Краткое содержание курса “Алгебра, 3 семестр” (Казахстанский филиал МГУ, лектор Марков В.Т.)

Предисловие

Этот текст не претендует ни на полноту изложения, ни на литературные достоинства — основной целью автора была краткость. В большинстве случаев приводятся только наброски доказательств (начало и конец доказательства отмечаются знаками ◀ и ▶, соответственно). Восстановление всех деталей всех доказательств — обязательное условие и хороший способ самостоятельной проверки усвоения курса.

Определения, теоремы, формулы и т.д. нумеруются с начала каждой лекции, ссылка на материал из другой лекции включает номер этой лекции, например, “теорема 5.1” означает теорему 1 из лекции 5.

Содержание

Лекция 1. Определение группы. Примеры групп. Гомоморфизм групп. Изоморфизм групп. Подгруппы. Циклические группы. Подгруппы циклических групп. Классификация циклических групп.

Определение 1. Множество $(G, \cdot)$ с одной бинарной операцией называется *группой*, если выполнены следующие аксиомы:
1. $\forall a, b, c \in G, a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (ассоциативность);
2. $\exists e \in G : \forall a \in G, e \cdot a = a \cdot e = a$ (существование нейтрального элемента — *единицы* группы);
3. $\forall a \in G\ \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = e$ (обратимость).
Единственность единицы и обратного элемента: $e = ee' = e'$, $a'a = aa'' = e \Rightarrow a'' = (a'a)a'' = a'(aa'') = a'$.
Конечные и бесконечные группы. Порядок группы $|G|$. Примеры групп ($(\mathbb{Z}, +)$ и т.д., F^*, S_n, $\mathrm{GL}(n, F)$ и т.д.).

Определение 2. Группа G называется коммутативной (абелевой), если в ней выполнено тождество *коммутативности* $\forall a, b \in G, a \cdot b = b \cdot a$.

Какие из перечисленных групп коммутативны?

Определение 3. Пусть G, H — группы. Отображение $f : G \to H$ называется *гомоморфизмом*, если $\forall a, b \in G : f(ab) = f(a)f(b)$.
Пример $\exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$. *Сохранение* единицы и обратного элемента при гомоморфизме.

Определение 4. Гомоморфизм групп, являющийся биективным (взаимно-однозначным) отображением, называется *изоморфизмом*. Если существует изоморфизм между группами G и H, то они называются *изоморфными*. Обозначение $G \cong H$.
Свойства изоморфных групп ($G \cong G$, $G \cong H \Rightarrow H \cong G$, $G \cong H\ \&\ H \cong K \Rightarrow G \cong K$.)

Определение 5. Пусть G — группа. Подмножество $H \subseteq G$ называется *подгруппой*, если H — группа относительно операции, определенной в G. Обозначение $H \leqslant G$.
Эквивалентно: H содержит единицу, H замкнута относительно умножения и обращения. Примеры ($n\mathbb{Z}$ — подгруппа, $\mathbb{N}$ — не подгруппа в $\mathbb{Z}$).
Свойства подгрупп: пересечение, гомоморфный образ.

Определение 6. Пусть G — группа, $g \in G$. Определим целые *степени* элемента g:

$$g^n = \begin{cases} \underbrace{gg\ldots g}_{n \text{ раз}} & \text{при} \quad n > 0, \\ e & \text{при} \quad n = 0 \\ (g^{-1})^{-n} & \text{при} \quad n < 0 \end{cases}$$

Подгруппа, *порождённая элементом* g: $< g >= \{g^n : n \in \mathbb{Z}\}$. Группа G называется *циклической*, если $G =< g >$ для некоторого элемента g группы G.

Определение 7. *Порядком* элемента g группы G называется наименьшее положительное число n такое, что $g^n = e$. Обозначение $n = \mathrm{ord}(g)$. Если такого числа n не существует, говорят, что g — элемент *бесконечного порядка*, $\mathrm{ord}(g) = \infty$.

Лемма. Для любого элемента g группы G, $\mathrm{ord}(g) = | < g > |$.

◀ Достаточно убедиться, что различные степени элемента бесконечного порядка различны, а среди степеней элемента G конечного порядка n различны $e = g^0, g = g^1, \ldots, g^{n-1}$.▶

Теорема 1. Подгруппы циклических групп — циклические.

◀ Пусть $G =< a >$, $H \leqslant G$. Если $H = \{e\}$, то $H =< e >$. Иначе существует $k = \min\{n > 0 : a^n \in H\}$. Тогда если $a^m \in H$, разделим с остатком m на k: $m = kq + r$, $0 \leqslant r < k$ и получим $a^r = a^m(a^k)^{-q} \in H$, и в силу выбора k, $r = 0$, т.е. $a^m = (a^k)^q$. Значит, $H =< a^k >$.▶

Теорема 2 (о классификации циклических групп). Бесконечная циклическая группа изоморфна $\mathbb{Z}$. Циклическая группа порядка n изоморфна *группе вычетов* $\mathbb{Z}_n$.

◀ Пусть $G =< a >$. Если $|G| = \infty$, то все степени $a^n : n \in \mathbb{Z}$ различны при разных показателях (см. предыдущую лемму). Поэтому отображение $n \mapsto a^n$ — изоморфизм. А если $|G| = n < \infty$, то все степени $a^k : 0 \leqslant k < n$ различны, поэтому отображение $[k] \mapsto a^k$ — изоморфизм.▶

Лекция 2. Смежные классы, их свойства. Теорема Лагранжа и её следствия. Нормальные подгруппы. Фактор-группа. Теорема о гомоморфизме. Теоремы об изоморфизме. Прямое произведение групп (внешнее), прямое произведение подгрупп, изоморфизм между ними.

Определение 1. Пусть $H \leqslant G$. Множество $gH = \{gh : h \in H\}$ называется *левым смежным классом* элемента $g \in G$ по подгруппе H. Мощность множества смежных классов по подгруппе H группы G называется *индексом* H в G (обозначение $(G : H)$).

Лемма. Пусть $H \leqslant G$, $g \in G$ и $g' \in gH$. Тогда $g'H = gH$.

◀ По условию, $g' = gh$ для некоторого $h \in H$. Но $hH = H$, и $g'H = ghH = gH$.▶

Следствие. Смежные классы по заданной подгруппе $H \leqslant G$ образуют *разбиение* группы G.

Теорема 1 (теорема Лагранжа). Пусть G — конечная группа, $H \leqslant G$. Тогда $|H| \,\big|\, |G|$.

◀ Заметим, что для любого $g \in G$, $|gH| = |H|$. Значит, $|G| = |H|(G : H)|$.▶

Следствие. Для любого элемента g конечной группы G, $\mathrm{ord}(g) \,\big|\, |G|$.

Следствие. Группа простого порядка является циклической.

Определение 2. Подгруппа $H \leqslant G$ называется *нормальной*, если $\forall g \in G : gH = Hg$, т. е. каждый левый смежный класс совпадает с правым. Обозначение $H \lhd G$.

Замечание 1. $H \lhd G \Leftrightarrow \forall g \in G, h \in H : g^{-1}hg \in H$.

Определение 3. Пусть $H \lhd G$. Множество (неважно, левых или правых) смежных классов $gH : g \in G$ с операцией $g_1Hg_2H = g_1g_2H$ называется *фактор-группой* группы G по нормальной подгруппе H.

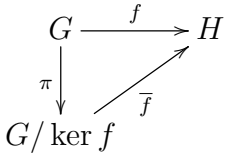
◀ Корректность! Если $g_1'H = g_1H$ и $g_2'H = g_2H$, то существуют $h_1, h_2 \in H$, такие, что $g_1' = g_1h_1$ и $g_2' = g_2h_2$. Значит, $g_1'g_2'H = g_1h_1g_2h_2H = g_1g_2\underbrace{(g_2^{-1}h_1g_2)h_2}_{\in H}H = g_1g_2H$▶

Определение 4. Пусть $H \lhd G$. Отображение $\pi : G \to G/H$, такое, что $\forall g \in G : \pi(g) = gH$, называется *каноническим гомоморфизмом* группы G на фактор-группу G/H.

Определение 5. Пусть $f : G \to H$ — гомоморфизм групп. *Ядром* гомоморфизма f называется множество $\ker f = \{g \in G : f(g) = e\}$.

