Лекция 1

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

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

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

Рассмотрим бинарную операцию $*$ на множестве G:

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

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

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

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

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

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

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

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

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

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

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

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

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

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 мощьность 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 каждго $g \in H$ есть обратный элемент g^{-1} в группе G и есть обратный элемент обратный элемент $g^{\vee}$ в группе H. Тогда $g * g^{-1} = e = g * g^{\vee}$. Умножив слева на g^{-1}, получаем $g^{-1} = g^{\vee}$. Поскольку для группы $(H, *)$ выполнена аксиома А3, то H замкнуто относительно взятия обратного.

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

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

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

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

г) (Обобщение примера 6а) Пусть X – некоторое множество (возможно бесконечное). Рассмотрим множество $\mathrm{S}(X)$ биекций $X \to X$ с операцией композиции. Если $|X| < \infty$, то получаем группу перестановок. В общем случае получаем *группу симметий множества X*. Нейтральный элемент – тождественное преобразование. Обратный – обратное преобразование. Ассоциативность следует из леммы 1.

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

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

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

в) $\mathrm{O}_n(\mathbb{K})$ – множество ортогональных матриц $n \times n$ с элементами из $\mathbb{K}$. Это подмножество в $\mathrm{GL}(\mathbb{K}$ 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 серидины 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:

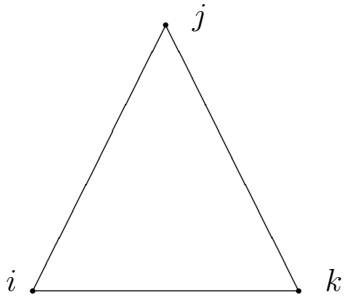
$$\{1, -1, i, -i, j, -j, k, -k\}.$$

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 движение 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 $\varphi\colon G \to H$ 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* $\varphi\colon (G, *) \to (H, \circ)$ *– гомоморфизм. Обозначим через* e_G *и* e_H *единицы группы* G *и* H *соответственно. Тогда*

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

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

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

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

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

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

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

.

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

Определение 7. Биективный гомоморфизм $\varphi\colon G \to H$ 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. Тождественное преобразование задает изоморфизм любой группы с собой. Рефлексивность доказана. Если $\varphi\colon G \to H$ – 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 $\varphi\colon G \to H$ и $\psi\colon H \to F$ – 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. □

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* $\varphi\colon \mathbb{R} \to \mathbb{R}_{>0}$, $\varphi(x) = 2^x$. *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* $\mathrm{GL}_n(\mathbb{C})$ *изоморфна группе невырожденных линейных преобразований векторного пространства* $\mathbb{C}^n$ *с операцией композиции. Чтобы получить изоморфизм между этими группами нужно выбрать некоторый базис в* $\mathbb{C}^n$ *и отобразить линейное преобразование в его матрицу в этом базисе.*

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* $\varphi\colon G \to H$ *– 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

$$h_1(h_2h_3) = \varphi(g_1)(\varphi(g_2)\varphi(g_3)) = \varphi(g_1)\varphi(g_2g_3) =$$
$$= \varphi(g_1(g_2g_3)) = \varphi((g_1g_2)g_3) = \varphi(g_1g_2)\varphi(g_3) = (\varphi(g_1)\varphi(g_2))\varphi(g_3) = (h_1h_2)h_3.$$

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. □

Теперь мы готовы доказать, что Q_8 – группа.

Предложение 2. *Q_8 – группа*

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

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

Здесь i – это мнимая единица (комплексное число).

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

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

Легко убедиться, что φ переводит умножение в Q_8 в матричное умножение. Следовательно, $(\overline{Q}_8, \cdot)$ – это замкнутое относительно умножения и взятия обратной матрицы подмножество в $\mathrm{GL}_2(\mathbb{C})$. Значит, $\overline{Q}_8$ – подгруппа. Тогда, по теореме 2, Q_8 – группа, изоморфная $\overline{Q}_8$. □

Особый интерес представляют гомоморфизмы и изоморфизмы из группы в себя.

Определение 8. Гомоморфизм $\varphi\colon G \to G$ называется *эндоморфизмом*. Изомомрфизм $\varphi\colon G \to G$ называется *автоморфизмом*.

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

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

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

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

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

Лекция 3

Предложение 4. Простые следствия из аксиом.

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

2) В моноиде есть единственная единица.

3) В группе для каждого элемента есть единственный обратный.

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

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

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

Доказательство. 1) Докажем это утверждение индукцией по k.

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

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

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

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. Длиной скобки назовем количество g_i, входящих в нее. Обозначим длину правой скобки через s.

Случай 1 $s = 1$. Наша расстановка скобок имеет вид $(\ldots) * g_n$. 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 $g=(g^{-1})^{-1}$. □

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

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

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 $k\neq\pm1$ гомоморфизм ψ не будет сюръективен. При $k=1$ и $k=-1$ получаем тождественное отображение и отображение $\{x\mapsto -x\}$. Легко видеть, что эти два автоморфизма с операцией композиции образуют группу, изоморфную $\mathbb{Z}_2$.

