

ЛЕКЦИЯ 1

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

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

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

Рассмотрим бинарную операцию $*$ на множестве G :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Соберем эти обозначения в таблице.

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

Определение 4. Порядок группы G – это количество элементов в этой группе. (То есть мощность множества G .) Порядок группы G обозначается $|G|$.

Определение 5. Подмножество H группы $(G, *)$ называется *подгруппой*, если $(H, *)$ является группой.

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

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

Доказательство. Если $(H, *)$ – группа, то операция $*$ корректно определена на H . Значит, H замкнуто относительно операции $*$. Пусть e – нейтральный элемент группы G , а s – нейтральный элемент группы H . Получаем $s * s = s$. В группе G есть обратный к s элемент s^{-1} . Умножая на него слева предыдущее равенство, получаем $s = e$. То есть единицы у групп G и H совпадают. Для каждого $g \in H$ есть обратный элемент g^{-1} в группе G и есть обратный элемент $g^\vee$ в группе H . Тогда $g * g^{-1} = e = g * g^\vee$. Умножив слева на g^{-1} , получаем $g^{-1} = g^\vee$. Поскольку для группы $(H, *)$ выполнена аксиома A3, то H замкнуто относительно взятия обратного.

Пусть теперь подмножество H замкнуто относительно операции и взятия обратного. Так как H замкнуто относительно операции, $(H, *)$ – группоид. Поскольку ассоциативность выполнена в G , то она выполнена и в H . Подмножество не пусто. Возьмем элемент $h \in H$. Так как H замкнуто относительно взятия обратного, $h^{-1} \in H$. Пользуясь замкнутостью H относительно операции, получаем $h * h^{-1} = e \in H$. Таким образом, в H выполнена аксиома A2. Поскольку H замкнуто относительно взятия обратного, в H выполнена и аксиома A3. $\square$

Примеры групп.

1а) 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.

1б) 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.

Обобщение примера 1б) 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 1. Приведите пример некоммутативного кольца R такого, что $R^\times$ – коммутативная группа порядка больше 1.

2) 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 1. Пусть есть четыре множества: X, Y, Z и W . И пусть фиксированы отображения между этими множествами $\varphi: X \rightarrow Y, \psi: Y \rightarrow Z$ и $\zeta: Z \rightarrow W$. 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 $X = Y = Z = W = \{1, 2, \dots, n\}$ получаем ассоциативность S_n . Порядок группы S_n равен $n!$. При $n > 3$ группа S_n не коммутативна.

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

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

г) (Обобщение примера б) Пусть X – некоторое множество (возможно бесконечное). Рассмотрим множество $S(X)$ биекций $X \rightarrow X$ с операцией композиции. Если $|X| < \infty$, то получаем группу перестановок. В общем случае получаем *группу симметрий множества X* . Нейтральный элемент – тождественное преобразование. Обратный – обратное преобразование. Ассоциативность следует из леммы 1.

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

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

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

в) $O_n(\mathbb{K})$ – множество ортогональных матриц $n \times n$ с элементами из $\mathbb{K}$. Это подмножество в $GL(\mathbb{K})$ замкнуто относительно умножения и взятия обратного. Следовательно, это подгруппа.

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

4) 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.

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

Упражнение 1. 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 четно, то половина симметрий проходит через 2 вершины, а половина – через две середины противоположных сторон. Если же n нечетно, 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.

5) 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 .

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

7) Группа кватернионов Q_8 . Рассмотрим множество из 8 элементов:

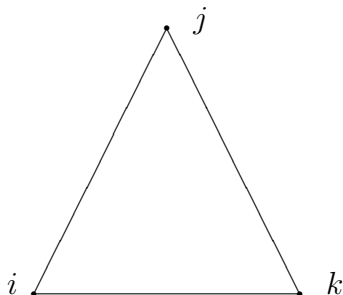
$$\{1, -1, i, -i, j, -j, k, -k\}.$$

Умножение устроено следующим образом: знаки умножаются отдельно,

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

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

Для того, чтобы запомнить правило умножения элементов i, j и k удобно изобразить их в вершинах треугольника.



Теперь, если мы хотим умножить два элемента, то, если направление движения от первого ко второму по часовой стрелке, получаем третий элемент, а если против часовой стрелки, то минус третий.

Легко видеть, что 1 – нейтральный элемент, и каждый элемент обратим. В самом деле, элементы 1 и -1 являются обратными к самим себе. А для любого другого элемента x выполнено $x^{-1} = -x$. Для того, чтобы утверждать, что Q_8 – группа, необходимо проверить ассоциативность. Сделаем это на следующей лекции.

ЛЕКЦИЯ 2

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

Пример 1. Построим таблицу сложения для группы $(\mathbb{Z}_3, +) = \{0, 1\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Ясно, что таблица Кэли симметрична (относительно главной диагонали) тогда и только тогда, когда группа коммутативна.

Определение 6. Пусть $(G, *)$ и $(H, \circ)$ – две группы. Отображение $\varphi: G \rightarrow H$ называется *гомоморфизмом*, если $\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2)$.

На самом деле, чтобы определить гомоморфизм нам не нужно, чтобы G и H были группами. Достаточно, чтобы на них были заданы некие операции (т.е., чтобы они были группоидами).

Докажем следующие элементарные свойства гомоморфизма.

Лемма 2. Пусть $\varphi: (G, *) \rightarrow (H, \circ)$ – гомоморфизм. Обозначим через e_G и e_H единицы группы G и H соответственно. Тогда

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

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

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

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

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

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

Задача 2. Пусть $(G, *)$ и $(H, \circ)$ – моноиды с единицами e_G и e_H соответственно. И пусть $\psi: G \rightarrow H$ – отображение такое, что $\psi(g_1 * g_2) = \psi(g_1) \circ \psi(g_2)$. Может ли так быть, что $\psi(e_G) \neq \psi(e_H)$?

Определение 7. Биективный гомоморфизм $\varphi: G \rightarrow H$ называется *изоморфизмом*, а группы G и H при наличии изоморфизма между ними называются *изоморфными*.

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.

Теорема 1. *Отношение изоморфности – это отношение эквивалентности.*

Доказательство. Нужно проверить, что отношение изоморфности удовлетворяет свойствам рефлексивности, симметричности и транзитивности. В самом деле. Тожественное преобразование задает изоморфизм любой группы с собой. Рефлексивность доказана. Если $\varphi: G \rightarrow H$ – изоморфизм, то в частности это биекция. Тогда существует обратное отображение φ^{-1} . Оно также является гомоморфизмом. В самом деле, пусть $a, b \in H$, в силу сюръективности φ , имеем $a = \varphi(u)$, $b = \varphi(v)$ для некоторых $u, v \in G$. Тогда $\varphi^{-1}(ab) = \varphi^{-1}(\varphi(u)\varphi(v)) = \varphi^{-1}(\varphi(uv)) = uv = \varphi^{-1}(a)\varphi^{-1}(b)$. Таким образом, φ^{-1} – изоморфизм. Симметричность доказана. Докажем, что композиция двух изоморфизмов – изоморфизм. Пусть $\varphi: G \rightarrow H$ и $\psi: H \rightarrow F$ – два гомоморфизма. Тогда

$$\psi \circ \varphi(g_1 g_2) = \psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\psi(\varphi(g_2)) = \psi \circ \varphi(g_1)\psi \circ \varphi(g_2).$$

То есть $\psi \circ \varphi$ – гомоморфизм. С другой стороны, $\psi \circ \varphi$ – биекция. Значит, $\psi \circ \varphi$ – изоморфизм. Транзитивность доказана. $\square$

Из этого предложения следует, что все группы распадаются на непересекающиеся классы изоморфности.

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

Пример 3. Группа $\mathbb{Z}_n$ изоморфна группе μ_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 $GL_n(\mathbb{C})$ 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.

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.

Теорема 2. Пусть G – группа, а H – группоид. И пусть $\varphi: G \rightarrow H$ – биекция и гомоморфизм (то есть $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$). (Можно сказать, что φ – изоморфизм группоидов.) Тогда H – также группа и φ – изоморфизм групп.

Доказательство. Докажем, что H – группа. Проверим ассоциативность. Пусть $h_1, h_2, h_3 \in H$. Обозначим $g_i = \varphi^{-1}(h_i)$, $i = 1, 2, 3$. Тогда

$$\begin{aligned} h_1(h_2 h_3) &= \varphi(g_1)(\varphi(g_2)\varphi(g_3)) = \varphi(g_1)\varphi(g_2 g_3) = \\ &= \varphi(g_1(g_2 g_3)) = \varphi((g_1 g_2)g_3) = \varphi(g_1 g_2)\varphi(g_3) = (\varphi(g_1)\varphi(g_2))\varphi(g_3) = (h_1 h_2)h_3. \end{aligned}$$

Проверим, что $l = \varphi(e)$ – нейтральный элемент. Действительно, пусть $h = \varphi(g)$. Тогда $hl = \varphi(g)\varphi(e) = \varphi(ge) = \varphi(g) = h$ и $lh = \varphi(e)\varphi(g) = \varphi(eg) = \varphi(g) = h$.

Теперь проверим наличие обратного к элементу $h = \varphi(g)$. Докажем, что это $f = \varphi(g^{-1})$. Действительно, $hf = \varphi(g)\varphi(g^{-1}) = \varphi(e) = l$ и $fh = \varphi(g^{-1})\varphi(g) = \varphi(e) = l$.

Итак, мы проверили, что H – группа. Таким образом φ – биективный гомоморфизм групп, то есть изоморфизм. $\square$

Теперь мы готовы доказать, что Q_8 – группа.

Предложение 2. Q_8 – группа

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

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

Здесь i – это мнимая единица (комплексное число).

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

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

Легко убедиться, что φ переводит умножение в Q_8 в матричное умножение. Следовательно, $(\overline{Q}_8, \cdot)$ – это замкнутое относительно умножения и взятия обратной матрицы подмножество в $GL_2(\mathbb{C})$. Значит, $\overline{Q}_8$ – подгруппа. Тогда, по теореме 2, Q_8 – группа, изоморфная $\overline{Q}_8$. $\square$

Особый интерес представляют гомоморфизмы и изоморфизмы из группы в себя.

Определение 8. Гомоморфизм $\varphi: G \rightarrow G$ называется *эндоморфизмом*. Изоморфизм $\varphi: G \rightarrow G$ называется *автоморфизмом*.

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

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

Лемма 3. 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 $\varphi_{g^{-1}}$. $\square$

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

Предложение 3. Множество внутренних автоморфизмов с операцией композиции образует подгруппу $\text{Inn}(G)$ в $\text{Aut}(G)$.

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 замкнутость $\text{Inn}(G)$ относительно композиции. Кроме того $\text{id} = \varphi_e \in \text{Inn}(G)$. Осталось проверить, что $\text{Inn}(G)$ замкнуто относительно взятия обратного. Для этого заметим, что $\varphi_g \circ \varphi_{g^{-1}} = \varphi_e = \text{id}$. $\square$

ЛЕКЦИЯ 3

Предложение 4. Простые следствия из аксиом.

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

2) В моноиде есть единственная единица.

3) В группе для каждого элемента есть единственный обратный.

4) Пусть $(G, *)$ – группа. Пусть $a, b \in G$. Тогда если $a * b = e$, то $b = a^{-1}$. Аналогично если $b * a = e$, то $b = a^{-1}$.

5) Пусть $(G, *)$ – группа, $a, b \in G$. Тогда $(a * b)^{-1} = b^{-1} * a^{-1}$.

6) Пусть $(G, *)$ – группа, $g \in G$. Тогда $(g^{-1})^{-1} = g$.

Доказательство. 1) Докажем это утверждение индукцией по k .

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

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

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

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 дает операцию от двух скобок. Длинной скобки назовем количество g_i , входящих в нее. Обозначим длину правой скобки через s .

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

Случай 2 $s > 2$. Последнее действие при нашей фиксированной расстановке скобок имеет вид $(a) * (b)$. Длина скобки b меньше n . По предположению индукции можно считать, что в скобке b расстановка скобок стандартная. Таким образом, стандартная расстановка скобок в скобке b дает $b = d * g_n$. То есть $g = a * (d * g_n) = (a * d) * g_n$. По случаю 1 мы получаем, что в g можно расставить скобки стандартным образом.

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 $g = (g^{-1})^{-1}$. $\square$

Теорема 3. 1) $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$,

2) $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$.

Замечание 1. 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 $\psi: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ имеет вид

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

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

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

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

Определение 9. Пусть $\varphi: G \rightarrow H$ – гомоморфизм групп. Ядром гомоморфизма φ называется множество

$$\text{Ker } \varphi = \{g \in G \mid \varphi(g) = e\} \subseteq G.$$

Образом гомоморфизма φ называется множество

$$\text{Im } \varphi = \{\varphi(g) \mid g \in G\} \subseteq H.$$

Поскольку $\varphi(e) = e$, нейтральный элемент всегда лежит в ядре.

Лемма 4. Пусть $\varphi: G \rightarrow H$ – гомоморфизм. Тогда

а) $\text{Ker } \varphi$ – подгруппа в G ,

б) $\text{Im } \varphi$ – подгруппа в H .