Замечание 2. Пусть $f : G \to H$ — гомоморфизм групп. Тогда $\ker f \lhd G$. Обратно, если $H \lhd G$, то $\ker \pi = H$. Гомоморфизм $f : G \to H$ является изоморфизмом $\Leftrightarrow ker f = \{e\}$ и $f(G) = H$.

Теорема 2 (теорема о гомоморфизме для групп). Пусть $f : G \to H$ — гомоморфизм групп, $\pi : G \to G/\ker f$ — канонический гомоморфизм. Тогда:
1. Существует единственный гомоморфизм $\overline{f} : G/\ker f \to H$, такой, что $\overline{f}\pi = f$ (см. диаграмму)



2. $G/\ker f \cong f(G)$.
3. Существует взаимно-однозначное соответствие между множествами $\mathcal{L}(f(G))$ подгрупп группы $f(G)$ и $\mathcal{L}(G, \ker f)$ подгрупп группы G, содержащих $\ker f$, сохраняющее включение (*решеточный изоморфизм*).
4. Указанное соответствие сохраняет нормальность подгрупп.

◀ 1. Обозначим $\ker f = K$. Положим $\overline{f}(gK) = f(g)$. Требуются очевидные проверки (корректность, сохранение операций)!
2. Заметим: $gK \in \ker \overline{f} \Leftrightarrow f(g) = e \Leftrightarrow g \in K \Leftrightarrow gK = e$ в фактор-группе.
3. Любой подгруппе $B \in \mathcal{L}(f(G))$ сопоставим ее полный прообраз $f^{-1}(B)$, а подгруппе $A \in \mathcal{L}(G, K)$ — подгруппу $f(A)$.
4. Непосредственная проверка.▶

Теорема 3 (Первая теорема об изоморфизме). Пусть $H \leqslant G$, $K \lhd G$. Тогда $HK \leqslant G$, и $HK/K \cong H/(K \cap H)$.

◀ Непосредственно проверяется, что $H \cap K \lhd H$. Рассмотрим гомоморфизм $f : H \to G/K$, такой, что $f(h) = hK$. Тогда $\ker f = H \cap K$ и $f(H) = KH/K$.▶

Теорема 4 (Вторая теорема об изоморфизме). Пусть $H \leqslant G$, $K \lhd G$ и $K \subseteq H$. Тогда $H/K \leqslant G/K$, и если $H \lhd G$, то $G/H \cong (G/K)/(H/K)$.

◀ Используем гомоморфизм $f : g \mapsto gK(H/K)$.▶

Определение 6. *Прямым произведением (внешним)* групп G и H называется группа с множеством элементов $G \times H$ и операцией $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Определение 7. Группа G называется *прямым произведением (внутренним)* своих подгрупп A и B, если
1. $A \lhd G$, $B \lhd G$,
2. Любой элемент $g \in G$ единственным образом представляется в виде $g = ab$, где $a \in A$, $b \in B$.
Обозначение: $G = A \times B$.

Теорема 5. Пусть $A \lhd G$, $B \lhd G$. Тогда $G = A \times B \Leftrightarrow (G = AB \;\&\; A \cap B = \{e\})$.

◀ Пусть $G = A \times B$. Тогда $G = AB$ из условия 2. Если $x \in A \cap B$, то $e = ee = xx^{-1}$, и из единственности $x = e$. Обратно, если $G = AB$, и $A \cap B = \{e\}$, то любой элемент $g \in G$ представляется в виде $g = ab$, где $a \in A$, $b \in B$, и если $ab = a'b'$ при $a' \in A$, $b' \in B$, то $a^{-1}a' = bb'^{-1} \in A \cap B$, поэтому $a = a'$ и $b = b'$.▶

Теорема 6. Если G — внутреннее прямое произведение подгрупп A и B, то $G \cong A \times B$

◀ Отображение $(a, b) \mapsto ab$ — биекция. Проверим сохранение операции. Заметим, что если $x \in A$, $y \in B$, то $\underbrace{xyx^{-1}}_{\in B} y^{-1} = x \underbrace{yx^{-1}y^{-1}}_{\in A} \in A \cap B$, поэтому $xy = yx$. Следовательно, $(a, b)(a', b') \mapsto aba'b' = aa'bb'$.▶

Теорема 7. Пусть $A \lhd G$, $B \lhd H$. Тогда $A \times B \lhd G \times H$, и $(G \times H)/(A \times B) \cong (G/A) \times (H/B)$.

◀ Рассмотрим гомоморфизм $(g, h) \mapsto (gA, hB)$.▶

Лекция 3. Конечно порождённые абелевы группы. Свободные абелевы группы. Подгруппы свободных абелевых групп.

По традиции, для абелевых групп используется аддитивная символика: операция в абелевой группе обозначается знаком "$+$" и называется сложением, соответственно нейтральный элемент — знаком 0, обратный (противоположный) элемент к элементу a обозначается $-a$, а вместо обозначения степени элемента a применяют обозначение na, где $n \in \mathbb{Z}$. Также вместо термина "прямое произведение" используют термин "прямая сумма" и знак "$\oplus$".

Определение 1. Абелева группа A называется *конечно порождённой*, если существует подмножество $\{a_1, \ldots, a_n\} \subseteq A$ (*система образующих*), такое, что $A =< a_1, \ldots, a_n >$. Иными словами, $A = \{k_1a_1 + \ldots + k_na_n : k_i \in \mathbb{Z}, 1 \leqslant i \leqslant n\}$.

Определение 2. Подмножество $\{a_1, \ldots, a_n\}$ абелевой группы A называется *линейно независимой системой*, если из равенства $k_1a_1 + \ldots + k_na_n = 0, k_i \in \mathbb{Z}, 1 \leqslant i \leqslant n$ следует, что $k_1 = \ldots = k_n = 0$.

Определение 3. Подмножество $\{a_1, \ldots, a_n\}$ абелевой группы A называется *базисом*, если $\{a_1, \ldots, a_n\}$ — линейно независимая система образующих группы A.

Определение 4. Абелева группа A называется *конечно порождённой свободной группой*, если она имеет (конечный) базис.
Пример: $\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n \text{ раз}}$.

Теорема 1. Если $\{a_1, \ldots, a_n\}$ — базис свободной абелевой группы A, то для любого элемента $a \in A$ существуют единственные коэффициенты $k_1, \ldots, k_n \in \mathbb{Z}$, такие, что $a = k_1a_1 + \ldots + k_na_n$.

◀ Существование коэффициентов $k_1, \ldots, k_n \in \mathbb{Z}$ следует из определения системы образующих, а единственность — из линейной независимости:

$$k_1a_1 + \ldots + k_na_n = k'_1a_1 + \ldots + k'_na_n \Rightarrow k_1 - k'_1 = \ldots = k_n - k'_n = 0 \Rightarrow k_1 = k'_1, \ldots, k_n = k'_n$$

▶

Теорема 2. Любые два базиса конечно порождённой абелевой группы содержат одно и то же число элементов.

