Лекция 1

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

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

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

Рассмотрим бинарную операцию $*$ на множестве G:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Рассмотрим некоторые элементарные следствия из аксиом.

Лемма 1. Простые следствия из аксиом.

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

2) В моноиде есть единственная единица.

3) В группе для каждого элемента есть единственный обратный.

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

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

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

Доказательство. 1) Докажем это утверждение индукцией по k.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Подмножество S группы $(G, *)$ называется *замкнутым относительно операции* $*$, если для любых $a, b \in S$ выполнено $a*b \in S$. Подмножество S группы $(G, *)$ называется

замкнутым относительно взятия обратного, если для любого $s \in S$ элемент s^{-1} также принадлежит S.

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

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

Пусть теперь подмножество H замкнуто относительно операции и взятия обратного. Так как H замкнуто относительно операции, $(H, *)$ – группоид. Поскольку ассоциативность выполнена в G, то она выполнена и в H. Подмножество не пусто. 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. □

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

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

Соберем эти обозначения в таблице.

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

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

Определение 6. Пусть g – элемент группы G, а n – целое число. Определим n-ю степень элемента g следующим образом. Если n положительное, то $g^n = g \cdot \ldots \cdot g$ – произведение n элементов g. Если n отрицательное, то $g^n = (g^{-1})^n$. Нулевая степень любого элемента равна нейтральному элементу e.

Упражнение 2. Выполнены следующие свойства степеней элемента группы:

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

Указание. Рассмотреть все случаи знаков m и n.

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

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

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

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

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

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

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

Отсюда

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

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

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

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

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

$+$	0	1
0	0	1
1	1	0

Примеры групп.

1) Числовые аддитивные группы:

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

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

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

3) Числовые мультипликативные группы:

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

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

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

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

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

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

6) Группы перестановок.

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

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

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

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

С другой стороны

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

□

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

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

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

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

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

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

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

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

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

а) Группа обратимых линейных преобразований V.

б) Группа ортогональных линейных преобразований V.

в) Группа обратимых аффинных преобразований V.

г) Группа движений V.

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

Лекция 2

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

Докажем следующие элементарные свойства гомоморфизма.

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

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

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

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

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

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

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

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

.

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

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

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

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

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

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

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

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

Группа кватернионов Q_8. Рассмотрим множество из 8 элементов:

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

Умножение устроено следующим образом: знаки умножаются отдельно,

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

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

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

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

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

Здесь i – это мнимая единица (комплексное число).

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

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

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

Еще один важный пример группы дает следующая конструкция.

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

Упражнение 3. а) Докажите, что в группе D_n ровно $2n$ элементов. Среди них n поворотов и n осевых симметрий. Все оси симметрий проходят через центр n- угольника. Если n 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.

Можно конструировать группу из уже известных с помощью следующей конструкции.

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

Особый интерес представляют гомоморфизмы и изоморфизмы из группы в себя.

Определение 11. Гомоморфизм $\varphi\colon G \to G$ называется *эндоморфизмом*. Изомомрфизм $\varphi\colon G \to G$ называется *автоморфизмом*.

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

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

Лемма 5. *Отображение φ_g является автоморфизмом группы G.*

Доказательство. Проверим, что φ_g – гомоморфизм:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Легко видеть, что ψ – изоморфизм. □

Теорема 2. *1) Подгруппа циклической группы циклическая.*
2) Все подгруппы в $\mathbb{Z}$ имеют вид $k\mathbb{Z}$.
3) Все подгруппы в $\mathbb{Z}_n$ имеют вид $\langle d \rangle = d\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{d}}$, где d делитель числа n. В частности, для каждого делителя q числа n есть ровно одна подгруппа в $\mathbb{Z}_n$, изоморфная $\mathbb{Z}_q$, а именно, $\langle \frac{n}{q} \rangle$.
4) Пусть $m \in \mathbb{Z}_n$, тогда $\langle m \rangle = \langle НОД(m, n) \rangle$.

Доказательство. 1) Пусть $G = \langle g \rangle$ и пусть H – некоторая подгруппа в G. Если $H = \{e\}$, то утверждение доказано. Пусть $H \ne \{e\}$. Если $g^k \in H$, то $g^{-k} \in H$. Значит существует положительное число k такое, что $g^k \in H$. Пусть l – наименьшее положительное число такое, что $g^l \in H$. Рассмотрим некоторое m такое, что $g^m \in H$. Разделим

m на l с остатком: $m = ls + r$, где $0 \leq r < l$. Получаем $g^r = g^m(g^l)^{-s} \in H$. Поскольку l минимальное положительное число такое, что $g^l \in H$, получаем $r = 0$. То есть в G все элементы имеют вид $(g^l)^s$, значит $G = \langle g^s \rangle$.

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

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

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

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

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

Лекция 3

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Правым смежным классом элемента g по подгруппе H называется множество

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

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

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

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

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

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

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

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

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

Симметричность:

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

Транзитивность:

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

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

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

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

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

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

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

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

Следствие 1. *(Следствия из теоремы Лагранжа)*

1) Порядок конечной группы делится на порядок ее подгруппы.

2) Порядок конечной группы делится на порядок ее элемента.

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

4) Группа простого порядка циклическая.

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

Доказательство. 1) Очевидно следует из теоремы Лагранжа.

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

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

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

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

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

□

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

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

Доказательство. Рассмотрим множество

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

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

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

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

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

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

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

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

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

Лемма 8. *Следующие условия равносильны:*

1) $G \triangleright H$,

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

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

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

$2 \Longrightarrow 3$ Очевидно.

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

Лекция 4

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Доказательство. Рассмотрим отображение

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

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

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

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

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

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

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

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

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

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

Определение 19. Пусть группа G содержит подмножество S. *Подгруппой, 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 10. *Пусть $G = \langle S\rangle$, тогда G совпадает с множеством конечных произведений элементов из S и обратных к ним, то есть*

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

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

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

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

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

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

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

По теореме о гомоморфизме получаем следующий изоморфизм:

$$S_4/V_4 \cong S_3.$$

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

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

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

Теперь докажем, что KH замкнуто относительно взятия обратного:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Лекция 5

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

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

При этом

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

□

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

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

В таком случае пишут

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

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

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

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

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

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

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

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

Лекция 6

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

Один из способов решить проблему равенства слов – это определить некий канонический вид, к которому можно привести каждое слово, 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 10. *В каждом классе эквивалентности есть только одно несократимое слово.*

Доказательство. Пусть есть два различных несократимых слова u и v, которые эквивалентны. Рассмотрим цепочку элементарных преобразований, переводящих u в v. Пусть в этой цепочке есть сокращение, идущее после приписывания. Докажем, что эту пару можно заменить либо на пару сокращение, а затем приписывание, либо убрать. В самом деле если ни один из 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. □

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

Внутреннее прямое произведение подгрупп.

Напомним, что прямым произведением групп K и H мы называли множество пар $(k, H) \mid k \in K, h \in H$ с покомпонентным умножением. 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. *Пусть K и H – подгруппы в G. Следующие условия эквивалентны:*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Доказательство. Рассмотрим отображение

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

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

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

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

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

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

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

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

1) НОД$(m, n) = 1$;

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

Доказательство. $1 \Rightarrow 2$. Рассмотрим

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

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

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

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

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

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

Лекция 7

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

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

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

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

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

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

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

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

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

Задача 6. Докажите, что

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

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

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

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

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

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

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

Домножим это равенство на произведение знаменателей и получим

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

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

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

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

Доказательство. Докажем это утверждение индукцией по n.

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

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

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

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

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

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

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

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

причем $\varphi(x_i) = a_i$.

Доказательство. Подходит гомоморфизм определенный по правилу

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

□

Применяя теорему о гомоморфизме, получаем следствие.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Случай 3. Все элементы первой строки и первого столбца делятся на p_{11}, но есть p_{ij}, не делящийся на p_{11}. Прибавим первую строку и первый столбец к остальным так, чтобы все элементы, кроме p_{11} стали равны нулю. При этом p_{ij} 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. □

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

□

Следствие 5. *Любая конечно порожденная абелева группа изоморфна*

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

где u_i делится на u_j, если $i > j$.

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

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

Применяя теорему о факторизации прямого произведения, получаем

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

□

Лекция 8

Докажем следующую полезную лемму.

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

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

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

По следствию 5 каждая конечно порожденная абелева группа A изоморфна

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

По теореме о факторизации прямого произведения

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

То есть

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

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

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

Доказательство. Пусть есть абелева группа A, у которой есть две различные первые канонические формы Φ_1 и Φ_2. Так как ранг свободной группы $A/\mathrm{Tor}\,A$ 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 15. □

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

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

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

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

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

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

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

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

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

Лекция 9

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

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

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

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

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

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

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

Очевидным следствием предыдущего предложения является следующее утверждение.

Следствие 7. *Мультипликативная группа конечного поля циклическая.*

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

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

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

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

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

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

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

Такое действие называется тавтологическим.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Следующие два определения играют центральную роль в теории действий.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

Лекция 10

Определение 36. *Ядро неэффективности* действия $\alpha\colon G \times X \to X$ – это множество $\mathrm{Ker}\,\alpha = \{g \in G \mid \forall x \in X :\ g \cdot x = x\}$. 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 $\operatorname{Ker}\alpha$ совпадает с ядром гомоморфизма $\operatorname{Ker}\varphi_\alpha$. □

Предложение 11. *Действия группы G на X с ядром неэффективности, содержащим H, находятся в биекции с действиями G/H на X.*

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

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 $\psi\colon G/H \to S(X)$. Если взять композицию с каноническим гомоморфизмом

$$\pi_H\colon G \to G/H,$$

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

Определение 37. Действия $\alpha\colon G \times X \to X$ и $\beta\colon G' \times Y \to Y$ называются *изоморфными*, если существуют изоморфизм $\varphi\colon G \to G'$ и биекция $\psi\colon X \to Y$ такие, что $\beta(\varphi(g), \psi(x)) = \psi(\alpha(g, x))$ для любых $g \in G$ и $x \in X$.

Определение 38. 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 39. Действие называется *свободным*, если стабилизатор каждого элемента $x \in X$ тривиален, то есть равен $\{e\}$.

Теорема 17. *Любое свободное транзитивное действие группы G на некотором множестве изоморфно действию G на себе левыми сдвигами.*

Доказательство. Пусть $\beta\colon G \times X \to X$ – свободное транзитивное действие. Пусть $\alpha\colon G \times G \to G$, $g \cdot g' = gg'$ – действие G правыми сдвигами на себе. Рассмотрим любой элемент $y \in X$. Определим отображение $\psi\colon G \to X$ 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 $g^{-1}g' \in \operatorname{St}(y)$. Но так как действие β свободно, получаем $\operatorname{St}(y) = \{e\}$, а значит, $g^{-1}g' = e$, то есть $g = g'$.

Положим $\varphi\colon G \to G$ тождественным отображением $\varphi = \mathrm{id}$. Тогда

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

С другой стороны

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

Таким образом,

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

то есть действия α и β изоморфны. □

Теорема 18 (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 $\varphi_\alpha\colon G \to S(G) \cong S_n$. (Явно этот гомоморфизм задается по правилу: элемент g переходит в биекцию $\overline{g} \mapsto g\overline{g}$ из G в G.) При этом ядро φ_α равно ядру неэффективности α. Но легко видеть, что $\mathrm{St}(e) = \{e\}$, а значит, $\mathrm{Ker}\,\alpha = \{e\}$. Значит, φ_α задает вложение G в S_n. □

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 $Cent(g)$. Следствие 9, примененное к действию G на себе сопряжениями, дает формулу $|C(g)| \cdot |Cent(g)| = |G|$.

Замечание 13. 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 $Cent_G(g) \neq Cent_H(g)$. Однако легко видеть, что всегда имеются включения в одну сторону: $C_H(g) \subset C_G(g)$, $Cent_H(g) \subset Cent_G(g)$.

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 $C(h) \subset H$. □

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 it 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:

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

В самом деле $\pi\colon \{1, 2, , \dots, n\} \to \{1, 2, \dots, n\}$ – 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 7. Найдите все нормальные подгруппы в S_4.

Задача 8. Пусть $\sigma \in A_n$.

а) Докажите, что $C_{S_n}(\sigma)$ либо совпадает с $C_{A_n}(\sigma)$, либо есть объединение двух классов сопряженности в A_n.

б) Как по перестановке $\sigma \in A_n$ определить, какой из случаев пункта а) реализуется?

Определение 40. 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

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

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, $Z(G) \neq \{e\}$. □

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 5. □

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

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

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. Приравнивая ко второму выражению для $|M|$ и разделив на $|G|$, получаем утверждение леммы. □

Замечание 14. 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 13. *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 врешины 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

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

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

Предложение 12. *Группа вращений куба изоморфна S_4.*

Доказательство. Группа $\mathrm{Sym}_+(K)$ 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 $\varphi\colon \mathrm{Sym}_+(K) \to S_4$. Поскольку $|\mathrm{Sym}_+(K)| = |S_4| = 24$, 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 $\xi \in \mathrm{Sym}_+(K)$.

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

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 13. *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. □

Лекция 11

Определение 41. 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 15. Обратный элемент к коммутатору является коммутатором. В самом деле:

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

Определение 42. *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 $[x, y] \neq e \in G'$. □

Лемма 32. *Сопряженный к коммутатору элемент является коммутатором.*

Доказательство.

$$\begin{aligned} g[x,y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = \\ = gx(g^{-1}g)y(g^{-1}g)x^{-1}(g^{-1}g)y^{-1}g^{-1} = \\ = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) = \\ = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} = [gxg^{-1}, gyg^{-1}]. \end{aligned}$$

□

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

Доказательство. Любой элемент G' имеет вид $[x_1, y_1] \cdot [x_2, y_2] \cdot \ldots \cdot [x_n, y_n]$. Тогда

$$\begin{aligned} g[x_1,y_1][x_2,y_2]\ldots[x_n,y_n]g^{-1} = \\ = g[x_1,y_1](g^{-1}g)[x_2,y_2](g^{-1}g)\ldots(g^{-1}g)[x_n,y_n]g^{-1} = \\ = (g[x_1,y_1]g^{-1})(g[x_2,y_2]g^{-1})\ldots(g[x_n,y_n]g^{-1}) = \\ = [gx_1g^{-1}, gy_1g^{-1}]\ldots[gx_ng^{-1}, gy_ng^{-1}]. \end{aligned}$$

□

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 20. *G' – минимальная нормальная подгруппа, фактор по которой абелев. (То есть, если $G \triangleright H$ и группа G/H – абелева группа то $G' \subset H$.)*

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

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

С другой стороны, 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 $G' \subset H$. □

Теорема 21. $S'_n = A_n$.

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 следующей леммы.

Лемма 34. *A_n порождается тройными циклами.*

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

□

Теорема 22. *1)* $A'_3 = \{id\}$,
2) $A'_4 = V_4$,
3) $A'_n = A_n$ *при* $n \geq 5$.

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

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

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

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 следующей леммы.

Лемма 35. *При $n \geq 5$ группа A_n порождается парами несмежных транспозиций $(i,j)(k,s)$.*

Доказательство. 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 23. *Пусть F – поле такое, что $|F| \geq 4$. Тогда*
1) $\mathrm{SL}_n(F)' = \mathrm{SL}_n(F)$
2) $\mathrm{GL}_n(F)' = \mathrm{SL}_n(F)$

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 есть a^{-1} и для любого $\mu \in F$ существует $\lambda = (a^2 - 1)^{-1}$. Заметим, что

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

$$= \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} a & a\lambda \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}\lambda \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & (a^2-1)\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$$

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

Группа $\mathrm{SL}_n(F)$ порождается элементами вида $E + \mu E_{ij}$. В самом деле, любую матрицу A из $\mathrm{SL}_n(F)$ 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) $\mathrm{GL}_n(F)' \supset \mathrm{SL}_n(F)' = \mathrm{SL}_n(F)$.

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

Лемма 36. *Пусть $\varphi\colon G \to K$ – 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

$[a,b] = [\varphi(x), \varphi(y)] = \varphi([x,y]) \subset \varphi(G')$. Значит, $\varphi(G') = K'$. □

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

Доказательство. Применим лемму к сюръективному каноническому гомоморфизму $\pi_H\colon G \to G/H$. Получим $(G/H)' = \pi_H(G')$. Рассмотрим ограничение $\pi_H \mid_{G'}$. Имеем $\mathrm{Ker}(\pi_H \mid_{G'}) = H \cap G'$, $\mathrm{Im}(\pi_H \mid_{G'}) = \pi_H(G')$ По теореме о гомоморфизме получаем утверждение следствия. □

Определение 43. Подгруппа $H \subset G$ называется *характеристической*, если для любого автоморфизма $\varphi\colon G \to G$ выполнено $\varphi(H) = H$.

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

Лемма 37. *Характеристическая подгруппа характеристической подгруппы является характеристической.*

Доказательство. Пусть H – характеристическая подгруппа G, а N – характеристическая подгруппа H. Пусть $\varphi \in \mathrm{Aut}(G)$. Тогда $\varphi(H) = H$. Поскольку $\varphi^{-1}(H) = H$, получаем, что $\varphi \mid_H\colon H \to H$ – автоморфизм H. Значит, поскольку N характеристическая, $\varphi(N) = \varphi \mid_H (N) = N$. □

Замечание 16. Напомним, что нормальная подгруппа нормальной подгруппы не всегда нормальна.

Предложение 14. *Коммутант и центр – характеристические подгруппы.*

Доказательство. Пусть G – группа. Рассмотрим $z \in Z(G)$, и пусть $\varphi \in \mathrm{Aut}(G)$. 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

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

□

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

Лекция 12

Определение 44. Группа G называется *разрешимой*, если существует $n \in \mathbb{N}$ такое, что $G^{(n)} = \{e\}$.

