. И такое разложение единственно с точностью до перестановки прямых слагаемых.*

Доказательство. Существование такого разложения в прямую сумму уже доказано (это и есть вторая каноническая форма). Пусть есть два таких разложения одной и той же группы A. Прежде всего докажем, что количество бесконечных циклических слагаемых в обоих разложениях одинаково. Для этого определим следующую подгруппу

Определение 30. Подгруппа кручения $\operatorname{Tor} A$ (абелевой) группы A – это подгруппа, состоящая из всех элементов конечного порядка.

Прежде всего нужно объяснить, что множество элементов конечного порядка действительно является подгруппой. Для этого заметим, что если $ka = 0$ и $mb = 0$, то $km(a+b) = 0$. То есть множество $\operatorname{Tor} A$ замкнуто относительно сложения. Кроме того $k(-a) = 0$, что означает замкнутость $\operatorname{Tor} A$ относительно взятия противоположного. Осталось заметить, что $0 \in \operatorname{Tor} A$.

Из леммы 19 следует, что элементы конечного порядка в разложении (1) имеют вид $(x_1, \ldots, x_N, 0, \ldots, 0)$, где в конечных слагаемых идут любые элементы $x_1, \ldots, x_N$, а в бесконечных слагаемых все элементы – нули. Таким образом,

$$\begin{aligned}\operatorname{Tor} A = \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_1^{a_2}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{a m_1}} \oplus \mathbb{Z}_{p_2^{b_1}} \oplus \mathbb{Z}_{p_2^{b_2}} \oplus \ldots \oplus \mathbb{Z}_{p_2^{b m_2}} \oplus \ldots \oplus \\ \oplus \mathbb{Z}_{p_k^{c_1}} \oplus \mathbb{Z}_{p_k^{c_2}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{c m_k}} \oplus \{0\} \oplus \ldots \oplus \{0\} \subset \\ \subset \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_1^{a_2}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{a m_1}} \oplus \mathbb{Z}_{p_2^{b_1}} \oplus \mathbb{Z}_{p_2^{b_2}} \oplus \ldots \oplus \mathbb{Z}_{p_2^{b m_2}} \oplus \ldots \oplus \\ \oplus \mathbb{Z}_{p_k^{c_1}} \oplus \mathbb{Z}_{p_k^{c_2}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{c m_k}} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} = A.\end{aligned}$$

По теореме о факторизации прямого произведения

$$A/\operatorname{Tor} A \cong \{0\} \oplus \ldots \oplus \{0\} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \cong \mathbb{Z}^r.$$

Таким образом, факторгруппа $A/\operatorname{Tor} A$ – это свободная абелева группа ранга r, где r равно количеству прямых слагаемых, изоморфных $\mathbb{Z}$ в разложении (1). Поскольку определение подгруппы кручения не зависит от разложения и ранг свободной абелевой группы определен однозначно, получаем, что если для группы A есть две вторых канонических формы, то количество прямых слагаемых $\mathbb{Z}$ в них одинаково. Назовем это число *рангом* (абелевой) группы A.

Разложение (1) состоит из второй канонической формы группы $\operatorname{Tor} A$, к которой добавлены $\operatorname{rk} A$ слагаемых $\mathbb{Z}$. Для того, чтобы доказать, что две вторых канонических формы группы A совпадают, осталось доказать, что для группы $\operatorname{Tor} A$ нет двух различных вторых канонических формы. Для этого рассмотрим следующие подгруппы в $\operatorname{Tor} A$.

Определение 31. Пусть p – простое число. Подгруппа p-кручения (абелевой) группы A – это подгруппа $\operatorname{Tor}_p A$, состоящая из всех элементов группы $a \in A$ таких, что $\operatorname{ord} a = p^k$ для некоторого $k \in \mathbb{N} \cup \{0\}$.