◀ Пусть $\{a_1, \ldots, a_n\}$ и $\{b_1, \ldots, b_m\}$ — два базиса абелевой группы A. Допустим, что $m < n$. Тогда элементы $a_1, \ldots, a_n$ можно выразить через $b_1, \ldots, b_m$:

$$\begin{array}{rcl} a_1 & = & k_{11}b_1 + \ldots + k_{1,m}b_m \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ a_n & = & k_{n,1}b_1 + \ldots + k_{n,m}b_m \end{array}.$$

Рассмотрим матрицу $\begin{pmatrix} k_{11} & \ldots & k_{1,m} \\ \ldots\ldots\ldots\ldots & & \\ k_{n,1} & \ldots & k_{n,m} \end{pmatrix}$ над полем $\mathbb{Q}$. Число строк этой матрицы больше числа столбцов, значит ее строки линейно зависимы над $\mathbb{Q}$, т.е. существуют рациональные числа $\lambda_1, \ldots, \lambda_n$, не все равные 0, такие, что

$$\lambda_1(k_{11}, \ldots, k_{1,m}) + \ldots + \lambda_n(k_{n,1}, \ldots, k_{n,m}) = (0, \ldots, 0). \quad (1)$$

Приведем дроби $\lambda_1, \ldots, \lambda_n$ к общему знаменателю: $\lambda_i = p_i/q,\ p_1, \ldots, p_n, q \in \mathbb{Z}$. Умножая (1) на q, получаем соотношение

$$p_1(k_{11}, \ldots, k_{1,m}) + \ldots + p_n(k_{n,1}, \ldots, k_{n,m}) = (0, \ldots, 0), \tag{2}$$

откуда следует, что

$$\begin{array}{l} p_1a_1 + \ldots + p_na_n = \\ p_1(k_{11}b_1 + \ldots + k_{1,m}b_m) + \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ +p_n(k_{n,1}b_1 + \ldots + k_{n,m}b_m) = \\ (p_1k_{11} + \ldots + p_nk_{n,1})b_1 + \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (p_1k_{1,m} + \ldots + p_nk_{n,m})b_m = 0, \end{array}$$

что противоречит линейной независимости системы $\{a_1, \ldots, a_n\}$.▶

Обозначение. Число элементов базиса свободной абелевой группы A будем обозначать $\operatorname{rk} A$ и называть *рангом* этой группы.

Замечание 1. Если A — свободная абелева группа ранга n, то $A \cong \mathbb{Z}^n$.

◀ Если $\{a_1, \ldots, a_n\}$ — базис свободной абелевой группы A, то отображение

$$k_1a_1 + \ldots + k_na_n \mapsto (k_1, \ldots, k_n)$$

корректно определено и является изоморфизмом.▶

Теорема 3 (о подгруппах свободной абелевой группы). Если A — конечно порождённая абелева группа ранга n, $B \leqslant A$ — ее подгруппа, то B — свободная абелева группа ранга не более n.

◀ Проведем доказательство индукцией по n. Если $n = 1$, то $A \cong \mathbb{Z}$, и либо $B = 0$, либо $B = r\mathbb{Z}$, где $r \neq 0$ (теорема о подгруппах циклических групп), т.е. $\operatorname{rk} B = 0$ или $\operatorname{rk} B = 1$. Пусть $n > 1$, и $\{a_1, \ldots, a_n\}$ — базис группы A. Положим $A_0 =< a_1, \ldots, a_{n-1} >$. Тогда A_0 — свободная абелева группа ранга $n-1$. Рассмотрим гомоморфизм $f : A \to \mathbb{Z}$, определенный правилом $f(k_1a_1 + \ldots + k_na_n) = k_n$. Тогда $f(B) \leqslant \mathbb{Z}$. Если $f(B) = \{0\}$, то $B \leqslant A_0$, и по предположению индукции B — свободная абелева группа ранга не более $n-1$. В противном случае $f(B) = r\mathbb{Z}$, где $r \neq 0$, и найдется элемент $b \in B$ такой, что $f(b) = r$, т.е. $b = u_1a_1 + \ldots + u_{n-1}a_{n-1} + ra_n$. Заметим, что $< b >$ — бесконечная циклическая группа, значит $< b > \cong \mathbb{Z}$. Положим $B_0 = B \cap A_0$. По предположению индукции B_0 — свободная абелева группа ранга $m \leqslant n-1$. Осталось проверить, что $B =< b > \oplus B_0$. Используем теорему 2.5 (в аддитивной символике). Сначала заметим, что $< b > \cap B_0 = \{0\}$, так как при $k \neq 0$ имеем $kb = ku_1a_1 + \ldots + u_{n-1}a_{n-1} + kra_n \notin A_0$. С другой стороны, если $b' \in B$, то $b' = u'_1a_1 + \ldots + u'_{n-1}a_{n-1} + r'a_n$, причем $r' = f(b') \in r\mathbb{Z} \Rightarrow \exists q \in \mathbb{Z} : r' = rq$. Значит, $b' = bq + (b' - bq)$, причем $b' - bq = (u'_1 - qu_1)a_1 + \ldots + (u'_{n-1} - qu_{n-1})a_{n-1} \in B \cap A_0 = B_0$. Следовательно, $B =< b > \oplus B_0 \cong \mathbb{Z}^m \oplus \mathbb{Z} = \mathbb{Z}^{m+1}$, и $m + 1 \leqslant (n-1) + 1 = n$. ▶

Теорема 4 (накрывающее свойство свободных абелевых групп). Любая конечно порождённая абелева группа изоморфна фактор-группе некоторой свободной конечно порождённой абелевой группы по некоторой ее подгруппе.

◀ Пусть $\{a_1, \ldots, a_n\}$ — система образующих абелевой группы A. Рассмотрим гомоморфизм $f : \mathbb{Z}^n \to A$, определенный равенством $f((k_1, \ldots, k_n)) = k_1a_1 + \ldots + k_na_n$. Тогда f — сюръективный гомоморфизм, и по теореме о гомоморфизме, $A \cong \mathbb{Z}^n / \ker f$.▶

Лекция 4. Теорема о существовании согласованных базисов свободной конечно порождённой абелевой группы и её подгруппы. Разложение конечно порождённой абелевой группы в прямую сумму бесконечных и примарных циклических групп (существование и единственность)

Определение 1. Пусть A — свободная абелева группа ранга n с базисом $a_1, \ldots, a_n$ и B — ее подгруппа с базисом $b_1, \ldots, b_m$ (вспомним теорему о подгруппах свободной абелевой группы). Эти два базиса называются *согласованными*, если существуют целые числа $d_1, \ldots, d_m$, такие, что $b_i = d_i a_i, i = 1, \ldots, m$.

Теорема 1 (о существовании согласованных базисов). Для любой конечно порождённой свободной абелевой группы A и любой ее подгруппы B существуют их согласованные базисы.

◄ Для доказательства выберем сначала произвольные базисы $a_1, \ldots, a_n$ в A и $b_1, \ldots, b_m$ в B и укажем, как их можно преобразовать в согласованные. Заметим, что если элемент a_i заменить на элемент $a_i + ra_j$, где $r \in \mathbb{Z}$, то новая система $a_1, \ldots, a_i + ra_j, \ldots, a_n$ снова будет базисом группы A. Действительно, $k_1a_1 + \ldots + k_i(a_i + ra_j) + \ldots + k_na_n = 0 \Leftrightarrow k_1a_1 + \ldots + k_ia_i + \ldots + (k_j + rk_i)a_j = 0$ $\Leftrightarrow k_1 = \ldots = k_i = \ldots = k_j + rk_i = \ldots = k_n = 0$, а из $k_i = 0$ и $k_j + rk_i = 0$ следует $k_j = 0$, поэтому новая система линейно независима. С другой стороны, $a_i = (a_i + ra_j) - ra_j$, поэтому $< a_1, \ldots, a_i + ra_j, \ldots, a_n >= A$.
Аналогичные замены можно проводить с базисом подгруппы.

Связь между базисами можно определять матрицей, как в предыдущей лекции:

$$(b_1, \ldots, b_m) = (a_1, \ldots, a_n)M,$$

где M — некоторая целочисленная матрица размера $n \times m$. Перестановке элементов базиса $a_1, \ldots, a_n$ (соответственно, базиса $b_1, \ldots, b_m$) отвечает перестановка строк (соответственно, столбцов) матрицы M, а рассмотренному выше преобразованию базиса группы A (соответственно, группы B) соответствует целочисленное элементарное преобразование строк (соответственно, столбцов) матрицы M.

Рассматриваемые базисы согласованы тогда и только тогда, когда матрица M диагональна. Поэтому достаточно показать, как с помощью целочисленных элементарных преобразований строк и столбцов произвольной целочисленной матрицы можно привести ее к диагональному виду.