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

Пример 14. *Группа G разрешима ступени 1 тогда и только тогда, когда G абелева.*

Пример 15.

- *Группа S_2 разрешима ступени 1.*
- *Группа S_3 разрешима ступени 2: $S_3' = A_3$, $A_3' = \{\mathrm{id}\}$.*
- *Группа S_4 разрешима ступени 3: $S_4' = A_4$, $A_4' = V_4$, $V_4' = \{\mathrm{id}\}$.*
- *Группа S_n при $n \geq 5$ не разрешима. Действительно, $S_n' = A_n$, $A_n' = A_n$.*

Лемма 38. *Подгруппа разрешимой группы разрешима.*

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

Лемма 39. *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 $(G/H)^{(n)} = \{e\}$. □

Теорема 24 (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. □

Следствие 13. *Пусть задан гомоморфизм $\psi\colon G \to H$. Тогда G разрешима если и только если $\operatorname{Ker}\psi$ и $\operatorname{Im}\psi$ разрешимы.*

Доказательство. Ядро гомоморфизма – нормальная подгруппа, фактор по которой изоморфен образу. □

Предложение 15. *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 $\varphi\colon B_n \to (F^\times)^n$,

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

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

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

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

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 $\psi_2\colon U_{n1} \to F^{n-2}$:

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

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. □

Теорема 25. *Группа G разрешима тогда и только тогда, когда она 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.

Доказательство. Если G разрешима, можно взять $G_i = G^{(i)}$.

Пусть G включается в такой ряд подгрупп. Тогда G/G_1 абелева, а значит, $G' \subset G_1$. Для доказательства разрешимости G достаточно доказать разрешимость G', а для этого достаточно доказать разрешимость G_1.

Аналогично, разрешимость G_1 сводится к разрешимости G_2 и т.д. Так как $G_n = \{e\}$, она разрешима. Следовательно, G разрешима. □

Определение 45. Группа G называется *простой*, если у нее нет нормальных подгрупп, отличных от $\{e\}$ и самой G.

Предложение 16. *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 $\langle a \rangle \cong \mathbb{Z}_b$. □

Теорема 26. *Группа A_n проста при $n \geq 5$.*

Сперва докажем следующие две леммы.

Лемма 40. *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

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

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

Лемма 41. *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

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

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

Доказательство теоремы 26. 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 40), 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 $\xi = (x_1x_3)(x_2x_4)$. Получаем

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

Тогда

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

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 41 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 случев 6, 4 или 5.

□

Замечание 17. При доказательстве теоремы 26 можно было воспользоваться теоремой Коши. Пусть в A_n есть некоторая нормальная подгруппа H и $|H|$ делится на простое число p. Тогда в H есть элемент σ порядка p. Если $p \geq 5$, то попадаем в случай 2. Если $p = 2$, то σ раскладывается в независимые циклы длины 2 и попадаем либо в случай 4, либо в случай 5. Если $p \geq 3$, то аналогично попадаем в случай 1 или 3. Это рассуждение избавляет от необходимости рассматривать случаи 6 и 7.

Лекция 13

Определение 46. Группа SO(3) – это всех ортогональных преобразований трехмерного вещественного пространства, сохраняющих ориентацию (то есть определитель матрицы равен 1).

В ортонормированном базисе матрицы преобразований из SO(3) – это ортогональные матрицы ($A^T = A^{-1}$) с определителем 1.

В курсе линейной алгебры доказывалось, что матрица элемента из SO(3) может быть приведена в ортонормированном базисе к виду

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

То есть любой элемент SO(3) – это поворот вокруг некоторой оси.

Лемма 42. *Пусть $h \in$ SO(3) – поворот на угол θ вокруг оси l. Тогда сопряженный элемент ghg^{-1} – это поворот на угол θ вокруг оси $g(l)$.*

Доказательство. У матрицы поворота на угол θ комплексные собственные значения равны 1, $\cos\theta + i\sin\theta$ и $\cos\theta - i\sin\theta$. Ясно, что у сопряженного оператора комплексные собственные значения такие же. Это доказывает равенство углов. Осталось объяснить, что ось вращения будет $g(l)$.

Пусть v – собственный вектор оператора h с собственным значением 1 (v направлен вдоль оси l). Тогда $(ghg^{-1})(gv) = ghv = gv$, то есть gv – собственный вектор с собственным значением 1 у оператора ghg^{-1}. Вектор gv направлен вдоль оси $g(l)$. □

Лемма 43. *Композиция двух поворотов на угол π с углом между осями l и l' равным α, равна повороту относительно оси m, перпендикулярной l и l', на угол 2α.*

Доказательство. Ось m переворачивается при каждом из данных поворотов, а значит, в итоге с осью m происходит тождественное преобразование. Ось l при первом повороте остается неподвижной, а при втором повернется на угол 2α. □

Теорема 27. *Группа* SO(3) *проста.*

Доказательство. Пусть $H \neq \{\mathrm{id}\}$ – нормальная подгруппа в SO(3). Найдется поворот $h \in H$ на угол $\alpha \in (0, 2\pi)$ вокруг оси l. Пусть g – поворот на угол π вокруг оси m, образующей с осью l угол $\beta \in [0, \frac{\pi}{2}]$. Тогда $s = g(hg^{-1}h^{-1}) = (ghg^{-1})h^{-1} \in H$. При этом $hg^{-1}h^{-1}$ – поворот на угол π вокруг оси $h(m)$, которая образует с осью m угол γ. А значит, s – поворот на угол 2γ вокруг оси, перпендикулярной m и $h(m)$.

Угол γ равен 0 при $\beta = 0$ и равен α при $\beta = \frac{\pi}{2}$. По соображениям непрерывности угол γ может принимать все значения от 0 до α, то есть в H найдутся повороты на все углы от нуля до α. Рассматривая степени данных поворотов, получим повороты на все углы. По лемме, если в H лежит поворот на некий угол, то там лежат и все повороты на данный угол. Значит, $H = \mathrm{SO}(3)$. □

Рассмотрим действие группы G на множестве всех подгрупп в группе G сопряжениями. В самом деле, легко убедиться, что если $H \subset G$ – подгруппа, то gHg^{-1} также подгруппа.

Определение 47. Стабилизатор подгруппы H при данном действии называется *нормализатором* H в G и обозначается $N_G(H)$.

Лемма 44. *1) $N_G(H)$ – подгруппа в G, содержащая H,*
2) H нормальна в $N_G(H)$,
3) Если H нормальна в K, где K – подгруппа G, то $K \subset N_G(H)$.

Доказательство. 1) По определению, $N_G(H)$ – стабилизатор, а значит, подгруппа в G.
2) При $g \in N_G(H)$ имеем $gHg^{-1} = H$, это доказывает нормальность H в $N_G(H)$.
3) Если $H \triangleleft K$, то для любого $k \in K$ выполнено $kHk^{-1} = H$, то есть

$$k \in St(H) = N_G(H).$$

□

Определение 48. Пусть G – конечная группа порядка $|G| = p^k m$, где p – простое число, а m – число не делящееся на p. Подгруппа $S \subset G$ называется *силовской p-подгруппой* в G, если $|S| = p^k$.

Теорема 28 (Первая теорема Силова)**.** *Для каждого простого делителя p порядка группы G существует силовская p-подгруппа $S \subset G$.*

Доказательство. Рассмотрим сначала случай абелевой группы. Если G – абелева группа, то $S = \mathrm{Tor}_p(G)$.

Для общего случая проведем доказательство по индукции по порядку G. База индукции – это случай абелевой группы. Проведем шаг индукции.

Случай 1. $|Z(G)|$ делится на p.

$Z(G)$ – абелева группа. В ней найдется некая подгруппа A такая, что $|A| = p$. Ясно, что A – нормальная подгруппа в G. При этом $|G/A| = \frac{n}{p}$, где $n = |G|$. По предположению индукции в G/A есть силовская p-подгруппа B в G/A. Рассмотрим $\pi_A^{-1}(B) \subset G$. Имеем, $|\pi_A^{-1}(B)| = |\mathrm{Ker}\,(\pi_a \mid_{\pi_A^{-1}(B)})| \cdot |\mathrm{Im}\,(\pi_a \mid_{\pi_A^{-1}(B)})| = |A| \cdot |B| = p^k$. Можно взять $S = \pi_A^{-1}(B)$.

Случай 2. $|Z(G)|$ не делится на p.

Расмотрим разложение группы G на классы сопряженных элементов. Классы сопряженности, состоящие из одного элемента – это элементы центра. Так как $|G|$ делится на p, найдется класс сопряженности C такой, что $|C| \neq 1$ не делится на p. Пусть $g \in C$. Рассмотрим $|Cent(g)| = \frac{|G|}{|C|} < |G|$. С другой стороны, $|Cent(g)|$ делится на p^k. По предположению индукции есть силовская подгруппа $S \subset Cent(g) \subset G$, при этом $|S| = p^k$. □

Лемма 45. *Если силовская подгруппа единственна, то она нормальна.*

Доказательство. Рассмотрим gSg^{-1} – это подгруппа G. Но $|gSg^{-1}| = |S|$. В самом деле, очевидно, что $|gSg^{-1}| \leq |S|$, с другой стороны, $S = g^{-1}(gSg^{-1})g$, значит, $S \leq |gSg^{-1}|$. Имеем, gSg^{-1} – силовская подгруппа G, а значит, $gSg^{-1} = S$, то есть S нормальна. □

Теорема 29 (Вторая теорема Силова)**.** *1) Любая p-подгруппа G содержится в некоторой силовской.*

2) Любые две силовские p-подгруппы сопряжены.

Доказательство. Случай $m = 1$ ясен. Пусть $m > 1$.

1) Пусть S – силовская p-подгруппа, $|S| = p^k$. Пусть $H \subset G$ – подгруппа порядка p^l, $l \leq k$. Рассмотрим действие H на множестве левых смежных классов по S:

$$h \cdot gS = (hg)S.$$

Корректность очевидна: если $gS = g'S$, то $g' = gs$ для некоторого $s \in S$. Тогда $hg' = hgs$ и $hgS = hg'S$. Из теоремы Лагранжа количество левых смежных классов по S равно $\frac{|G|}{|S|} = m$. Имеем, $|H| = p^l = |St(gS)| \cdot |Orb(gS)|$, значит, порядок каждой орбиты либо 1, либо степень p. Так как сумма порядков орбит не делится на p, есть орбита из одного элемента. То есть $hgS = gS$. Отсюда $g^{-1}hg \in S$, то есть $h \in gSg^{-1}$. Значит, $H \subset gSg^{-1}$, где $|gSg^{-1}| = p^k$.

2) Если H – силовская подгруппа, то $|H| = p^k$. По доказанному в пункте 1) выполнено $H \subset gSg^{-1}$. Поскольку $|H| = |gSg^{-1}$, имеем $H = gSg^{-1}$. Значит, любая силовская p-подгруппа H сопряжена фиксированной силовской p-подгруппе S. □

Лекция 14

Пусть $|G| = p^k m$. Обозначим через n_p число силовских p-подгрупп в группе G.

Теорема 30 (Третья теорема Силова)**.**

1) n_p сравнимо с 1 по модулю p,

2) n_p делит m.

Доказательство. 1) Пусть S – одна из силовских p-подгрупп. Рассмотрим действие S на множестве N силовских p-подгрупп сопряжениями. То есть $s \cdot S' = sS's^{-1}$. Пусть $Orb(S')$ – некая орбита. Тогда $|Orb(S')| \cdot |St(S')| = |S| = p^k$. Значит, $|Orb(S')| = p^l$. Среди орбит есть $Orb(S)$, которая состоит только из одной подгруппы S, таким образом, $|Orb(S)| = 1$.

Пусть $S' \neq S$, допустим, что $|Orb(S')| = 1$. Тогда для любых $s \in S, s' \in S'$ имеем $ss's^{-1} \in S'$. Рассмотрим $H = SS' = \{ss' \mid s \in S, s' \in S'\}$. Докажем, что H – подгруппа. Действительно,

$$(s_1s'_1) \cdot (s_2s'_2) = s_1(s_2s_2^{-1})s'_1s_2s'_2 = s_1s_2(s_2^{-1}s'_1s_2)s'_2 \in H.$$

Значит, H замкнуто относительно произведения. Осталось проверить занмкнутость H относительно взятия обратного. Это следует из равенства.

$$(ss')^{-1} = s'^{-1}s^{-1} = (ss^{-1})s'^{-1}s^{-1} = s(s^{-1}s'^{-1}s^{-1}) \in H.$$

Итак, H – подгруппа в G. Получаем, что $|G| = p^k m$ делится на $|H|$, а $|H|$ делится на $|S| = p^k$. Значит, $|H| = p^k r$, где НОД$(r, p) = 1$. Поскольку, S и S' – силовские подгруппы в H, они сопряжены. То есть существует $h \in H$ такой, что $hS'h^{-1} = S$. Но $h = ss'$. Значит, $ss'S'(ss')^{-1} = S$. Имеем

$$ss'S'(ss')^{-1} = s(s'S's'^{-1})s^{-1} \subset sS's^{-1}.$$

Но так как $|Orb(S')| = 1$, то $sS's^{-1} = S'$. Противоречие.

Итак, множество N силовских p-подгрупп состоит из орбит, одна из них имеет порядок 1, а остальные имеют порядки p^l, где $l \neq 0$. Следовательно, $n_p = |N|$ имеет остаток 1 при делении на p.

2) Рассмотрим действие группы G на множестве M всех подгрупп в G. То есть $g \cdot H = gHg^{-1}$. По второй теореме Силова все силовские p-подгруппы образуют одну орбиту $\mathcal{O}$. Пусть S – одна из силовских p-подгрупп. Тогда

$$|G| = |\mathcal{O}| \cdot |St(S)| = n_p \cdot |St(S)|.$$

Отсюда $|G| = p^k m$ делится на n_p. Так как НОД$(n_p, p) = 1$, получаем m делится на n_p. □

Следствие 14. *Группа порядка pq, где p и q – различные простые числа, разрешима.*

Доказательство. Пусть $|G| = pq$. Можно считать, что $p < q$. Тогда n_p делит q и сравнимо с 1 по модулю p. Значит, $n_p = 1$. Тогда силовская p-подгруппа S нормальна. Так как $|S| = p$ и $|G/S| = q$ эти группы циклические, а значит, разрешимы. По критерию разрешимости G разрешима. □

Предложение 17. *Группа порядка p^k разрешима.*

Доказательство. Докажем по индукции по порядку группы. База индукции $|G| = p$, тогда группа циклическая, и следовательно, разрешима. Шаг индукции. У p- группы центр неединичен. Если $Z(G) = G$, то эта группа абелева, и следовательно, разрешима. Если $|Z(G)| < |G|$, то по предположению индукции $Z(G)$ и $G/Z(G)$ разрешимы. Значит, G разрешима. □

Следствие 15. *Группа порядка p^2q, где p и q – различные простые числа, разрешима.*

Доказательство. По 3 теореме Силова n_p сравнимо с 1 по модулю p и делит q. Если $n_p = 1$, то силовская p-группа S нормальна. Так как $|S| = p^2$, она абелева, а так как $|G/S| = q$, эта группа циклическая. Значит, G разрешима.

Пусть $n_p = q$. Значит, $q = pk + 1$ (в частности, $q > p$). Рассмотрим теперь n_q, оно сравнимо с 1 по модулю q и делит p^2. Если $n_q = 1$, то единственная силовская q-подгруппа нормальна и циклическая, а фактор по ней абелев. Следовательно, G разрешима. Если $n_q = p$, то $p > q$, противоречие. Остался случай $n_q = p^2$.

Каждая силовская q-подгруппа состоит из e и $q - 1$ элемента порядка q. Так как силовские q-подгруппы порождаются любым элементом порядка q, они пересекаются только по e. Получаем, что в p^2 силовских q-подгруппах содержится $p^2(q-1) = p^2q - p^2$ элементов порядка q. Значит, элементов порядка не q в G ровно p^2, то есть $n_p = 1$. □

Определение 49. Пусть N, H – группы. Пусть задан гомоморфизм $\psi\colon H \to \mathrm{Aut}(N)$. Рассмотрим множество пар (n, h) с операцией

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \psi(h_1)(n_2), h_1 \cdot h_2).$$

Получим группу (это мы докажем в следующей лемме), которая называется *полупрямым произведением* групп N и H, (соответствующим гомоморфизму ψ). Обозначать эту группу мы будем $N \leftthreetimes H$.

Лемма 46. *Полупрямое произведение $N \leftthreetimes H$ – группа.*

Доказательство. Проверим ассоциативность операции.

$$((n_1,h_1)\cdot(n_2,h_2))\cdot(n_3,h_3) = (n_1\cdot\psi(h_1)(n_2),h_1\cdot h_2)\cdot(n_3,h_3) = \\ = (n_1\cdot\psi(h_1)(n_2)\cdot\psi(h_1h_2)(n_3),h_1\cdot h_2\cdot h_3).$$

С другой стороны

$$(n_1,h_1)\cdot((n_2,h_2)\cdot(n_3,h_3)) = (n_1,h_1)\cdot(n_2\cdot\psi(h_2)(n_3),h_2\cdot h_3) = \\ = (n_1\cdot\psi(h_1)(n_2\cdot\psi(h_2)(n_3)),h_1\cdot h_2\cdot h_3) = (n_1\cdot\psi(h_1)(n_2)\cdot\psi(h_1h_2)(n_3),h_1\cdot h_2\cdot h_3).$$

Поскольку получили одинаковый результат, умножение ассоциативно.