Опять-таки нужно доказать, что $\mathrm{Tor}_p A$ – подгруппа A. Для этого заметим, что если $\mathrm{ord}\, a = p^k$, $\mathrm{ord}\, b = p^m$, то $p^{\max\{k,m\}}(a+b) = 0$, а значит, $\mathrm{ord}\,(a+b)$ делит $p^{\max\{k,m\}}$. Таким образом, множество $\mathrm{Tor}_p A$ замкнуто относительно сложения. Кроме того $\mathrm{ord}\,(-a) = p^k$, то есть $\mathrm{Tor}_p A$ замкнуто относительно взятия противоположного элемента. Так как $0 \in \mathrm{Tor}_p A$, это подмножество является подгруппой в A. Легко видеть, что подгруппа p-кручения содержится в подгруппе кручения.

Из леммы 19 следует, что элемент $\overline{a} = (a_1, \ldots, a_N)$ содержится в $\mathrm{Tor}_p A$ тогда и только тогда, когда порядок каждого a_i является степенью p. В разложении (1) каждый элемент a_i содержится в некоторой примарной циклической группе. Если $a_i \in \mathbb{Z}_{p^\alpha}$, то порядок a_i равен степени p. Если же $a_i \in \mathbb{Z}_{q^\beta}$ для некоторого простого $q \neq p$, то порядок a_i равен степени p тогда и только тогда, когда $a_i = 0$. Итак, подгруппа $\mathrm{Tor}_p A$ изоморфна прямой сумме тех слагаемых разложения (1), порядок которых равен p^α для всех $\alpha \in \mathbb{N}$. Например,

$$\mathrm{Tor}_{p_1} A \cong \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_1^{a_2}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{a_{m_1}}}.$$

Таким образом, вторая каноническая форма A состоит из прямой суммы вторых канонических форм $\mathrm{Tor}_{p_i} A$ для всех p_i (нетривиальные разложения будут только для p_i, делящих порядок A) и $\mathrm{rk}A$ слагаемых $\mathbb{Z}$.

Если есть две различные вторые канонические формы у некоторой группы A, то существует некоторое простое число p, для которого у группы $B = \mathrm{Tor}_p A$ есть две различные вторые канонические формы.

Пусть H – абелева группа, а n – натуральное число. Тогда $nH = \{nh \mid h \in H\}$ – подгруппа H. Проверим это. Возьмем два элемента nh_1 и nh_2 из nH. Тогда

$$nh_1 + nh_2 = n(h_1 + h_2) \in nH.$$

При этом $-(nh) = (-n)h \in nH$ и $0 = n0 \in nH$. Таким образом мы доказали, что nH – группа. Легко видеть, что $n(H_1 \oplus H_2) = nH_1 \oplus nH_2$. Теперь рассмотрим случай, когда $H \cong \mathbb{Z}^\alpha$, а $n = p^\beta$ для некоторого простого p. Из описания подгрупп в циклической группе следует, что при $\beta < \alpha$ подгруппа $p^\beta \mathbb{Z}_{p^\alpha}$ циклическая, порождена p^β и изоморфна $\mathbb{Z}_{p^{\alpha-\beta}}$. Если же $\beta \geq \alpha$, то $p^\beta \mathbb{Z}_{p^\alpha} = \{0\}$. Заметим, что

$$p^\beta \mathbb{Z}_{p^\alpha} / p^{\beta+1} \mathbb{Z}_{p^\alpha} \cong \begin{cases} \mathbb{Z}_p, & \text{при } \beta < \alpha, \\ \{0\}, & \text{при } \beta \geq \alpha. \end{cases}$$

Пусть теперь во второй канонической форме группы $B = \mathrm{Tor}_p A$ содержится s_1 прямых слагаемых $\mathbb{Z}_p$, s_2 прямых слагаемых $\mathbb{Z}_{p^2}$, s_3 прямых слагаемых $\mathbb{Z}_{p^3}$ и т.д. Тогда B/pB изоморфно прямой сумме $s_1 + s_2 + \ldots$ копий $\mathbb{Z}_p$, то есть $|B/pB| = p^{s_1+s_2+\cdots}$. Аналогично pB/p^2B изоморфно $s_2 + s_3 + \ldots$ копий $\mathbb{Z}_p$, то есть $|pB/p^2B| = p^{s_2+s_3+\cdots}$. Продолжая таким образом, получаем $p^lB/p^{l+1}B$ изоморфно $s_{l+1} + s_{l+2} + \ldots$ копий $\mathbb{Z}_p$, то есть $|p^lB/p^{l+1}B| = p^{s_{l+1}+s_{l+2}+\cdots}$. Отсюда

$$p^{s_l} = \frac{|p^{l-1}B/p^lB|}{|p^lB/p^{l+1}B|}.$$

То есть

$$s_l = \log_p \frac{|p^{l-1}B/p^lB|}{|p^lB/p^{l+1}B|}.$$

Таким образом, все s_i определены однозначно, то есть вторая каноническая форма группы B определена однозначно. Как доказано выше, из этого следует, что вторая каноническая форма группы A определена однозначно. Теорема 15 доказана. $\square$