Доказательство. а) Пусть $g_1, g_2 \in \text{Ker } \varphi$. Тогда $\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) = ee = e$. Значит, $g_1 g_2 \in \text{Ker } \varphi$. То есть ядро замкнуто относительно операции. Кроме того $\varphi(g_1^{-1}) = \varphi(g_1^{-1}) \varphi(g_1) = \varphi(g_1^{-1} g_1) = \varphi(e) = e$. Значит, $g_1^{-1} \in \text{Ker } \varphi$. Таким образом, ядро замкнуто относительно взятия обратного. Осталось заметить, что $e \in \text{Ker } \varphi$. Следовательно, $\text{Ker } \varphi$ – подгруппа в G .

б) Пусть $h_1, h_2 \in \text{Im } \varphi$. Тогда найдутся $g_1, g_2 \in G$ такие, что $h_1 = \varphi(g_1)$, $h_2 = \varphi(g_2)$. Тогда $h_1 h_2 = \varphi(g_1 g_2) \in \text{Im } \varphi$ и $h_1^{-1} = \varphi(g_1^{-1}) \in \text{Im } \varphi$. Кроме того $e = \varphi(e) \in \text{Im } \varphi$. То есть образ замкнут относительно операции, взятия обратного и содержит единицу. Следовательно, $\text{Im } \varphi$ – подгруппа в H . $\square$

Теорема 4. (Критерий инъективности гомоморфизма) Гомоморфизм $\varphi: G \rightarrow H$ инъективен тогда и только тогда, когда $\text{Ker } \varphi = \{e\}$.

Доказательство. Пусть $\text{Ker } \varphi \neq \{e\}$. Тогда существует $g \neq e$, $g \in \text{Ker } \varphi$. То есть $\varphi(g) = e = \varphi(e)$. Следовательно, гомоморфизм φ не инъективен.

Допустим, гомоморфизм φ не инъективен. Тогда $\varphi(g_1) = \varphi(g_2)$ для некоторых $g_1 \neq g_2 \in G$. Значит, $\varphi(g_1 g_2^{-1}) = \varphi(g_1) \varphi(g_2)^{-1} = e$. То есть $g_1 g_2^{-1} \in \text{Ker } \varphi$, но $g_1 g_2^{-1} \neq e$. Значит, $\text{Ker } \varphi \neq \{e\}$. $\square$

Определение 10. Пусть g – элемент группы G , а n – целое число. Определим n -ю степень элемента g следующим образом. Если n положительное, то $g^n = g \cdot \dots \cdot g$ – произведение n элементов g . Если n отрицательное, то $g^n = (g^{-1})^n$. Нулевая степень любого элемента равна нейтральному элементу e .

Упражнение 2. Выполнены следующие свойства степеней элемента группы:

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

Указание. Рассмотреть все случаи знаков m и n .

Определение 11. Пусть g – элемент группы G . Порядок g – это минимальное натуральное число n такое, что $g^n = e$. Если такого числа не существует, то порядок элемента g равен бесконечности. Порядок элемента g обозначается $\text{ord}(g)$.

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

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

Замечание 2. 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 $\mathbb{Z}_n = \langle 1 \rangle$.

ЛЕКЦИЯ 4

Лемма 5. Циклическая группа $\langle g \rangle$ изоморфна

- $\mathbb{Z}_n$ при условии $\text{ord } g = n$;
- $\mathbb{Z}$ при условии $\text{ord } g = \infty$.

Доказательство. Пусть $\text{ord } g = n$. 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 $0 \leq r < n$. 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 $\text{ord}(g) = n$.

Рассмотрим отображение $\psi: \mathbb{Z}_n \rightarrow \langle g \rangle$, $\psi(k) = g^k$. Элементы $\mathbb{Z}_n$ – это не числа, а классы чисел с одинаковым остатком. Поэтому нам надо доказать, что отображение ψ определено корректно. А именно, пусть $k' = mn + k$ для некоторого $m \in \mathbb{Z}$. Тогда $\psi(k') = g^{k'} = (g^n)^m g^k = g^k = \psi(k)$. Корректность доказана. Теперь проверим, что ψ – гомоморфизм. Действительно, $\psi(k + l) = g^{k+l} = g^k g^l = \psi(k)\psi(l)$. Заметим, что $\mathbb{Z}_n$ состоит из классов чисел $0, 1, \dots, n-1$. При отображении ψ эти классы переходят в элементы множества S . Причем это отображение очевидно сюръективно и инъективно так как элементы S не совпадают. Итак, ψ – гомоморфизм и биекция, то есть изоморфизм.

Пусть теперь $\text{ord } g = \infty$. Рассмотрим отображение $\psi: \mathbb{Z} \rightarrow \langle g \rangle$, $\psi(k) = g^k$. Как и в прошлом случае получим, что ψ – гомоморфизм. (В этом случае проверять корректность не нужно, так как элементы $\mathbb{Z}$ – числа, а не классы чисел.) Сюръективность ψ следует из определения циклической группы. Докажем инъективность. Предположим, что $g^a = g^b$, где $a > b$. Домножим это равенство на g^{-b} и получим $g^{a-b} = e$, что противоречит тому, что $\text{ord } g = \infty$. Итак, ψ – гомоморфизм и биекция, то есть изоморфизм. $\square$

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

Замечание 3. Для каждого элемента g некоторой группы G можно рассмотреть циклическую подгруппу, порожденную этим элементом: $\langle g \rangle \subset G$.

Лемма 6. Пусть g – элемент группы G такой, что $\text{ord } g = n$, а m – целое число. Тогда

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

Доказательство. Докажем это утверждение только для положительных m , так как $\text{ord}(g^{-m}) = \text{ord}((g^m)^{-1}) = \text{ord}(g^m)$, а также $\text{ord}(g^0) = 1$.

Рассмотрим группу $\langle g \rangle$. По предыдущей лемме она изоморфна $\mathbb{Z}_n$. Более того при построенном изоморфизме этих групп элемент g соответствует $1 \in \mathbb{Z}_n$, и элемент g^m соответствует $m \in \mathbb{Z}_n$. Таким образом, нам нужно доказать, что порядок $m \in \mathbb{Z}_n$ равен $\frac{n}{\text{НОД}(m, n)} = \frac{\text{НОК}(m, n)}{m}$. Порядок – это такая минимальная натуральная степень k , в которой элемент равен e . В аддитивных обозначениях получаем $\text{ord}(m) = k$, если k – это минимальное натуральное число такое, что $mk = 0$ в $\mathbb{Z}_n$. Для целых чисел условие переписывается как mk делится на n . Получается, что mk – общее кратное m и n . Таким образом, $k \geq \frac{\text{НОК}(m, n)}{m}$. С другой стороны $k = \frac{\text{НОК}(m, n)}{m}$ подходит, так как $mk = \frac{\text{НОК}(m, n)}{m} m = \text{НОК}(m, n)$ делится на n . $\square$

Теорема 5. 1) Подгруппа циклической группы циклическая;

2) Все подгруппы $\mathbb{Z}$ имеют вид $\langle k \rangle = k\mathbb{Z} \cong \mathbb{Z}$;

3) Все подгруппы $\mathbb{Z}_n$ имеют вид $\langle d \rangle = d\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{d}}$ для некоторого d – делителя n ;

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

Доказательство. 1) Следует из пунктов 2) и 3).

2) Пусть H – подгруппа в $\mathbb{Z}$. Если $H = \{0\}$, то $H = \langle 0 \rangle$, что укладывается в утверждение задачи. Пусть $H \neq \{0\}$. Если $h \in H$ – отрицательное число, то положительное число $-h$ также лежит в H . Значит, в H есть натуральные числа. Выберем k – минимальное натуральное число из H . Пусть $h \in H$. Тогда $h = kq + r$, где $0 \leq r < k$. При этом $kq \in H$, $h \in H$, следовательно, $r \in H$. Если $r \neq 0$, получаем противоречие с выбором k . Значит, $r = 0$ и h делится на k . Отсюда $H = \langle k \rangle$.

3) Пусть H – подгруппа в $\mathbb{Z}_n$. Если $H = \{0\}$, то $H = \langle n \rangle$, что укладывается в утверждение задачи. Пусть $H \neq \{0\}$. Рассмотрим минимальное натуральное число d такое, что его класс лежит в H . Ясно, что $d < n$. Пусть $h \in H$. Тогда $h = dq + r$, где $0 \leq r < d$. При этом $dq \in H$, $h \in H$, следовательно, $r \in H$. Если $r \neq 0$, получаем противоречие с выбором d . Значит, $r = 0$ и h делится на d . Отсюда $H = \langle d \rangle$. Докажем, что d – делитель n . Если это не так, то $n = kd + s$, $0 < s < d$. Но тогда в $\mathbb{Z}_n$ выполнено $s = kd \in H$, противоречие с выбором d . Итак, d – делитель n . Осталось сказать, что порядок d в группе $\mathbb{Z}_n$ равен $\frac{n}{d}$. Значит, $H = \langle d \rangle \cong \mathbb{Z}_{\frac{n}{d}}$.

4) $\langle m \rangle$ – циклическая группа. По лемме 6, $\text{ord}(m) = \frac{n}{\text{НОД}(m,n)}$. Значит $|\langle m \rangle| = \frac{n}{\text{НОД}(m,n)}$. Следовательно, по пункту 3), $\langle m \rangle = \langle \text{НОД}(m,n) \rangle$. $\square$

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

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

Правым смежным классом элемента g по подгруппе H называется множество

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

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

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

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

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

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

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

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

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

Симметричность:

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

Транзитивность:

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

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

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

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

Задача 3. Докажите, что $gH \leftrightarrow Hg^{-1}$ – биекция между левыми и правыми смежными классами, и следовательно мощность правых смежных классов также равна индексу подгруппы. (То, что количество левых и правых смежных классов одинаково для конечной группы будет следовать из теоремы Лагранжа, но это верно и для бесконечных групп.)

ЛЕКЦИЯ 5

Теорема 6. (Лагранж) Пусть G – конечная группа и H – подгруппа G . Тогда

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

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

Следствие 1. (Следствия из теоремы Лагранжа)

- 1) Порядок конечной группы делится на порядок ее подгруппы.
- 2) Порядок конечной группы делится на порядок ее элемента.
- 3) Для любого элемента g конечной группы G выполнено $g^{|G|} = e$.
- 4) Группа простого порядка циклическая.
- 5) (Теорема Эйлера) Пусть m и n – взаимно простые натуральные числа. Тогда $n^{\varphi(m)}$ имеет остаток 1 при делении на m .

Доказательство. 1) Очевидно следует из теоремы Лагранжа.

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

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

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

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

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

$\square$

Задача 4. Приведите пример конечной группы и делителя ее порядка такого, что в группе нет подгруппы такого порядка.

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 $gHg^{-1} \subseteq H$,

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

$2 \implies 3$ Очевидно.

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

Пример 6. Любая подгруппа в абелевой группе нормальна, так как $ghg^{-1} = h$.

Пример 7. $SL_n(\mathbb{C})$ – нормальная подгруппа в $GL_n(\mathbb{C})$. Действительно, пусть $A \in GL_n(\mathbb{C})$, $B \in SL_n(\mathbb{C})$. Тогда $\det(ABA^{-1}) = \det A \det B (\det A)^{-1} = 1$. То есть $ABA^{-1} \in SL_n(\mathbb{C})$.

Пример 8. Подгруппа $\langle (1, 2) \rangle = \{\text{id}, (1, 2)\} \subseteq S_3$ не является нормальной. В самом деле,

$$(1, 2, 3)(1, 2)(1, 2, 3)^{-1} = (1, 2, 3)(1, 2)(1, 3, 2) = (2, 3) \notin \langle (1, 2) \rangle.$$

Упражнение 3. Найдите явно разбиение группы S_3 на левые и правые смежные классы по подгруппе $\langle (1, 2) \rangle$.

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 $g_1H = g'_1H$, $g_2H = g'_2H$, но при этом смежный класс g_1g_2H может не совпадать с $g'_1g'_2H$. Тогда умножение называется некорректным.

Предложение 5. 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 $g_1H = g'_1H$, $g_2H = g'_2H$. 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. $\square$

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 $|G/H| = \frac{|G|}{|H|}$.

Пример 9. Найдём, чему изоморфна факторгруппа $\mathbb{Z}/n\mathbb{Z}$. Подгруппа $n\mathbb{Z}$ нормальна, так как группа $\mathbb{Z}$ абелева. Смежные классы имеют вид $k+n\mathbb{Z}$. При этом $k+n\mathbb{Z} = l+n\mathbb{Z}$ тогда и только тогда, когда k и l имеют одинаковые остатки при делении на n . Сопоставим смежному классу $k+n\mathbb{Z}$ остаток при делении k на n . Докажем, что это сопоставление – это изоморфизм ψ между $\mathbb{Z}/n\mathbb{Z}$ и $\mathbb{Z}_n$. Действительно, сложению смежных классов соответствует сложение остатков. Кроме того ψ сюръективно, так как любой остаток – это остаток некоторого числа k , а значит, он равен $\psi(k+n\mathbb{Z})$. Для проверки инъективности ψ , воспользуемся критерием инъективности. Ядро ψ – это то, что переходит в остаток ноль, то есть смежный класс $n\mathbb{Z}$, который является нейтральным элементом фактор-группы.

Пусть $\varphi: G \rightarrow \tilde{G}$ – гомоморфизм групп.

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

2) Образ $\text{Im } \varphi$ – подгруппа в группе $\tilde{G}$.

Доказательство. Все, кроме нормальности ядра уже было доказано в лемме 4. Докажем, что подгруппа $\text{Ker } \varphi \subseteq G$ нормальна. Пусть $g \in G$, $h \in \text{Ker } \varphi$. Тогда

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

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

Определение 17. Рассмотрим следующее отображение $\pi_H: G \rightarrow G/H$, $g \mapsto gH$. 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 7. (Теорема о гомоморфизме) Пусть $\varphi: G \rightarrow \tilde{G}$ – гомоморфизм групп. Тогда $G/\text{Ker } \varphi \cong \text{Im } \varphi$.