Единичный елемент (e_N,e_H), действительно

$$(e_N,e_H)\cdot(n,h) = (e_N\psi(e_H)(n),e_Hh) = (e_N\mathrm{id}(n),h) = (n,h)$$

и

$$(n,h)\cdot(e_N,e_H) = (n\psi(h)(e_N),he_H) = (n,h).$$

Обратный к элементу (n,h) – это элемент $(\psi(h^{-1})(n^{-1}),h^{-1})$. В самом деле

$$(n,h)(\psi(h^{-1})(n^{-1}),h^{-1}) = (n\psi(h)(\psi(h^{-1})(n^{-1})),hh^{-1}) = \\ = (n\psi(hh^{-1})(n^{-1}),e_H) = (n\psi(e)(n^{-1}),e_H) = (n\mathrm{id}(n^{-1}),e_H) = (nn^{-1},e_H) = (e_N,e_H).$$

и

$$(\psi(h^{-1})(n^{-1}),h^{-1})(n,h) = (\psi(h^{-1})(n^{-1})\psi(h^{-1})(n),h^{-1}h) = \\ = (\psi(h^{-1})(n^{-1}n),e_H) = (\psi(h^{-1})(e_N),e_H) = (e_N,e_H).$$

□

Замечание 18. Подгруппа $(N,\{e\})\cong N$ изоморфна N нормальна в G. В самом деле

$$(\widehat{n},\widehat{h})(n,e_H)(\widehat{n},\widehat{h})^{-1} = (*,\widehat{h})(*,e_H)(*,\widehat{h}^{-1}) = (*,\widehat{h}e_H\widehat{h}^{-1}) = (*,e_H).$$

Замечание 19. Если ψ переводит все в тождественный автоморфизм, то $N\leftthreetimes H\cong N\times H$.

Предложение 18. *Пусть в некоторой группе G есть две подгруппы N и H, причем $N\cap H=\{e\}$, $G=\langle N,H\rangle$ и N нормальна. Тогда $G\cong N\leftthreetimes H$ – полупрямое произведение, соответствующее гомоморфизму $\psi\colon H\to\mathrm{Aut}(N)$ такому, что $\psi(h)(n)=hnh^{-1}$.*

Доказательство. В самом деле, мы уже знаем, что $G=NH=\{nh\mid n\in N,h\in H\}$. Отождествим nh с парой (n,h). Так как $N\cap H=\{e\}$, если $n_1h_1=n_2h_2$, то выполнено $n_2^{-1}n_1=h_2h_1^{-1}$. Этот элемент лежит в N с одной стороны и в H с другой. Так как $N\cap H=\{e\}$, то есть $n_2^{-1}n_1=h_2h_1^{-1}=e$. Следовательно, $n_1=n_2$ и $h_1=h_2$. Значит, соответствие $nh\leftrightarrow(n,h)$ является биекцией.

При этом

$$(n_1h_1)\cdot(n_2h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 = n_1\psi(h_1)(n_2)h_1h_2.$$

Значит, соответствие $nh\leftrightarrow(n,h)$ является гомоморфизмом. Итак, это гомоморфизм и биекция, то есть изоморфизм. □

Пример 16. *Группа D_n изоморфна полупрямому произведению $\mathbb{Z}_n\leftthreetimes\mathbb{Z}_2$, соответствующему гомоморфизму $\psi\colon\mathbb{Z}_2\to\mathrm{Aut}(\mathbb{Z}_n)$, такому, что $\psi(0)=\mathrm{id}$, $\psi(1)\colon x\mapsto -x$.*

Действительно, рассмотрим группу поворотов $N\cong\mathbb{Z}_n$ и подгруппу $H=\{\mathrm{id},s\}$, где s – некоторая симметрия. Тогда $N\lhd D_n$ и $s\circ R_\alpha\circ s^{-1}=R_{-\alpha}$.

Пример 17. *Группа S_n изоморфна полупрямому произведению $A_n \leftthreetimes \mathbb{Z}_2$ В самом деле при $H = \{\mathrm{id}, (1,2)\} \cong \mathbb{Z}_2$ имеем $A_n \cap H = \{\mathrm{id}\}$, $A_n \lhd S_n$ и $S_n = \langle A_n, H\rangle$.*

Теорема 31. *Пусть $p > q$ – простые числа. Если p не сравнимо с 1 по модулю q, то существует единственная группа порядка pq (это $\mathbb{Z}_{pq}$). Если же p не сравнимо с 1 по модулю q, то существует ровно две группы порядка pq: одна $\mathbb{Z}_{pq}$, а другая – не абелева.*

Доказательство. По 3 теореме Силова n_p делит q и сравнимо с 1 по модулю p. Значит, $n_p = 1$. Пусть N – это единственная силовская p-подгруппа, она нормальна в G. Обозначим через H силовскую q-подгруппу. Тогда $N \cap H = \{e\}$ так как они циклические разных простых порядков. С другой стороны так как порядок группы, порожденной H и N делится на p и на q, получаем $G = \langle N, H\rangle$. Таким образом $G = N \leftthreetimes H$. Это полупрямое произведение соответствует некоторому гомоморфизму

$$\psi\colon \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}.$$

Если p не сравнимо с 1 по модулю q, то $p-1$ не делится на q и образ $\psi(\mathbb{Z}_q)$ равен $\{e\}$. Значит, $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

Пусть p сравнимо с 1 по модулю q. Рассмотрим образ $\psi(\mathbb{Z}_q)$ в $\mathbb{Z}_{p-1}$. Это некая подгруппа в циклической группе. Ее порядок может быть равен либо 1 (и тогда мы получаем $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$) либо q. Если порядок образа равен q, то $\mathrm{Im}\,\psi$ – единственная подгруппа порядка q в $\mathbb{Z}_{p-1}$, то есть $\left\langle \frac{p-1}{q} \right\rangle$. При этом гомоморфизм ψ каким-то образом отображает $H \cong \mathbb{Z}_q$ изоморфно на $\mathrm{Im}\,\psi \cong \mathbb{Z}_q$.

Рассмотрим 2 таких полупрямых произведения, соответствующие гомоморфизмам $\psi_1\colon H_1 \to \left\langle \frac{p-1}{q} \right\rangle$ и $\psi_2\colon H_2 \to \left\langle \frac{p-1}{q} \right\rangle$. Заметим, что так как ψ_2 – изоморфизм, к нему есть орбатный. Рассмотрим отображение

$$\varphi\colon N \leftthreetimes H_1 \to N \leftthreetimes H_2,$$

заданное по правилу

$$\varphi(n,h) = (n, \psi_2^{-1} \circ \psi_1(h)).$$

Проверим, что ψ – гомоморфизм. Имеем:

$$\varphi((n,h)\cdot(n',h')) = \varphi(n \cdot \psi_1(h)(n'), hh') = (n \cdot \psi_1(h)(n'), \psi_2^{-1} \circ \psi_1(hh'))$$

С другой стороны

$$\begin{aligned}\varphi(n,h)\varphi(n',h') &= (n, \psi_2^{-1} \circ \psi_1(h))(n', \psi_2^{-1} \circ \psi_1(h')) = \\ &= (n \cdot \psi_2(\psi_2^{-1} \circ \psi_1(h))(n'), \psi_2^{-1} \circ \psi_1(h) \cdot \psi_2^{-1} \circ \psi_1(h')) = (n \cdot \psi_1(h)(n'), \psi_2^{-1} \circ \psi_1(hh'))\end{aligned}$$

Таким образом $\varphi((n,h)\cdot(n',h')) = \varphi(n,h)\varphi(n',h')$, то есть φ – гомоморфизм.

Проверим, что φ – биекция. Первая компонента при φ не меняется, а ко второй применяется композиция изоморфизмов $\psi_2^{-1} \circ \psi_1$. Это доказывает биективность φ.

Итак, гомоморфизм φ является биекцией, а значит, изоморфизмом. Это доказывает, что все полупрямые произведения $\mathbb{Z}_p \leftthreetimes \mathbb{Z}_q$, соответствующие нетривиальным гомоморфизмам $\mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$ изоморфны. Таким образом, существуют ровно две неизоморфные группы порядка pq при p сравнимом с 1 по модулю q. Так как абелева группа порядка pq всего одна, группа, соответствующая нетривиальным гомоморфизмам, не абелева. □

Лекция 15

Теорема 32. *Пусть G – нормальная подгруппа в H и группа G/H не простая. Тогда существует нормальная подгруппа N в G такая, что $H \subsetneq N \subsetneq G$ – цепочка строгих включений. При этом $G \triangleright N \triangleright H$.*

Доказательство. Раз G/H – не простая группа, то существует собственная нормальная подгруппа L в ней. Рассмотрим канонический гомоморфизм $\pi_H \colon G \to G/H$. Положим $N = \pi_H^{-1}(L)$. Так как подгруппа L собственная, N не совпадает ни с G, ни с H. Подгруппа N нормальна в G. В самом деле, пусть $g \in G, n \in N$. Тогда $\pi_H(gng^{-1}) = \pi_H(g)\pi_H(n)\pi_H(g)^{-1}$. При этом $\pi_H(n) \in L$, а подгруппа L нормальна в G/H. Значит, $\pi_H(gng^{-1}) \in L$, то есть $gng^{-1} \in N$, что доказывает нормальность N. □

Следствие 16. *Любая конечная группа G может быть включена в композиционный ряд, то есть такой ряд подгрупп*

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

что G_{i-1}/G_i простая.

Теорема 33 (Жордан-Гельдер)**.** *Факторы G_i/G_{i+1} композиционного ряда определены однозначно с точностью до перестановки.*

Теорема Жордана-Гельдера связываетс с любой группой некоторый набор простых групп (факторов композиционного ряда). Это дает мотивацию изучать простые группы. Например, очень популярной темой является классификация конечных простых групп. Конечные простые группы содержат несколько серий (одна из котрорых – это группы $A_n, n \in \mathbb{N}$). Также есть (довольно большие) единичные примеры групп, они называются *монстрами*. Различные математики не сходятся во мнении, можно ли считать классификацию конечных простых групп завершенной. Дело в том, что она содержится в большом количестве работ и все эти работы не может прочитать за свою жизнь один человек.

Стоит упомянуть, что изучение простых факторов композиционного ряда не дачт полной классификации групп, так как могут быть различные группы с одинаковым набором факторов.

Представления.

Пусть V – векторное пространство над некоторым полем F. Обозначим через $\mathrm{GL}(V)$ группу обратимых операторов $V \to V$.

Определение 50. *Линейным представлением* группы G называется гомоморфизм $G \to \mathrm{GL}(V)$.

Если в V выбрать базис из n векторов, то каждому оператору сопоставляется матрица $n \times n$. Это устанавливает изоморфизм между $\mathrm{GL}(V)$ и $\mathrm{GL}_n(F)$.

Определение 51. *Матричным представлением* группы G называется гомоморфизм $G \to \mathrm{GL}_n(F)$.

Выбор базиса в V устанавливает биекцию между линейными и матричными представлениями. Если выбрать другой базис, то все операторы представления сопрягутся матрицей перехода.

Размерностью представления называется размерность пространства V. Мы ограничимся рассмотрением конечномерных представлений.

Пример 18. *Отображение* $\sigma \mapsto \mathrm{sgn}(\sigma)$ *дает одномерное представление группы* S_n.

Замечание 20. Одномерные представления отождествляются с гомоморфизмами $G \to F^\times$.

Пример 19. *Пусть* ε_1 *и* ε_2 *– корни из 1 степени* n. *Отображение* $k \mapsto \begin{pmatrix} \varepsilon_1^k & 0 \\ 0 & \varepsilon_2^k \end{pmatrix}$ *дает двумерное представление группы* $\mathbb{Z}_n$.

Пример 20. *Группа* $\mathrm{GL}_n(F)$ *имеет естественное* n*-мерное представление, при котором каждая матрица переходит в себя. Такое представление называется тавтологическим. Аналогичное представление можно рассмотреть для любой матричной группы:* $\mathrm{SL}_n(F)$, $\mathrm{O}_n(F)$ *и др.*

Замечание 21. Линейное представление задает действие группы G на V.

Определение 52. Предаставление $G \to \mathrm{GL}(V)$ называется *точным*, если его ядро состоит только из нейтрального элемента.

Определение 53. Пусть задан гомоморфизм групп $\varphi\colon G \to H$. Тогда по представлению $\rho\colon H \to \mathrm{GL}(V)$ можно построить представление $\rho \circ \varphi\colon G \to \mathrm{GL}(V)$.

Такая ситуация имеет место, например, если G – это подгруппа в H. В этом случае в качестве φ берем вложение $G \subset H$. Полученное представление $\rho \circ \varphi\colon G \to \mathrm{GL}(V)$ называется *индуцированным* представлением.

Определение 54. Пусть даны представления $\rho\colon G \to \mathrm{GL}(V)$ и $\zeta\colon G \to \mathrm{GL}(W)$. *Морфизмом* представлений называется линейное отображение $\varphi\colon V \to W$ такое, что для каждого $g \in G$ и для каждого $v \in V$ выполнено $\varphi(\rho(g)(v)) = \zeta(g)(\varphi(v))$.

Если φ – изоморфизм векторных пространств, то мы называем его *изоморфизмом* представлений.

Замечание 22. Если ρ и ζ – изоморфные линейные представления, то пространства V и W можно отождествить по изоморфизму φ. При этом базис V перейдет в базис W. Если взять эти соответствующие друг другу базисы и получить матричные представления, то получим одинаковые матричные представления.

Таким образом, матричные представления $\rho\colon G \to \mathrm{GL}_n(F)$ и $\zeta\colon G \to \mathrm{GL}_n(F)$ изоморфны тогда и только тогда, когда существует невырожденная матрица C такая, что для каждого $g \in G$ выполнено $C\rho(g)C^{-1} = \zeta(g)$.

Теорема 34. *Существует* n *различных (неизоморфных) комплексных одномерных представлений группы* $\mathbb{Z}_n$

Доказательство. Пусть $\rho\colon \mathbb{Z}_n \to F^\times$ – одномерное представление. Тогда $\rho(1)^n = \rho(n) = \rho(0) = 1$. То есть $\varepsilon = \rho(1)$ – корень n-ой степени из 1. При этом $\rho(k) = \varepsilon^k$, то есть образом единицы задается ρ. Получаем, что одномерных представлений группы $\mathbb{Z}_n$ столько же, сколько корней из 1 степени n, то есть n. И все они имеют вид $\rho(k) = \varepsilon^k$. □

Следствие 17. *Пусть* G *– абелева группа порядка* n. *Существует* n *различных (неизоморфных) комплексных одномерных представлений группы* G.

Доказательство. Группа G изоморфна прямой сумме циклических групп $\mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$. Аналогично теореме элемент $(0, \ldots, 0, 1, 0, \ldots 0)$, где 1 стоит на i-м месте может переходить в любой корень n_i степени из 1. Если же $\rho((0, \ldots, 0, 1, 0, \ldots 0)) = \varepsilon_i$, то $\rho((a_1, \ldots, a_k)) = \varepsilon_1^{a_1} \ldots \varepsilon_k^{a_k}$. Число способов выбрать $\varepsilon_1, \ldots, \varepsilon_k$ равно n. □

Пример 21. *Рассмотрим следующее n-мерное представление группы S_n: перестановка σ переходит в матрицу A, где*

$$a_{ij} = \begin{cases} 1, \text{ если } \sigma(j) = i, \\ 0 \text{ иначе.} \end{cases}$$

Такое представление называется мономиальным.

Например, при $n = 3$ получаем

$$\mathrm{id} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad (1,2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad (1,3) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$(2,3) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad (1,2,3) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad (1,3,2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Пример 22. *Пусть G – конечная группа порядка n. Рассмотрим n-мерное пространство FG, базисные векторы которого мы индексируем элементами группы: $e_{g_1}, \ldots, e_{g_n}$, где $G = \{g_1, \ldots, g_n\}$. Зададим представление $\rho\colon G \to \mathrm{GL}(FG)$ по правилу $\rho(g)(e_{g_i}) = e_{g \cdot g_i}$.*

Такое представление называется регулярным представлением группы G.

На самом деле данное представление есть композиция вложения $G \hookrightarrow S_n$, которое строится в теореме Кэли, и мономиального представления $S_n \to \mathrm{GL}_n(F)$.

На самом деле FG имеет более богатую структуру, чем просто векторное пространство. Элементы FG можно умножать друг на друга по правилу

$$(\sum_i \lambda_i e_{g_i})(\sum_j \mu_j e_{g_j}) = \sum_{i,j} \lambda_i \mu_j e_{g_i g_j}.$$

Определение 55. Множество R с двумя бинарными операциями $+$ и $\cdot$ называется *кольцом*, если выполнено

1) $(a + b) + c = a + (b + c)$,
2) существует 0 такой, что $a + 0 = 0 + a = a$,
3) для каждого a существует $(-a)$ такой, что $a + (-a) = (-a) + a = 0$,
4) $a + b = b + a$,
5) $a(b + c) = ab + ac$,
6) $(a + b)c = ac + bc$.

Кольцо ассоциативно, если

7) $(ab)c = a(bc)$.

Кольцо с единицей, если

8) существует 1 такой, что $1a = a1 = a$.

Кольцо коммутативно, если 9) $ab = ba$.

Коммутативное ассоциативное кольцо с единицей называется *полем*, если выполнено

10) для каждого $a \neq 0$ найдется a^{-1} такой, что $aa^{-1} = a^{-1}a = 1$.

Определение 56. Пусть фиксировано поле F. Множество A называется *алгеброй* (над F), если на нем определены три операции: сложение, умножение и умножение на скаляр (элемент поля F) такие, что

1) A с операциями сложения и умножения – это кольцо,

2) A с операциями сложения и умножения на скаляр – это векторное пространство над F,
3) $(\lambda a)b = a(\lambda b) = \lambda(ab)$.