Следствие 6. *Первая каноническая форма конечно порожденной абелевой группы A определена однозначно.*

Доказательство. Пусть есть абелева группа A, у которой есть две различные первые канонические формы Φ_1 и Φ_2. Так как ранг свободной группы $A/\mathrm{Tor}\, A$ определчн однозначно, количество прямых слагаемых $\mathbb{Z}$ в этих разложениях одинаково. Значит, эти формы отличаются конечными слагаемыми. Тогда найдется простое число p и его степень k такие, что количество u_i, делящихся на p^k в одной форме (можно считать, что в Φ_1) строго больше, чем в другой (в Φ_2). Напомним, что пользуясь китайской теоремой об остатках можно из первой канонической формы получить вторую. Но тогда во второй канонической форме, полученной из Φ_1 будет больше слагаемых $\mathbb{Z}_{p^\alpha}$ с условием $\alpha \geq k$, чем во второй канонической форме, полученной из Φ_2. Это противоречит теореме 15. □

Определение 32. Экспонента группы G – это минимальное натуральное число k такое, что для любого $g \in G$ выполнено $g^k = e$. Если такого числа не существует, то будем говорить, что экспонента G равна бесконечности. Обозначать экспоненту будем $\exp G$.

Лемма 20. *Экспонента группы равна наименьшему общему кратному порядков элементов. (Имеется в виду, что если есть элемент бесконечного порядка или нет конечного общего кратного у всех порядков, то экспонента бесконечна.)*

Доказательство. Если $g^k = e$, то k делится на $\mathrm{ord}\, g$. Так как $\exp G$ – минимальное натуральное число, что $g^{\exp G} = e$ для всех $g \in G$, получаем, что $\exp G$ – минимальное натуральное число, делящееся на порядки всех элементов. □

Предложение 8 (Критерий цикличности абелевой группы)**.** *Пусть A – конечная абелева группа. Группа A циклическая тогда и только тогда, когда* $\exp A = |A|$.

Доказательство. Пусть A циклическая. Тогда есть элемент, порядок которого равен $|A|$, то есть $\exp A \geq |A|$. Порядки всех элементов – делители $|A|$, значит, $\exp A \leq |A|$. Получаем $\exp A = |A|$.

Пусть наоборот, $\exp A = |A| = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, где p_i – простые числа. Так как $\exp A$ – наименьшее общее кратное порядков всех элементов, для каждого $1 \leq j \leq m$ найдется $b_j \in A$ такое, что $\mathrm{ord}\, b_j = p_j^{k_j} t$, где t не делится на p_j. Обозначим $a_j = tb_j$. Легко видеть, что $\mathrm{ord}\, a_j = p_j^{k_j}$. Рассмотрим элемент $a = a_1 + \ldots + a_m$, докажем, что его порядок равен $|A|$. Для этого заметим, что $|A|a = 0$ по теореме Лагранжа, но

$$\frac{|A|}{p_j} a = p_1^{k_1} p_2^{k_2} \dots p_j^{k_j - 1} \dots p_m^{k_m} (a_1 + \ldots + a_j + \ldots a_m) =$$

$$= 0 + \ldots + 0 + p_1^{k_1} p_2^{k_2} \dots p_j^{k_j - 1} \dots p_m^{k_m} a_j + 0 + \ldots + 0 = p_1^{k_1} p_2^{k_2} \dots p_j^{k_j - 1} \dots p_m^{k_m} a_j \neq 0.$$

А значит, простое число p_j входит в $\mathrm{ord}\, a$ именно в степени k_j. Так как это выполняется для всех j, порядок a равен $|A|$. Следовательно, группа A циклическая. □

Лекция 9

Напомним, что полем называется множество F с двумя бинарными операциями: сложением и умножением, удовлетворяющим следующим аксиомам.