Если $M = 0$, то доказывать нечего. В противном случае введем параметр $d(M)$, равный наименьшему модулю ненулевого элемента матрицы M. Переставляя строки и столбцы, добьемся того, что $d(M) = |m_{11}|$. Если некоторый элемент $m_{1,i}$ не делится на m_{11}, разделим его на m_{11} с остатком: $m_{1,i} = m_{11}q + r,\ 0 < r < d(M)$. Вычитая первый столбец, умноженный на q, из i-го столбца, получаем новую матрицу M', причем $d(M') \leqslant r < d(M)$. Последовательно уменьшая $d(M)$, получим матрицу, у которой все элементы первой строки и первого столбца делятся на m_{11}. Но тогда элементарными преобразованиями можно сделать из нее матрицу вида $\begin{pmatrix} m_{11} & 0 \\ 0 & M' \end{pmatrix}$. Затем те же действия повторяем для меньшей матрицы M' и т.д. ►

Теорема 2 (критерий цикличности прямой суммы конечных циклических групп, или китайская теорема об остатках). Группа $\mathbb{Z}_n \oplus \mathbb{Z}_m$ является циклической $\Leftrightarrow\ (m, n) = 1$.

◄ Рассмотрим гомоморфизм $f : \mathbb{Z} \to \mathbb{Z}_n \oplus \mathbb{Z}_m$, определенный равенством $f(x) = ([x]_n, [x]_m)$. Ясно, что если $(m, n) = 1$, то $\ker f = \{r : m \,\big|\, r \ \&\ n \,\big|\, r\} = \{r : mn \,\big|\, r\} = mn\mathbb{Z}$. Значит, $|f(\mathbb{Z})| = |\mathbb{Z}_{mn}| = |\mathbb{Z}_n \oplus \mathbb{Z}_m|$, т.е. $\mathbb{Z}_{mn} \cong \mathbb{Z}_n \oplus \mathbb{Z}_m$. Обратное утверждение нам не понадобится и оставляется

в качестве упражнения.►

Определение 2. Конечная циклическая группа A называется *примарной*, если $|A| = p^k$, где p — простое число, $k \geq 1$.

Теорема 3 (Существование канонического разложения). Если A — конечно порождённая абелева группа, то существует её *каноническое разложение* в прямую сумму бесконечных и примарных циклических групп:

$$A \cong \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_s}} \oplus \mathbb{Z}^t. \tag{1}$$

◄ Как известно, любая конечно порождённая абелева группа A изоморфна факторгруппе некоторой свободной конечно порождённой группы L по ее подгруппе B. Выберем в L и в B согласованные базисы $a_1, \ldots, a_n$ и $b_1 = d_1 a_1, \ldots, b_m = d_m a_m$ (теорема 1). Тогда

$$L = < a_1 > \oplus \ldots \oplus < a_m > \oplus < a_{m+1} > \oplus \ldots \oplus < a_n >,$$

$$B = < d_1 a_1 > \oplus \ldots \oplus < d_m a_m > \oplus < 0 a_{m+1} > \oplus \ldots \oplus < 0 a_n > .$$

По теореме 2.7, $L/B \cong \mathbb{Z}_{d_1} \oplus \ldots \oplus \mathbb{Z}_{d_m} \oplus \mathbb{Z}^{n-m}$. Остается заметить, что если $d = p_1^{k_1} \ldots p_r^{k_r}$, где $p_1, \ldots, p_r$ — различные простые числа, то $\mathbb{Z}_d = \mathbb{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p_r^{k_r}}$.►

Теорема 4 (Единственность канонического разложения). Разложение (1) произвольной конечно порождённой группы A определено однозначно, с точностью до перестановки слагаемых.

◄ Достаточно доказать, что количество слагаемых вида $\mathbb{Z}$ и вида $\mathbb{Z}_{p^k}$ с фиксированными p и k в разложении (1) определено однозначно. Для этого понадобятся следующие общие понятия.

Определение 3. *Периодической частью*, или *кручением* абелевой группы A называется множество $T(A)$ элементов конечного порядка в A.
Заметим, что из (1) следует, что $T(A) = \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_s}}$, следовательно, $A/T(A) \cong \mathbb{Z}^t$, т.е. число $t = \mathrm{rk}(A/T(A))$ определено однозначно (теорема 3.2). Пусть теперь A — конечная абелева группа.

Определение 4. Для простого числа p, *p-периодической частью*, или *p-кручением* группы A называется множество $T_p(A)$ элементов порядка p^k, $k \in \mathbb{Z}$, в A.
Ясно, что $T_p(A)$ — это сумма слагаемых из (1), для которых $p_i = p$. Пусть теперь A — конечная абелева p-группа, т.е. $A = T_p(A) \cong \mathbb{Z}_{p^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{k_r}}$. Рассмотрим гомоморфизм $f : A \to A$, такой, что $f(x) = px$. Тогда для каждого слагаемого, изоморфного $\mathbb{Z}_{p^k}$, его образ будет изоморфен $\mathbb{Z}_{p^{k-1}}$, значит, $|\ker f| = p^r$, и число слагаемых в разложении A определено однозначно. С другой стороны, число слагаемых в разложении $f(A)$ равно числу слагаемых в разложении A, порядок которых больше p (слагаемые порядка p аннулируются гомоморфизмом f). Индукция по порядку группы завершает доказательство.►

Лекция 5. Действие группы на множестве. Примеры. Теорема Кэли. Орбиты и стабилизаторы. Теорема (о центре конечной p-группы).

Определение 1. *Действие* группы G на непустом множестве M — это отображение $G \times M \to M$, $(g, m) \mapsto gm$, удовлетворяющее условиям:
1. $\forall g, h \in G, m \in M : g(hm) = (gh)m$
2. $\forall m \in M : em = m$.
Примеры: $\mathrm{GL}(V)$ на V, S_n на $\{1, \ldots, n\}$, G на G левыми сдвигами ($gx = gx$) и сопряжениями ($x^g = gxg^{-1}$).
Эквивалентное определение действия: гомоморфизм G в группу $S(M)$ биекций множества M. Действительно, для любого $g \in G$ определим отображение $f(g) : M \to M$ правилом $\forall x \in M : f(g)(x) = gx$. Тогда в силу 1. $f(gh) = f(g) \circ f(h)$, а в силу 1. и 2. $f(g^{-1}) = f(g)^{-1}$, значит, $f(g) \in S(M)$.

Теорема 1 (теорема Кэли). Любая группа G изоморфна подгруппе группы биекций $S(G)$. В частности, если $|G| = n < \infty$, то группа G изоморфна подгруппе группы S_n.

◀ Действие левыми сдвигами дает гомоморфизм $f : G \to S(G)$. При этом если $g \in \ker f$, то $f(g)(e) = ge = e$, т.е. $g = e$. Следовательно, $\ker f = \{e\}$, и $G \cong f(G) \subseteq S(G)$.▶

Определение 2. Пусть задано действие группы G на множестве M. *Орбитой* элемента $m \in M$ называется множество $\{gm : g \in G\}$ (обозначение Gm или $\mathrm{orb}(m)$). *Стабилизатором*, или *стационарной подгруппой* элемента $m \in M$ называется подгруппа $\{g \in G : gm = m\}$ (обозначение: G_m или $\mathrm{St}(m)$). Орбиты относительно действия сопряжениями называются *классами сопряженных элементов*, или *классами сопряженности*, или просто сопряженными классами, класс сопряженности элемента $g \in G$ обозначается через g^G.
Стационарная подгруппа элемента $g \in G$ относительно этого действия называется *централизатором* элемента g и обозначается $C_G(g)$.

Лемма. Пусть задано действие группы G на множестве M. Если $m \in M$ и $m' \in Gm$, то $Gm' = Gm$.

◀ По условию, $m' = gm$ для некоторого $g \in G$. Но $Gg = G$, и $Gm' = Ggm = Gm$.▶

Следствие. Орбиты элементов множества M относительно действия группы G образуют разбиение множества M.

Теорема 2. Пусть задано действие конечной группы G на множестве M. Тогда для любого элемента $m \in M$,

$$|\mathrm{orb}(m)||\mathrm{St}(m)| = |G|. \tag{1}$$

◀ Рассмотрим отображение $\varphi : G \to M$, заданное правилом $\varphi(g) = gm$. Заметим, что $g' \in \varphi^{-1}(gm) \Leftrightarrow g'm = gm \Leftrightarrow g^{-1}g'm = m \Leftrightarrow g^{-1}g' \in \mathrm{St}(m) \Leftrightarrow g' \in g\,\mathrm{St}(m)$, т.е. $\varphi^{-1}(gm) = g\,\mathrm{St}(m)$ и $|\varphi^{-1}(gm)| = |g\,\mathrm{St}(m)| = |\mathrm{St}(m)|$. Итак, в каждый элемент орбиты переходит одинаковое число — $|\mathrm{St}(m)|$ — элементов группы G, откуда следует (1).▶
Для действия сопряжениями (1) принимает вид

$$|g^G||C_G(g)| = |G|. \tag{2}$$

Определение 3. *Центром* группы G называется множество таких элементов $z \in G$, что $\forall g \in G : gz = zg$ (обозначение $Z(G)$).
Пример: $Z(G) = G \Leftrightarrow G$ — коммутативная группа.