Доказательство. Рассмотрим отображение

$$\Psi: G/\text{Ker } \varphi \rightarrow \text{Im } \varphi, \quad \Psi(g\text{Ker } \varphi) = \varphi(g).$$

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 $g\text{Ker } \varphi = g'\text{Ker } \varphi$, то $g'^{-1}g = h \in \text{Ker } \varphi$. Тогда $g = g'h$. Получаем $\varphi(g) = \varphi(g'h) = \varphi(g')\varphi(h) = \varphi(g')e = \varphi(g')$. Таким образом, отображение Ψ определено корректно.

Докажем, что Ψ – изоморфизм. То, что Ψ – гомоморфизм следует из равенства:

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

Инъективность Ψ проверим по критерию инъективности. Если $g\text{Ker } \varphi \in \text{Ker } \Psi$, то $\Psi(g\text{Ker } \varphi) = \varphi(g) = e$. Значит, $g \in \text{Ker } \varphi$. То есть $g\text{Ker } \varphi = \text{Ker } \varphi$ – единица факторгруппы. Сюръективность Ψ очевидна, так как для любого элемента $\varphi(g)$ в $\text{Im } \varphi$ в него отображается смежный класс $g\text{Ker } \varphi$. $\square$

Следствие 2. Если $|G| < \infty$ и $\varphi: G \rightarrow \tilde{G}$ – гомоморфизм, то

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

Пример 10. Найдём, чему изоморфна факторгруппа $\mathbb{Z}/n\mathbb{Z}$ по теореме о гомоморфизме. Для того, чтобы применить теорему о гомоморфизме, нам нужно построить гомоморфизм $\varphi: \mathbb{Z} \rightarrow G'$ для некоторой группы G' такой, что $\text{Ker } \varphi = n\mathbb{Z}$. Легко видеть, что подходит следующий гомоморфизм

$$\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_n, \quad k \mapsto k \pmod{n}$$

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

ЛЕКЦИЯ 6

Определение 18. 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 10. 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 $Z(G) \neq \emptyset$, так как $e \in Z(G)$.

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

Предложение 6. Факторгруппа группы G по центру изоморфна группе внутренних автоморфизмов $\text{Inn}(G)$.

Доказательство. По предложению 3(б) отображение $\Psi: G \rightarrow \text{Inn}(G)$, $g \mapsto \varphi_g$ является гомоморфизмом. По определению внутренних автоморфизмов гомоморфизм Ψ сюръективен. Ядро Ψ состоит из тех элементов $g \in G$, для которых $\varphi_g = \text{id}$, то есть $\forall h \in G$ выполнено $ghg^{-1} = h$. Это означает $g \in Z(G)$. Итак, $\text{Ker } \varphi = Z(G)$, $\text{Im } \varphi = \text{Inn}(G)$. По теореме о гомоморфизме $G/Z(G) \cong \text{Inn}(G)$. $\square$

Предложение 7. 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, $G/Z(G) \cong \{e\}$.) $\square$

Определение 19. Пусть G и H – две группы. *Прямым произведением* $G \times H$ называется множество пар (g, h) , где $g \in G$, $h \in H$, с операцией $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Замечание 5. Прямое произведение групп является группой. Действительно, ассоциативность умножения следует из ассоциативности умножения в каждой из групп G и H , нейтральным элементом является элемент (e_G, e_H) , обратным к элементу (g, h) является элемент (g^{-1}, h^{-1}) .

Определение 20. Пусть группа G содержит подмножество S . *Подгруппой, порожденной 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 11. 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 нем лежит $ss^{-1} = e$. Значит, это подгруппа, содержащая S , и следовательно, совпадает с G . $\square$

Упражнение 4. Докажите, что

- а) $\mathbb{Z} = \langle 1 \rangle$,
- б) $S_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle = \langle (1, 2), (1, 2, \dots, n) \rangle$,
- в) $A_n = \langle (1, 2, 3), (1, 2, 4), \dots, (1, 2, n) \rangle$.

Пример 11. Построим сюръективный гомоморфизм $S_4 \rightarrow S_3$. Рассмотрим 4 переменные x_1, x_2, x_3, x_4 и три многочлена от этих переменных:

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

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 $S_4 \rightarrow S_3$.

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

По теореме о гомоморфизме получаем следующий изоморфизм:

$$S_4/V_4 \cong S_3.$$

Лемма 12. Пусть G – группа, $H \triangleleft G$ – 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 . $\square$

Теорема 8. (Вторая теорема о гомоморфизме) Пусть G – группа, $H \triangleleft G$ – 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 $(H \cap K) \triangleleft K$.

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

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

ЛЕКЦИЯ 7

Теорема 9. (Третья теорема о гомоморфизме) Пусть $\varphi: G \rightarrow \tilde{G}$ – сюръективный гомоморфизм, $K = \text{Кер } \varphi$, $\tilde{H} \subset \tilde{G}$ – подгруппа. Пусть $H = \varphi^{-1}(\tilde{H})$ – полный прообраз. Тогда

- 1) $\tilde{H} \leftrightarrow H$ – биекция между подгруппами в $\tilde{G}$ и подгруппами в G , содержащими K .
- 2) Подгруппа H нормальна в G тогда и только тогда, когда $\tilde{H}$ нормальна в $\tilde{G}$.
- 3) Если H и $\tilde{H}$ нормальны, то $G/H \cong \tilde{G}/\tilde{H}$.

Доказательство. 1) Для подгруппы $\tilde{H} \subset \tilde{G}$ обозначим через $\Omega(\tilde{H}) = H$ подгруппу $\varphi^{-1}(\tilde{H}) \subset G$. Легко видеть, что $\Omega(\tilde{H})$ содержит $K = \varphi^{-1}(e)$. Пусть H – подгруппа G , содержащая K , обозначим через $\Theta(H)$ образ $\varphi(H)$, это подгруппа в $\tilde{G}$. Докажем, что Ω и Θ – взаимно обратные отображения. Для этого надо проверить, что $\Omega \circ \Theta = \text{id}$ и $\Theta \circ \Omega = \text{id}$. Действительно, $\Theta \circ \Omega(\tilde{H})$ – это образ от полного прообраза $\tilde{H}$, то есть $\tilde{H}$. 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 $\tilde{h} \in \tilde{H}$, $\tilde{g} \in \tilde{G}$. Так как гомоморфизм φ сюръективный, найдутся $h \in H$ и $g \in G$ такие, что $\varphi(h) = \tilde{h}$, $\varphi(g) = \tilde{g}$. Тогда $ghg^{-1} \in H$, а значит, $\tilde{g}\tilde{h}\tilde{g}^{-1} = \varphi(ghg^{-1}) \in \tilde{H}$. Таким образом, $\tilde{H} \triangleleft \tilde{G}$.

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

3) Рассмотрим композицию гомоморфизмов $\Psi = \pi_{\tilde{H}} \circ \varphi: G \rightarrow \tilde{G}/\tilde{H}$. Так как φ и $\pi_{\tilde{H}}$ – сюръекции, Ψ – также сюръекция. Заметим, что $\Psi(g) = e\tilde{H}$ тогда и только тогда, когда $\varphi(g) \in \tilde{H}$, то есть $g \in H$. Получаем, что $\text{Кер } \Psi = H$. По теореме о гомоморфизме получаем $G/H \cong \tilde{G}/\tilde{H}$. $\square$

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

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

Менее формально можно написать

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

Доказательство. Гомоморфизм $\pi_N: G \rightarrow G/N$ 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 $\text{Кер } \pi_N = N$, $\pi_N(H) \cong H/N$. По пункту 3) третьей теоремы о гомоморфизме

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

$\square$

Пример 12. 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 11), $|A_4/V_4| = 3$, 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

$$(S_4/V_4)(A_4/V_4) \cong S_3/A_3 \cong \mathbb{Z}_2.$$

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 $\emptyset$. 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, $(xux^{-1})(xzzx) = xux^{-1}xzzx$.

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 . $\square$

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 $\mathfrak{F}(S)$.*

Мощность $|S|$ называется *рангом* свободной группы $\mathfrak{F}(S)$.

Замечание 6. Легко видеть, что свободная группа действительно является группой. Ассоциативность конкатенации очевидна. Нейтральный элемент – класс пустого слова. Обратный элемент к каждому слову легко выписать.

Теорема 10. *Пусть G группа с порождающими $g_1, \dots, g_k$. Существует единственный гомоморфизм из свободной группы $\mathfrak{F}(x_1, \dots, x_k)$ 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 $g_1, \dots, g_k$. $\square$

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 gtg^{-1} для всех $t \in M, g \in G$.

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

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

При этом

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

□

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 $\varphi: \mathfrak{F}(x_1, \dots, x_k) \rightarrow G, x_i \mapsto g_i$ ядро совпадает с $N(x_1^{\alpha_1} \dots x_k^{\alpha_k}, \dots, x_1^{\beta_1} \dots x_k^{\beta_k})$. Тогда

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

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 13. 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 $\varphi: \langle x_1, x_2 \rangle \rightarrow D_n, x_1 \mapsto a, x_2 \mapsto b$ ядро содержит $N(x_1^2, x_2^2, (x_1 x_2)^n)$. Наша цель – доказать, что $\text{Ker } \varphi = N(x_1^2, x_2^2, (x_1 x_2)^n)$. Если это не так, то по следствию 3 имеем:

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

Тогда порядок группы G будет строго меньше, чем $H = \langle a, b \mid a^2, b^2, (ab)^n \rangle = \langle x_1, x_2 \rangle / N(x_1^2, x_2^2, (x_1 x_2)^n)$. Докажем, что в H не более $2n$ элементов. Легко видеть, что любой элемент H может быть записан либо в виде конечного слова $abab \dots$, либо в виде $ba ba \dots$. 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 $abab \dots$ различными являются слова длины $0, 1, 2, \dots, 2n - 1$. С другой стороны $ba = b^{-1}a^{-1} = (ab)^{-1}$. Значит, $(ba)^n = e$ и среди слов $ba ba \dots$ также различными являются слова длины $0, 1, 2, \dots, 2n - 1$. 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 $ba ba \dots$ представляются словами вида $abab \dots$. Значит, $|H| \leq 2n$. Отсюда следует, что $D_n = H$.

ЛЕКЦИЯ 8

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 $\mathfrak{F}(S)$? Этот вопрос называется проблемой равенства слов.

Один из способов решить проблему равенства слов – это определить некий канонический вид, к которому можно привести каждое слово, причем 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 11. *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 сокращенных символов не совпадает с только что приписанными, то можно поменять эти две операции. Остается 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. Назовем 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 . $\square$

Замечание 7. 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 $N(r_1, \dots, r_k)$, где r_i – соотношения. Оказывается, что проблема равенства слов может стать гораздо сложнее, более того она не всегда разрешима. Более точно, существует конечно порожденная группа с конечным числом соотношений, в которой проблема равенства слов алгоритмически не разрешима.

Напомним, что прямым произведением групп K и H мы называли множество пар $(k, h) \mid k \in K, h \in H$ с покомпонентным умножением. Назовем 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. 1) Внешнее прямое произведение групп K и H является внутренним прямым произведением подгрупп $K \times \{e\}$ и $\{e\} \times H$.

2) Пусть K и H – подгруппы в G . И пусть группа G – это внутреннее прямое произведение подгрупп K и H . Тогда G изоморфно внешнему прямому произведению $K \times H$.

Доказательство. 1) Рассмотрим подгруппы $K \times \{e\} = \{(k, e) \mid k \in K\}$ и $\{e\} \times H = \{(e, h) \mid h \in H\}$ во внешнем прямом произведении $K \times H$. (Проверку, что это подгруппы оставляю читателю.) Тогда

$$(a, b)(k, e)(a, b)^{-1} = (a, b)(k, e)(a^{-1}, b^{-1}) = (aka^{-1}, beb^{-1}) = (aka^{-1}, e) \in K \times \{e\}.$$

Значит, подгруппа $K \times \{e\}$ нормальна в $K \times H$. Аналогично, подгруппа $\{e\} \times H$ нормальна в $K \times H$. Пересечение этих подгрупп – это единственный элемент (e, e) , являющийся нейтральным элементом группы. Кроме того, любой элемент (k, h) есть произведение элементов (k, e) и (e, h) , то есть эти подгруппы порождают $K \times H$. Таким образом, группа $K \times H$ является внутренним прямым произведением подгрупп $K \times \{e\}$ и $\{e\} \times H$.

2) Так как группа G порождена подгруппами K и H и подгруппа H нормальна, то по лемме 12 любой элемент $g \in G$ представляется в виде $g = kh$. Значит отображение

$$\varphi: K \times H \rightarrow G, \quad \varphi(k, h) = kh$$

сюръективно. Докажем, что φ – изоморфизм групп.

Предположим, что $k_1 h_1 = k_2 h_2$. Тогда, умножая слева на k_2^{-1} , а справа – на h_1^{-1} , получаем $k_2^{-1} k_1 = h_2 h_1^{-1} \in K \cap H$. Следовательно, $k_2^{-1} k_1 = h_2 h_1^{-1} = e$, то есть $k_1 = k_2$ и $h_1 = h_2$. Итак, представление $g = kh$ единственно. Это означает инъективность φ .