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

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

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

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

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

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

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

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

Образом гомоморфизма φ называется множество

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

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

Лемма 4. *Пусть $\varphi\colon G\to H$ – гомоморфизм. Тогда*

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

б) $\mathrm{Im}\,\varphi$ *– подгруппа в* H.

Доказательство. а) Пусть $g_1,g_2\in\mathrm{Ker}\,\varphi$. Тогда $\varphi(g_1g_2)=\varphi(g_1)\varphi(g_2)=ee=e$. Значит, $g_1g_2\in\mathrm{Ker}\,\varphi$. 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, $g_1^{-1}\in\mathrm{Ker}\,\varphi$. Таким образом, ядро замкнуто относительно взятия обратного. Осталось заметить, что $e\in\mathrm{Ker}\,\varphi$. Следовательно, $\mathrm{Ker}\,\varphi$ – подгруппа в G.

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

Теорема 4. *(Критерий инъективности гомоморфизма) Гомоморфизм $\varphi\colon G \to H$ инъективен тогда и только тогда, когда $\operatorname{Ker}\varphi = \{e\}$.*

Доказательство. Пусть $\operatorname{Ker}\varphi \neq \{e\}$. Тогда существует $g \neq e$, $g \in \operatorname{Ker}\varphi$. 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 $g_1 g_2^{-1} \in \operatorname{Ker}\varphi$, но $g_1 g_2^{-1} \neq e$. Значит, $\operatorname{Ker}\varphi \neq \{e\}$. □

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

Упражнение 2. Выполнены следующие свойства степеней элемента группы:
1) $g^m g^n = g^{m+n}$,
2) $(g^m)^n = g^{mn}$
Указание. Рассмотреть все случаи знаков m и n.

Определение 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 $\operatorname{ord}(g)$.

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

Доказательство. Пусть $\operatorname{ord} g = n$. Рассмотрим множество элементов

$$S = \{g^0 = e, g, g^2, \ldots g^{n-1}\}.$$

Докажем, что все элементы группы $\langle g \rangle$ лежат в S и что все элементы S различны. В самом деле, пусть g^k – некоторый элемент $\langle g \rangle$. Разделим k на n с остатком: $k = nm + r$, где $0 \leq k < n$. Тогда $g^k = (g^n)^m g^r = g^r \in S$.

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

Рассмотрим отображение $\psi\colon \mathbb{Z}_n \to \langle g\rangle$, $\psi(k) = g^k$. 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 $0, 1, \ldots, n-1$. 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 $\operatorname{ord} g = \infty$. Рассмотрим отображение $\psi\colon \mathbb{Z} \to \langle g\rangle$, $\psi(k) = g^k$. 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 $\operatorname{ord} g = \infty$. Итак, ψ – гомоморфизм и биекция, то есть изоморфизм. □

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* $\operatorname{ord} g = n$, *а m – целое число. Тогда*

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

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

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 $\operatorname{ord}(m) = k$, если k – это минимальное натуральное число такое, что $mk = 0$ в $\mathbb{Z}_n$. Для целых чисел условие перепишется 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. □

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

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, $\mathrm{ord}(m) = \frac{n}{\text{НОД}(m,n)}$. Значит $|\langle m \rangle| = \frac{n}{\text{НОД}(m,n)}$. Следовательно, по пункту 3), $\langle m \rangle = \langle \text{НОД}(m, n) \rangle$. □

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

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

Правым смежным классом элемента g по подгруппе H называется множество

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

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

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

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

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

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

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

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

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

Симметричность:

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

Транзитивность:

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

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

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

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

Задача 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. □

Следствие 1. *(Следствия из теоремы Лагранжа)*

1) Порядок конечной группы делится на порядок ее подгруппы.

2) Порядок конечной группы делится на порядок ее элемента.

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

4) Группа простого порядка циклическая.

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

Доказательство. 1) Очевидно следует из теоремы Лагранжа.

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

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

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

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

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

□

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

$2 \Longrightarrow 3$ Очевидно.

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

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

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

Пример 8. *Подгруппа* $\langle (1,2) \rangle = \{\mathrm{id}, (1,2)\} \subseteq S_3$ *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

$$(g_1 H) \cdot (g_2 H) = (g_1 g_2) H.$$

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 $g_1 H = g_1' H$, $g_2 H = g_2' H$, но при этом смежный класс $g_1 g_2 H$ может не совпадать с $g_1' g_2' H$. 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 $g_1 H = g_1' H$, $g_2 H = g_2' H$. Получаем, что $g_1'^{-1} g_1 \in H$ и $g_2'^{-1} g_2 \in H$. Обозначим $g_1'^{-1} g_1$ через h. Имеем

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

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

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

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

Пример 9. *Найдем, 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* $k+n\mathbb{Z} = l+\mathbb{Z}$ *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 $\varphi \colon G \to \widetilde{G}$ – гомоморфизм групп.