Определение 4. Пусть p — простое число. Группа G называется конечной *p-группой*, если $|G| = p^k$ для некоторого натурального числа p.
Пример — группа простого порядка.

Теорема 3 (о центре конечной p-группы). Если G — конечная p-группа, то $Z(G) \neq \{e\}$.

◄ Пусть $|G| = p^k$. Рассмотрим действие G на G сопряжениями и обозначим через $g_1^G, \ldots, g_s^G$ все классы сопряженности. Ясно, что $|g^G| = 1 \Leftrightarrow g \in Z(G)$. Пусть $|g_1^G| = \ldots = |g_r^G| = 1$, $|g_i^G| > 1$ при $i > r$. Тогда $r = |Z(G)| \geqslant 1$, т.к. $e \in Z(G)|$. Из (1) получаем $|g_i^G| = p^{k_i}$, $k_i > 0$ при $r < i \leqslant s$, и $|G| = |Z(G)| + \sum\limits_{i=r+1}^{s} p^{k_i}$, т.е. число $|Z(G)| = p^k - \sum\limits_{i=r+1}^{s} p^{k_i}$ делится на p.►

Теорема 4. Если G — некоммутативная группа, то группа $G/Z(G)$ не является циклической.

◄ Предположим противное: $G/Z(G) =< gZ(G) >$. Пусть $a, b \in G$. Тогда

$$\exists r, s \in \mathbb{Z} : aZ(G) = (gZ(G))^r = g^r Z(G), bZ(G) = (gZ(G))^s = g^s Z(G).$$

В частности, $a = g^r x$ и $b = g^s y$, где $x, y \in Z(G)$, откуда $ab = g^r x g^s y = g^r g^s xy = g^s y g^r x = ba$, что противоречит условию — некоммутативности группы G.►

Теорема 5. Группа порядка p^2, где p — простое число, коммутативна.

◄ По теореме о центре конечной p-группы, $|Z(G)| > 1$. Если $|Z(G)| = p^2$, то G — коммутативная группа. Вариант $|Z(G)| = p$ невозможен, так как в этом случае группа $G/Z(G)$ имела бы простой порядок и была бы циклической, чего не может быть по предыдущей теореме.►

Лекция 6. Три теоремы Силова.
В этой лекции p — простое число, G — конечная группа, $|G| = n = p^k m$, где $p \nmid m$.

Определение 1. *Силовской p-подгруппой* группы G называется подгруппа порядка p^k (т.е. p-подгруппа максимального возможного порядка).

Теорема 1 (первая теорема Силова — теорема существования). Силовская p-подгруппа произвольной конечной группы существует.

◄ Докажем первую теорему Силова индукцией по n. При $n = 1$ доказывать нечего. Пусть $n > 1$ и $k > 0$. Представим группу G как объединение классов сопряженности: $G = \cup_{i=1}^{s} g_i^G$. Считаем, что $|g_i^G| = 1$ при $1 \leqslant i \leqslant r$ и $|g_i^G| > 1$ при $r < i \leqslant s$. При этом $r >= 1$, так один одноэлементный класс e^G существует. Возможны 2 случая.

1. Каждое из чисел $|g_i^G|, r < i \leqslant s$ делится на p. Тогда $|Z(G)| = |G| - \sum\limits_{i=r+1}^{s} |g_i^G|$ делится на p. Но $Z(G)$ — абелева группа, поэтому она изоморфна прямому произведению примарных циклических подгрупп. Значит, хотя бы один нетривиальный сомножитель H, порядок которого равен p^t, где $t > 0$. Тогда $H \lhd G$ и $|G/H| = |G|/p^r = p^{k-t}m < |G|$. Применяя индуктивное предположение к группе G/H, найдем силовскую p-подгруппу $\overline{S}$ в группе G/H. Если $\pi : G \to G/H$ — канонический гомоморфизм, то $S = \pi^{-1}(\overline{S})$ — силовская p-подгруппа в G.
2. Одно из чисел $|g_i^G|, r < i \leqslant s$ не делится на p. Обозначим $g_i = g$ и рассмотрим подгруппу $H = C_G(g)$. По (2), $|H| = |G|/|g^G| = p^k m'$ для некоторого натурального числа $m' < m$. Силовская p-подгруппа в H существует по предположению индукции и является также силовской p-подгруппой в G.►

Теорема 2 (вторая теорема Силова — теорема о сопряженности).
1. Для любой p-подгруппы $H \leqslant G$ существует силовская p-подгруппа $S \leqslant G$, такая, что $H \subseteq S$.
2. Любые две силовские p-подгруппы в G сопряжены.

◄ 1. Пусть S_0 — некоторая силовская p-подгруппа в G. Рассмотрим действие H левыми сдвигами на множестве M левых смежных классов G по подгруппе S_0 ($h(gS_0) = (hg)S_0$). Очевидно, что каждая орбита этого действия содержит p^l элементов, $p^l \leqslant |H|$, и найдется хотя бы одна орбита из одного элемента (иначе $|M| = m$ было бы кратно p). Иными словами, существует элемент $g \in G$ такой, что $HgS_0 = gS_0$. Тогда $g^{-1}Hg \subseteq S_0$ и $H \subseteq S = gS_0g^{-1}$.
2. Пусть S_0, S_1 — две силовские p-подгруппы в G. Применим предыдущее рассуждение к $H = S_1$. Получим, что для некоторого элемента $g \in G$, $S_1 \subseteq S = gS_0g^{-1}$. Но группы S_1 и S имеют одинаковые порядки p^k, значит, $S_1 = S$.►

Теорема 3 (третья теорема Силова — теорема о количестве силовских p-подгрупп). Пусть $n_p(G)$ — количество силовских p-подгрупп группы G. Тогда $n_p(G) \equiv 1 \pmod p$.

◄ Рассмотрим действие сопряжениями какой-либо одной силовской p-подгруппы S на множестве N всех силовских p-подгрупп группы G. Допустим, что есть какая-то орбита из одного элемента $\{S_1\}$. Это значит, что для любого $x \in S$, $xS_1x^{-1} = S_1$. Рассмотрим подмножество SS_1 и заметим, что это подгруппа в G. Действительно, $e = ee \in SS_1$, если $x, x_1 \in S$, $y, y_1 \in S_1$, то по доказанному $xyx_1y_1 = xx_1(\underbrace{x_1^{-1}yx_1}_{\in S_1})y_1 \in SS_1$ и $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}(\underbrace{xy^{-1}x^{-1}}_{\in S_1}) \in SS_1$).
Проверим, что $S_1 \lhd SS_1$ ($\forall x \in S, y \in S_1$, $xyS_1(xy)^{-1} = xS_1x^{-1} = S_1$). По первой теореме об изоморфизме $SS_1/S_1 \cong S/S_1 \cap S$. Следовательно, если $|S_1 \cap S| = p^l$, то $l \leqslant k$ и $|SS_1| = |S_1||SS_1/S_1| = p^k|S/S_1 \cap S| = p^k p^{k-l} = p^{2k-l}|$. По определению k имеем $2k - l \leqslant k$,

откуда $l \geqslant k$. Получаем $l = k$ и $S = S_1$. Таким образом, единственная орбита $\{S\}$ содержит один элемент, а порядки остальных орбит делятся на p. Значит, $n_p(G) = |N| = 1 + pq$.▶
Заметим, что из второй и третьей теорем Силова следует также, что $n_p(G) \,\big|\, m$.

Лекция 7. Коммутант группы, его свойства. Разрешимые группы, их свойства. Разрешимость группы верхнетреугольных матриц. Разрешимость конечной p-группы. Разрешимость группы порядка pq (где p, q — простые числа).