Осталось проверить, что φ – гомоморфизм. Пусть теперь $k_1, k_2 \in K$ и $h_1, h_2 \in H$. Докажем, что $h_1 k_2 h_1^{-1} k_2^{-1} = e$. В самом деле так как K – нормальная подгруппа, $h_1 k_2 h_1^{-1} = \hat{k} \in K$, с другой стороны, так как H – нормальна подгруппа, $k_2 h_1^{-1} k_2^{-1} = \hat{h} \in H$. Тогда

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

Итак, $h_1 k_2 h_1^{-1} k_2^{-1} = e$. Значит, $h_1 k_2 = k_2 h_1$. Но тогда

$$\varphi(k_1, h_1) \varphi(k_2, h_2) = k_1 h_1 k_2 h_2 = k_1 k_2 h_1 h_2 = \varphi(k_1 k_2, h_1 h_2).$$

□

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

Теорема 12 (Теорема о факторизации прямого произведения). Пусть $G_1, \dots, G_k$ – группы. В каждой группе G_i фиксируем нормальную подгруппу H_i . Тогда $H_1 \times \dots \times H_k$ является нормальной подгруппой $G_1 \times \dots \times G_k$ и

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

Доказательство. Рассмотрим отображение

$$\varphi: G_1 \times \dots \times G_k \rightarrow G_1/H_1 \times \dots \times G_k/H_k,$$

$$\varphi: (g_1, \dots, g_k) \mapsto (g_1 H_1, \dots, g_k H_k).$$

Легко видеть, что φ – это сюръективный гомоморфизм, ядро которого совпадает с $H_1 \times \dots \times H_k$. Это доказывает оба утверждения. $\square$

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 13 (Китайская теорема об остатках.). Пусть m и n – натуральные числа. Тогда следующие условия эквивалентны:

- 1) $\text{НОД}(m, n) = 1$;
- 2) $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Доказательство. $1 \Rightarrow 2$. Рассмотрим

$$\varphi: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n, \quad \varphi(u) = (u \bmod m, u \bmod n).$$

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

Пусть $u \in \text{Кер } \varphi$. 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, $\text{Кер } \varphi = \{0\}$, а значит, 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 $\text{НОД}(m, n) = d > 1$. Тогда для любого элемента $(a, b) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$ выполнено

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

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

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 обозначаться kg .

Замечание 9. То, что абелева группа A порождается подмножеством $S \subset A$ означает, что каждый элемент $a \in A$ представляется в виде $a = k_1 s_1 + \dots + k_n s_n$, 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 $k_1 s_1 + \dots + k_n s_n = 0$ 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 $\{s_1, \dots, s_k\}$ выполнено $ns_1 = 0$, что противоречит линейной независимости этой системы.

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

$$\mathcal{A}(e_1, \dots, e_n, \dots).$$

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

Задача 5. Докажите, что

$$\mathcal{A}(e_1, \dots, e_n) = \langle e_1, \dots, e_n \mid e_i e_j e_i^{-1} e_j^{-1}, 1 \leq i < j \leq n \rangle.$$

Лемма 16. Пусть в абелевой группе A есть базис $\{e_1, \dots, e_n\}$. Тогда любой другой базис этой группы также состоит из n элементов. (То есть ранг свободной абелевой группы определен однозначно.)

Доказательство. Пусть в группе A есть другой базис $\{e'_1, \dots, e'_m, \dots\}$ и количество элементов в нем не равно n . Без ограничения общности мы можем считать, что в нем больше, чем n элементов. Рассмотрим $e'_1, \dots, e'_{n+1}$. Так как $\{e_1, \dots, e_n\}$ – базис, каждый элемент e'_j выражается через $\{e_1, \dots, e_n\}$ с целыми коэффициентами: $e'_j = c_{1j}e_1 + \dots + c_{nj}e_n$. Можно собрать все коэффициенты c_{ij} в целочисленную матрицу C размера $n \times n + 1$ такую, что

$$(e'_1, \dots, e'_{n+1}) = (e_1, \dots, e_n)C.$$

Интерпретируем столбцы $C^{(1)}, \dots, C^{(n+1)}$ матрицы C как векторы из пространства $\mathbb{Q}^n$ строк с рациональными коэффициентами длины n . Тогда столбцы – это $n + 1$ векторов в n -мерном векторном пространстве. По основной лемме о линейной зависимости столбцы C линейно зависимы, то есть есть рациональные числа $\frac{p_1}{q_1}, \dots, \frac{p_{n+1}}{q_{n+1}}$ не все равные нулю такие, что

$$\frac{p_1}{q_1} C^{(1)} \dots + \frac{p_{n+1}}{q_{n+1}} C^{(n+1)} = 0.$$

Домножим это равенство на произведение знаменателей и получим

$$k_1 C^{(1)} \dots + k_{n+1} C^{(n+1)} = 0$$

для некоторых $k_i \in \mathbb{Z}$ не всех равных нулю. Но тогда $k_1 e'_1 + \dots + k_{n+1} e'_{n+1} = 0$, что противоречит линейной независимости $\{e'_1, \dots, e'_{n+1}, \dots\}$. $\square$

Замечание 10. Пусть $F = \mathcal{A}(e_1, \dots, e_n)$. Тогда $F = \langle e_1 \rangle \oplus \dots \oplus \langle e_n \rangle \cong \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$. В самом деле, сопоставим элементу $k_1 e_1 + \dots + k_n e_n \in \mathcal{A}(e_1, \dots, e_n)$ элемент $(k_1 e_1, \dots, k_n e_n) \in \langle e_1 \rangle \oplus \dots \oplus \langle e_n \rangle$. Легко проверить, что это изоморфизм.

ЛЕКЦИЯ 9

Предложение 8. 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 5(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

$$P = \mathcal{A}(e_1, \dots, e_{n-1}) \subset F.$$

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 $L \neq B$. Рассмотрим гомоморфизм $\pi: F \rightarrow \mathbb{Z}$, $\pi(k_1 e_1 + \dots + k_n e_n) = k_n$. Тогда образ π – циклическая группа и найдется $l \in L$ такой, что $\text{Im } \pi = \langle \pi(l) \rangle$. Пусть $s = t_1 e_1 + \dots + t_n e_n \in L$. Тогда $\pi(s) \in \langle \pi(s) \rangle$. То есть $\pi(s) = q\pi(l)$ для некоторого целого q . Получаем $\pi(s - ql) = 0$, то есть $s - ql \in B$. Значит, $s \in B \oplus \langle l \rangle$ (данные две подгруппы пересекаются только по нулю, так как $\pi(l) \neq 0$). Получаем $L = B \oplus \langle l \rangle$ – свободная абелева группа ранга $\text{rk } B + 1 \leq n$. $\square$

Теорема 14 (Универсальное свойство свободной абелевой группы). *Пусть A – абелева группа с образующими $a_1, \dots, a_n$. Тогда существует сюръективный гомоморфизм*

$$\varphi: \mathcal{A}(x_1, \dots, x_n) \rightarrow A,$$

причем $\varphi(x_i) = a_i$.

Доказательство. Подходит гомоморфизм определенный по правилу

$$\varphi(k_1 x_1 + \dots + k_n x_n) = k_1 a_1 + \dots + k_n a_n.$$

$\square$

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 $\text{GL}_n(\mathbb{Z})$ множество целочисленных матриц $n \times n$, обратные к которым также являются целочисленными.

Замечание 11. Множество $\text{GL}_n(\mathbb{Z})$ является группой по умножению матриц. В самом деле, умножение двух целочисленных матриц A и B дает целочисленную матрицу, обратная к которой равна $(AB)^{-1} = B^{-1}A^{-1}$, а значит, целочисленная. Таким образом, $\text{GL}_n(\mathbb{Z})$ замкнуто относительно умножения. Замкнутость относительно взятия обратного элемента очевидна. Также $E \in \text{GL}_n(\mathbb{Z})$. Мы проверили, что $\text{GL}_n(\mathbb{Z})$ – подгруппа в $\text{GL}_n(\mathbb{Q})$.

Лемма 17. *Группа $\text{GL}_n(\mathbb{Z})$ состоит из целочисленных матриц с определителем ± 1*

Доказательство. У целочисленной матрицы целый определитель. Значит, если $A \in \text{GL}_n(\mathbb{Z})$, то $\det A, \det A^{-1} \in \mathbb{Z}$. Но $(\det A)(\det A^{-1}) = 1$. Значит, $\det A = \pm 1$.

Напротив, если для целочисленной матрицы выполнено $\det A = \pm 1$, то применяя формулу через алгебраические дополнения, получаем, что обратная матрица A^{-1} также является целочисленной. $\square$

Предложение 9. *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 $C \in \text{GL}_n(\mathbb{Z})$.

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 $CD = E$. Значит, $C \in \text{GL}_n(\mathbb{Z})$.

$2 \Rightarrow 1$. Для любого $f \in F$ выполняется

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

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 . $\square$

Примерами матриц из $\text{GL}_n(\mathbb{Z})$ 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. Назовем данные элементарные преобразования базиса *допустимыми*.

Рассмотрим пару состоящую из свободной абелевой группы $F = \mathcal{A}(x_1, \dots, x_n)$ и ее подгруппы $L = \mathcal{A}(y_1, \dots, y_m)$, $m \leq n$. Тогда

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

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

Теорема 15 (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} все 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. $\square$

Замечание 12. Легко доказать, что при допустимых элементарных преобразованиях НОД всех элементов матрицы не меняется. Поэтому u_1 равен НОД всех элементов матрицы. $\square$

Следствие 5. Любая конечно порожденная абелева группа изоморфна

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

где u_i делится на u_j , если $i > j$.

Доказательство. Пусть A – конечно порожденная абелева группа. По теореме 14 существует сюръективный гомоморфизм φ из свободной абелевой группы F конечного ранга n в группу A . Применим теорему о согласованных базисах к паре $\text{Ker } \varphi \subset F$. Получаем

$$F = \langle e_1 \rangle \oplus \dots \oplus \langle e_m \rangle \oplus \langle e_{m+1} \rangle \oplus \dots \oplus \langle e_n \rangle,$$

$$\text{Ker } \varphi = \langle u_1 e_1 \rangle \oplus \dots \oplus \langle u_m e_m \rangle \oplus \{0\} \oplus \dots \oplus \{0\}.$$

Применяя теорему о факторизации прямого произведения, получаем

$$\begin{aligned} A \cong F/\text{Ker } \varphi &\cong \langle e_1 \rangle / \langle u_1 e_1 \rangle \oplus \dots \oplus \langle e_m \rangle / \langle u_m e_m \rangle \oplus \langle e_{m+1} \rangle / \{0\} \oplus \dots \cong \\ &\cong \mathbb{Z}_{u_1} \oplus \dots \oplus \mathbb{Z}_{u_m} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}. \end{aligned}$$

□

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 $u = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Тогда

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

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

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

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 16 (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.*

ЛЕКЦИЯ 10

Лемма 19. Пусть $G_1, \dots, G_k$ – группы и $g_i \in G_i$. Тогда

$$\text{ord}(g_1, \dots, g_k) = \text{НОК}(\text{ord}(g_1), \dots, \text{ord}(g_k)).$$

Доказательство. $m = \text{ord}(g_1, \dots, g_k)$ – это минимальное натуральное число такое, что $(g_1, \dots, g_k)^m = (e, \dots, e)$. Это означает, что $g_i^m = e$ для всех $1 \leq i \leq k$. То есть m делится на все $\text{ord}(g_i)$. Минимальное такое число – это $\text{НОК}(\text{ord}(g_1), \dots, \text{ord}(g_k))$. □

Доказательство. (Доказательство теоремы 16) 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 $\text{Тог } A$ (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 $\text{Tor } A$ замкнуто относительно сложения. Кроме того $k(-a) = 0$, что означает замкнутость $\text{Tor } A$ относительно взятия противоположного. Осталось заметить, что $0 \in \text{Tor } A$.

Элементы конечного порядка в разложении (1) имеют вид $(x_1, \dots, x_N, 0, \dots, 0)$, где в конечных слагаемых идут любые элементы $x_1, \dots, x_N$, а в бесконечных слагаемых все элементы – нули. Таким образом,

$$\begin{aligned} \text{Tor } A &= \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_1^{a_2}} \oplus \dots \oplus \mathbb{Z}_{p_1^{a_{m_1}}} \oplus \mathbb{Z}_{p_2^{b_1}} \oplus \mathbb{Z}_{p_2^{b_2}} \oplus \dots \oplus \mathbb{Z}_{p_2^{b_{m_2}}} \oplus \dots \oplus \\ &\quad \oplus \mathbb{Z}_{p_k^{c_1}} \oplus \mathbb{Z}_{p_k^{c_2}} \oplus \dots \oplus \mathbb{Z}_{p_k^{c_{m_k}}} \oplus \{0\} \oplus \dots \oplus \{0\} \subset \\ &\subset \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_1^{a_2}} \oplus \dots \oplus \mathbb{Z}_{p_1^{a_{m_1}}} \oplus \mathbb{Z}_{p_2^{b_1}} \oplus \mathbb{Z}_{p_2^{b_2}} \oplus \dots \oplus \mathbb{Z}_{p_2^{b_{m_2}}} \oplus \dots \oplus \\ &\quad \oplus \mathbb{Z}_{p_k^{c_1}} \oplus \mathbb{Z}_{p_k^{c_2}} \oplus \dots \oplus \mathbb{Z}_{p_k^{c_{m_k}}} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z} = A. \end{aligned}$$

По теореме о факторизации прямого произведения

$$A/\text{Tor } A \cong \{0\} \oplus \dots \oplus \{0\} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z} \cong \mathbb{Z}^r.$$

Таким образом, факторгруппа $A/\text{Tor } A$ – 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 $\text{Tor } A$, к которой добавлены $\text{rk } A$ слагаемых $\mathbb{Z}$. Для того, чтобы доказать, что две вторых канонических формы группы A совпадают, осталось доказать, что для группы $\text{Tor } A$ (то есть для конечной группы) нет двух различных вторых канонических форм.