1) $\forall a, b, c \in F$: $(a + b) + c = a + (b + c)$,

2) $\exists\, 0 \in F$: $\forall x$ выполнено $0 + x = x + 0 = x$,

3) $\forall x \in F\ \exists\,(-x) : x + (-x) = (-x) + x = 0$,
4) $\forall a, b \in F$: $a + b = b + a$,
5) $\forall a, b, c \in F$: $(a + b)c = ac + bc$,
6) $\forall a, b, c \in F$: $(ab)c = a(bc)$,
7) $\forall a, b \in F$: $ab = ba$,
8) $\exists\, e \in F$: $\forall x$ выполнено $ex = xe = x$,
9) $\forall x \neq 0 \in F\ \exists\, x^{-1} : xx^{-1} = x^{-1}x = e$.

Поле является частным случаем кольца. Мы ранее говорили, что для произвольного кольца R можно рассмотреть группу $(R^\times, \cdot)$, состоящую из всех обратимых по умножению элементов, с операцией множения. Для поля $F^\times = F \setminus \{0\}$ и группа $(F^\times, \cdot)$ называтся *мультипликативной группой поля* F.

Предложение 9. *Конечная подгруппа в мультипликативной группе поля циклическая.*

Доказательство. Пусть G – конечная подгруппа в мультипликативной группе поля $F^\times$. Предположим, что G не является циклической. Так как $F^\times$ коммутативна, ее подгруппа G также коммутативна. По предложению 8 экспонента G не равна $|G|$. Значит, $\exp G = k < |G|$. Тогда в поле F у многочлена $x^k - e$ как минимум $|G|$ корней (все элементы группы G являются такими корнями). Однако ненулевой многочлен не может иметь в поле больше корней, чем его степень. В самом деле это следует из того, что, если $f(c) = 0$, то по теореме Безу $f(x)$ делится на $x - c$. Получаем противоречие. Следовательно, исходное предположение, что G не циклическая не верно. □

Очевидным следствием предыдущего предложения является следующее утверждение.

Следствие 7. *Мультипликативная группа конечного поля циклическая.*

Определение 33. Пусть G – группа, а X – множество. *Действием* группы G на множестве X называется отображение $\alpha\colon G \times X \to X$, удовлетворяющее следующим условиям:
1) для любых $g, h \in G$ и $x \in X$ выполнено $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$,
2) для любого $x \in X$ выполнено $\alpha(e, x) = x$.

Если задано действие группы G на множестве X, то говорят, что G *действует* на X и обозначают $G \curvearrowright X$ (в некоторой литературе обозначают $G : X$). При этом $\alpha(g, x)$ называется действием (или применением) элемента g к элементу x, и $\alpha(g, x)$ обозначается $g \cdot x$. В таких обозначениях свойства действия из определения 33 принимают вид:
1) для любых $g, h \in G$ и $x \in X$ выполнено $g \cdot (h \cdot x) = (gh) \cdot x$,
2) для любого $x \in X$ выполнено $e \cdot x = x$.

Пример 10. *Пусть $X = \{1, 2, \ldots, n\}$. Тогда есть естественное действие симметрической группы S_n на X, заданное по формуле $\sigma \cdot i = \sigma(i)$.*

То, что это действие сводится к проверкам
1) $\sigma \cdot (\delta \cdot i) = \sigma(\delta(i)) = (\sigma \circ \delta)(i) = (\sigma \circ \delta) \cdot i$,
2) $\mathrm{id} \cdot i = \mathrm{id}(i) = i$.

Пример 11. *Пусть K – поле. Тогда зададим действие $\mathrm{GL}(K) \curvearrowright K^n$ по следующей формуле. Для $A \in \mathrm{GL}(K)$ и $Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \in K^n$ положим $A \cdot Y = AY$. Доказательство того, что это действие сводится к проверкам*

1) $A \cdot (B \cdot Y) = ABY = (AB) \cdot Y$,

2) $E \cdot Y = EY = Y$.

Такое действие называется тавтологическим.