Определение 1. Подгруппа, *порождённая подмножеством* S группы G — это наименьшая подгруппа в G, содержащая S. Обозначение $< S >$.

Замечание 1.

$$< S >= \{x_1^{\pm 1} x_2^{\pm 1} \dots x_m^{\pm 1} : x_i \in S,\ i = 1, \dots, m,\ m \geqslant 0\} \tag{3}$$

Определение 2. *Коммутатором* элементов x, y группы G называется элемент $[x, y] = xyx^{-1}y^{-1}$. *Коммутантом* группы G называется ее подгруппа, порождённая всеми коммутаторами ее элементов. Обозначение G' или $[G, G]$.

Замечание 2. $[x, y]^{-1} = [y, x]$,

$$G' = \{[x_1, y_1][x_2, y_2] \dots [x_m, y_m] : x_i, y_i \in G,\ i = 1, \dots, m,\ m \geqslant 0\}. \tag{4}$$

Теорема 1 (свойства коммутанта).
1. Если $f : G \to H$ — гомоморфизм групп, то $f(G') \subseteq H'$ (функториальность). Если гомоморфизм f сюръективен, то $f(G') = H'$. Если $H \leqslant G$, то $H' \subseteq H \cap G'$.
2. Для любой группы G, $G' \lhd G$.
3. $G' = \{e\} \Leftrightarrow G$ — коммутативная группа.
4. Если $N \lhd G$, то группа G/N коммутативна $\Leftrightarrow G' \subseteq N$.

◀
1. Прямо следует из (4) и того, что $f([x, y]) = f(xyx^{-1}y^{-1}) = [f(x), f(y)]$.
2. Следует из того, что $\forall g, x, y \in G : g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$.
3. $\forall x, y \in G : [x, y] = e \Leftrightarrow xyx^{-1}yg^{-1} = e \Leftrightarrow xy = yx$.
4. Вытекает из п. 3 и пп. 1, 2, примененных к каноническому гомоморфизму $\pi : G \to G/N$. ▶

Определение 3. *Ряд коммутантов* группы G строится по индукции: $G^{(0)} = G$, $G^{(n)} = (G^{(n-1)})'$ при $n > 0$.

Замечание 3. $G^{(n)} \lhd G$ при всех $n > 0$.

◀ Достаточно заметить, что для любой нормальной подгруппы $N \lhd G$ и любого элемента $g \in G$ отображение $x \mapsto x^g = gxg^{-1}$ является гомоморфизмом из N в N, и применить n раз свойство 2 коммутанта группы.▶

Замечание 4. Если $f : G \to H$ — гомоморфизм групп, то $f(G^{(n)}) \subseteq H^{(n)}$ (функториальность). Если гомоморфизм f сюръективен, то $f(G^{(n)}) = H^{(n)}$. Если $H \leqslant G$, то $H^{(n)} \subseteq H \cap G^{(n)}$.

◀ Очевидная индукция по n с применением свойства 1 коммутанта.▶

Определение 4. Группа G называется *разрешимой*, если существует такое $n > 0$, что $G^{(n)} = \{e\}$.
Примеры: любая абелева группа разрешима ($n = 1$), S_3 разрешима ($n = 2$), S_4 разрешима ($n = 3$).

Теорема 2 (свойства разрешимых групп).
1. Любая подгруппа и любая фактор-группа разрешимой группы разрешимы.
2. Если $N \lhd G$, причем группы N и G/N разрешимы, то и группа G разрешима.

◄ 1. Разрешимость подгруппы $H \leqslant G$ следует из $H^{(n)} \subseteq H \cap G^{(n)}$. Разрешимость фактор-группы следует из предыдущего замечания, примененного к каноническому гомоморфизму $\pi : G \to G/N$, где $N \lhd G$.
2. Пусть $(G/N)^{(n)} = \{e\}$, $N^{(m)} = \{e\}$. Рассмотрим канонический гомоморфизм $\pi : G \to G/N$. Имеем $\pi(G^{(n)}) = \{e\} \Rightarrow G^{(n)} \subseteq N \Rightarrow G^{(n+m)} \subseteq N^{(m)} = \{e\}$.►

Теорема 3. Группа $T_n(F)$ обратимых верхнетреугольных матриц любого порядка $n \geqslant 1$ над произвольным полем F разрешима.

◄ Сначала докажем по индукции разрешимость группы $UT_n(F)$ верхних унитреугольных матриц, т.е. матриц вида $\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$. При $n = 1$ эта группа тривиальна. При $n > 1$ рассмотрим отображение $f : UT_n(F) \to UT_{n-1}(F)$, сопоставляющее матрице A ее верхний левый угол:

$$A = \begin{pmatrix} f(A) & * \\ & \vdots \\ 0 \dots 0 & 1 \end{pmatrix}.$$

Легко проверить, что f — гомоморфизм, и что $\ker f$ — абелева (следовательно, разрешимая) группа матриц вида

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & u_1 \\ 0 & 1 & 0 & \dots & 0 & u_2 \\ 0 & 0 & 1 & \dots & 0 & u_3 \\ \dots & \dots & \dots & \ddots & \vdots & \\ 0 & 0 & 0 & \dots & 1 & u_{n-1} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

При этом $UT_n(F)/\ker f \cong UT_{n-1}(F)$ — разрешимая группа, по предположению индукции. По свойству 2 разрешимых групп, $UT_n(F)$ — разрешимая группа.

Теперь рассмотрим отображение $g : T_n(F) \to T_n(F)$, которое сопоставляет каждой матрице диагональную матрицу:

$$g : \begin{pmatrix} \alpha_1 & * & \dots & * \\ 0 & \alpha_2 & \dots & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & \dots & \alpha_n \end{pmatrix} \mapsto \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & \alpha_n \end{pmatrix}.$$

Снова проверяем, что g — гомоморфизм. При этом $g(T_n(F)) \cong T_n(F)/\ker g$ — группа обратимых диагональных матриц, которая коммутативна, $\ker g = UT_n(F)$ — разрешимая группа, по доказанному выше, значит, $T_n(F)$ — разрешимая группа. ►

Теорема 4. Конечная p-группа разрешима.

◀ Пусть G — конечная p-группа, т.е. $|G| = p^k$, p — простое число. Проведем индукцию по k. При $k = 1$ группа G циклическая, следовательно, коммутативная и подавно разрешимая. При $k > 1$ группа $G/Z(G)$ имеет меньший порядок, чем G (так как $Z(G) \neq \{e\}$ по теореме 5.3), следовательно, по предположению индукции, она разрешима, а группа $Z(G)$ коммутативна. По свойству 2, группа G разрешима.▶

Теорема 5. Группа порядка pq, где p, q — простые числа, разрешима.

◀ Если $p = q$, то группа G коммутативна, как группа порядка p^2 (теорема 5.5). В противном случае предположим для определенности, что $p < q$. Заметим, что тогда $n_q(G) \equiv 1 \pmod{q}$ и $n_q(G) \,\vdots\, p$, значит $n_q(G) = 1$ и силовская q-подгруппа S нормальна в G. При этом S и G/S — циклические, следовательно, коммутативные группы. Поэтому G — разрешимая группа ($G^{(2)} = \{e\}$).▶

Лекция 8. Группа подстановок. Простые группы. Простота групп A_n при $n \geqslant 5$.
Известно, что группа S_n порождена транспозициями.

Определение 1. Подстановка $\sigma \in S_n$ называется *циклом длины* k, если существуют такие числа $i_1, \ldots, i_k$, что $\sigma(i_1) = i_2, \sigma(i_1) = i_3, \ldots, \sigma(i_k) = i_1$, а при $i \notin \{i_1, \ldots, i_k\}$, $\sigma(i) = i$. Обозначение $\sigma = (i_1, \ldots, i_k)$
Пример: транспозиция (i, j) — цикл длины 2.

Определение 2. Циклы $(i_1, \ldots, i_k)$ и $(j_1, \ldots, j_m)$ называются *независимыми*, если множества $\{i_1, \ldots, i_k\}$ и $\{j_1, \ldots, j_m\}$ имеют пустое пересечение.

Теорема 1. Любая подстановка разлагается в произведение попарно независимых циклов, причем единственным образом, с точностью до перестановки этих циклов (в частности, независимые циклы коммутируют).