Пример 23. *Матрицы $n \times n$ образуют ассоциативную алгебру с единицей.*

Упражнение 6. Проверьте, что FG – это ассоциативная алгебра с единицей. Она называется *групповой алгеброй* группы G.
В каком случае алгебра FG коммутативна?

Определение 57. Пусть $\rho\colon G \to \mathrm{GL}(V)$ – линейное представление. Подпространство $U \subset V$ называется *инвариантным*, если для любого $g \in G$ выполнено $\rho(g)(U) \subset U$.

Если U – инвариантное подпространство и мы выберем базис $e_1, \ldots, e_k$ в U, а затем дополним его до базиса $e_1, \ldots, e_n$ в V, то матрицы $\rho(g)$ в базисе $e_1, \ldots, e_n$ будут иметь блочно-верхнетреугольный вид

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

Определение 58. Представление $\rho\colon G \to \mathrm{GL}(V)$ называется *неприводимым* если не существует инвариантных подпространств $U \subset V$ кроме $\{0\}$ и V.

Определение 59. Пусть $\rho\colon G \to \mathrm{GL}(V)$ и $\zeta\colon G \to \mathrm{GL}(W)$ – два представления одной и той же группы G. *Прямой суммой* представлений ρ и ζ называется представление $\rho \oplus \zeta\colon G \to \mathrm{GL}(V \oplus W)$, определенное по правилу:

$$\rho \oplus \zeta(g)(v + w) = \rho(g)(v) + \zeta(g)(w).$$

Если выбрать базис в $V \oplus W$, являющийся объединением базисов V и W, то матрица оператора $\rho \oplus \zeta(g)$ имеет в этом базисе блочно-диагональный вид

$$\begin{pmatrix} \rho(g) & 0 \\ 0 & \zeta(g) \end{pmatrix}.$$

Пример 24. *Следующее отображение дает двумерное представление группы $\mathbb{Z}_2$:*

$$\rho(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Оно является прямой суммой двух одномерных.

Определение 60. Представление называется *вполне приводимым*, если оно изоморфно прямой сумме неприводимых.

Замечание 23. В частности любое неприводимое представление вполне приводимо.

Пусть U – инвариантное пространство представления $\rho\colon G \to \mathrm{GL}(V)$. Назовем U' *дополнительным* инвариантным пространством, если U' инвариантно и $V = U \oplus U'$.

Предложение 19. *Если для любого инвариантного подпространства найдется дополнительное инвариантное подпространство, то представление вполне приводимо.*

Доказательство. Докажем по индукции по размерности представления n. База при $n = 1$ очевидна.

Шаг индукции. Если ρ неприводимо, то оно вполне приводимо. Пусть это не так. Тогда есть инвариантное подпространство $U \subset V$. Тогда $V = U \oplus U'$, где U' – дополнительное инвариантное подпространство. И значит, $\rho = \rho\,|_U \oplus \rho\,|_{U'}$. По предположению индукции представления $\rho\,|_U$ и $\rho\,|_{U'}$ вполне приводимы. Тогда ρ также вполне приводимо. □

Лекция 16

Пример 25. *Группа S_3 изоморфна группе симметрий треугольника D_3. Построим следующее двумерное представление группы S_3. Поместим начало координат в центр треугольника. Тогда любая симметрия треугольника задает линейное преобразование плоскости. Например, повороты запишутся матрицами*

$$\begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

Данное представление неприводимо (даже над $\mathbb{C}$).

В самом деле, если двумерное представление приводимо, то у всех его операторов есть общий собственный вектор. Если взять треугольник с горизонтальной стороной, то одна из симметрий запишется матрицей $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. У такой матрицы два собственный вектора (с точностью до пропорциональности): $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ и $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Но ни один из них не является собственным вектором матриц поворотов.

Пример 26 (Пример не вполне приводимого представления)**.** *Рассмотрим следующее представление группы $\mathbb{Z}$ (над полем $\mathbb{R}$ или $\mathbb{C}$):*

$$n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Видно, что $\langle e_1 \rangle$ – инвариантное подпространство. Но если бы это представление было вполне приводимым, оно бы раскладывалось в сумму двух одномерных. Тогда в подходящем базисе все матрицы были бы диагональны. Однако матрица $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ не диагонализуема.

Следующее представление устанавливает связь между одномерными представлениями группы и ее фактора по коммутанту.

Предложение 20. *Пусть $\rho\colon G \to F^\times$ – одномерное представление группы G. Тогда*
1) $G' \subset \operatorname{Ker}\rho$,
2) $\rho = \zeta \circ \pi_{G'}$ для некоторого (одномерного) представления группы G/G',
3) соответствие $\rho \leftrightarrow \zeta$ является биекцией между множествами 1-мерных представлений G и G/G'.

Доказательство. 1) Так как группа $F^\times$ абелева, ее коммутант тривиален. А при гомоморфизме образ коммутанта попадает в коммутант.

2) Определим $\zeta(gG') = \rho(g)$. Нужно проверить корректность, то есть, что если $gG' = hG'$, то $\rho(g) = \rho(h)$. Действительно, если $gG' = hG'$, то $g = hs$, $s \in G'$. Тогда $\rho(g) = \rho(h)\rho(s) = \rho(h)$. Получаем, что ζ определено корректно и $\rho = \zeta \circ \pi_{G'}$, так как $\zeta \circ \pi_{G'}(g) = \zeta(gG') = \rho(g)$.

3) По каждому $\zeta\colon G/G' \to F^\times$ однозначно строится $\rho = \zeta \circ \pi_{G'}$ и так получаются все одномерные представления G. □

Из предыдущего предложения и следствия 17 вытекает следующее утверждение.

Следствие 18. *У группы G ровно $|G/G'|$ одномерных представлений.*

Предложение 21. *Если F – алгебраически замкнутое поле, то любое неприводимое представление ρ абелевой группы G одномерно.*

Доказательство. Операторы $\rho(g)$ коммутируют между собой. Пусть $V_\lambda \neq \{0\}$ – собственное подпространство одного оператора $\rho(g_0)$. Тогда V_λ инвариантно относительно всех операторов $\rho(g)$. Действительно, при $v \in V_\lambda$ имеем

$$\rho(g_0)(\rho(g)(v)) = \rho(g_0) \circ \rho(g)(v) = \rho(g) \circ \rho(g_0)(v) = \rho(g)(\lambda v) = \lambda\rho(g)(v).$$

То есть $\rho(g)(v)$ – собственный вектор $\rho(g)$ с собственным значением λ.

Докажем по индукции по размерности n, что у представления абелевой группы над алгебраически замкнутым полем F есть одномерное инвариантное подпространство. База $n = 1$ очевидна. Шаг индукции. Если все операторы $\rho(g)$ скалярны, возьмем любое одномерное подпространство. Если есть $\rho(g_0)$ не скалярный. Пусть λ – его собственное значение. Тогда V_λ инвариантно относительно всех операторов $\rho(g)$, а значит, у представления $\rho\,|_{V_\lambda}$ есть одномерное инвариантное подпространство. Оно же будет одномерным инвариантным подпространством для ρ. □

Замечание 24. Если отказаться от алгебраической замкнутости поля, то утверждение предыдущего предложения будет неверным. Действительно $x \mapsto \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x. \end{pmatrix}$ является неприводимым 2-мерным представлением $(\mathbb{R}, +)$ над $\mathbb{R}$

Следующая теорема является ключевой в изучении представлений конечных групп. Она во многом сводит изучение любых конечномерных представлений к изучению неприводимых.

Теорема 35 (Теорема Машке)**.** *Пусть $|G| = n$ не делится на характеристику поля F. Тогда любое представление ρ группы G вполне приводимо.*

Доказательство. Для доказательства полной приводимости достаточно доказать, что у каждого инвариантного подпространства есть дополнительное инвариантное подпространство. Пусть $U \subset V$ – инвариантное подпространство. Рассмотрим некоторое (не обязательно инвариантное) дополнительное подпространство W, то есть выполнено $V = U \oplus W$. Можно рассмотреть проектор P на второе подпространство: $P(u+w) = w$. При этом $P^2 = P$.

Напомним, что любой оператор Q с условием $Q^2 = Q$ является проектором на $\operatorname{Im} Q$ вдоль $\operatorname{Ker} Q$. Наша цель – изменить проектор P так, чтобы измененный проектор P' был также проектором вдоль U на некоторое инвариантное подпространства W'. Тогда $V = U \oplus W'$.

Определим

$$P' = \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ P \circ \rho(g)^{-1}.$$

Поскольку $P(u) = 0$ для любого $u \in U$, выполнено $P \circ \rho(g)^{-1}(u) = 0$. Получаем

$$P'(u) = \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ P \circ \rho(g)^{-1}(u) = 0.$$

То есть $U \subset \operatorname{Ker} P'$. Поскольку P – проектор на W вдоль U, для любого $g \in G$ выполнено $P \circ \rho(g)^{-1}(v) - \rho(g)^{-1}(v) \in U$. Домножая на $\rho(g)$, получаем

$$\rho(g) \circ P \circ \rho(g)^{-1}(v) - v \in U.$$

Следовательно, $P'(v) - v \in U$. Применяя P', получаем $P'^2(v) - P'(v) = 0$. То есть $P'^2 = P'$, что означает, что P' – проектор на свой образ, который мы обозначим W'.

Если $P'(v) = 0$, то $-v = P'(v) - v \in U$. Значит, $\operatorname{Ker} P' = U$.

Мы уже доказали, что $V = U \oplus W'$. Осталось объяснить, что W' – инвариантное подпространство.

Докажем, что для любого $h \in G$ выполнено $\rho(h) \circ P' = P' \circ \rho(h)$.

$$\rho(h) \circ P' = \rho(h) \circ \left(\frac{1}{|G|} \sum_{g \in G} \rho(g) \circ P \circ \rho(g)^{-1} \right) = \frac{1}{|G|} \sum_{g \in G} \rho(hg) \circ P \circ \rho(g)^{-1} =$$

$$= \left(\frac{1}{|G|} \sum_{hg \in G} \rho(hg) \circ P \circ \rho(hg)^{-1} \right) \circ \rho(h) = P' \circ \rho(h).$$

Пусть $w' \in W'$, тогда существует $v \in V$ с условием $P'(v) = w'$. Имеем

$$\rho(g)(w') = \rho(g) \circ P'(v) = P' \circ \rho(g)(v) \subset W'.$$

Значит, W' инвариантно. □

Приведем примеры, показывающие, что условие конечности группы и условие, что $\operatorname{char} F \nmid n$ в теореме Машке существенные.

Пример 27 (уже был)**.** *Представление группы $\mathbb{Z}$ (над полем $\mathbb{R}$ или $\mathbb{C}$):*

$$n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

приводимо, но не вполне приводимо. К этому примеру не применима теорема Машке, так как группа бесконечна.

Пример 28. *Представление группы $\mathbb{Z}_p$ (над полем $\mathbb{Z}_p$):*

$$n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Аналогично предыдущему примеру, это представление приводимо, но не вполне приводимо .

Пример 29. *Мономиальное представление ρ группы S_n вполне приводимо. Оно раскладывается в прямую сумму 2-х подпредставлений. Первое подпредставление одномерно (и следовательно неприводимо) и является ограничением ρ на инвариантное подпространство $U = \langle e_1 + \ldots + e_n \rangle$.*

Второе подпредставление – это ограничесние ρ на инвариантное подпространство $W = \{(x_1, \ldots, x_n) \mid \sum x_i = 0\}$. Осталось объяснить, что $\rho\,|_W$ неприводимо.

Пусть $L \subset W$ – ненулевое инвариантное подпространство. Возъмем вектор

$$v = (x_1, \dots, x_n) \neq (0, \dots, 0) \in L.$$

Тогда найдутся $i \neq j$ такие, что $x_i \neq x_j$. Применим $\rho((i,j))$ к вектору v. При этом x_i и x_j поменяются местами. Тогда

$$v - \rho((i,j))(v) = (0, \dots, x_i - x_j, 0, \dots, 0, x_j - x_i, 0 \dots, 0) \in L.$$

То есть $e_i - e_j \in L$. Применяя к $e_i - e_j$ оператор $\rho(\sigma)$, где $\sigma(i) = k$, $\sigma(j) = m$ получаем $e_k - e_m \in L$. Однако $\langle e_1 - e_2, \dots, e_1 - e_n \rangle = W$. То есть $L = W$.

Лекция 17

Теорема 36 (Лемма Шура)**.** *Пусть $\rho\colon G \to \mathrm{GL}(V)$ и $\zeta\colon G \to \mathrm{GL}(W)$ – два неприводимых представления. И пусть $\varphi\colon V \to W$ – морфизм этих представлений. Тогда*

1) если ρ и ζ не изоморфны, то $\varphi = 0$,

2) если ρ и ζ изоморфны, то φ – либо нулевое отображение, либо изоморфизм,

3) если $V = W$ – пространства над алгебраически замкнутым полем и $\rho = \zeta$, то $\varphi = \lambda \,\mathrm{id}$.

Доказательство. 1 и 2) Докажем, что $\mathrm{Ker}(\varphi)$ является ρ-инвариантным подпространством в V. Действительно, пусть $v \in \mathrm{Ker}(\varphi)$. Тогда для любого $g \in G$ выполнено $\zeta(g) \circ \varphi(v) = 0$. Однако $\zeta(g) \circ \varphi = \varphi \circ \rho(g)$. Значит, $\rho(g)(v) \in \mathrm{Ker}\,\varphi$. Следовательно, так как ρ неприводимо, либо $\mathrm{Ker}\,\varphi = V$ и тогда φ – нулевое отображение, либо $\mathrm{Ker}\,\varphi = \{0\}$ и φ – инъекция.

Докажем, что $\mathrm{Im}\,\varphi \subset W$ является ζ-инвариантным подпространством. Возьмем $\varphi(v) \in \mathrm{Im}\,\varphi$ и применим ζ. Получаем $\zeta \circ \varphi(v) = \varphi \circ \rho(v) \in \mathrm{Im}\,\varphi$. Так как ζ – неприводимое представление, либо $\mathrm{Im}\,\varphi = \{0\}$ и тогда φ – нулевое отображение, либо φ – сюръекция.

Итак, либо $\varphi = 0$, либо φ – биекция, то есть изоморфизм.

3) Пусть F алгебраически замкнуто и $V = W$ и $\rho = \zeta$. Так как F алгебраически замкнуто, у оператора φ есть собственное значение λ. Тогда у оператора $\varphi - \lambda \,\mathrm{id}$ есть нетривиальное ядро. Докажем, что $\varphi - \lambda \,\mathrm{id}$ также является морфизмом. Действительно

$$\rho(g) \circ (\varphi - \lambda \mathrm{id}) = \rho(g) \circ \varphi - \lambda\rho = \varphi \circ \rho(g) - \lambda\rho = (\varphi - \lambda \mathrm{id}) \circ \rho(g).$$

По предыдущему тогда $\mathrm{Ker}\,(\varphi - \lambda \mathrm{id}) = V$, то есть $\varphi = \lambda \,\mathrm{id}$. □

Следствие 19. *Пусть $\rho\colon G \to \mathrm{GL}(V)$ и $\zeta\colon G \to \mathrm{GL}(W)$ – два неприводимых комплексных представления конечной группы G. И пусть $\varphi\colon V \to W$ – произвольное линейное отображение. Положим*

$$\widetilde{\varphi} = \frac{1}{|G|} \sum_{g \in G} \zeta(g) \circ \varphi \circ \rho(g)^{-1}.$$

Тогда

1) если ρ и ζ не изоморфны, то $\widetilde{\varphi} = 0$,

2) если $V = W$ и $\rho = \zeta$, то $\widetilde{\varphi} = \lambda \,\mathrm{id}$, где $\lambda = \frac{tr\,\varphi}{\dim V}$.

Доказательство. Нужно проверить, что $\widetilde{\varphi}$ – морфизм представлений.

$$\zeta(g)\circ\widetilde{\varphi}=\zeta(g)\circ\left(\frac{1}{|G|}\sum_{h\in G}\zeta(h)\circ\varphi\circ\rho(h)^{-1}\right)=\frac{1}{|G|}\sum_{h\in G}\zeta(gh)\circ\varphi\circ\rho(h)^{-1}=$$
$$=\frac{1}{|G|}\sum_{gh\in G}\zeta(gh)\circ\varphi\circ\rho(gh)^{-1}\circ\rho(g)=\widetilde{\varphi}\circ\rho(g).$$

Из леммы Шура следуют оба утверждения. Причем

$$\lambda\dim V=\operatorname{tr}\lambda E=\operatorname{tr}\widetilde{\varphi}=\frac{1}{|G|}\sum_{g\in G}\operatorname{tr}\left(\rho(g)\circ\varphi\circ\rho(g)^{-1}\right)=\frac{1}{|G|}\sum_{g\in G}\operatorname{tr}\varphi=\operatorname{tr}\varphi.$$

□

Выберем некоторые базисы в V и W. Тогда представления ρ и ζ соответствуют матричным представлениям.

Определение 61. *Матричным элементом* ρ_{ij} называется функция $G\to F$, которая переводит элемент $g\in G$ в (i,j)-й элемент матрицы $\rho(g)$.