Пусть B – конечная абелева группа. Для любого натурального числа t можно рассмотреть гомоморфизм $\varphi_t: B \rightarrow B$, $\varphi_t(b) = tb$. Легко видеть, что если $B = B_1 \oplus B_2$, то $\varphi_t(b_1, b_2) = (tb_1, tb_2) = (\varphi_t|_{B_1}(b_1), \varphi_t|_{B_2}(b_2))$. Фиксируем простое число p . Рассмотрим второе каноническое разложение группы B :

$$\begin{aligned} B &= \mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \oplus \dots \oplus \mathbb{Z}_{p^2} \oplus \dots \oplus \mathbb{Z}_{p^k} \oplus \dots \oplus \mathbb{Z}_{p^k} \oplus \mathbb{Z}_{q_1^{r_1}} \oplus \dots \oplus \mathbb{Z}_{q_s^{r_s}} = \\ &= \mathbb{Z}_p^{m_1} \oplus \mathbb{Z}_{p^2}^{m_2} \oplus \dots \oplus \mathbb{Z}_{p^k}^{m_k} \oplus \mathbb{Z}_{q_1^{r_1}} \oplus \dots \oplus \mathbb{Z}_{q_s^{r_s}}. \end{aligned}$$

Возьмем $t = p^\alpha$, где p – простое число. Рассмотрим, ядро гомоморфизма φ_t . Пусть некоторый элемент разложения, умноженный на p^α равен нулю. Тогда его координаты лежат в ядрах ограничений гомоморфизма φ_t на каждое слагаемое. При этом ядра ограничений на $\mathbb{Z}_{q_1^{r_1}}, \dots, \mathbb{Z}_{q_s^{r_s}}$ равны нулю, так как $t = p^\alpha$ и $q_i^{r_i}$ взаимно просты. В группе $\mathbb{Z}_{p^\beta}$ при умножении на p^α в ноль переходит

- вся группа, если $\beta < \alpha$.
- подгруппа $\langle p^{\beta-\alpha} \rangle \cong \mathbb{Z}_{p^\alpha}$, если $\beta \geq \alpha$.

Отсюда

$$\text{Ker } \varphi_{p^\alpha} = \mathbb{Z}_p^{m_1} \oplus \mathbb{Z}_{p^2}^{m_2} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha-1}}^{m_{\alpha-1}} \oplus \mathbb{Z}_{p^\alpha}^{m_\alpha} \oplus \mathbb{Z}_{p^{\alpha+1}}^{m_{\alpha+1}} \oplus \dots \oplus \mathbb{Z}_{p^\alpha}^{m_k}.$$

Таким образом,

$$|\text{Ker } \varphi_{p^\alpha}| = p^{m_1 + 2m_2 + \dots + (\alpha-1)m_{\alpha-1} + \alpha(m_\alpha + m_{\alpha+1} + \dots + m_k)}.$$

Получаем

$$\frac{|\text{Ker } \varphi_{p^\alpha}|}{|\text{Ker } \varphi_{p^{\alpha-1}}|} = p^{m_\alpha + m_{\alpha+1} + \dots + m_k}.$$

Следовательно,

$$p^{m_\alpha} = \frac{|\text{Ker } \varphi_{p^\alpha}|}{|\text{Ker } \varphi_{p^{\alpha-1}}|} \cdot \frac{|\text{Ker } \varphi_{p^\alpha}|}{|\text{Ker } \varphi_{p^{\alpha+1}}|}$$

То есть

$$\begin{aligned} m_\alpha &= \log_p \left(\frac{|\text{Ker } \varphi_{p^\alpha}|^2}{|\text{Ker } \varphi_{p^{\alpha+1}}| \cdot |\text{Ker } \varphi_{p^{\alpha-1}}|} \right) = \\ &= 2 \log_p(|\text{Ker } \varphi_{p^\alpha}|) - \log_p(|\text{Ker } \varphi_{p^{\alpha+1}}|) - \log_p(|\text{Ker } \varphi_{p^{\alpha-1}}|). \end{aligned}$$

Заметим, что эта формула верна и при $\alpha = 1$, тогда $\varphi_{p^{\alpha-1}} = \text{id}$. Эта формула показывает, что количество слагаемых $\mathbb{Z}_{p^\alpha}$ во втором каноническом разложении конечной абелевой группы B не зависит от этого разложения. Это доказывает теорему. $\square$

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 $A/\text{Tor } A$ определен 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 16. $\square$

Определение 31. 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 $\text{exp } G$.

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 $\text{ord } g$. Так как $\text{exp } G$ – минимальное натуральное число, что $g^{\text{exp } G} = e$ для всех $g \in G$, получаем, что $\text{exp } G$ – минимальное натуральное число, делящееся на порядки всех элементов. $\square$

Предложение 10 (Критерий цикличности конечной абелевой группы). *Пусть A – конечная абелева группа. Группа A циклическая тогда и только тогда, когда $\text{exp } A = |A|$.*

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

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

$$\begin{aligned} \frac{|A|}{p_j} a &= p_1^{k_1} p_2^{k_2} \dots p_j^{k_j-1} \dots p_m^{k_m} (a_1 + \dots + a_j + \dots + a_m) = \\ &= 0 + \dots + 0 + p_1^{k_1} p_2^{k_2} \dots p_j^{k_j-1} \dots p_m^{k_m} a_j + 0 + \dots + 0 = p_1^{k_1} p_2^{k_2} \dots p_j^{k_j-1} \dots p_m^{k_m} a_j \neq 0. \end{aligned}$$

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

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 умножения. Для поля $F^\times = F \setminus \{0\}$ и группа $(F^\times, \cdot)$ называется *мультипликативной группой поля F* .

Предложение 11. *Конечная подгруппа в мультипликативной группе*

$$F^\times = (F \setminus \{0\}, \cdot)$$

поля F 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 10 экспонента G не равна $|G|$. Значит, $\text{exp } G = k < |G|$. 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. $\square$

Очевидным следствием предыдущего предложения является следующее утверждение.

Следствие 7. *Мультипликативная группа конечного поля циклическая.*

Определение 32. Пусть G – группа, а X – множество. Действием группы G на множестве X называется отображение $\alpha: G \times X \rightarrow X$, 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 32 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 14. Пусть $X = \{1, 2, \dots, n\}$. 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) $\text{id} \cdot i = \text{id}(i) = i$.

Пример 15. Пусть K – поле. Тогда зададим действие $\text{GL}(K) \curvearrowright K^n$ по следующей

формуле. Для $A \in \text{GL}(K)$ 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 16. 1) Действие G на себе левыми сдвигами.

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

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

2) Действие G на себе правыми сдвигами.

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

$$g_1 \cdot (g_2 \cdot \bar{g}) = g_1 \cdot (\bar{g}g_2^{-1}) = (\bar{g}g_2^{-1})g_1^{-1} = \bar{g}(g_1g_2)^{-1} = (g_1g_2) \cdot \bar{g},$$

$$e \cdot \bar{g} = \bar{g} \cdot e = \bar{g}.$$

3) Действие G на себе сопряжениями.

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

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

$$e \cdot \bar{g} = e \bar{g} e^{-1} = \bar{g}.$$

Замечание 13. Заметим, что нельзя определить правое действие (действие правыми сдвигами) таким образом $g \cdot \bar{g} = \bar{g}g$, так как при этом

$$g_1 \cdot (g_2 \cdot \bar{g}) = g_1 \cdot (\bar{g}g_2) = \bar{g}g_2g_1, \quad (g_1g_2) \cdot \bar{g} = \bar{g}g_1g_2.$$

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

$$\bar{g}g_2g_1 \neq \bar{g}g_1g_2.$$

ЛЕКЦИЯ 11

Заметим, что при фиксированном $g \in G$ отображение $\alpha_g: X \rightarrow X$, $\alpha_g(x) = \alpha(g, x)$ является биекцией. В самом деле, легко убедиться, что $\alpha_g \circ \alpha_h = \alpha_{gh}$, при этом $\alpha_e = \text{id}$. 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 $X \rightarrow X$. Гомоморфизм φ_α определяется следующим образом: $\varphi_\alpha(g) = \alpha_g$.

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

Лемма 21. *Отображения $\Phi: \alpha \mapsto \varphi_\alpha$ и $\Psi: \varphi \mapsto \alpha_\varphi$ 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 $\Psi \circ \Phi = \text{id}$.

Пусть теперь $\varphi: G \rightarrow S(X)$ – 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 $\Phi \circ \Psi = \text{id}$. $\square$

Следующие два определения играют центральную роль в теории действий.

Определение 33. 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 34. Пусть G действует на X и $x \in X$. Стабилизатором элемента x называется множество $\text{St}(x) = G_x = \{g \in G \mid g \cdot x = x\}$.

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 $x = g \cdot y$, $y = \bar{g} \cdot z$. Тогда $x = (g\bar{g}) \cdot z$. Следовательно, $x \sim z$. $\square$

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

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

Если $g \in \text{St}(x)$, 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, $g^{-1} \in \text{St}(x)$, то есть $\text{St}(x)$ замкнут относительно взятия обратного.

Осталось заметить, что единица группы лежит в стабилизаторе любого элемента. $\square$

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 $\text{St}(y) = g\text{St}(x)g^{-1}$. (Стабилизаторы элементов одной орбиты сопряжены.)

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

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

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

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

Теорема 17. Существует биекция между множеством левых смежных классов группы G по подгруппе $\text{St}(x)$ и элементами орбиты Gx .

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

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

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

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

С помощью только что доказанной формулы посчитаем количество элементов в группе вращений куба $\text{Sym}_+(K)$. 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 12. Порядок группы $\text{Sym}_+(K)$ равен 24.

Доказательство. Рассмотрим куб K с вершинами $ABCD A'B'C'D'$. Есть естественное действие $\text{Sym}_+(K)$ на множестве $\{A, B, C, D, A'B'C'D'\}$. В группе $\text{Sym}_+(K)$ 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

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

Осталось найти $|H|$, где $H = \text{St}(A)$. 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

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

(Здесь мы используем индекс в $\text{St}_H(B)$, чтобы подчеркнуть, что это стабилизатор при действии группы H , а не при действии группы G .) Осталось найти $|\text{St}_H(B)|$. Пусть $\xi \in |\text{St}_H(B)|$. 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, $\psi = \text{id}$. Следовательно, $|\text{St}_H(B)| = 1$. Таким образом

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

□

Теперь разберемся более подробно с группой $\text{Sym}_+(K)$ вращений куба.

Предложение 13. *Группа вращений куба изоморфна S_4 .*

Доказательство. Группа $\text{Sym}_+(K)$ действует на множестве диагоналей куба. (Очевидно, что любой элемент этой группы переводит диагонали в диагонали, то есть производит перестановку диагоналей. При этом композиция элементов дает композицию перестановок.) То есть мы имеем гомоморфизм $\varphi: \text{Sym}_+(K) \rightarrow S_4$. Поскольку $|\text{Sym}_+(K)| = |S_4| = 24$, для того, чтобы доказать, что φ – изоморфизм достаточно доказать, что φ – сюръекция. Пусть K – середина ребра AA' , а L – середина ребра CC' . Рассмотрим ξ вращение на π вокруг KL . Ясно, что $\xi \in \text{Sym}_+(K)$.

$$\xi(A) = A', \xi(A') = A, \xi(C) = C', \xi(C') = C, \xi(B) = D', \xi(D') = B, \xi(B') = D, \xi(D) = B'.$$

Значит, применение ξ меняет местами диагонали AC' и $A'C$ и оставляет на месте диагонали BD' и $B'D$. То есть образ ξ в S_4 – это транспозиция. Но аналогично мы можем доказать, что любая транспозиция лежит в образе φ . Поскольку S_4 порождается транспозициями, φ – сюръекция. □

Аналогично докажем другую геометрическую реализацию группы S_4 . Напомним, что группа симметрий фигуры – это группа всех движений пространства (для плоской фигуры – плоскости), сохраняющих данную фигуру. (Группа симметрий не состоит только из симметрий относительно плоскостей/прямых!)

Предложение 14. *Группа симметрий правильного тетраэдра изоморфна S_4 .*

Доказательство. Группа симметрий правильного тетраэдра действует на множестве его вершин (их 4). получаем гомоморфизм из этой группы в S_4 . Этот гомоморфизм инъективен, так как у него тривиальное ядро. В самом деле, если некое преобразование плоскости лежит в ядре, то оно оставляет на месте вершины тетраэдра (4 точки, не лежащие в одной плоскости), а значит, это тождественное преобразование. Теперь докажем сюръективность данного гомоморфизма. Рассмотрим симметрию относительно плоскости, проходящей через ребро тетраэдра и середину противоположного ребра. Данная симметрия меняет ровно 2 вершины. Значит, в образе нашего гомоморфизма лежат транспозиции. Так как они порождают S_4 , гомоморфизм сюръективен. Итак, мы построили гомоморфизм из группы симметрий правильного тетраэдра в S_4 , который является биекцией, то есть изоморфизмом. □

Определение 35. *Ядро неэффективности* действия $\alpha: G \times X \rightarrow X$ – это множество $\text{Ker } \alpha = \{g \in G \mid \forall x \in X : g \cdot x = x\}$. Если ядро действия состоит только из единицы группы G , то действие называется *эффективным*.