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

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

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

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

Определение 17. Рассмотрим следующее отображение $\pi_H \colon G \to G/H$, $g \mapsto gH$. Из определения операции в факторгруппе следует, что π_H – гомоморфизм. Легко видеть, что он сюръективен. Гомоморфизм π_H называется *каноническим гомоморфизмом.*

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

Теорема 7. *(Теорема о гомоморфизме) Пусть* $\varphi \colon G \to \widetilde{G}$ *– гомоморфизм групп. Тогда* $G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.

Доказательство. Рассмотрим отображение

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

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

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

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

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

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

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

Пример 10. *Найдем, чему изоморфна факторгруппа* $\mathbb{Z}/n\mathbb{Z}$ *по теореме о гомоморфизме. Для того, чтобы применить теорему о гомоморфизме, нам нужно построить гомоморфизм* $\varphi \colon Z \to G'$ *для некторой группы* G' *такой, что* $\operatorname{Ker}\varphi = n\mathbb{Z}$. *Легко видеть, что подходит следующий гомоморфизм*

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

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

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

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

Предложение 6. *Факторгруппа группы G по центру изоморфна группе внутренних атоморфизмов* $\mathrm{Inn}(G)$.

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

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

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. □

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

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

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

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

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

По теореме о гомоморфизме получаем следующий изоморфизм:

$$S_4/V_4 \cong S_3.$$

Лемма 12. *Пусть G – группа, $H \lhd G$ – нормальная подгруппа, $K \subset G$ – подгруппа. Тогда $\langle K \cup H \rangle = KH = \{kh \mid k \in K, h \in H\}$.*

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

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

Теперь докажем, что KH замкнуто относительно взятия обратного:

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

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

Теорема 8. *(Вторая теорема о гомоморфизме) Пусть G – группа, $H \lhd G$ – нормальная подгруппа, $K \subset G$ – подгруппа.*
1) $H \cap K$ – нормальная подгруппа в K и H – нормальная подгруппа в KH,
2) $KH/H \cong K/(H \cap K)$.

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

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

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

Лекция 7

Теорема 9. *(Третья теорема о гомоморфизме) Пусть $\varphi\colon G \to \widetilde{G}$ – сюръективный гомоморфизм, $K = \operatorname{Ker}\varphi$, $\widetilde{H} \subset \widetilde{G}$ –подгруппа. Пусть $H = \varphi^{-1}(\widetilde{H})$ – полный прообраз. Тогда*

1) $\widetilde{H} \leftrightarrow H$ – биекция между подгруппами в $\widetilde{G}$ и подгруппами в G, содержащими K.

2) Подгруппа H нормальна в G тогда и только тогда, когда $\widetilde{H}$ нормальна в $\widetilde{G}$.

3) Если H и $\widetilde{H}$ нормальны, то $G/H \cong \widetilde{G}/\widetilde{H}$.

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

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

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

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

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

Менее формально можно написать

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

Доказательство. Гомоморфизм $\pi_N\colon G \to G/N$ 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 $\operatorname{Ker}\pi_N = N$, $\pi_N(H) \cong H/N$. По пункту 3) третьей теоремы о гомоморфизме

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

□

Пример 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 $\varnothing$. Два слова назовем *эквивалентными*, если одно переводится в другое некой конечной цепочкой следующих элементарных преобразований:

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

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

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

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

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

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

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 $g_1, \ldots, g_k$. Существует единственный гомоморфизм из свободной группы $\mathfrak{F}(x_1, \ldots, x_k)$ ранга k в группу G такой, что $\varphi(x_i) = g_i$. Гомоморфизм φ сюръективен.*

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

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

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 $g_1, \ldots, g_k$. □

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

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

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

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

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

При этом

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

□

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

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

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 $\varphi\colon \langle x_1, x_2\rangle \to D_n$, $x_1 \mapsto a, x_2 \mapsto b$ ядро содержит $N(x_1^2, x_2^2, (x_1x_2)^n)$. Наша цель – доказать, что $\operatorname{Ker}\varphi = N(x_1^2, x_2^2, (x_1x_2)^n)$. Если это не так, то по следствию 3 имеем:

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

Тогда порядок группы G будет строго меньше, чем $H = \langle a, b \mid a^2, b^2, (ab)^n\rangle = \langle x_1, x_2\rangle/N(x_1^2, x_2^2, (x_1x_2)^n)$. Докажем, что в H не более $2n$ элементов. Легко видеть, что любой элемент H может быть записан либо в виде конечного слова $abab\dots$, либо в виде $baba\dots$. 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 $baba\dots$ 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 $baba\dots$ представляются словами вида $abab\dots$. Значит, $|H| \leq 2n$. Отсюда следует, что $D_n = H$.