Определение 62. Пусть $|G|$ не делится на $\operatorname{char}F$. Введем следующую билинейную форму на множестве функций из G в F:

$$\langle f,h\rangle=\frac{1}{|G|}\sum_{g\in G}f(g)h(g^{-1}).$$

Следствие 20. *Если представления ρ и ζ не изоморфны, то для любых натуральных чисел $1\le a,b\le\dim W$; $1\le c,d\le\dim V$ выполнено $\langle\zeta_{ab},\rho_{cd}\rangle=0$.*

Доказательство. Возьмем в следствии 1 отображение φ, задающееся в выбранных базисах матрицей E_{bc}. Тогда так как $\widetilde{\varphi}=\frac{1}{|G|}\sum_{g\in G}\zeta(g)\circ\varphi\circ\rho(g)^{-1}=0$, получаем
$0=\widetilde{\varphi}_{ad}=\frac{1}{|G|}\sum_{g\in G}\sum_{i,j}\zeta_{ai}(g)\varphi_{ij}\rho_{jd}(g^{-1})==\frac{1}{|G|}\sum_{g\in G}\zeta_{ab}(g)\rho_{cd}(g^{-1})=\langle\zeta_{ab},\rho_{cd}\rangle$. □

Следствие 21. *Пусть $V=W$ и $\rho=\zeta$. Тогда*

$$\langle\rho_{ab},\rho_{cd}\rangle=\begin{cases}\frac{1}{\dim V},\ \textit{если } a{=}d \textit{ и } b{=}c;\\ 0,\ \textit{иначе.}\end{cases}$$

Доказательство. Опять берем φ, задающееся матрицей E_{bc}. Получаем

$$\langle\rho_{ab},\rho_{cd}\rangle=\left(\frac{\operatorname{tr}\varphi}{\dim V}\operatorname{id}\right)_{ad}=\begin{cases}\frac{1}{\dim V},\ \text{если a=d и b=c;}\\ 0,\ \text{иначе.}\end{cases}$$

□

Определение 63. *Характером* конечномерного представления $\rho\colon G\to\mathrm{GL}_n(F)$ называется функция $\chi_\rho\colon G\to F$, где $\chi_\rho(g)=\operatorname{tr}\rho(g)$.

Замечание 25. Если мы возьмем изоморфное матричное представление ρ', то $\operatorname{tr}\rho'(g)=\operatorname{tr}C\rho(g)C^{-1}=\operatorname{tr}\rho(g)$. То есть характеры изоморфных представлений совпадают. В частности характер можно связать с линейным (а не матричным) представлением, так как он не зависит от того, какой базис мы выбрали.

Далее мы будем в основном интересоваться *комплексными характерами*, то есть характерами комплексных представлений.

Будем говорить, что характер *неприводим*, если соответствующее представление неприводимо.

Предложение 22. *Пусть χ_ρ – характер комплексного представления ρ в пространстве V. Тогда*

1) $\chi_\rho(e) = \dim V$;

2) $\chi_\rho(hgh^{-1}) = \chi_\rho(g)$, то есть характеры постоянны на классах сопряженности;

3) $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$ для любого элемента g конечного порядка;

4) если $\rho = \rho_1 \oplus \rho_2$, то $\chi_\rho = \chi_{\rho_1} + \chi_{\rho_2}$.

Доказательство. 1) Единичный элемент группы при представлении переходит в единичную матрицу, ее след равен размерности пространства.

2) $\chi_\rho(hgh^{-1}) = \operatorname{tr}(\rho(h)\rho(g)\rho(h)^{-1}) = \operatorname{tr}\rho(g) = \chi_\rho(g)$.

3) Если $g \in G$ – элемент порядка n, то $\rho(g)$ – диагонализуемая матрица, собственные значения которой – корни n-ой степени из 1. То есть в некотором базисе

$$\rho(g) = \begin{pmatrix} \varepsilon_1 & 0 & \dots, 0 & \\ 0 & \varepsilon_2 & \dots, 0 & \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \varepsilon_{\dim V} \end{pmatrix}.$$

Тогда

$$\rho(g^{-1}) = \begin{pmatrix} \varepsilon_1^{-1} & 0 & \dots, 0 & \\ 0 & \varepsilon_2^{-1} & \dots, 0 & \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \varepsilon_{\dim V}^{-1} \end{pmatrix} = \begin{pmatrix} \overline{\varepsilon_1} & 0 & \dots, 0 & \\ 0 & \overline{\varepsilon_2} & \dots, 0 & \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \overline{\varepsilon_{\dim V}} \end{pmatrix}.$$

Так как если $\varepsilon_i = (\cos\varphi + i\sin\varphi)$, то $\varepsilon_i^{-1} = (\cos(-\varphi) + i\sin(-\varphi)) = (\cos\varphi - i\sin\varphi) = \overline{\varepsilon_i}$.

4) В базисе, состоящем из базисов подпространств, на которых реализуются представления ρ_1 и ρ_2, имеем

$$\rho(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}.$$

Отсюда $\operatorname{tr}\rho(g) = \operatorname{tr}\rho_1(g) + \operatorname{tr}\rho_2(g)$. □

Определение 64. Обозначим пространство всех функций $G \to \mathbb{C}$ через $\mathbb{C}^G$.

Функцию будем называть *центральной*, если она постоянна на классах сопряженности.

Лемма 47. *Если группа G конечна, то полуторалинейная форма*

$$(f,h) = \frac{1}{|G|}\sum_{g\in G} f(g)\overline{h(g)}, \qquad f,h \in \mathbb{C}^G$$

превращает $\mathbb{C}^G$ в эрмитово пространство.

Доказательство. Ясно, что $(\cdot,\cdot)$ – полуторалинейная функция и $(f,h) = \overline{(h,f)}$. Надо проверить лишь положительную определенность.

$$(f,f)=\frac{1}{|G|}\sum_{g\in G}f(g)\overline{f(g)}=\frac{1}{|G|}\sum_{g\in G}|f(g)|^2>0,\ \text{если } f\neq 0.$$

□

Замечание 26. Если применять две введенные формы к характерам, то они совпадают, то есть $(\chi_\rho,\chi_\zeta)=\langle\chi_\rho,\chi_\zeta\rangle$. В самом деле

$$\langle\chi_\rho,\chi_\zeta\rangle=\frac{1}{|G|}\sum_{g\in G}\chi_\rho(g)\chi_\zeta(g^{-1})=\frac{1}{|G|}\sum_{g\in G}\chi_\rho(g)\overline{\chi_\zeta(g)}=(\chi_\rho,\chi_\zeta).$$

Теорема 37 (Свойство ортогональности характеров)**.** *Пусть ρ и ζ – неприводимые комплексные представления конечной группы G. Тогда*

$$(\chi_\rho,\chi_\zeta)=\begin{cases}1, & \text{если } \rho\cong\zeta;\\ 0, & \text{если } \rho\ncong\zeta.\end{cases}$$

Доказательство. Имеем $(\chi_\rho,\chi_\zeta)=\langle\chi_\rho,\chi_\zeta\rangle=\left\langle\sum_{i=1}^{\dim V}\rho_{ii},\sum_{j=1}^{\dim W}\zeta_{jj}\right\rangle=\sum_{i,j}\langle\rho_{ii},\zeta_{jj}\rangle$. Если $\rho\ncong\zeta$, то $\langle\rho_{ii},\zeta_{jj}\rangle=0$ для любых i,j. Если же $\rho\cong\zeta$, можно считать $\rho=\zeta$. Тогда $\langle\rho_{ii},\rho_{jj}\rangle=\begin{cases}0, & \text{если } i\neq j;\\ \frac{1}{\dim V} & \text{если } i=j.\end{cases}$ В итоге $\langle\chi_\rho,\chi_\zeta\rangle=\sum_{i=1}^{\dim V}\frac{1}{\dim V}=1$. □

Следствие 22. *Пусть $\rho=m_1\rho_1\oplus\ldots,\oplus m_k\rho_k$ – разложение в прямую сумму неприводимых. Тогда $m_i=(\chi_\rho,\chi_{\rho_i})$.*

Доказательство. $\chi_\rho=\sum m_j\chi_{\rho_j}$. Следовательно

$$(\chi_\rho,\chi_{\rho_i})=\sum m_j(\chi_{\rho_j},\chi_{\rho_i})=m_i.$$

□

Лекция 18

Определение 65. Пусть Γ – центральная функция на конечной группе G и пусть $\rho\colon G\to\mathrm{GL}(V)$ – комплексное представление. Обозначим через $\psi(\rho,\Gamma)$ оператор $V\to V$, определенный по правилу

$$\psi(\rho,\Gamma)=\sum_{g\in G}\overline{\Gamma(g)}\rho(g).$$

Предложение 23. *Если ρ – неприводимое представление, то $\psi(\rho,\Gamma)=\lambda\,\mathrm{id}$, где*

$$\lambda=\frac{|G|}{\chi_\rho(e)}(\chi_\rho,\Gamma).$$

Доказательство. Имеем

$$\rho(g)\psi(\rho,\Gamma)\rho(g)^{-1}=\rho(g)\left(\sum_{h\in G}\overline{\Gamma(h)}\rho(h)\right)\rho(g)^{-1}=$$
$$=\sum_{h\in G}\overline{\Gamma(h)}\rho(g)\rho(h)\rho(g)^{-1}=\sum_{h\in G}\overline{\Gamma(h)}\rho(ghg^{-1})=\sum_{ghg^{-1}\in G}\overline{\Gamma(h)}\rho(ghg^{-1})=$$
$$=\sum_{s\in G}\overline{\Gamma(g^{-1}sg)}\rho(s)=\sum_{s\in G}\overline{\Gamma(s)}\rho(s)=\psi(\rho,\Gamma).$$

Таким образом, $\rho(g)\psi(\rho,\Gamma) = \psi(\rho,\Gamma)\rho(g)$. По лемме Шура $\psi(\rho,\Gamma) = \lambda\,\mathrm{id}$.
Теперь найдем λ.

$$\lambda\,\chi_\rho(e) = \lambda\ \dim V = \mathrm{tr}\,(\lambda\,\mathrm{id}) = \mathrm{tr}\,\psi(\rho,\Gamma) = \mathrm{tr}\,\left(\sum_{g\in G}\overline{\Gamma(g)}\rho(g)\right) =$$

$$= \sum_{g\in G}\overline{\Gamma(g)}\mathrm{tr}\,\rho(g) = \sum_{g\in G}\overline{\Gamma(g)}\chi_\rho(g) = |G|\frac{1}{|G|}\sum_{g\in G}\overline{\Gamma(g)}\chi_\rho(g) = |G|(\chi_\rho,\Gamma).$$

Получаем $\lambda = \frac{|G|(\chi_\rho,\Gamma)}{\chi_\rho(e)}$. □

Следствие 23. *Если $(\chi_{\rho_i},\Gamma) = 0$ для всех неприводимых характеров конечной группы G, то $\psi(\rho,\Gamma) = 0$ для любого представления ρ.*

Доказательство. По теореме Машке любое представление группы G является прямой суммой неприводимых $\rho = m_1\rho_1 \oplus \ldots \oplus m_s\rho_s$. Тогда $\psi(\rho,\Gamma) = \bigoplus_{i=1}^{s} m_i\psi(\rho_i,\Gamma) = 0$. □

Теорема 38. *Характеры неприводимых комплексных представлений образуют ортонормированный базис в пространстве центральных функций.*

Доказательство. Мы знаем, что характеры неизоморфных неприводимых представлений ортогональны. Нужно лишь доказать, что они образуют полную систему. Для этого докажем, что если центральная функция ортогональна всем неприводимым характерам, то она нулевая.

Пусть Γ – центральная функция такая, что $(\chi_\rho,\Gamma) = 0$ для всех неприводимых ρ. Тогда для любого представления σ оператор $\psi(\sigma,\Gamma)$ нулевой. В частности это верно для регулярного представления $\sigma\colon G \to \mathbb{C}[G]$. Базис групповой алгебры $\mathbb{C}[G]$ обозначим через $\{u_g \mid g \in G\}$. Имеем $0 = \psi(\sigma,\Gamma)(u_e) = \sum_{g\in G}\overline{\Gamma(g)}\sigma(g)(u_e) = \sum_{g\in G}\overline{\Gamma(g)}u_g$. Значит, $\overline{\Gamma(g)} = 0$ для всех g. То есть $\Gamma = 0$. □

Следствие 24. *Количество неизоморфных комплексных представлений группы G равно количеству классов сопряженности в G.*

Доказательство. Размерность пространства центральных функций равно количеству классов сопряженности в G. С другой стороны размерность пространства центральных функций равно мощности базиса, то есть количеству неприводимых представлений. □

Предложение 24. *Каждое неприводимое комплексное представление ρ размерности n группы G входит в регулярное представление σ с кратностью n.*

Доказательство. Кратность вхождения ρ в σ равно $(\chi_\sigma,\chi_\rho) = = \frac{1}{|G|}\sum_{g\in G}\chi_\sigma(g)\overline{\chi_\rho(g)}$. Но при $g \neq e$ оператор $\sigma(g)$ не оставляет ни одного вектора u_h на месте. Значит, $\chi_\sigma(g) = 0$ при $g \neq e$. При этом $\chi_\sigma(e) = |G|$. Получаем

$$(\chi_\sigma,\chi_\rho) = \frac{1}{|G|}|G|\overline{\chi_\rho(e)} = \chi_\rho(e) = n.$$

□

Теорема 39. *Пусть $\rho_1,\ldots,\rho_k$ – все неизоморфные неприводимые комплексные представления группы G. Пусть размерность представления ρ_i равна n_i. Тогда $n_1^2 + \ldots + n_k^2 = |G|$.*

Доказательство. Мы знаем, что $\sigma = n_1\rho_1 \oplus \ldots \oplus n_k\rho_k$. Получаем $|G| = \dim\sigma = n_1 \dim\, \rho_1 + \ldots + n_k \dim\, \rho_k = n_1^2 + \ldots + n_k^2$. □

Пример 30 (Комплексные представления S_3)**.** $|S_3| = 6 = n_1^2 + \ldots + n_k^2$. *При этом, так как* $|S_3/S_3'| = 2$, *есть два одномерных представления группы* S_3. *Легко видеть, что это тривиальное представление (все переходит в 1) и знаковое (четные перестановки переходят в 1, а нечетные – в* -1*). Получаем, что есть еще ровно одно двумерное неприводимое представление. Мы знаем, что у* S_3 *есть неприводимое представление, полученное из изоморфизма* S_3 *и* D_3.

Заметим, что в S_3 *есть ровно 3 класса сопряженности.*

Пример 31 (Комплексные представления S_4)**.** $|S_4| = 24 = n_1^2 + \ldots + n_k^2$. *При этом* $|S_4/S_4'| = 2$, *и значит, у* S_4 *есть ровно 2 одномерных представления: тривиальное и знаковое. При этом 22 единственным образом раскладывается в сумму квадратов целых чисел* ≥ 2, *а именно* $22 = 2^2 + 3^2 + 3^2$. *Значит, у* S_4 *есть 2 одномерных, одно двумерное и два трехмерных неприводимых комплексных представлений. Двумерное неприводимое представление* S_4 *получается как композиция сюръективного гомоморфизма* $S_4 \to S_3$ *и неприводимого двумерного представления* S_3. *Трехмерные представления получаются из того, что* S_4 *изоморфна группе симметрий правильного тетраэдра и группе вращений куба. Надо проверить, что эти представления неприводимы и не изоморфны.*

Трехмерное представление, если оно приводимо, может разлагаться в прямую сумму либо двумерного и одномерного, либо трех одномерных. Так или иначе должно быть одномерное инвариантное подпространство, то есть собственный вектор общий для всех операторов представления. Можно убедиться непосредственно выписав несколько операторов в некотором базисе, что данные представления неприводимы.

Другой подход к доказательству неприводимости ρ *– это посчитать* (χ_ρ, χ_ρ) *и убедиться, что получится 1. Действительно, если* $\rho = m_1\rho_1 \oplus m_k\rho_k$ *– разложение на неприводимые, то* $(\chi_\rho, \chi_\rho) = \sum m_j^2$. *Для группы симметрий тетраэдра 6 операторов – это симметрии относительно плоскости (след 1), 6 – это зеркальные повороты на* $\frac{\pi}{2}$ *(след 1), восемь – повороты вокгру оси на* $\frac{\pi}{3}$ *(след 0), три – повороты вокгру оси на* π *(след* -1*) и один – тождественное преобразование (след 3). Итого*

$$(\chi_\rho, \chi_\rho) = \frac{1}{24}(6 \cdot 1^2 + 6 \cdot 1^2 + 8 \cdot 0^2 + 3 \cdot (-1)^2 + 1 \cdot 3^2) = 1.$$

Аналогично для куба 6 операторов – вращения на $\frac{\pi}{2}$ *(след 1), 9 операторов – вращения на* π *(след* -1*), 8 операторов – вращения на* $\frac{\pi}{3}$ *(след 0) и один – тождественное преобразование (след 3). Итого*

$$(\chi_\rho, \chi_\rho) = \frac{1}{24}(6 \cdot 1^2 + 9 \cdot (-1)^2 + 8 \cdot 0^2 + 1 \cdot 3^2) = 1.$$

То, что данные представления не изоморфны следует, например, из того, что в представлении, построенном по тетраэдру, определители некоторых операторов равны -1. *Для представления, построенного по кубу, определители всех операторов равны 1. Определитель оператора не меняется при сопряжении, а значит, должен быть одинаков у изоморфных представлений.*

Лекция 19

Определение 66. Кольцо – это множество R с двумя бинарными операциями $+$ и $\cdot$ такими, что $(R, +)$ является абелевой группой и $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

Пример 32. *1)* $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ *– это поля.*
2) $\mathbb{Z}, \mathbb{Z}_n, \mathbb{R}[x]$ *– коммутативные кольца.*
3) $\mathrm{Mat}_n(F), \mathbb{C}[G]$ *– вообще говоря не коммутативные, но ассоциативные кольца.*
4) $(\mathbb{R}^3, +, [,])$ *– не ассоциативное кольцо.*

Замечание 27. Далее в нашем курсе мы будем рассматривать только ассоциативные кольца. Таким образом все кольца, о которых будет идти речь, предполагаются ассоциативными.