◀ Алгоритм разложения: берем любое число $i \in \{1, \ldots, n\}$ и строим последовательность $i, \sigma(i), \sigma^2(i), \ldots$. В ней конечное число различных элементов, значит, какие-то два совпадают, скажем, $\sigma^k(i) = \sigma^l(i)$. Тогда $\sigma^{l-k}(i) = i$. Получаем цикл, начинающийся с i. Затем берем число, не вошедшее в уже построенный цикл, и строим следующий цикл, и т.д. Полезно заметить, что более формально независимые циклы описываются как орбиты действия циклической группы $< \sigma >$ на $\{1, \ldots, n\}$, откуда следует единственность разложения. Перестановочность независимых циклов очевидна.▶
Следующее важное соотношение позволяет описывать классы сопряженных элементов в группе S_n:

$$\forall \pi \in S_n,\ \pi((i_1, \ldots, i_k)\pi^{-1} = (\pi(i_1), \ldots, \pi(i_k)). \tag{5}$$

Теорема 2. Группа A_n при $n \geqslant 3$ порождена циклами длины 3.

◀ Любую подстановку из S_n можно разложить в произведение транспозиций. Четная подстановка разлагается в произведение четного числа транспозиций, поэтому достаточно представить в виде произведения тройных циклов произведение любых двух транспозиций. Но $(a, b)(b, c) = (a, b, c)$, $(a, b)(c, d) = (a, b)(b, c)(b, c), (c, d) = (a, b, c)(b, c, d)$.▶

Определение 3. Группа G называется *простой*, если у нее ровно две нормальные подгруппы: $\{e\}$ и G.

Замечание 1. Коммутативные простые группы — это циклические группы простого порядка.

Теорема 3. При $n \geqslant 5$ группа A_n является простой.

◀ Пусть $N \lhd A_n$ и $N \neq \{e\}$. Необходимо доказать, что $N = A_n$.
Для этого докажем несколько вспомогательных утверждений.

Лемма 1. Если хотя бы один цикл длины 3 принадлежит N, то $N = A_n$.
◀ Пусть $(a, b, c) \in N$. Для любых различных $x, y, z \in \{1, \ldots, n\}$ существует подстановка $\pi \in S_n$, такая, что $\pi(a, b, c)\pi^{-1} = (x, y, z)$ ($\pi = \begin{pmatrix} \ldots & a & \ldots & b \ldots & c \ldots \\ \ldots & x & \ldots & y \ldots & z \ldots \end{pmatrix}$). Если $\pi \in A_n$, то $(x, y, z) \in N$.
Иначе выберем числа $u, v \in \{1, \ldots, n\}$, отличные от x, y, z ($n \geqslant 5!$), и заменим π на $\pi' = (u, v)\pi$. Получим $\pi'(a, b, c)\pi'^{-1} = (u, v)\pi(a, b, c)\pi^{-1}(u, v) = (u, v)(x, y, z)(u, v) = (x, y, z) \in N$. Теперь применяем теорему 2.▶

Лемма 2. Если в N содержится подстановка, разложение которой содержит цикл длины не менее 4, то $N = A_n$.

◀ Пусть $N \ni \sigma = (i_1, \ldots, i_k)\sigma_1$, где σ_1 — произведение всех остальных независимых циклов, входящих в разложение σ, и $k \geqslant 4$. Тогда $N \ni \sigma(i_1, i_2, i_3)\sigma^{-1}(i_1, i_2, i_3)^{-1} = (i_1, \ldots, i_k)\sigma_1(i_1, i_2, i_3)\sigma_1^{-1}(i_1, \ldots, i_k)^{-1}(i_3, i_2, i_1)$, и σ_1 сокращается. Значит,
$N \ni \underbrace{(i_1, \ldots, i_k)(i_1, i_2, i_3)(i_1, \ldots, i_k)^{-1}}(i_3, i_2, i_1) \overset{(5)}{=} (i_2, i_3, i_4)(i_3, i_2, i_1) = (i_1, i_4, i_2)$. Применяем лемму 1. ▶

Лемма 3. Если в N содержится подстановка, разложение которой содержит два цикла длины 3, то $N = A_n$.

◀ Пусть $N \ni \sigma = (i_1, i_2, i_3)(i_4, i_5, i_6)\sigma_1$, где σ_1 — произведение всех остальных независимых циклов, входящих в разложение σ. Тогда $N \ni \sigma(i_1, i_2, i_4)\sigma^{-1}(i_1, i_2, i_4)^{-1} = \underbrace{(i_1, i_2, i_3)(i_4, i_5, i_6)(i_1, i_2, i_4)((i_1, i_2, i_3)(i_4, i_5, i_6))^{-1}}(i_4, i_2, i_1) \overset{(5)}{=} (i_2, i_3, i_5)(i_4, i_2, i_1)$ (опять сократили σ_1). Вычисляя последнее произведение, получаем $N \ni (i_1, i_4, i_3, i_5, i_2)$. Применяем лемму 2.▶

Лемма 4. Если в N содержится подстановка, разложение которой содержит произведение двух независимых транспозиций, то $N = A_n$.

◀ Пусть $N \ni \sigma = (i_1, i_2)(i_3, i_4)\sigma_1$, где σ_1 — произведение всех остальных независимых циклов, входящих в разложение σ. Тогда $N \ni \sigma(i_1, i_2, i_4)\sigma^{-1}(i_1, i_2, i_4)^{-1} = \underbrace{(i_1, i_2)(i_3, i_4)(i_1, i_2, i_4)(i_1, i_2)(i_3, i_4)}(i_4, i_2, i_1) \overset{(5)}{=} (i_2, i_1, i_3)(i_4, i_2, i_1)$ (опять сократили σ_1). Значит, $N \ni (i_1, i_4)(i_2, i_3)$. Но можно выбрать пятый элемент i_5, отличный от i_1, i_2, i_3, i_4, так как $n \geqslant 5$. Получаем: $N \ni \underbrace{(i_2, i_3, i_5)(i_1, i_4)(i_2, i_3)(i_2, i_3, i_5)^{-1}}(i_1, i_4)(i_2, i_3) \overset{(5)}{=} (i_1, i_4)(i_3, i_5)(i_1, i_4)(i_2, i_3) = (i_3, i_5)(i_2, i_3) = (i_5, i_3, i_2)$ (см. доказательство теоремы 2).▶

Для завершения доказательства теоремы остается заметить, что любая <u>четная</u> нетривиальная подстановка удовлетворяет условию по крайней мере одной из лемм 1–4. Действительно, если в ее разложении нет "длинных" циклов (см. лемму 2), и нет двух циклов длины 3 (см. лемму 3), то остается либо один цикл длины 3 (см. лемму 1), либо произведение <u>четного</u> числа транспозиций, возможно умноженное на цикл длины 3, и тогда выполнено условие леммы 4. ▶

Определение 4. *Специальная ортогональная группа* $SO_n(\mathbb{R})$ — это группа ортогональных ($A^T = A^{-1}$) вещественных матриц порядка n с определителем 1.

Теорема 4. Группа $SO_3(\mathbb{R})$ является простой.

◀ Пусть $N \lhd SO_3(\mathbb{R})$ и $N \neq \{E\}$. Покажем, что N совпадает со всей группой $SO_3(\mathbb{R})$.