Из определения следует, что ядро неэффективности совпадает с пересечением всех стабилизаторов всех элементов $x \in X$.

Лемма 25. *Ядро неэффективности действия α является нормальной подгруппой в группе G .*

Доказательство. Утверждение следует из того, что $\text{Ker } \alpha$ совпадает с ядром гомоморфизма $\text{Ker } \varphi_\alpha$. $\square$

Предложение 15. *Действия группы G на X с ядром неэффективности, содержащим H , находятся в биекции с действиями G/H на X .*

Доказательство. Пусть $\varphi_\alpha: G \rightarrow S(X)$ – гомоморфизм, соответствующий α . При этом $H \subset \text{Ker } \alpha$. Рассмотрим $\psi: G/H \rightarrow S(X)$, $\psi(gH) = \varphi(g)$. Проверим, что ψ определено корректно, то есть что если $gH = \bar{g}H$, то $\varphi(g) = \varphi(\bar{g})$. В самом деле если $gH = \bar{g}H$, то $g^{-1}\bar{g} = h \in H$. Тогда $\bar{g} = gh$ и $\varphi(\bar{g}) = \varphi(g)\varphi(h) = \varphi(g)$.

Отображение ψ является гомоморфизмом, так как

$$\psi((g_1H) \cdot (g_2H)) = \psi(g_1g_2H) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1H)\psi(g_2H).$$

Гомоморфизм ψ соответствует действию α_ψ группы G/H на X .

Напротив, если дано действие $G/H \curvearrowright X$, то ему соответствует гомоморфизм $\psi: G/H \rightarrow S(X)$. Если взять композицию с каноническим гомоморфизмом

$$\pi_H: G \rightarrow G/H,$$

то получим гомоморфизм $\varphi = \psi \circ \pi_H: G \rightarrow S(X)$. Последний гомоморфизм соответствует действию G на X . Поскольку $\text{Ker } \pi_H = H$, ядро ψ содержит H , а значит, H содержится в ядре неэффективности полученного действия G на X . $\square$

Определение 36. Действия $\alpha: G \times X \rightarrow X$ и $\beta: G \times Y \rightarrow Y$ называются *изоморфными*, если существует биекция $\psi: X \rightarrow Y$ такие, что $\beta(g, \psi(x)) = \psi(\alpha(g, x))$ для любых $g \in G$ и $x \in X$.

Определение 37. Действие $G \curvearrowright X$ называется *транзитивным*, если у него ровно одна орбита, то есть если для любых $x, y \in X$ существует $g \in G$ такое, что $g \cdot x = y$.

Как уже было упомянуто, ядро неэффективности действия – это пересечение всех стабилизаторов. Действие эффективно, если пересечение всех стабилизаторов состоит только из единицы.

Определение 38. Действие называется *свободным*, если стабилизатор каждого элемента $x \in X$ тривиален, то есть равен $\{e\}$.

Теорема 18. *Любое свободное транзитивное действие группы G на некотором множестве изоморфно действию G на себе левыми сдвигами.*

Доказательство. Пусть $\beta: G \times X \rightarrow X$ – свободное транзитивное действие. Пусть $\alpha: G \times G \rightarrow G$, $g \cdot g' = gg'$ – действие G правыми сдвигами на себе. Рассмотрим любой элемент $y \in X$. Определим отображение $\psi: G \rightarrow X$ по формуле

$$\psi(g) = \beta(g, y) = g \cdot y.$$

Докажем, что ψ – биекция. Сюръективность ψ следует из того, что действие β транзитивно. Проверим инъективность. Пусть $\psi(g) = \psi(g')$. Тогда $g \cdot y = g' \cdot y$. Следовательно, $(g^{-1}g) \cdot y = y$, то есть $g^{-1}g' \in \text{St}(y)$. Но так как действие β свободно, получаем $\text{St}(y) = \{e\}$, а значит, $g^{-1}g' = e$, то есть $g = g'$.

Имеем

$$\beta(g, \psi(\bar{g})) = \beta(g, \bar{g} \cdot y) = g \cdot (\bar{g} \cdot y) = (g\bar{g}) \cdot y.$$

С другой стороны

$$\psi(\alpha(g, \bar{g})) = \psi(g\bar{g}) = (g\bar{g}) \cdot y.$$

Таким образом,

$$\beta(g, \psi(\bar{g})) = \psi(\alpha(g, \bar{g})),$$

то есть действия α и β изоморфны. $\square$

Теперь рассмотрим действие группы G на себе сопряжениями. Орбиты и стабилизаторы при этом действии имеют отдельные названия. Орбиты называются *классами сопряженности*, а стабилизаторы – *централизаторами*. Класс сопряженности элемента $g \in G$ обозначается $C(g)$, а централизатор элемента g обозначается $Z(g)$. Следствие 9, примененное к действию G на себе сопряжениями, дает формулу $|C(g)| \cdot |Z(g)| = |G|$.

Замечание 14. Заметим, что и класс сопряженности и централизатор зависят не только от самого элемента g , но и от того, элементом какой группы он рассматривается. Путаница может произойти, например, в случае, когда в группе G есть подгруппа H . Тогда любой элемент $h \in H$ можно рассматривать как элемент G , а можно – как элемент H . Чтобы различать эти ситуации будем там, где это необходимо писать группу в качестве индекса. При этом может так случиться, что $C_G(g) \neq C_H(g)$ и $Z_G(g) \neq Z_H(g)$. Однако легко видеть, что всегда имеются включения в одну сторону: $C_H(g) \subset C_G(g)$, $Z_H(g) \subset Z_G(g)$.

Следующее утверждение следует непосредственно из определений.

Лемма 26. *Подгруппа $H \subset G$ является нормальной тогда и только тогда, когда H состоит из классов сопряженности. (Имеется в виду, что каждый класс сопряженности либо целиком содержится в H , либо целиком содержится в дополнении к H .)*

Доказательство. Подгруппа H нормальна тогда и только тогда, когда для любых $h \in H$ и $g \in G$ выполнено $ghg^{-1} \in H$. То есть для любого $h \in H$ выполнено $C(h) \subset H$. $\square$

Для того, чтобы описывать нормальные подгруппы (и для других целей) бывает удобно явно описать классы сопряженности в группе. Сделаем это для группы S_n . Назовем *цикловой структурой* перестановки $\sigma \in S_n$ неупорядоченный набор длин независимых циклов этой перестановки.

Лемма 27. *Пусть $\sigma \in S_n$. Тогда $C_{S_n}(\sigma)$ состоит из всех перестановок $\delta \in S_n$ с такой же цикловой структурой.*

Доказательство. Пусть разложение σ в независимые циклы имеет вид

$$\sigma = (a_1, \dots, a_k)(b_1, \dots, b_m) \dots (c_1, \dots, c_l).$$

Возьмем $\pi \in S_n$. Имеем:

$$\pi\sigma\pi^{-1} = (\pi(a_1), \dots, \pi(a_k))(\pi(b_1), \dots, \pi(b_m)) \dots (\pi(c_1), \dots, \pi(c_l)). \quad (*)$$

В самом деле $\pi: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ – биекция. А значит, любой элемент $i \in \{1, 2, \dots, n\}$ равен $\pi(j)$. С другой стороны $\pi\sigma\pi^{-1}(\pi(j)) = \pi(\sigma(j))$. Отсюда следует приведенная выше формула (*). Видно, что перестановка $\pi\sigma\pi^{-1}$ имеет ту же цикловую структуру, что и σ .

Напротив, пусть

$$\delta = (a'_1, \dots, a'_k)(b'_1, \dots, b'_m) \dots (c'_1, \dots, c'_l)$$

имеет такую же цикловую структуру, что и σ . Положим

$$\pi = \begin{pmatrix} a_1 \dots a_k b_1 \dots b_m \dots c_1 \dots c_l \\ a'_1 \dots a'_k b'_1 \dots b'_m \dots c'_1 \dots c'_l \end{pmatrix}.$$

Тогда $\pi\sigma\pi^{-1} = \delta$. □

Задача 6. Найдите все нормальные подгруппы в S_4 .

Задача 7. Пусть $\sigma \in A_n$. Докажите, что $C_{S_n}(\sigma)$ либо совпадает с $C_{A_n}(\sigma)$, либо есть объединение двух равномошных классов сопряженности в A_n . А именно, $C_{S_n}(\sigma)$ совпадает с $C_{A_n}(\sigma)$, если в разложении на независимые циклы перестановки из данного класса сопряженности есть цикл четной длины или 2 цикла одинаковой нечетной длины.

Определение 39. Группа G называется p -группой, если $|G| = p^k$ для простого p и некоторого натурального k .

Теорема 19. Центр p -группы не равен $\{e\}$.

Доказательство. Заметим, что центр состоит из всех элементов, классы сопряженности которых состоят ровно из одного элемента. Пусть $|G| = p^k$. В пусть $g \in G$. Тогда

$$|C(g)| = \frac{|G|}{|Z(g)|} = p^m, m \in \mathbb{N} \cup \{0\}.$$

Таким образом, порядок любого смежного класса $C(g)$ либо равен 1, либо делится на p . Получаем, что $G \setminus Z(G)$ разбивается на классы сопряженности, порядок которых делится на p , а значит, $|G| - |Z(G)|$ делится на p . Отсюда $|Z(G)|$ делится на p . Следовательно, $Z(G) \neq \{e\}$. □

ЛЕКЦИЯ 12

Следствие 10. Группа порядка p^2 абелева.

Доказательство. Пусть $|G| = p^2$. Тогда, так как $|G|$ делится на $|Z(G)|$, есть 3 варианта: $|Z(G)| = 1$, $|Z(G)| = p^2$ и $|Z(G)| = p$. Первый случай не возможен по предыдущей теореме. Второй соответствует абелевой группе. Осталось показать, что не может быть $|Z(G)| = p$. Допустим, что $|Z(G)| = p$, тогда $|G/Z(G)| = p$. Значит, группа $G/Z(G)$ циклическая. Это противоречит предложению 7. □

Теорема 20 (Теорема Кэли). Пусть G – конечная группа порядка n . Тогда G изоморфна некоторой подгруппе в S_n .

Доказательство. Пусть $|G| = n$. Рассмотрим α – действие G на себе левыми сдвигами. Это действие соответствует гомоморфизму $\varphi_\alpha: G \rightarrow S(G) \cong S_n$. (Явно этот гомоморфизм задается по правилу: элемент g переходит в биекцию $\bar{g} \mapsto g\bar{g}$ из G в G .) При этом ядро φ_α равно ядру неэффективности α . Но легко видеть, что $\text{St}(e) = \{e\}$, а значит, $\text{Ker } \alpha = \{e\}$. Значит, φ_α задает вложение G в S_n . □

Пусть задано действие G на X . Для $g \in G$ обозначим через X^g множество

$$X^g = \{x \in X \mid g \cdot x = x\}.$$

Лемма 28 (Лемма Бернсайда). Пусть конечная группа G действует на множестве X тогда количество орбит этого действия равно

$$\frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Доказательство. Посчитаем двумя различными способами количество пар (x, g) таких, что $g \cdot x = x$. Обозначим множество таких пар за M . Тогда с одной стороны

$$|M| = \sum_{g \in G} |X^g|.$$

С другой стороны

$$|M| = \sum_{x \in X} |\text{St}(x)| = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|Gx|}. \quad (**)$$

В последней сумме заметим, что суммирование по всему X можно разбить на суммирование по непересекающимся орбитам. Пусть O – одна из орбит. Тогда

$$\sum_{x \in O} \frac{1}{|Gx|} = \sum_{x \in O} \frac{1}{|O|} = 1$$

Значит, самое правое выражение в $(**)$ равно $|G|$ умножить на количество орбит. Приравнявая ко второму выражению для $|M|$ и разделив на $|G|$, получаем утверждение леммы. $\square$

Замечание 15. Если множество X бесконечно, то обе части равенства из леммы Бернсайда будут бесконечны. В самом деле, количество орбит бесконечно так как количество элементов в каждой орбите не больше $|G|$. Выражение $\frac{1}{|G|} \sum_{g \in G} |X^g|$ бесконечно, так как $X^e = X$ – бесконечное множество.

Пример 17. Решим с помощью леммы Бернсайда такую задачу: сколько существует различных способов покрасить ребра проволочного правильного 7-угольника в 3 цвета? (Имеется в виду, что этот проволочный 7-угольник находится в трехмерном пространстве и две покраски одинаковы, если их можно совместить.)

Рассмотрим закрепленные покраски 7-угольника, то есть занумеруем ребра и для каждого ребра будет 3 варианта покрасить его. Таких закрепленных покрасок существует 3^7 . На множестве X закрепленных покрасок действует группа D_7 и нам нужно посчитать количество орбит (так как фраза "окраски одинаковы, если их можно совместить" означает, что покраски считаются одинаковыми, если лежат в одной орбите).