Определение 67. Если $a, b \in R$ и выполнено $a \neq 0$, $b \neq 0$, $ab = 0$, то элемент a называется *левым делителем нуля*, а элемент b – *правым делителем нуля.*

Объединение множества левых и правых делителей нуля называется множеством делителей нуля.

Лемма 48. *Обратимые элементы не являются делителями нуля.*

Доказательство. Пусть $a \neq 0$, $b \neq 0$, $ab = 0$. В пусть при этом элемент a обратим. Тогда $b = a^{-1}ab = a^{-1}0 = 0$. Противоречие. □

Определение 68. Элемент $x \neq 0$ называется *нильпотентным*, если существует натуральное n такое, что $x^n = 0$.

Замечание 28. Так как $x^n = x \cdot x^{n-1} = x^{n-1} \cdot x$, нильпотент является (двусторонним) делителем нуля.

Пример 33. *1) В кольце* $\mathbb{Z}_6$ *выполнено* $2 \cdot 3 = 0$*, то есть 2 и 3 – делители нуля (но не нильпотенты).*
2) В кольце $\mathbb{Z}_4$ *выполнено* $2^2 = 0$*, то есть 2 – нильпотент.*
3) В кольце $\mathrm{Mat}_2(\mathbb{R})$ *выполнено* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$*, то есть это делители нуля (не нильпотенты).*
4) В кольце $\mathrm{Mat}_2(\mathbb{R})$ *выполнено* $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$*, то есть это нильпотент.*

Определение 69. *Алгебра* над полем F – это множество A с тремя операциями. Две из них бинарные: сложение и умножение. А последняя – умножение на число (элемент поля F). При этом выполнены следующие свойства.
1) $(a + b) + c = a + (b + c)$;
2) существует $0 \in A$ такой, что $a + 0 = 0 + a = a$;
3) $\forall a \in A$ существует $-a \in A$: $a + (-a) = (-a) + a = 0$;
4) $a + b = b + a$;
5) $a(b + c) = ac + ac$;
6) $(a + b)c = ac + bc$;
7) $\lambda(a + b) = \lambda a + \lambda b$;
8) $(\lambda + \mu)a = \lambda a + \mu a$;
9) $(\lambda\mu)a = \lambda(\mu)a$;
10) $1a = a$;
11) $\lambda(ab) = (\lambda a)b = a(\lambda b)$.

Пример 34. *1)* $\mathrm{Mat}_{n\times n}(F)$ *– алгебра над* F*;*
2) $F[x_1, \ldots, x_n]$ *– алгебра над* F*;*
3) $F[G]$ *– алгебра над* F*;*

4) Если $F \subset K$ – вложение полей, то K – алгебра над F. (Например, $\mathbb{C}$ – алгебра над $\mathbb{R}$);

5) $\mathbb{H}$ – алгебра кватернионов над $\mathbb{R}$.

$\mathbb{H} = \langle 1, i, j, k\rangle_{\mathbb{R}}$, где умножение базисных элементов происходит как в Q_8. $\mathbb{H}$ – ассоциативная не коммутативная 4-мерная алгебра с единицей над $\mathbb{R}$.

Пусть $q = a + bi + cj + dk$. Определим сопряженный кватернион $\overline{q} = a - bi - cj - dk$. Тогда $q\overline{q} = a^2 - (bi + cj + dk)^2 = a^2 + b^2 + c^2 + d^2 = |q|^2$.

Определение 70. Алгебра называется *алгеброй с делением*, если любой ненулевой элемент в ней обратим.

Из доказанного выше получаем следующую лемму.

Лемма 49. *$\mathbb{H}$ – алгебра с делением.*

Определение 71. *Гомоморфизм колец* – это отображение $\varphi\colon R \to S$ такое, что для любых $r_1, r_2 \in R$ выполнено $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ и $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$.

Гомоморфизм алгебр – это гомоморфизм колец $\varphi\colon A \to B$ такой, что, $\varphi(\lambda a) = \lambda\varphi(a)$.

Изоморфизм – это биективный гомоморфизм.

Замечание 29. Если A – алгебра с единицей 1_A, то поле F вкладывается в A по правилу $f \mapsto f1_A$. Поэтому если A – алгебра с единицей, то любой гомоморфизм колец $A \to B$ в алгебру B автоматически является гомоморфизмом алгебр.

Упражнение 7. Докажите, что алгебра $\mathbb{H}$ изоморфна алгебре вещественных матриц вида

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & -c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix},$$

а также алгебре комплексных матриц вида

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}.$$

Определение 72. Пусть R – кольцо. Подмножество I в R называется *левым идеалом*, если I – подгруппа по сложению и для любых $r \in R, i \in I$ выполнено $ri \in I$.

Пусть R – кольцо. Подмножество I в R называется *правым идеалом*, если I – подгруппа по сложению и для любых $r \in R, i \in I$ выполнено $ir \in I$.

Идеал *двусторонний*, если он и левый и правый идеал.

Пример 35. *Пусть $x \in R$ рассмотрим $I = (x) = \{rx\}$. Легко видеть, что I – левый идеал.*

Аналогично, $J = \{xr\}$ – правый идеал.

Пусть M – подмножество R. Тогда $I = (M) = \{\sum r_i m_i \mid r_i \in R, m_i \in M\}$ – левый идеал M.

Лемма 50. *Пусть R – кольцо с единицей. Тогда (M) – минимальный левый идеал, содержащий M.*

Доказательство. Пусть $u = \sum r_i m_i$ и $v = \sum r'_i m_i$ – произвольные элементы в (M).Тогда $u + v = \sum(r_i + r'_i)m_i \in (M)$, $-u = \sum(-r_i)m_i \in M$, $ru = \sum rr_i m_i \in (M)$. Таким образом, (M) – левый идеал.

Если J – левый идеал, содержащий M, то $r_i m_i \in J$, а значит, $\sum r_i m_i \in J$. То есть $(M) \subset J$. □

Определение 73. Пусть $\varphi\colon R \to S$ – гомоморфизм. Ядро φ – это полный прообраз нуля, то есть $\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\}$. Образ гомоморфизма – это множество образов всех элементов.

Лемма 51. *Пусть $\varphi\colon R \to S$ – гомоморфизм. Тогда ядро – это двусторонний идеал в R, а образ – подкольцо в S.*

Доказательство. Пусть $u, v \in \operatorname{Ker}\varphi$. Тогда $\varphi(u+v) = \varphi(u) + \varphi(v) = 0$, то есть $u + v \in \operatorname{Ker}\varphi$. Кроме того $\varphi(-u) = -\varphi(u) = 0$. Значит, $-u \in \operatorname{Ker}\varphi$. А также $\varphi(ru) = \varphi(r)\varphi(u) = \varphi(r)0 = 0, \qquad \varphi(ur) = 0\varphi(r) = 0$. То есть $ru, ur \in \operatorname{Ker}\varphi$. Значит, ядро – это двусторонний идеал.

Образ гомоморфизма замкнут относительно суммы, взятия противоположного и произведения. В самом деле $\varphi(a) + \varphi(b) = \varphi(a+b)$, $\varphi(-a) = -\varphi(a)$, $\varphi(a)\varphi(b) = \varphi(ab)$. Значит, образ – подкольцо. □

Определение 74. Факторкольцо R/I кольца R по двустороннему идеалу I – это множество смежных классов $r + I$ с операциями

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I;$$

$$(r_1 + I)(r_2 + I) = (r_1 r_2) + I.$$

Теорема 40 (Теорема о гомоморфизме)**.** *Пусть $\varphi\colon R \to S$ – гомоморфизм колец. Тогда $R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.*

Доказательство. Построим отображение $\Psi\colon R/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$, $r + \operatorname{Ker}\varphi \mapsto \varphi(r)$. Надо проверить 1) что это отображение корректно, 2) что это гомоморфизм, 3) что это биекция.

1) Пусть $r + \operatorname{Ker}\varphi = s + \operatorname{Ker}\varphi$. Это означает, что $r - s \in \operatorname{Ker}\varphi$. Тогда $\varphi(r) = \varphi(s)$.

2) Проверим, что Ψ – гомоморфизм:

$$\Psi((r + \operatorname{Ker}\varphi) + (s + \operatorname{Ker}\varphi)) = \Psi((r+s) + \operatorname{Ker}\varphi) = \\ = \varphi(r+s) = \varphi(r) + \varphi(s) = \Psi(r + \operatorname{Ker}\varphi) + \Psi(s + \operatorname{Ker}\varphi)$$

$$\Psi((r + \operatorname{Ker}\varphi)(s + \operatorname{Ker}\varphi)) = \Psi((rs) + \operatorname{Ker}\varphi) = \varphi(rs) = \\ = \varphi(r)\varphi(s) = \Psi(r + \operatorname{Ker}\varphi)\Psi(s + \operatorname{Ker}\varphi).$$

3) $\operatorname{Ker}\Psi = \{r + \operatorname{Ker}\varphi \mid \varphi(r) = 0\}$. То есть $\operatorname{Ker}\Psi$ состоит только из одного смежного класса $\operatorname{Ker}\varphi$. Это доказывает инъективность.

Сюръективность Ψ очевидна.

□

Лекция 20

Определение 75. Прямое произведение колец R_1 и R_2 – это кольцо $R_1 \times R_2$, состоящее из множества пар (r_1, r_2), $r_1 \in R_1$, $r_2 \in R_2$ с операциями $(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', r_2 + r_2')$, $(r_1, r_2) \cdot (r_1', r_2') = (r_1 \cdot r_1', r_2 \cdot r_2')$.

В $R_1 \times R_2$ всегда есть делители нуля: $(a, 0) \cdot (0, b) = (0, 0)$.

Пример 36 (Примеры применения теоремы о гомоморфизме колец.)**. 1.** *Рассмотрим гомоморфизм* $\varphi\colon R_1 \times R_2 \to R_2$, $\varphi(r_1, r_2) = r_2$. *Имеем,* $\operatorname{Ker}\varphi = R_1 \times \{0\}$. *По теореме о гомоморфизме* $(R_1 \times R_2)/(R_1 \times \{0\}) \cong R_2$.

2. Теорема о факторизации прямого произведения. *Пусть* $R_1, \ldots, R_n$ *– кольца. И в каждом* R_j *фиксирован идеал* I_j. *Тогда*

$$(R_1 \times \ldots \times R_n)/(I_1 \times \ldots \times I_n) \cong R_1/I_1 \times \ldots \times R_n/I_n.$$

Доказательство. *Рассмотрим гомоморфизм* $\varphi\colon R_1 \times \ldots \times R_n \to R_1/I_1 \times \ldots \times R_n/I_n$, $\varphi(r_1, \ldots, r_n) = (r_1 + I_1, \ldots, r_n + I_n)$.

Гомоморфизм φ *сюръективен и* $\operatorname{Ker}\varphi = I_1 \times \ldots \times I_n$.

3. *Пусть* F *– поле. Рассмотрим идеал* $(x - c)$ *в кольце* $F[x]$. *Тогда* $F[x]/(x - c) \cong F$. *Для доказательство рассмотрим гомоморфизм* $\varphi\colon F[x] \to F$, $\varphi(f(x)) = f(c)$. *Легко видеть, что* $\operatorname{Ker}\varphi = (x - c)$ *и* $\operatorname{Im}\varphi = F$.

4. *Докажем, что* $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$. *Для этого рассмотрим гомоморфизм* $\varphi\colon \mathbb{R}[x] \to \mathbb{C}$, *определенный по правилу* $\varphi(f(x)) = f(i)$. *Так как образ всех линейных многочленов* $a+bx$ *дает все комплексные числа* $a+bi$, *гомоморфизм* φ *сюръективен. Докажем, что* $\operatorname{Ker}\varphi$ *совпадает с* $(x^2 + 1)$. *Пусть* $f(x) \in \operatorname{Ker}\varphi$. *Поделим* $f(x)$ *на* $x^2 + 1$ *с остатком. Получим* $f(x) = q(x)(x^2+1) + ax + b$. *Тогда* $0 = \varphi(f(x)) = f(i) = q(i) \cdot 0 + ai + b = ai + b$.

Значит, $a = b = 0$, *то есть* $f(x)$ *делится на* $x^2 + 1$.

5. $\mathbb{R}[x]/(x^2 - 1) \cong \mathbb{R} \oplus \mathbb{R} \ncong \mathbb{C}$. *Для доказательства надо рассмотреть гомоморфизм* $\varphi\colon \mathbb{R}[x] \to \mathbb{R} \oplus \mathbb{R}$, $\varphi(f(x)) = (f(1), f(-1))$.

Теорема 41. *Пусть* F *– поле. Кольцо* $F[x]/(f)$ *является полем тогда и только тогда, когда многочлен* f *неприводим.*

Доказательство. Ясно, что $F[x]/(f)$ – коммутативное ассоциативное кольцо с единицей.

Если $f(x) = g(x)h(x)$, где $g(x)$ и $h(x)$ меньшей степни, то $g + (f) \neq 0 + (f)$, $h + (f) \neq 0 + (f)$, но $(g + (f)) \cdot (h + (f)) = 0 + (f)$. То есть в факторкольце есть делители нуля. Значит, это не поле.

Пусть теперь f неприводим и $g(x)$ не делится на $f(x)$, что эквивалентно тому, что $g(x) + (f(x)) \neq 0$. Найдем обратный к элементу $g + (f)$. Заметим, что НОД$(f, g) = 1$. Следовательно, существуют $u(x)$ и $v(x)$ такие, что $u(x)f(x) + v(x)g(x) = 1$. В факторкольце имеем $(u + (f))(f + (f)) + (v + (f))(g + (f)) = 1 + (f)$. Но $f + (f) = 0 + (f)$. Отсюда $(v + (f))(g + (f)) = 1 + (f)$. □

Заметим, что $F[x]/(f)$ – алгебра над F.

Лемма 52. *Базис этой алгебры* $\{1 + (f), x + (f), \ldots, x^{n-1} + (f)\}$, *где* $n = \deg f$.

Доказательство. Пусть $g(x) \in F[x]$. Поделим g на f с остатком: $g(x) = q(x)f(x) + r(x)$. Тогда $g + (f) = r + (f)$. Но $\deg r(x) \leq n - 1$. Значит, $r(x)$ является линейной комбинацией $1, x, \ldots, x^{n-1}$. Мы доказали, что $\{1 + (f), x + (f), \ldots, x^{n-1} + (f)\}$ – полная система.

Докажем линейную независимость. Пусть $\sum_{i=0}^{n-1} \alpha_i(x^i + (f)) = 0$. Положим $h(x) = \sum_{i=0}^{n-1} \alpha_i x^i$. Тогда $h + (f) = 0 + (f)$. Это значит, что $h \in (f)$, то есть h делится на f, чего не может быть, так как $\deg h(x) < \deg f(x)$. □

Замечание 30. Если мы имеем алгебру A размерности n над полем $\mathbb{Z}_p$, то $|A| = p^n$. В самом деле, пусть $\{e_1, \ldots, e_n\}$ – базис A. Тогда $A = \{\lambda_1 e_1 + \ldots + \lambda_n e_n \mid \lambda_i \in \mathbb{Z}_p\}$. Каждый коэффициент λ_i принимает p значений. Значит, всего p^n вариантов.

Пример 37. *Рассмотрим многочлен $f(x) = x^2 + x + 1$ в кольце $\mathbb{Z}_2[x]$. Проверим, что у $f(x)$ нет корней в $\mathbb{Z}_2$. Действительно, $f(0) = 1$, $f(1) = 1$. Так как f – многочлен второй степени и у него нет корней, он неприводим. Значит, кольцо $\mathbb{Z}_2[x]/(x^2+x+1)$ является полем из 4 элементов. Построим таблицы сложения и умножения.*

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$\mathbf{x+1}$	$\mathbf{1}$
$x+1$	0	$x+1$	$\mathbf{1}$	$\mathbf{x}$

Например, $(x + (f)) \cdot (x + (f)) = x^2 + (f) = x + 1 + (f)$.

Определение 76. Кольцо R называется *простым*, если в R нет других (двусторонних) идеалов, кроме $\{0\}$ и R.

Теорема 42. *Кольцо квадратных матриц $n \times n$ над полем является простым.*

Доказательство. Пусть I – ненулевой идеал в кольце матриц. Возьмем $A \neq 0 \in I$. Тогда найдутся i и j такие, что $a_{ij} \neq 0$. Рассмотрим $E_{ki}AE_{jl} = B \in I$. Несложно видеть, что $B = a_{ij}E_{kl}$. Так как $a_{ij} \neq 0$, получаем, $E_{kl} \in I$. Но так как числа k и l произвольные, все матричные единицы лежат в I. Но тогда для любой матрицы X имеем $X = \sum x_{ij}E_{ij} \in I$. □

Заметим, что нетривиальные односторонние (например, левые) идеалы к кольце матриц есть. Например, множество матриц, у которых первый столбец нулевой, является левым идеалом.

Задача 9. Опишите все левые и правые идеалы в кольце матриц.

Лемма 53. *Левый (правый) идеал в кольце с единицей, содержащий обратимый элемент совпадает со всем кольцом.*

Доказательство. Пусть $I \triangleleft R$ – левый идеал некоторого кольца и пусть $a \in I$ – обратимый элемент. Тогда $a^{-1}a = 1 \in I$. Но тогда для любого $r \in R$ имеем $r = r1 \in I$. □

Предложение 25. *Коммутативное (ассоциативное) кольцо с единицей является простым тогда и только тогда, когда это поле.*

Доказательство. Пусть R – поле. Тогда любой ненулевой идеал содержит обратимый элемент, и следовательно, совпадает с R.