Важный частный случай действий – это действия группы на себе, то есть случай, когда $X = G$. Есть три естественных действия $G \curvearrowright G$.

Пример 12. *1)* **Действие G на себе левыми сдвигами.**

По определению $g \cdot \overline{g} = g\overline{g}$.

Тогда $g_1 \cdot (g_2 \cdot \overline{g}) = g_1 g_2 \overline{g} = (g_1 g_2) \cdot \overline{g}$ и $e \cdot \overline{g} = e\overline{g} = \overline{g}$.

2) **Действие G на себе правыми сдвигами.**

По определению $g \cdot \overline{g} = \overline{g} g^{-1}$. Проверим, что это действие.

$$g_1 \cdot (g_2 \cdot \overline{g}) = g_1 \cdot (\overline{g} g_2^{-1}) = (\overline{g} g_2^{-1}) g_1^{-1} = \overline{g} (g_1 g_2)^{-1} = (g_1 g_2) \cdot \overline{g},$$
$$e \cdot \overline{g} = \overline{g} \cdot e = \overline{g}.$$

3) **Действие G на себе сопряжениями.**

По определению $g \cdot \overline{g} = g\overline{g}g^{-1}$. Проверим, что это действие.

$$g_1 \cdot (g_2 \cdot \overline{g}) = g_1 \cdot (g_2 \overline{g} g_2^{-1}) = g_1 g_2 \overline{g} g_2^{-1} g_1^{-1} = (g_1 g_2) \overline{g} (g_1 g_2)^{-1} = (g_1 g_2) \cdot \overline{g}.$$
$$e \cdot \overline{g} = e\overline{g}e^{-1} = \overline{g}.$$

Замечание 12. Заметим, что нельзя определить правое действие (действие правыми сдвигами) таким образом $g \cdot \overline{g} = \overline{g} g$, так как при этом

$$g_1 \cdot (g_2 \cdot \overline{g}) = g_1 \cdot (\overline{g} g_2) = \overline{g} g_2 g_1, \qquad (g_1 g_2) \cdot \overline{g} = \overline{g} g_1 g_2.$$

Если группа G не коммутативная, то найдутся два элемента g_1 и g_2 такие, что

$$\overline{g} g_2 g_1 \neq \overline{g} g_1 g_2.$$

Заметим, что при фиксированном $g \in G$ отображение $\alpha_g \colon X \to X$, $\alpha_g(x) = \alpha(g, x)$ является биекцией. В самом деле, легко убедиться, что $\alpha_g \circ \alpha_h = \alpha_{gh}$, при этом $\alpha_e = \mathrm{id}$. Это означает, что $\alpha_{g^{-1}}$ – обратное отображение к α_g. Таким образом, мы получаем гомоморфизм φ_α из G в $S(X)$. Напомним, что $S(X)$ – это группа биекций $X \to X$. Гомоморфизм φ_α определяется следующим образом: $\varphi_\alpha(g) = \alpha_g$.

Наоборот, если дан гомоморфизм $\varphi \colon G \to S(X)$, то можно определить действие α_φ группы G на X следующим образом: $g \cdot x = \varphi(g)(x)$.

Лемма 21. *Отображения $\Phi \colon \alpha \mapsto \varphi_\alpha$ и $\Psi \colon \varphi \mapsto \alpha_\varphi$ являются взаимно обратными и, следовательно, устанавливают биекцию между действиями G на X и гомоморфизмами из G в $S(X)$.*

Доказательство. Пусть β – некоторое действие G на X. Имеем $\Psi \circ \Phi(\beta) = \Psi(\varphi_\beta)$. По определению, это действие устроено по правилу $g \cdot x = \varphi_\beta(g)(x)$. С другой стороны по определению $\varphi_\beta(g) = \beta_g$, то есть $\varphi_\beta(g)(x) = \beta_g(x) = \beta(g, x)$. Таким образом $\Psi \circ \Phi(\beta) = \beta$, то есть $\Psi \circ \Phi = \mathrm{id}$.