Чтобы применить формулу из леммы Бернсайда нужно посчитать $|X^g|$ для всех $g \in D_7$. Для $g = e$ имеем $|X^e| = 3^7$. Для любого нетривиального поворота легко видеть, что X^g состоит только из одноцветных закрепленных покрасок, а значит, $|X^g| = 3$. Для симметрии все вершины 7-угольника разбиваются на 3 пары симметричных вершин и одну, лежащую на оси симметрии. Количество покрасок из $|X^g|$ равно 3^4 так как каждую пару надо покрасить в один цвет. В итоге количество орбит равно

$$\frac{1}{14}(3^7 + 6 \cdot 3 + 7 \cdot 3^4) = 198.$$

Определение 40. Пусть x и y – элементы группы G . Коммутатором элементов x и y называется элемент

$$[x, y] = xyx^{-1}y^{-1}.$$

Лемма 29. $[x, y] = e$ тогда и только тогда, когда элементы x и y перестановочны (то есть $xy = yx$).

Доказательство.

$$xy = yx \Leftrightarrow xyx^{-1} = y \Leftrightarrow xyx^{-1}y^{-1} = e.$$

□

Замечание 16. Обратный элемент к коммутатору является коммутатором. В самом деле:

$$[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x].$$

Определение 41. Коммутант группы G – это подгруппа, порожденная всеми коммутаторами пар элементов из G . Коммутант группы G обозначается G' или $[G, G]$.

Лемма 30. Коммутант состоит из произведений коммутаторов.

Доказательство. По определению, G' состоит из произведений коммутаторов и обратных к ним. Но, так как обратный к коммутатору – коммутатор, G' состоит из произведения коммутаторов. □

Лемма 31. $G' = \{e\}$ тогда и только тогда, когда G коммутативна.

Доказательство. Если G коммутативна, то все коммутаторы равны e , и значит, коммутант также равен $\{e\}$.

Если же G не абелева, то найдутся два элемента x и y такие, что $xy \neq yx$. Тогда $[x, y] \neq e \in G'$. □

Определение 42. Подгруппа $H \subset G$ называется *характеристической*, если для любого автоморфизма $\varphi: G \rightarrow G$ выполнено $\varphi(H) = H$.

Характеристическая подгруппа автоматически является нормальной. Для доказательства этого достаточно рассмотреть внутренний автоморфизм $\varphi_g: h \mapsto ghg^{-1}$.

Лемма 32. Характеристическая подгруппа характеристической подгруппы является характеристической.

Доказательство. Пусть H – характеристическая подгруппа G , а N – характеристическая подгруппа H . Пусть $\varphi \in \text{Aut}(G)$. Тогда $\varphi(H) = H$. Поскольку $\varphi^{-1}(H) = H$, получаем, что $\varphi|_H: H \rightarrow H$ – автоморфизм H . Значит, поскольку N характеристическая, $\varphi(N) = \varphi|_H(N) = N$. □

Замечание 17. Напомним, что нормальная подгруппа нормальной подгруппы не всегда нормальна.

Предложение 16. Коммутант и центр – характеристические подгруппы.

Доказательство. Пусть G – группа. Рассмотрим $z \in Z(G)$, и пусть $\varphi \in \text{Aut}(G)$. Тогда для любого $g \in G$ выполнено

$$\varphi(z)g = \varphi(z\varphi^{-1}(g)) = \varphi(\varphi^{-1}(g)z) = g\varphi(z).$$

То есть $\varphi(z) \in Z(G)$. Пусть теперь $g \in G'$. Тогда

$$g = [x_1, y_1] \dots [x_k, y_k].$$

Получаем

$$\varphi(g) = [\varphi(x_1), \varphi(y_1)] \dots [\varphi(x_k), \varphi(y_k)] \in G'.$$

□

Следствие 11. Коммутант G' – нормальная подгруппа в G .

Рассмотрим ряд кратных коммутантов. $G \supset G' \supset G'' \supset G^{(3)} \supset G^{(4)} \supset \dots$ Имеется в виду, что $(G^{(i)})' = G^{(i+1)}$. Из предложения следует, что $G^{(i)}$ – характеристическая (и в частности нормальная) подгруппа в G .

Лемма 33. Группа G/G' коммутативна.

Доказательство. Рассмотрим коммутатор двух произвольных элементов из G/G' :

$$[gG', hG'] = gG' \cdot hG' \cdot (gG')^{-1} \cdot (hG')^{-1} = [g, h]G' = G'.$$

То есть коммутатор любых элементов из G/G' равен единице группы G/G' . Значит, G/G' – абелева группа. □

Теорема 21. а) Пусть H – подгруппа в G и $G' \subseteq H$. Тогда H – нормальная подгруппа и G/H – абелева группа.

б) Если $G \triangleright H$ и группа G/H – абелева группа то $G' \subset H$.

Доказательство. а) Пусть $g \in G$, $h \in H$. Тогда $ghg^{-1} = [g, h]h \in H$. Значит, $G \triangleright H$.

Рассмотрим коммутатор двух произвольных элементов из G/H :

$$[g_1H, g_2H] = g_1H \cdot g_2H \cdot (g_1H)^{-1} \cdot (g_2H)^{-1} = [g_1, g_2]H = H.$$

Значит, $(G/H)' = \{e\}$, то есть G/H – коммутативная группа.

б) Рассмотрим коммутатор двух произвольных элементов из G/H :

$$[g_1H, g_2H] = g_1H \cdot g_2H \cdot (g_1H)^{-1} \cdot (g_2H)^{-1} = [g_1, g_2]H.$$

Так как G/H – абелева группа, $[g_1H, g_2H] = H$. Получаем $[g_1, g_2]H = H$, следовательно, $[g_1, g_2] \in H$. Поскольку коммутаторы порождают G' , выполняется $G' \subset H$. □

Лемма 34. а) A_n порождается тройными циклами.

б) При $n \geq 5$ группа A_n порождается парами несмежных транспозиций $(i, j)(k, s)$.

Доказательство. а) Пусть $\sigma \in A_n$. Любая перестановка разлагается в произведение транспозиций. Поскольку σ – четная перестановка, $\sigma = \tau_1 \dots \tau_{2m}$. Рассмотрим $\tau_{2l-1}\tau_{2l}$. Возможны 3 варианта:

1) $\tau_{2l-1} = \tau_{2l}$. Тогда из произведения можно их удалить.

2) $\tau_{2l-1} = (i, j)$, $\tau_{2l} = (j, k)$. Тогда $\tau_{2l-1}\tau_{2l} = (i, j, k)$.

3) $\tau_{2l-1} = (i, j)$, $\tau_{2l} = (k, s)$. Тогда $\tau_{2l-1}\tau_{2l} = (i, j)(j, k)(j, k)(k, s) = (i, j, k)(j, k, s)$.

б) Пусть H – подгруппа A_n , $n \geq 5$ порожденная всеми парами несмежных транспозиций.

$$(i, j)(k, s) \cdot (k, s)(j, r) = (i, j)(j, r) = (i, j, r).$$

Значит, H содержит все тройные циклы. Но, как уже доказано, тройные циклы порождают A_n . Следовательно, $H = A_n$. □

Теорема 22. $S'_n = A_n$.

Доказательство. Как известно, $A_n \triangleleft S_n$ и $S_n/A_n \cong \mathbb{Z}_2$ – абелева группа. Следовательно, $S'_n \subset A_n$.

Обратное включение будет следовать из явных выкладок.

$$[(i, j), (j, k)] = (i, j)(j, k)(i, j)(j, k) = (i, k, j).$$

Значит, любой тройной цикл (i, k, j) лежит в S'_n . Далее утверждение теоремы следует из леммы 34 а). $\square$

Теорема 23. 1) $A'_3 = \{id\}$,

2) $A'_4 = V_4$,

3) $A'_n = A_n$ при $n \geq 5$.

Доказательство. 1) Группа A_3 изоморфна $\mathbb{Z}_3$ и является абелевой.

2) $|A_4| = 12$, $|V_4| = 4$, следовательно, $|A_4/V_4| = 3$, то есть $A_4/V_4 \cong \mathbb{Z}_3$ – абелева группа. Значит, $A'_4 \subset V_4$. С другой стороны

$$[(i, j, k), (j, k, s)] = (i, j, k)(j, k, s)(i, k, j)(j, s, k) = (i, s)(j, k).$$

Следовательно, $V_4 \subset A'_4$. Итак, $A'_4 = V_4$.

3) Как следует из предыдущего пункта при $n \geq 4$ выполнено $(i, s)(j, k) \in A'_n \forall i, j, k, s$.

Далее утверждение теоремы вытекает из леммы 34 б). $\square$

Теорема 24. Пусть F – поле такое, что $|F| \geq 4$. Тогда

1) $\text{SL}_n(F)' = \text{SL}_n(F)$

2) $\text{GL}_n(F)' = \text{SL}_n(F)$

Доказательство. 1) Для удобства записи сделаем нужную выкладку при $n = 2$. Поскольку $|F| \geq 4$, найдется $a \in F$ такое, что $a \notin \{0, 1, -1\}$. Тогда существует $(a^2 - 1)^{-1}$, и для любого $\mu \in F$ можно рассмотреть $\lambda = (a^2 - 1)^{-1}\mu$. Заметим, что

$$\begin{aligned} \left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \right] &= \\ &= \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} = \\ &= \begin{pmatrix} a & a\lambda \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}\lambda \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & (a^2 - 1)\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Аналогично, при любом n выполняется $E + \mu E_{ij} \in \text{SL}_n(F)'$ при всех $i \neq j$.

Группа $\text{SL}_n(F)$ порождается элементами вида $E + \mu E_{ij}$. В самом деле, любую матрицу A из $\text{SL}_n(F)$ можно привести элементарными преобразованиями первого типа к матрице E . При этом происходит умножение на матрицы вида $E + \mu E_{ij}$. Получаем

$$(E + \mu_k E_{i_k j_k}) \dots (E + \mu_1 E_{i_1 j_1}) A = E.$$

Значит,

$$A = (E - \mu_1 E_{i_1 j_1}) \dots (E - \mu_k E_{i_k j_k}).$$

2) $\text{GL}_n(F)' \supset \text{SL}_n(F)' = \text{SL}_n(F)$.

С другой стороны $\text{GL}_n(F)/\text{SL}_n(F) \cong F^\times$ – абелева группа, а значит, $\text{GL}_n(F)' \subset \text{SL}_n(F)$. Получаем $\text{GL}_n(F)' = \text{SL}_n(F)$. $\square$

ЛЕКЦИЯ 13

Лемма 35. Пусть $\varphi: G \rightarrow K$ – гомоморфизм групп. Тогда $\varphi(G') \subset K'$. Если гомоморфизм φ сюръективен, то $\varphi(G') = K'$.

Доказательство. Поскольку φ – гомоморфизм,

$$\varphi([x, y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = [\varphi(x), \varphi(y)].$$

Значит, $\varphi([x, y]) \in K'$, и следовательно, $\varphi(G') \subset K'$.

Если же φ сюръективен, то для любых $a, b \in K$ найдутся $x, y \in G$ такие, что $\varphi(x) = a$, $\varphi(y) = b$. Тогда

$$[a, b] = [\varphi(x), \varphi(y)] = \varphi([x, y]) \in \varphi(G'). \text{ Значит, } \varphi(G') = K'. \quad \square$$

Следствие 12. Пусть $G \triangleright H$. Тогда $(G/H)' \cong G'/(H \cap G')$.

Доказательство. Применим лемму к сюръективному каноническому гомоморфизму $\pi_H: G \rightarrow G/H$. Получим $(G/H)' = \pi_H(G')$. Рассмотрим ограничение $\pi_H|_{G'}$. Имеем $\text{Ker}(\pi_H|_{G'}) = H \cap G'$, $\text{Im}(\pi_H|_{G'}) = \pi_H(G')$. По теореме о гомоморфизме получаем утверждение следствия. $\square$

Определение 43. Группа G называется *разрешимой*, если существует $n \in \mathbb{N}$ такое, что $G^{(n)} = \{e\}$.

Число n называется *степенью (степенью) разрешимости* G .

Пример 18. Группа G разрешима степени 1 тогда и только тогда, когда G абелева.

Пример 19.

- Группа S_2 разрешима степени 1.
- Группа S_3 разрешима степени 2: $S'_3 = A_3$, $A'_3 = \{\text{id}\}$.
- Группа S_4 разрешима степени 3: $S'_4 = A_4$, $A'_4 = V_4$, $V'_4 = \{\text{id}\}$.
- Группа S_n при $n \geq 5$ не разрешима. Действительно, $S'_n = A_n$, $A'_n = A_n$.

Лемма 36. Подгруппа разрешимой группы разрешима.

Доказательство. Пусть H – подгруппа G . Тогда $H' \subset G'$, $H'' \subset G''$ и т.д. Значит, $H^{(n)} \subset G^{(n)} = \{e\}$. $\square$

Лемма 37. Факторгруппа разрешимой группы разрешима.

Доказательство. Пусть $G \triangleright H$. По следствию 12 выполнено $(G/H)' \cong G'/(H \cap G')$. Применяя эту же формулу, получаем

$$(G'/(H \cap G'))' \cong G''/((H \cap G') \cap G'') = G''/(H \cap G'').$$

Значит, $(G/H)'' \cong G''/(H \cap G'')$. Аналогично, $(G/H)^{(i)} \cong G^{(i)}/(H \cap G^{(i)})$. Поскольку G разрешима, найдется натуральное n такое, что $G^{(n)} = \{e\}$. Тогда $(G/H)^{(n)} = \{e\}$. $\square$

Теорема 25 (Критерий разрешимости группы). Пусть $G \triangleright H$. Тогда G разрешима тогда и только тогда, когда H разрешима и G/H разрешима.