Пусть теперь R – простое коммутативное кольцо. Рассмотрим $r \neq 0 \in R$. Тогда можно рассмотреть идеал (r). Так как в этом идеале содержится $r \neq 0$, это ненулевой идеал. Значит, $(r) = R$. Тогда $1 \in (r)$, что означает $1 = xr$. □

Определение 77. Коммутативное кольцо с единицей называется *областью целостности* или, что то же самое *целостным кольцом*, если в нем нет делителей нуля.

Определение 78. Идеал I в кольце R называется *простым*, если из того, что $ab \in I$ следует, что $a \in I$ или $b \in I$.

Пример 38. *Идеал (n) в кольце $\mathbb{Z}$ является простым тогда и только тогда, когда число n простое.*

Предложение 26. *Факторкольцо R/I не имеет делителей нуля тогда и только тогда, когда I – простой идеал.*

Доказательство. Пусть $a + I$ и $b + I$ – ненулевые смежные классы. Это значит, что $a, b \notin I$. Тогда $(a + I)(b + I) = 0$ равносильно $ab \in I$. Но существование таких a и b, что $a, b \notin I$, а $ab \in I$ равносильно тому, что идеал I не простой. □

Определение 79. Идеал I в кольце R называется *максимальным*, если не существует идеала $J \lhd R$ такого, что $I \subsetneq J \subsetneq R$.

Лемма 54. *Пусть $\psi\colon R \to S$ – гомоморфизм колец. Пусть J – идеал в S. Тогда полный прообраз $\psi^{-1}(J)$ – это идеал в R.*

Доказательство. Пусть $a, b \in \psi^{-1}(J)$. Тогда $\psi(a + b) = \psi(a) + \psi(b) \in J$ и $\psi(-a) = -\psi(a) \in J$, то есть $a + b \in \psi^{-1}(J)$ и $-a \in \psi^{-1}(J)$. Кроме того $\psi(ra) = \psi(r)\psi(a) \in J$, $\psi(ar) = \psi(a)\psi(r) \in J$, то есть $ra, ar \in \psi^{-1}(J)$. □

Лемма 55. *Пусть $\psi\colon R \to S$ – сюръективный гомоморфизм колец. И пусть I – идеал в R. Тогда $\psi(I)$ – идеал в S.*

Доказательство. Пусть $a = \psi(x)$, $b = \psi(y)$, где $x, y \in I$. Тогда $x + y \in I$ и $\psi(x + y) = a + b \in \psi(I)$. И $-a = \psi(-x) \in \psi(I)$. Для любого $s \in S$ имеем $s = \psi(r)$ для некоторого $r \in R$. Тогда $sa = \psi(rx) \in \psi(I)$. □

Теорема 43. *Пусть R – коммутативное кольцо с единицей. Факторкольцо R/I – поле тогда и только тогда, когда I – максимальный идеал.*

Доказательство. Рассмотрим канонический гомоморфизм (колец) $\pi_I\colon R \to R/I$, $\operatorname{Ker} \pi_I = I$. Существование собственного идеала J такого, что $I \subsetneq J \subsetneq R$ равносильно существованию промежуточного идеала $\{0\} \subsetneq L \subsetneq R/I$ такого, что $\pi_I^{-1}(L) = J$. Но существование такого L равносильно тому, что R/I – не поле. □

Определение 80. Пусть R – область целостности, не являющаяся полем. Тогда R называется *евклидовым кольцом*, если задана функция (*евклидова норма*) $N\colon R\setminus\{0\} \to \mathbb{N} \cup \{0\}$ такая, что

1) $N(ab) \geq N(a)$ для любых $a, b \in R \setminus \{0\}$

2) для любых $a, b \in R$, $b \neq 0$ возможно "деление с остатком то есть существуют такие $q, r \in R$, что $a = bq + r$, причем либо $N(r) < N(b)$, либо $r = 0$.

Пример 39. *1)* $R = \mathbb{Z}$, $N(a) = |a|$.

2) $R = F[x]$, $N(f) = \deg f$.

3) **Задача.** *Докажите, что $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ – евклидово кольцо с нормой $N(z) = |z|$.*

4) **Задача.** *Для каких $c \in \mathbb{R}$ кольцо $\mathbb{Z}[ci] = \{a + bci \mid a, b \in \mathbb{Z}\}$ является евклидовым кольцом с нормой $N(z) = |z|$?*

Лекция 21

Определение 81. Коммутативное кольцо R с единицей назовем *кольцом главных идеалов*, если любой идеал в нем главный, то есть равен (r) для некоторого $r \in R$.

Пример 40. *Идеал (x, y) в $F[x, y]$ не является главным. Действительно, если $(x, y) = (f)$, то f делит и x и y. Тогда f – константа и $(f) = F[x, y]$.*

Теорема 44. *Евсклидово кольцо является кольцом главных идеалов.*

Доказательство. Пусть R – евклидово кольцо с нормой N. И пусть $I \triangleleft R$. Если $I \neq \{0\}$, рассмотрим ненулевой элемент $a \in I$ с минимальной нормой. Пусть $b \in I$. Тогда $b = aq + r$. Предположим, что $r \neq 0$. Получаем $r \in I$, $N(r) < N(a)$. Противоречие с выбором a. Значит, $r = 0$, то есть $b \in (a)$. Следовательно, $I = (a)$. □

Определение 82. Пусть a и b – два элемента кольца главных идеалов. Рассмотрим $(a, b) = (d)$. Назовем d *наибольшим общим делителем* a и b. (НОД определен с точностью до обратимого множителя.)

Имеем $d \mid a$, $d \mid b$, $d = ua + vb$.

Определение 83. 1) Пусть R – область целостности. Необратимый элемент $r \in R$ называется *неприводимым*, если из $ab = r$ следует, что либо a, либо b обратим.

2) Два элемента $u, v \in R$ называются *ассоциированными*, если $u = cv$, где c – обратимый элемент.

3) Кольцо R называется *факториальным*, если любой элемент раскладывается в произведение неприводимых единственным способом с точностью до порядка и ассоциированности сомножителей.

Лемма 56. *Пусть R – кольцо главных идеалов, p – неприводимый элемент. Допустим, что $p \mid ab$. Тогда либо $p \mid a$, либо $p \mid b$.*

Доказательство. Пусть $s = \text{НОД}(a, p)$. Тогда $s \mid p$. Значит, либо s ассоциирован с p, либо с 1. Если $s = p$, то $p \mid a$. Если же $s = 1$, то существуют $u, v \in R$ такие, что $ua + vp = 1$. Домножим это равенство на b. Получим $uab + vpb = b$. Левая часть делится на p. Значит, и правая часть делится на p. □

Следствие 25. *Пусть R – кольцо главных идеалов, p – неприводимый элемент. Допустим, что $p \mid a_1 a_2 \dots a_k$. Тогда найдется j такой, что $p \mid a_j$.*

Теорема 45. *Кольцо главных идеалов факториально.*

Доказательство. **Существование.** Пусть R – кольцо главных идеалов и $a \in R$. Если a не является неприводимым, то $a = bc$ для некоторых необратимых b и c. Тогда имеем $(a) \subsetneq (b)$ и $(a) \subsetneq (c)$. Если оба множителя неприводимы, то получено разложение. Иначе какой-то из них снова можно разложить, что даст увеличение идеала и т.д. Если разложения так и не будет, получим бесконечно возрастающую цепочку $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \dots$

Рассмотрим $I = \cup(a_i)$. Легко видеть, что I – идеал. Значит, $I = (b)$. Но $b \in \cup(a_i)$, значит, найдется j такой, что $b \in (a_j)$. Тогда $I = (a_j)$. То есть бесконечно возрастающих цепочек не может быть.

Единственность. Пусть $a = p_1 \dots p_k = q_1 \dots q_m$ – два разложения на неприводимые. Тогда $p_1 \mid q_1 \dots q_m$. Значит, существует j такое, что $p_1 \mid q_j$. Так как p_1 и q_j неприводимы, они ассоциированы. Значит, перебрасывая обратимый элемент в другой множитель и меняя нумерацию, можно считать $p_1 = q_1$.

$$p_1 p_2 \dots p_k = p_1 q_2 \dots q_m.$$

Перенесем все в одну часть.

$$p_1(p_2 \dots p_k - q_2 \dots q_m) = 0.$$

Так как $p_1 \neq 0$ и в R нет делителей нуля, получаем $p_2 \dots p_k = q_2 \dots q_m$ и т.д. □

Определение 84. Пусть F – поле. *Характеристика* поля F – это минимальное натуральное n такое, что сумма n единиц равна нулю $1 + 1 + \ldots + 1 = 0$. Если такого n не существует, характеристика поля равна нулю. Обозначается характеристика через $\operatorname{char} F$.

Пример 41. *1)* $\operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C} = \operatorname{char}\mathbb{Q} = 0$.
2) $\operatorname{char}\mathbb{Z}_p = p$.
3) $\operatorname{char}\mathbb{Z}_p[x]/(f) = p$.

Лемма 57. *Характеристика поля – либо ноль, либо простое число.*

Доказательство. Допустим, что характеристика поля F равна lm.
$0 = \underbrace{1 + 1 + \ldots + 1}_{lm \text{ раз}} = (\underbrace{1 + \ldots + 1}_{l \text{ раз}})(\underbrace{1 + \ldots + 1}_{m \text{ раз}})$.
Так как в поле нет делителей нуля, одна из скобок равна 0. □

Определение 85. Простое поле – это поле, в котором нет собственных подполей. (Мы считаем, что в поле $0 \neq 1$, а значит, $\{0\}$ – не подполе.)

Предложение 27. *В каждом поле F есть простое подполе. Если* $\operatorname{char} F = 0$*, то оно изоморфно $\mathbb{Q}$. Если же* $\operatorname{char} F = p$*, то оно изоморфно $\mathbb{Z}_p$.*

Доказательство. 1) Пусть $\operatorname{char} F = p$, рассмотрим
$K = \{0, 1, \underbrace{1 + 1, 1 + 1 + 1, \ldots, 1 + 1 + \ldots + 1}_{\text{(p-1) раз}}\}$
Тогда K – подполе в F, изоморфное $\mathbb{Z}_p$.
2) Пусть $\operatorname{char} F = 0$. Рассмотрим $L = \{0, 1, -1, 1 + 1, -(1 + 1), \ldots\}$. Тогда L – подкольцо в F, изоморфное $\mathbb{Z}$. Рассмотрим отношения всех элементов из L, такие, что знаменатель не ноль. Получим подполе K, изоморфное $\mathbb{Q}$. □

Следствие 26. *Количество элементов в конечном поле является степенью простого числа (равного характеристике данного поля).*

Доказательство. Если поле F конечно, то его характеристика не равна нулю. Значит, в нем содержится простое подполе $E \cong \mathbb{Z}_p$. Тогда F – векторное пространство над E. Так как $|F| < \infty$, то и $\dim_E F < \infty$. Пусть $\dim_E F = n$. Тогда $|F| = p^n$. □

Пусть $\operatorname{char} F = p$. Рассмотрим следующее отображение $\varphi\colon F \to F$, $\varphi(x) = x^p$.

Предложение 28. *Отображение φ является инъективным гомоморфизмом.*

Доказательство. Очевидно, что $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$. Проверим сохранение сложения: $\varphi(a+b) = (a+b)^p = \sum_{i=0}^{p} C_p^i a^i b^{p-i}$. Так как число p простое, биномиальный коэффициент $C_p^i = \frac{p!}{i!(p-i)!}$ делится на p при $i \notin \{0, p\}$. Так как характеристика поля F равна p, в поле F коэффициент C_p^i равен 0. Значит, в F выполнено $(a+b)^p = a^p + b^p$.

Итак, φ – гомоморфизм. При этом $\operatorname{Ker}\varphi = \{0\}$, поскольку из $a^p = 0$ следует $a = 0$. (В поле нет делителей нуля.) □

Определение 86. При $|F| < \infty$, φ – автоморфизм, он называется *автоморфизмом Фробениуса*. Если $|F| = \infty$, то φ может быть не сюръективен.

Заметим, что гомоморфизм из поля в какое-либо кольцо либо нулевой, либо вложение (так как в поле нет нетривиальных идеалов). Значит, изучение гоморфизмов между полями сводится к изучению вложений.

Определение 87. Пусть E – подполе поля F. Тогда поле F называется *расширением* поля E.

Определение 88. Элемент $a \in F$ называется *алгебраическим* над E, если существует ненулевой многочлен $h(x)$ с коэффициентами из E такой, что $h(a) = 0$.

Иначе элемент a называется *трансцендентным* над E.

Определение 89. Расширение полей $E \subset F$ называется *алгебраическим*, если любой элемент $a \in F$ является алгебраическим над E.

Расширение полей $E \subset F$ конечным, если $\dim_E F < \infty$.

Предложение 29. *Конечное расширение алгебраическое.*

Доказательство. Пусть $a \in F$ и $\dim_E F = n$. Тогда элементы $1, a, a^2, \ldots, a^n$ линейно зависимы над E. Значит, существуют $c_0, c_1, \ldots, c_n \in E$ такие, что $c_0 + c_1 a + c_2 a^2 + \ldots + c_n a^n = 0$, то есть a алгебраический над E. □

Для любого алгебраического элемента a можно определить минимальный многочлен $f_{min}(x)$ такой, что это многочлен минимальной степени с коэффициентами из E, для которого верно $f_{min}(a) = 0$. Легко показать, что f_{min} неприводим над E и любой многочлен $h(x)$, для которого $h(a) = 0$ делится на f_{min}. Отсюда следует, что f_{min} определен однозначно с точностью до пропорциональности.

Теорема 46 (Теорема о башне расширений)**.** *Пусть $E \subset F$ и $F \subset K$ – конечные расширения полей, причем $\dim_E F = m$, $\dim_F K = n$. Тогда расширение $E \subset K$ такиже конечное и $\dim_E K = mn$.*

Доказательство. Пусть $\{f_1, \ldots, f_m\}$ – базис F над E и $\{k_1, \ldots, k_n\}$ – базис K над F. Тогда для любого $k \in K$ выполнено $k = \sum \lambda_i k_i$, $\lambda_i \in F$. При этом $\lambda_i = \sum_{j=1}^{n} \mu_{ij} f_j$, $\mu_{ij} \in E$. Получается, что $k = \sum_{i,j} \mu_{ij} f_j k_i$. Таким образом, система $f_j k_i$ полная в K над E. Докажем линейную независимость. Пусть $\sum_{ij} \mu_{ij} f_j k_i = 0$. Тогда $\sum_i (\sum_j \mu_{ij} f_j) k_i = 0$. Так как $\{k_1, \ldots, k_n\}$ – базис K, имеем для каждого i: $\sum_j \mu_{ij} f_j = 0$. Значит, так как $\{f_1, \ldots, f_m\}$ – базис F, получаем $\mu_{ij} = 0$ для всех i и j. □

Определение 90. Пусть $E \subset F$ – расширение полей. Пусть S – некоторое подмножество F. Назовем минимальное подполе в F, содержащее E и S *полем, порожденным S над E* и будем обозначать $E(S)$.

Лемма 58. *Поле $E(S)$ состоит из элементов $\frac{g(s_1,\ldots,s_n)}{h(s_1,\ldots,s_n)}$ для всех возможных конечных наборов $s_1, \ldots, s_n$ и многочленов $g, h \in E[y_1, \ldots, y_n]$ с условием $h(s_1, \ldots, s_n) \neq 0$.*

Доказательство. Так как в поле $E(S)$ лежат все s_i и коэффициенты из E, и в этом поле можно складывать и умножать, значит, любой многочлен $g(s_1, \ldots, s_n) \in E(S)$. Так как в этом поле можно делить, $\frac{g(s_1,\ldots,s_n)}{h(s_1,\ldots,s_n)} \in E(S)$. С другой стороны, множество дробей $\frac{g(s_1,\ldots,s_n)}{h(s_1,\ldots,s_n)}$ замкнуто относительно сложения, умножения, взятия противоположного и обратного к ненулевому элементу. Значит, это подполе. □

Лемма 59. *Пусть элемент $a \in F$ алгебраический над $E \subset F$ причем $\deg f_{min} = n$. Тогда $E(a) = \{P(a) \mid \deg P < \deg f_{min}\}$. В частности расширение $E \subset E(a)$ конечное степени n.*

Доказательство. Рассмотрим $\frac{g(a)}{h(a)} \in E(a)$. Так как $h(a) \neq 0$, $h(x)$ не делится на $f_{min}(x)$. Значит, так как f_{min} неприводим, НОД$(h, f_{min}) = 1$, то есть существуют $u(x)$ и $v(x)$ такие, что $uh + vf_{min} = 1$. Домножим числитель $\frac{g(x)}{h(x)}$ на 1:

$\frac{g(x)}{h(x)} = \frac{g(uh+vf_{min})}{h} = gu + \frac{gvf_{min}}{h}$.

Теперь подставим сюда $x = a$, учитывая $f_{min}(a) = 0$, получаем $\frac{g(a)}{h(a)} = g(a)u(a) = Q(a)$. Далее поделим $Q(x)$ на $f_{min}(x)$ с остатком: $Q(x) = q(x)f_{min}(x) + P(x)$, $\deg P < n$. Подставляя a, получаем $Q(a) = P(a)$. □

Следствие 27. *Поле, порожденное конечным числом алгебраических элементов дает конечное расширение.*

Доказательство. В цепочке $E \subset E(a_1) \subset E(a_1, a_2) \subset \dots E(a_1, \dots, a_n)$ все расширения конечны. Значит, и $E \subset E(a_1, \dots, a_n)$ конечно. □

Лекция 22

Предложение 30. *Пусть $f(x) \in F[x]$ – неразложимый многочлен. Тогда $F[x]/(f(x)) = F(x + (f(x)))$*

Доказательство. $F[x]/(f) = \{g(x) + (f)\}$. Элемент $y = x + (f)$ алгебраический над F так как $f(y) = f(x) + (f) = 0$. Так как f неприводим, это минимальный многочлен y. Значит, $F(y) = F[y] = F[x]/(f)$. □

Определение 91. Расширение $F[x]/(f)$ называется *присоединением корня* многочлена f к полю F.