Пусть теперь $\varphi\colon G \to S(X)$ – гомоморфизм. Тогда $\Phi \circ \Psi(\varphi) = \Phi(\alpha_\varphi)$. По определению Φ имеем $\Phi(\alpha_\varphi)(g)(x) = \alpha_\varphi(g, x) = \varphi(g)(x)$. Так как это верно для любого x и для любого g имеем $\Phi \circ \Psi(\varphi) = \varphi$, то есть $\Phi \circ \Psi = \mathrm{id}$. □

Следующие два определения играют центральную роль в теории действий.

Определение 34. Пусть G действует на X и $x \in X$. Орбитой элемента x называется множество $Gx = \{g \cdot x \mid g \in G\} \subset X$.

Определение 35. Пусть G действует на X и $x \in X$. Стабилизатором элемента x называется множество $\mathrm{St}(x) = G_x = \{g \in G \mid g \cdot x = x\}$.

Лемма 22. *Орбиты – это классы эквивалентности, и следовательно, орбиты либо не пересекаются, либо совпадают.*

Доказательство. Докажем, что отношение "$x \sim y$ если x лежит в орбите Gy"является отношением эквивалентности.

1) Рефлексивность. $x \sim x$ так как $e \cdot x = x$, а значит, $x \in Gx$.

2) Симметричность. Если $x \sim y$, то найдется $g \in G$ такое, что $g \cdot y = x$. Значит, $g^{-1} \cdot x = y$, то есть $y \sim x$.

3) Транзитивность. Пусть $x \sim y$ и $y \sim z$. Тогда $x = g \cdot y$, $y = \overline{g} \cdot z$. Тогда $x = (g\overline{g}) \cdot z$. Следовательно, $x \sim z$. □

Лемма 23. *Стабилизатор* $\mathrm{St}(x)$ *является подгруппой в* G.

Доказательство. Пусть $g, h \in \mathrm{St}(x)$. Тогда $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, то есть $gh \in \mathrm{St}(x)$, а значит, множество $\mathrm{St}(x)$ замкнуто относительно умножения.

Если $g \in \mathrm{St}(x)$, то $g \cdot x = x$. Подействуем на обе части этого равенства элементом g^{-1}. Получим $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$. Но $g^{-1} \cdot (g \cdot x) = e \cdot x = x$. Значит, $g^{-1} \in \mathrm{St}(x)$, то есть $\mathrm{St}(x)$ замкнут относительно взятия обратного.

Осталось заметить, что единица группы лежит в стабилизаторе любого элемента. □

Пусть G группа и H – ее подгруппа. Пусть $g \in G$. Через gHg^{-1} мы обозначаем множество $\{ghg^{-1} \mid h \in H\}$. Отображение $h \mapsto ghg^{-1}$ устанавливает изоморфизм (биекцию, переводящую умножение в умножение) между H и gHg^{-1}. Следовательно, gHg^{-1} – подгруппа, изоморфная H. Эта подгруппа называется подгруппой, сопряженной к H.

Лемма 24. *Пусть* $y = g \cdot x$. *Тогда* $\mathrm{St}(y) = g\mathrm{St}(x)g^{-1}$. *(Стабилизаторы элементов одной орбиты сопряжены.)*

Доказательство. Докажем, что $\mathrm{St}(y) \supseteq g\mathrm{St}(x)g^{-1}$. Пусть $h \in \mathrm{St}(x)$. Тогда

$$(ghg^{-1}) \cdot y = (ghg^{-1}) \cdot (g \cdot x) = g \cdot (h \cdot x) = g \cdot x = y.$$

Но аналогично, так как $x = g^{-1} \cdot y$, имеем $\mathrm{St}(x) \supseteq g^{-1}\mathrm{St}(y)g$. А значит,

$$g\mathrm{St}(x)g^{-1} \supseteq \mathrm{St}(y).$$

Так как доказаны включения в обе стороны, получаем $\mathrm{St}(y) = g\mathrm{St}(x)g^{-1}$. □

Следствие 8. *Если группа* G *абелева, то стабилизаторы элементов в одной орбите совпадают.*

Теорема 16. *Существует биекция между множеством левых смежных классов группы* G *по подгруппе* $\mathrm{St}(x)$ *и элементами орбиты* Gx.