Доказательство. В одну сторону (из разрешимости G следует разрешимость H и G/H) утверждение теоремы сводится к предыдущим леммам.

Пусть теперь H и G/H разрешимы. Как было доказано ранее $(G/H)^{(i)} \cong G^{(i)}/(H \cap G^{(i)})$. Найдется такое натуральное m , что $(G/H)^{(m)} = \{e\}$. Тогда $G^{(m)}/(H \cap G^{(m)}) = \{e\}$, а значит, $G^{(m)} \subset H$. Но поскольку H разрешима, найдется натуральное k такое, что $H^{(k)} = \{e\}$. Следовательно $G^{(m+k)} = \{e\}$. То есть G разрешима. $\square$

Следствие 13. Пусть задан гомоморфизм $\psi: G \rightarrow H$. Тогда G разрешима если и только если $\text{Ker } \psi$ и $\text{Im } \psi$ разрешимы.

Доказательство. Ядро гомоморфизма – нормальная подгруппа, фактор по которой изоморфен образу. $\square$

Предложение 17. Группа B_n невырожденных верхнетреугольных матриц над полем F разрешима.

Доказательство. Пусть U_n – группа верхнетреугольных матриц $n \times n$ с единицами на диагонали. Рассмотрим гомоморфизм $\varphi: B_n \rightarrow (F^\times)^n$,

$$\varphi: \begin{pmatrix} a_1 & * & \dots & * \\ 0 & a_2 & \dots & * \\ \vdots & \vdots & \ddots & * \\ 0 & 0 & \dots & a_n \end{pmatrix} \mapsto (a_1, \dots, a_n)$$

Очевидно, что $\text{Ker } \varphi = U_n$, а $\text{Im } \varphi = (F^\times)^n$. Так как образ – абелева группа, он разрешим. Значит, чтобы доказать разрешимость B достаточно доказать разрешимость U_n .

Рассмотрим гомоморфизм (проверьте это!) $\psi: U_n \rightarrow F^{n-1}$, заданный по правилу

$$\psi: \begin{pmatrix} 1 & b_1 & * & \dots & * \\ 0 & 1 & b_2 & \dots & * \\ \vdots & \vdots & \ddots & \ddots & * \\ 0 & 0 & \dots & 1 & b_{n-1} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \mapsto (b_1, \dots, b_n)$$

Образ ψ лежит в коммутативной группе. Значит, он разрешим. Ядро ψ – подгруппа

$$U_{n1} = \left\{ \begin{pmatrix} 1 & 0 & * & \dots & * \\ 0 & 1 & 0 & \dots & * \\ \vdots & \vdots & \ddots & \ddots & * \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \right\}.$$

Рассмотрим гомоморфизм $\psi_2: U_{n1} \rightarrow F^{n-2}$:

$$\psi_2: \begin{pmatrix} 1 & 0 & c_1 & * & \dots & * \\ 0 & 1 & 0 & c_2 & \dots & * \\ \vdots & \vdots & \ddots & \ddots & \ddots & * \\ 0 & 0 & \dots & 1 & 0 & c_{n-2} \\ 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix} \mapsto (c_1, \dots, c_n).$$

Образ ψ_2 абелев, и значит разрешим, а ядро – подгруппа U_{n2} ,

$$U_{n2} = \left\{ \begin{pmatrix} 1 & 0 & 0 & * & \dots & * \\ 0 & 1 & 0 & 0 & \dots & * \\ \vdots & \vdots & \ddots & \ddots & \ddots & * \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix} \right\}.$$

И т.д. Каждый раз разрешимость U_{ni} сводится к разрешимости $U_{n,i+1}$. Поскольку $U_{n,n-1} = \{e\}$, она разрешима. Это завершает доказательство разрешимости B_n . $\square$

Лемма 38. Пусть H – нормальная подгруппа группы G . Допустим, что в группе G/H есть нормальная подгруппа $\{e\} \subsetneq K \subsetneq G/H$. Тогда $L = \pi_H^{-1}(K)$ – нормальная подгруппа в группе G , причём $H \subsetneq L \subsetneq G$.

Доказательство. Проверим то, что прообраз группы при гомоморфизме является группой. Пусть $l_1, l_2 \in L$. Тогда $\pi_H(l_1 l_2) = \pi_H(l_1) \pi_H(l_2) \in K$. Следовательно, $l_1 l_2 \in L$. Также $\pi_H(l_1^{-1}) = \pi_H(l_1)^{-1} \in K$, значит, $l_1^{-1} \in L$. Кроме того $e \in L$. Значит, L – подгруппа.

Пусть $g \in G, l \in L$. Тогда $\pi_H(g l g^{-1}) = \pi_H(g) \pi_H(l) \pi_H(g)^{-1} \in K$. Значит, $g l g^{-1} \in L$. То есть L нормальна в G .

Так как π_H – сюръекция и $K \neq \{e\}$, получаем $L = \pi_H^{-1}(K) \supsetneq \pi_H^{-1}(e) = H$. Аналогично так как $K \neq G/H$, получаем $L = \pi_H^{-1}(K) \subsetneq \pi_H^{-1}(G/H) = G$. $\square$

Определение 44. Группа G называется *простой*, если у нее нет нормальных подгрупп, отличных от $\{e\}$ и самой G .

Определение 45. Назовем *субнормальным* рядом группы G ряд подгрупп

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 \triangleright \dots \triangleright G_n = \{e\},$$

каждая следующая из которых нормальна в предыдущей. Этот ряд называется *композиционным рядом группы G* , если все факторгруппы G_i/G_{i+1} простые.

Предложение 18. Для конечной группы любой субнормальный ряд может быть уплотнён до композиционного.

Доказательство. Если факторгруппа G_i/G_{i+1} не простая, то по лемме 38 можно уплотнить субнормальный ряд, то есть добавить в него ещё одну подгруппу. Так как группа G конечна, уплотнение не может происходить бесконечно. $\square$

Предложение 19. Абелева группа проста тогда и только тогда, когда она изоморфна $\mathbb{Z}_p$ для простого p .

Доказательство. В абелевой группе все подгруппы являются нормальными. Поэтому абелева группа проста тогда и только тогда, когда в ней нет других подгрупп, кроме $\{e\}$ и G . Для каждого $g \in G$ можно рассмотреть циклическую подгруппу $\langle g \rangle \subset G$. Если $g \neq e$, то $\langle g \rangle \neq \{e\}$. Значит, $\langle g \rangle = G$, то есть G – циклическая. Если $G \cong \mathbb{Z}$, то в ней есть нетривиальные подгруппы $k\mathbb{Z}$. Если же $G \cong \mathbb{Z}_{ab}$, где $a \neq 1$ и $b \neq 1$, то в G есть нетривиальная подгруппа $\langle a \rangle \cong \mathbb{Z}_b$. $\square$

Теорема 26. Пусть G – конечная группа. Следующие условия эквивалентны.

- 1) Группа G разрешима.
- 2) G включается в ряд подгрупп

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 \triangleright \dots \triangleright G_n = \{e\},$$

где G_i/G_{i+1} абелевы.

- 3) G включается в ряд подгрупп

$$G = \tilde{G}_0 \triangleright \tilde{G}_1 \triangleright \tilde{G}_2 \triangleright \tilde{G}_3 \triangleright \dots \triangleright \tilde{G}_m = \{e\},$$

где $\tilde{G}_i/\tilde{G}_{i+1}$ – циклические простого порядка (то есть $\mathbb{Z}_p$ для некоторого простого p).

Доказательство. $1 \Rightarrow 2$. Если G разрешима, можно взять $G_i = G^{(i)}$. Тогда $G_i/G_{i+1} = G^{(i)}/G^{(i+1)}$ – абелева группа.

$2 \Rightarrow 3$. По лемме 38 ряд $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 \triangleright \dots \triangleright G_n = \{e\}$ можно уплотнить до композиционного

$$G = \tilde{G}_0 \triangleright \tilde{G}_1 \triangleright \tilde{G}_2 \triangleright \tilde{G}_3 \triangleright \dots \triangleright \tilde{G}_m = \{e\}.$$

Так как факторгруппы G_i/G_{i+1} абелевы, $G'_i \subseteq G_{i+1}$. Отсюда следует, что $\tilde{G}'_j \subseteq G_{j+1}$. Тогда факторгруппы $\tilde{G}_j/G_{j+1}$ абелевы. По предложению 19, они изоморфны $\mathbb{Z}_p$.

$3 \Rightarrow 1$. Пусть G включается в такой ряд подгрупп. Тогда $G/\tilde{G}_1$ абелева, а значит, $G' \subseteq \tilde{G}_1$. Аналогично $G^{(2)} \subseteq \tilde{G}_2 \dots G^{(m)} \subseteq \tilde{G}_m = \{e\}$. Значит, G разрешима. $\square$

Теорема 27. *Группа A_n проста при $n \geq 5$.*

Сперва докажем следующие две леммы.

Лемма 39. *При $n \geq 5$ все циклы длины 3 сопряжены в A_n .*

Доказательство. Докажем, что любой тройной цикл (a, b, c) сопряжен циклу $(1, 2, 3)$. В S_n эти циклы сопряжены перестановкой

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots \\ a & b & c & u & v & \dots \end{pmatrix},$$

то есть $\sigma(1, 2, 3)\sigma^{-1} = (a, b, c)$. Если σ – четная перестановка, то $(1, 2, 3)$ и (a, b, c) сопряжены в A_n . Если же σ – нечетная перестановка, то рассмотрим

$$\hat{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots \\ a & b & c & v & u & \dots \end{pmatrix} \in A_n.$$

Тогда $\hat{\sigma}(1, 2, 3)\hat{\sigma}^{-1} = (a, b, c)$ $\square$

Лемма 40. *В A_n все пары несмежных транспозиций сопряжены.*

Доказательство. Пусть $\sigma = (a, b)(c, d)$ – пара несмежных транспозиций. Докажем, что σ сопряжена $(1, 2)(3, 4)$. Возьмем

$$\xi = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ a & b & c & d & \dots \end{pmatrix} \in S_n.$$

Тогда $\xi(1, 2)(3, 4)\xi^{-1} = \sigma$. Если $\xi \in A_n$, то $(1, 2)(3, 4)$ и σ сопряжены в A_n . Если же ξ – нечетная перестановка, то рассмотрим

$$\hat{\xi} = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ b & a & c & d & \dots \end{pmatrix} \in A_n.$$

Имеем $\hat{\xi}(1, 2)(3, 4)\hat{\xi}^{-1} = \sigma$, то есть $(1, 2)(3, 4)$ и σ сопряжены в A_n . $\square$

Доказательство теоремы 27. Пусть H – нормальная подгруппа в A_n .

Случай 1. В H есть тройной цикл (abc) . Поскольку H нормальна в A_n , а все тройные циклы в A_n сопряжены (по лемме 39), то все тройные циклы лежат в H . Поскольку A_n порождается тройными циклами (см. лемму 34), $H = A_n$.

Случай 2. В H есть перестановка δ , в разложении которой есть цикл длины не менее 5.

$$\delta = (x_1, x_2, x_3, x_4, x_5, \dots, x_m)(\dots) \dots (\dots)$$

Сопряжем δ с помощью перестановки $\xi = (x_1 x_3)(x_2 x_4)$. Получаем

$$\begin{aligned}\xi\delta\xi^{-1} &= (x_1x_3)(x_2x_4)(x_1, x_2, x_3, x_4, x_5, \dots, x_m)(\dots) \dots (\dots)(x_1x_3)(x_2x_4) = \\ &= (x_3x_4x_1x_2x_5 \dots, x_m)(\dots) \dots (\dots) \in H.\end{aligned}$$

Тогда

$$\begin{aligned}[(x_3, x_4, x_1, x_2, x_5, \dots, x_m)(\dots) \dots (\dots)]^{-1} \circ [(x_1, x_2, x_3, x_4, x_5, \dots, x_m)(\dots) \dots (\dots)] = \\ = (x_2x_mx_4) \in H\end{aligned}$$

Попадаем в случай 1.

Случай 3. В H есть перестановка σ , в разложении которой есть хотя бы два цикла длины 3.

$$\sigma = (a, b, c)(d, e, f) \dots$$

Тогда

$$(a, b, c, d, e)\sigma(a, b, c, d, e)^{-1} = (b, c, d)(e, a, f) \dots = \delta.$$

Имеем $\delta^{-1}\sigma = (a, d, f, c, e)$. Попадаем в случай 2.

Случай 4. В H есть перестановка σ , в разложении которой есть хотя бы три цикла длины 2. Сопряжем $\sigma = (a, b)(c, d)(e, f) \dots$ с помощью (a, b, c, d, e) , получим

$$\delta = (bc)(de)(af) \dots$$

Перемножив $\delta^{-1}\sigma$, получаем $(a, c, e)(b, f, d)$ и попадем в случай 3.

Случай 5. В H есть перестановка, разлагающаяся в 2 цикла длины 2. По лемме 40 там есть все пары несмежных транспозиций. А они порождают A_n .

Случай 6. В H есть перестановка σ , в разложении которой есть циклы длины 2 и 3 при этом есть хотя бы 1 цикл длины 3. Если мы не в условиях случая 3, то в σ есть лишь 1 цикл длины 3. Возведем σ в квадрат, попадем в случай 1.

Случай 7. В H есть перестановка σ , в разложении которой есть циклы длины 2, 3 и 4 при этом есть хотя бы 1 цикл длины 4. Возведем σ в квадрат, попадем в один из случаев 6, 4 или 5.

□