Определение 92. Пусть $h(x) \in F[x]$. Расширение $F \subset K$ называется полем разложения $h(x)$, если $h(x)$ разлагается в $K[x]$ на линейные множители и K порождается над F корнями $h(x)$.

Теорема 47. *Поле разложения любого многочлена $h \in F[x]$ существует.*

Доказательство. Разложим $h(x)$ на неприводимые множители над F. Пусть h_1 – один из этих неприводимых множителей степени больше 1. (Если таких нет, то $K = F$.) Положим $F_1 = F[x]/(h_1)$. Это расширение F, в котором у h_1 есть корень. Таким образом, $h(x)$ над F_1 разлагается на большее число неприводимых множителей, чем над F. Если все они линейны, то $K = F_1$. Иначе снова выберем один из множителей степени ≥ 2 и присоединим его корень и так далее пока не дойдчм до поля, в котором h разлагается на линейные множители. Так как мы каждый раз присоединяли некоторый корень $h(x)$, в итоге мы получим поле разложения h над F. □

Следствие 28. *Для любого простого p и натурального n существует поле из p^n элементов.*

Доказательство. Рассмотрим поле разложения многочлена $x^{p^n} - x$ над $\mathbb{Z}_p$. У этого многочлена нет кратных корней. В самом деле, кратные корни – это общие корни многочлена и его производной. Но $(x^{p^n} - x)' = p^n x^{p^n - 1} - 1 = -1$. Последнее равенство верно так как мы находимся над $\mathbb{Z}_p$. Значит, у многочлена $x^{p^n} - x$ ровно $q = p^n$ корней. Докажем, что множество корней образует подполе.

В самом деле, пусть $a^q = a$ и $b^q = b$. Так как возведение в p^n степень – это n-я степень автоморфизма Фробениуса, $(ab)^q = a^q b^q = ab$, $(a+b)^q = a^q + b^q$,$(-a)^q = -a$, $(a^{-1})^q = a^{-1}$. Значит, множество корней многочлена $x^{p^n} - x$ образует подполе. □

Предложение 31. *Пусть $f(x) = a_n x^n + \ldots + a_0 \in F[x]$ – неприводимый многочлен. Пусть $F(\alpha)$ – поле, полученное присоединением корня α к полю F. И пусть φ – вложение $F \hookrightarrow K$, где K – некоторое поле. Вложение φ продолжается до вложения $\widetilde{\varphi}\colon F(\alpha) \hookrightarrow K$ столькими способами, сколько различных корней у многочлена $\varphi(f)(x) = \varphi(a_n)x^n + \ldots + \varphi(a_0)$.*

Доказательство. Пусть $\widetilde{\varphi}$ существует. Положим $\beta = \varphi(\alpha)$. Тогда

$$0 = \widetilde{\varphi}(0) = \widetilde{\varphi}(a_n\alpha^n + \ldots + a_0) = \varphi(a_n)\alpha^n + \ldots + \varphi(a_0) = \varphi(f)(\beta).$$

То есть β – это корень $\varphi(f)$.

Напротив, если β – это корень $\varphi(f)$, то формула

$$\widetilde{\varphi}(b_k\alpha^k + \ldots + b_0) = \varphi(b_k)\beta^k + \ldots + \varphi(b_0)$$

задает некоторое продолжение вложения φ, которое является ненулевым гомоморфизмом $F(\alpha) \to K$, а следовательно, вложением. □

Теорема 48. *Поле разложения многочлена $h(x)$ над F единственно с точностью до изоморфизма над F. (То есть этот изоморфизм оставляет элементы F на месте.)*

Доказательство. Мы построили L – одно из полей разложения $h(x)$ как цепочку расширений $L_0 = F \subset L_1 \subset \ldots \subset L_s = L, L_{i+1} = L_i(\alpha)$ для некоторого корня α неприводимого делителя $f(x)$, $\deg f \geq 2$, многочлена $h(x)$. Пусть K – некоторое другое поле разложения h над F. Тогда есть естественное вложение $\varphi_0\colon F \hookrightarrow K$. Докажем по индукции, что для каждого i существует вложение $\varphi_{i+1}\colon L_{i+1} \hookrightarrow K$ продолжающее вложение $\varphi_i\colon L_i \hookrightarrow K$. По предложению φ_i может быть продолжен до φ_{i+1} столькими способами, сколько корней у $\varphi_i(f)(x)$ в K. Однако $\varphi_i(f)(x)$ – делитель $h(x)$ в $K[x]$. Значит, у него есть корень. Итак, существует вложение $\varphi_s\colon L \hookrightarrow K$, которое неподвижно на F. Осталось доказать сюръективность φ_s. Но если вложение φ_s не сюръективно, то его образ – это собственное подполе K, в котором h разлагается на линейные множители. Значит, K – не поле разложения. □

Лемма 60. *Пусть $|F| = p^n = q$. Тогда каждый элемент $a \in F$ является корнем многочлена $x^q ? x$.*

Доказательство. Очевидно, что ноль является корнем данного многочлена. Пусть $a \in F \setminus \{0\}$. Тогда a лежит в мультипликативной группе $F^\times$. При этом $|F^\times| = q-1$. Значит, по следствию из теоремы Лагранжа, $a^{q-1} = 1$. Умножая обе части на a, получаем $a^q = a$. □

Следствие 29. *F – поле разложения $x^q - x$ над $\mathbb{Z}_p$.*

Доказательство. Так как $|F| = p^n$, имеем $\mathrm{char}F = p$. А значит, в F содержится простое подполе, изоморфное $\mathbb{Z}_p$. Так как любой элемент F – это корень $x^q - x$ и $|F| = q$, многочлен $x^q - x$ имеет q корней в F, а значит, раскладывается на линейные множители. □

Из теоремы 48 и следствия 29 следует следующая теорема.

Теорема 49. *. Поле из p^n элементов единственно с точностью до изоморфизма.*

Поле из p^n элементов обозначается $\mathbb{F}_{p^n}$.

Лемма 61. *Пусть ψ – автоморфизм поля F. Тогда неподвижные относительно ψ элементы в F образуют подполе $E \subset F$.*

Доказательство. Пусть $\psi(a) = a$ и $\psi(b) = b$. Тогда $\psi(a+b) = \psi(a) + \psi(b) = a + b$, $\psi(ab) = \psi(a)\psi(b) = ab$, $\psi(-a) = -a$, если $a \neq 0$, то $\psi(a^{-1}) = a^{-1}$. То есть множество неподвижных элементов замкнуто относительно сложения, умножения, взятия противоположного и взятия обратного к ненулевому элементу. Значит, это подполе. □

Теорема 50. *В поле F_{p^n} есть подполе, изоморфное F_{p^m} тогда и только тогда, когда $m \mid n$.*

Доказательство. Если $L = F_{p^n}$ содержит подполе $K = F_{p^m}$, то L – векторное пространство над K, а значит, $p^n = |L| = |K|^s = p^{sm}$ где $s = \dim_K L$. То есть $n = sm$.

Наоборот, пусть $n = sm$. Тогда $p^n - 1 = (p^m)^s - 1 = (p^m - 1)t$. Откуда

$$x^{p^n} - x = x(x^{p^n-1} - 1) = x(x^{p^m-1} - 1)T.$$

Таким образом, $x^{p^n} - x$ делится на $x^{p^m} - x$. Элементы, являющиеся корнями $x^{p^m} - x$ образуют подполе, так как это элементы, неподвижные относительно автоморфизма $\psi\colon a \to a^{p^m}$, который является m-ой степенью автоморфизма Фробениуса. Таких элементов p^m, так как $x^{p^n} - x$ имеет p^n различных корней. □

Лекция 23

Теорема 51. *Пусть K – расширение поля F. Рассмотрим множество $\overline{F}_K \subset K$, состоящее из всех элементов K, алгебраичных над F. Тогда $\overline{F}_K$ – поле и если $k \in K$ алгебраичен над $\overline{F}_K$, то он алгебраичен над F.*

Доказательство. Возьмем $a, b \in \overline{F}_K$. Так как a алгебраичен над F, $F \subset F(a)$ – конечное расширение. Элемент b алгебраичен над F, и следовательно, он алгебраичен и над $F(a)$. Тогда $F(a) \subset F(a)(b) = F(a,b)$ – конечное расширение. По теореме о башне расширений $F \subset F(a,b)$ – конечное расширение. Элементы $a+b, ab, -a, a^{-1}$ лежат в $F(a,b)$. Значит, все они алгебраические над F.

Пусть k удовлетворяет уравнению $a_n k^n + \ldots + a_0 = 0$, $a_i \in \overline{F}_K$. Рассмотрим $F(a_0, \ldots, a_n)$ – конечное расширение F. Получаем, что k алгебрачен над $F(a_0, \ldots, a_n)$, то есть $F(a_0, \ldots, a_n)(k)$ – конечное расширение $F(a_0, \ldots, a_n)$. По теореме о башне расширений $F(a_0, \ldots, a_n)(k) = F(a_0, \ldots, a_n, k)$ – конечное расширение F, а значит, $k \in \overline{F}_K$. □

Поле $\overline{F}_K$ называется *алгебраическим замыканием* поля F в K.

Зачастую есть необходимость вложить поле F в алгебраически замкнутое поле. Минимальное по включению такое поле называется *алгебраическим замыканием* $K = \overline{F}$ поля F. Минимальность по включению означает, что $\overline{F}_K = K$.

Как это сделать? Нужно добавить все корни всех многочленов с коэффициентами из F. Однако поскольку коэффициентов вообще говоря бесконечное количество и многочленов также бесконечное количество, то вообще говоря здесь нужны трансфинитные методы. проследим за конечным полем $\mathbb{F}_p = \mathbb{Z}_p$.

Теорема 52. *Объединение цепочки вложенных полей $K = \mathbb{F}_p \subset \mathbb{F}_{p^{2!}} \subset \mathbb{F}_{p^{3!}} \subset \ldots$ – это алгебраическое замыкание $\overline{\mathbb{F}_p}$.*

Доказательство. Пусть $f(x) = a_m x^m + \ldots + a_0$ – неприводимый многочлен над K. Тогда существует n такое, что все a_i лежат в $\mathbb{F}_{p^{n!}}$. Тогда можно рассмотреть поле $\mathbb{F}_{p^{n!}}[x]/(f) \cong \mathbb{F}_{p^{n!\cdot m}}$, в котором у f есть корень. Тогда $\mathbb{F}_{p^{n!\cdot m}} \subset \mathbb{F}_{p^{(mn)!}} \subset K$, а значит, у $f(x)$ есть корень в поле K.

С другой стороны поле K сочтоит из элементов, каждый из которых является корнем некоторого многочлена над $\mathbb{F}_p$, а значит, оно минимальное расширение $\mathbb{F}_p$ с условием алгебраической замкнутости. □

Алгебры с делением.

Определение 93. (Ассоциативное) кольцо с единицей называется *телом*, если каждый ненулевой элемент в нем обратим.

Алгебра, являющаяся телом, называется *алгеброй с делением.*

Замечание 31. Центр $Z(D)$ любого тела D – это поле. И тело D является алгеброй с делением над $Z(D)$.

Если A – алгебра с единицей над полем F, то элементы $\lambda 1 \in A$, $\lambda \in F$ образуют подполе, изоморфное F. Далее мы будем отождествлять элементы $\lambda \in F$ и $\lambda 1 \in A$.

Лемма 62. *Пусть A – (ассоциативная) алгебра с единицей размерности n над полем F. Тогда каждый элемент $a \in A$ удовлетворяет некоторому уравнению $f(a) = 0$, где многочлен $f(x) \in F[x]$ степени не больше n. Выберем многочлен $\mu_a(x)$ минимальной степени такой, что $\mu_a(a) = 0$. Элемент a обратим тогда и только тогда, когда $\mu_a(0) \neq 0$. Если A без делителей нуля, то $\mu_a(x)$ неприводим над F и любой аннулирующий a многочлен $f(x)$ делится на $\mu_a(x)$. Алгебра A в этом случае является алгеброй с делением. Если при этом F алгебраически замкнуто, то $A = F$.*

Доказательство. Элементы $1, a, a^2, \ldots, a^n$ линейно зависимы над F, значит существуют не все нулевые c_i такие, что $\sum c_i a^i = 0$, что дает аннулирующий многочлен. Если $\mu_a(0) \neq 0$, то $0 \neq -c_0 = c_1 a + \ldots + c_k a^k = a(c_1 + \ldots + c_k a^{k-1})$. Если же $\mu_a(0) = 0$, то $a(c_1 + \ldots + c_k a^{k-1}) = 0$, то есть a – делитель нуля.

Как видно из последнего рассуждения, A либо алгебра с делением, либо допускает делители нуля. Если F алгебраически замкнуто, то неприводимый многочлен μ_a линеен. □

Теорема 53 (Теорема Фробениуса)**.** *Над полем $\mathbb{R}$ существует только 3 конечномерные ассоциативные алгебры с делением: $\mathbb{R}$, $\mathbb{C}$ и $\mathbb{H}$.*

Доказательство. Пусть $a \in A$, тогда μ_a – неприводимый над $\mathbb{R}$ многочлен. То есть либо $\mu_a(x) = x - \alpha$, тогда $a \in \mathbb{R}$, либо $\mu_a(x) = x^2 - 2\alpha x + \beta$, где $\alpha^2 < \beta$. Тогда положим $b = a - \alpha$, имеем $\mu_b(x) = x^2 + (\beta - \alpha^2)$. То есть в любом случае $a = \alpha + y$, где $y = 0$, либо $y^2 = \gamma < 0$.

Лемма 63. *Подмножество $A' = \{u \in A \mid u^2 \in \mathbb{R}, u^2 \leq 0\}$ является векторным подпространством.*

Доказательство. Ясно, что A' замкнуто относительно умножения на константу. Действительно при $\alpha \in \mathbb{R}$, $u \in A$ имеем $(\alpha u)^2 = (\alpha u)(\alpha u) = \alpha^2 u^2 \in \mathbb{R}_{\leq 0}$. Последнее равенство верно так как A – алгебра над $\mathbb{R}$.

Надо доказать, что если $u, v \in A'$, то $u + v \in A'$. Для пропорциональных u и v это ясно, поэтому далее считаем, что u и v не пропорциональны. Сначала проверим, что не может быть верным равенство $u = \alpha v + \beta$, где $\alpha, \beta \in \mathbb{R}$. Действительно иначе

имеем $\gamma = u^2 = (\alpha v + \beta)^2 = \alpha^2 v^2 + 2\alpha\beta v + \beta^2 \in \mathbb{R}$. Так как $v \notin \mathbb{R}$, имеем $\alpha\beta = 0$. То есть либо $\alpha = 0$ и u вещественное (чего не может быть), либо $\beta = 0$ и векторы u и v пропорциональны, что не так.

Итак, u, v и 1 линейно независимы.

Элементы $u + v$ и $u - v$ не лежат в $\mathbb{R}$, а значит, минимальные многочлены этих элементов квадратичны. То есть существуют $p, q, r, s \in \mathbb{R}$ такие, что $(u + v)^2 = p(u + v) + q$, $(u - v)^2 = r(u - v) + s$. Будем использовать обозначения $u^2 = \gamma, v^2 = \delta \in \mathbb{R}_{\leq 0}$. Тогда

$\gamma + uv + vu + \delta = p(u + v) + q$,

$\gamma - uv - vu + \delta = r(u - v) + s$.

Сложим эти равенства. Получим $2\gamma + 2\delta = p(u + v) + r(u - v) + q + s$, то есть $(p + r)u + (p - r)v + (q + s - 2\gamma - 2\delta) = 0$. Так как $\{1, u, v\}$ – линейно независимая система, получаем $p = r = 0$. Таким образом, $(u + v)^2 = q \in \mathbb{R}$. Но $u + v \notin \mathbb{R}$. Если $q \geq 0$, то $q = l^2$ и $(u + v - l)(u + v + l) = 0$. Значит, $q < 0$, то есть $u + v \in A'$.

Лемма доказана. □

Пусть теперь $\mathbb{R}[i] \subsetneq A$, то есть $A' \neq \mathbb{R}i$. Тогда можно выбрать $j \in A'$, $f(i, j) = 0$, $q(j) = 1$. Получаем $j^2 = -1$ и $ij + ji = 0$. Положим $k = ij$. Тогда

$$k^2 = ijij = i(ji)j = i(-ij)j = -i^2 j^2 = -1.$$

Кроме того

$$ik = iij = -j, \qquad ki = iji = i(-k) = j, \qquad kj = ijj = -i, \qquad jk = jij = (-k)j = i.$$

Таким образом, $f(i, k) = f(j, k) = 0$, то есть $\{i, j, k\}$ – линейно независимая система в A'. Значит, $\{1, i, j, k\}$ – линейно независимая система в A. Умножение в $\langle 1, i, j, k\rangle$ совпадает с умножением в $\mathbb{H}$. Если $A' = \langle i, j, k\rangle$, то теорема доказана.

Пусть теперь $A' \neq \langle i, j, k\rangle$. Тогда существует $l \neq 0 \in A'$ такой, что

$$f(i, l) = f(j, l) = f(k, l) = 0.$$

То есть $il = -li$, $jl = -lj$, $kl = -lk$. Но тогда

$$lk = l(ij) = (li)j = -(il)j = -i(lj) = i(jl) = (ij)l = kl.$$

Получаем $lk = -lk$, то есть $lk = 0$, что дает делители нуля в A. Противоречие.

□