Доказательство. Определим отображение ψ, которое сопоставляет смежному классу $g\mathrm{St}(x)$ элемент орбиты $g \cdot x$. Прежде всего нужно проверить корректность этого отображения, то есть что если $g\mathrm{St}(x) = h\mathrm{St}(x)$, то $g \cdot x = h \cdot x$. В самом деле $g\mathrm{St}(x) = h\mathrm{St}(x)$ тогда и только тогда, когда $h^{-1}g \in \mathrm{St}(x)$, то есть $g = hs$, где $s \in \mathrm{St}(x)$. Получаем $g \cdot x = h \cdot (s \cdot x) = h \cdot x$. Итак, ψ определено корректно.

Пусть $\psi(g\mathrm{St}(x)) = \psi(h\mathrm{St}(x))$, тогда $g \cdot x = h \cdot x$. Подействуем на последнее равенство элементом h^{-1}. Получим $(h^{-1}g) \cdot x = x$, то есть $h^{-1}g \in \mathrm{St}(x)$. Тогда $g\mathrm{St}(x) = h\mathrm{St}(x)$, то есть ψ – инъекция.

То, что ψ сюръективно следует из того, что в элемент орбиты $g \cdot x$ переходит смежный класс $g\mathrm{St}(x)$. □

Следствие 9. *Пусть G – конечная группа. Тогда $|G| = |Gx| \cdot |\mathrm{St}(x)|$.*

С помощью только что доказанной формулы посчитаем количество элементов в группе вращений куба $\mathrm{Sym}_+(K)$. Данная группа состоит из всех движений $\mathbb{R}^3$, сохраняющих ориентацию. (Так как центр куба остается неподвижен, то движение, сохраняющее куб является линейным преобразованием. Ориентацию сохраняют те движения, определитель которых равен 1.)

Предложение 10. *Порядок группы $\mathrm{Sym}_+(K)$ равен 24.*

Доказательство. Рассмотрим куб K с вершинами $ABCDA'B'C'D'$. Есть естественное действие $\mathrm{Sym}_+(K)$ на множестве $\{A, B, C, D, A'B'C'D'\}$. В группе $\mathrm{Sym}_+(K)$ содержится вращение относительно оси, соединяющей две противоположные грани. С помощью композиции таких вращений можно перевести любую вершину в любую другую. Значит, орбита точки A состоит из 8 точек. По следствию 9 получаем

$$|\mathrm{Sym}_+(K)| = |\mathrm{Sym}_+(K)A| \cdot |\mathrm{St}(A)| = 8 \cdot |\mathrm{St}(A)|.$$

Осталось найти $|H|$, где $H = \mathrm{St}(A)$. Пусть вершины, смежные с A – это B, D и A'. Получаем естественное действие H на множестве $\{B, D, A'\}$. Легко видеть, что в группе H лежат вращения относительно диагонали AC' на углы $\frac{2\pi}{3}$ и $\frac{4\pi}{3}$. Они переводят B в D и A' соответственно. Значит, действие H на $\{B, C, D\}$ имеет единственную орбиту $|HB| = 3$. При этом по следствию 9 получаем

$$|H| = |HB| \cdot |\mathrm{St}_H(B)| = 3|\mathrm{St}_H(B)|.$$

(Здесь мы используем индекс в $\mathrm{St}_H(B)$, чтобы подчеркнуть, что это стабилизатор при действии группы H, а не при действии группы G.) Осталось найти $|\mathrm{St}_H(B)|$. Пусть $\xi \in |\mathrm{St}_H(B)$. Тогда $\psi(A) = A$, $\psi(B) = B$. Поскольку смежные с A вершины – это B, D и A', получаем, что либо $\psi(D) = D$ и $\psi(A') = A'$, либо $\psi(D) = A'$ и $\psi(A') = D$. Но если $\psi(D) = A'$ и $\psi(A') = D$, то ψ меняет ориентацию. Следовательно, $\psi(A) = A$, $\psi(B) = B$, $\psi(D) = D$ и $\psi(A') = A'$. То есть ψ сохраняет 4 точки не лежащие в одной плоскости. Значит, $\psi = \mathrm{id}$. Следовательно, $|\mathrm{St}_H(B)| = 1$. Таким образом

$$|\mathrm{Sym}_+(K)| = 8 \cdot |\mathrm{St}(A)| = 24 \cdot |\mathrm{St}_H(B)| = 24.$$

□