Известно, что любой ортогональный оператор на трехмерном пространстве есть поворот на некоторый угол φ относительно какой-то оси (переходя от произвольного поворота к противоположному, будем считать, что угол любого поворота положителен) и в некотором ортонормированном базисе задается матрицей

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix}.$$

Следовательно, если подгруппа N содержит поворот на некоторый угол относительно какой-то оси, она содержит повороты на тот же угол относительно любой оси. При этом можно выбрать

матрицу $A \in N$ с $\varphi \neq 0$ (т.е. $A \neq E$). Возьмем произвольную матрицу

$$D = D(\psi) = \begin{pmatrix} \cos\psi & -\sin\psi & 0 \\ \sin\psi & \cos\psi & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SO_3(\mathbb{R}).$$

Имеем

$$DA = \begin{pmatrix} \cos\psi & -\cos\varphi\sin\psi & \sin\varphi\sin\psi \\ \sin\psi & \cos\varphi\cos\psi & -\sin\varphi\cos\psi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix} \tag{1}$$

и

$$D^{-1}A^{-1} = \begin{pmatrix} \cos\psi & \cos\varphi\sin\psi & \sin\varphi\sin\psi \\ -\sin\psi & \cos\varphi\cos\psi & \sin\varphi\cos\psi \\ 0 & -\sin\varphi & \cos\varphi \end{pmatrix}. \tag{2}$$

Но $[D, A] = DAD^{-1}A^{-1} \in N$. Рассмотрим функцию

$$\begin{aligned} f(\psi) = \operatorname{tr}[D(\psi), A] = (\cos^2\psi + \cos\varphi\sin^2\psi) + \\ (\cos\varphi\sin^2\psi + \cos^2\varphi\cos^2\psi + \sin^2\varphi\cos\psi) + (\sin^2\varphi\cos\psi + \cos^2\varphi) = \\ \cos^2\psi(1-\cos\varphi)^2 + 2\cos\psi(1-\cos^2\varphi) + \cos^2\varphi + 2\cos\varphi. \end{aligned} \tag{3}$$

Видно, что $f(0) = 3$ и $f(\pi/2) = \cos^2\varphi + 2\cos\varphi < 3$. Значит, функция $f(\psi)$ принимает все значения в некотором интервале $[3-\varepsilon, 3]$, где $\varepsilon > 0$. Поскольку каждый оператор $[D(\psi), A]$ также есть поворот на некоторый угол $\omega = \omega(\psi)$, а след матрицы оператора не зависит от выбора базиса, получаем, что $f(\psi) = 1 + 2\cos\omega$, и при изменении $f(\psi)$ от 3 до $3-\varepsilon$ угол $\omega = \arccos(3-\psi)/2$ принимает все значения от 0 до некоторого $\delta > 0$. Значит, все такие повороты (относительно ЛЮБОЙ ОСИ!) принадлежат N. Теперь возьмем произвольный поворот $g \in G$ на угол α относительно произвольной оси. Существует натуральное число n, для которого $\alpha/n < \delta$. Но тогда поворот g_1 относительно той же оси на угол α/n принадлежит N, а значит, и $g = g_1^n \in N$.▶

Лекция 9. Ассоциативные кольца, идеалы. Фактор-кольцо. Теорема о гомоморфизме. Поля. Расширения полей. Теорема о башне полей. Присоединение корня многочлена к полю. Поле разложения многочлена.

Определение 1. Множество $(R, +, \cdot)$ с двумя бинарными операциями (*сложением* и *умножением*) называется *кольцом*, если выполнены следующие аксиомы:
1. $(R, +)$ — абелева группа (*аддитивная группа*) кольца R;
2. $\forall a, b, c \in R, a \cdot (b + c) = a \cdot b + a \cdot c$ и $(b + c) \cdot a = b \cdot a + c \cdot a$ (дистрибутивность слева и справа).
Если сверх того выполняется аксиома
3. $\forall a, b, c \in R, a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (ассоциативность умножения),
то кольцо R называется *ассоциативным*;
если выполнена аксиома
4. $\exists 1 \in R : \forall a \in R,\ 1 \cdot a = a \cdot 1 = a$ (существование нейтрального элемента по умножению), — *кольцом с единицей*;
если выполнена аксиома
5. $\forall a, b \in R, a \cdot b = b \cdot a$ (коммутативность умножения) —
коммутативным кольцом.
Отметим, что аксиомы 4 — 5 независимы. **В данном курсе, если прямо не указано противное, слово "кольцо" означает ассоциативное кольцо с единицей (не обязательно коммутативное).**
Примеры: поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, кольцо целых чисел $\mathbb{Z}$, кольцо $F[x]$ многочленов над полем F, кольцо $M_n(F)$ квадратных матриц порядка n.

Определение 2. Подмножество S кольца R называется *подкольцом*, если оно является кольцом относительно операций сложения и умножения, определенных в R. Если рассматриваются только кольца с единицей, накладывается дополнительное условие: $1 \in S$.

Определение 3. Подгруппа I аддитивной группы кольца R называется *идеалом*, если $\forall x \in I, r \in R :\ xr \in I$ и $rx \in I$ (обозначение $I \lhd R$).

Определение 4. Пусть R — кольцо и $I \lhd R$. Фактор-группа R/I (относительно сложения), с операцией умножения смежных классов $(a + I)(b + I) = ab + I$, называется *фактор-кольцом* кольца R по идеалу I.

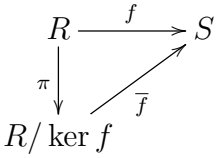
◀ Корректность! Если $a' + I = a + I$ и $b' + I = b + I$, то $a' = a + x$ и $b' = b + y$ для некоторых $x, y \in I$. Значит, $a'b' = (a + x)(b + y) = ab + \underbrace{xb + ay + xy}_{\in I} \Rightarrow a'b' + I = ab + I$. ▶

Определение 5. Пусть R, S — кольца. Отображение $f : R \to S$ называется *гомоморфизмом*, если $\forall a, b \in R : f(a + b) = f(a) + f(b)$ и $f(ab) = f(a)f(b)$. Если рассматриваются только кольца с единицей, накладывается дополнительное условие: $f(1_R) = 1_S$. Гомоморфизм колец, являющийся биективным (взаимно-однозначным) отображением, называется *изоморфизмом*
Пример: *канонический гомоморфизм* $\pi : R \to R/I$ для $I \lhd R$ ($\pi(r) = r + I$).

Определение 6. Пусть $f : R \to S$ — гомоморфизм колец. *Ядром* гомоморфизма f называется множество $\ker f = \{r \in R : f(r) = 0\}$.

Замечание 1. Пусть $f : R \to S$ — гомоморфизм колец. Тогда $\ker f \lhd R$. Обратно, если $I \lhd R$, то $\ker \pi = I$. Гомоморфизм $f : R \to S$ является изоморфизмом $\Leftrightarrow ker f = \{0\}$ и $f(R) = S$.

Теорема 1 (Теорема о гомоморфизме для колец). Пусть $f : R \to S$ — гомоморфизм колец, $\pi : R \to R/\ker f$ — канонический гомоморфизм. Тогда:
1. Существует единственный гомоморфизм $\overline{f} : R/\ker f \to S$, такой, что $\overline{f}\pi = f$ (см. диаграмму)



2. $R/\ker f \cong f(R)$.
3. Существует взаимно-однозначное соответствие между множествами $\mathcal{L}(f(R))$ подколец кольца $f(R)$ и $\mathcal{L}(R, \ker f)$ подколец кольца R, содержащих $\ker f$, сохраняющее включение (*решеточный изоморфизм*).
4. Указанное соответствие сохраняет свойство подкольца быть идеалом.

◀ См. теорему о гомоморфизме для групп.▶

Теорема 2 (Первая теорема об изоморфизме для колец). Пусть R — кольцо, $S \leqslant R$ и $I \lhd R$. Тогда $I \cap S \lhd S$ и $(S + I)/I \cong S/(S \cap I)$.

Определение 7. Элемент $a \in R$ называется *обратимым*, если $\exists a^{-1} \in R : \ aa^{-1} = a^{-1}a = 1$. Множество всех обратимых элементов кольца R является группой относительно умножения (*мультипликативная группа кольца*) и обозначается R^*.

Замечание 2. Если идеал I кольца R содержит обратимый элемент, то $I = R$.

◀ Если $a \in I$ и $a \in R^*$, то $\forall r \in R : \ r = ra^{-1}a \in I$.▶

Определение 8. *Телом*, или *кольцом с делением* называется ассоциативное кольцо с $1 \neq 0$, в котором каждый ненулевой элемент обратим. Коммутативное тело называется *полем*.
Примеры полей: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Замечание 3. В поле нет идеалов, кроме всего поля и $\{0\}$.

Определение 9. Если F и E — поля, причем F — подкольцо в E, то F называется *подполем* поля E, а E — *расширением* поля F.

Определение 10. Если E — расширение поля F, то E можно рассматривать как линейное пространство над F (конечномерное или бесконечномерное). Размерность $\dim_F E$ называется *степенью* расширения и обозначается $[E : F]$. Если $[E : F] < \infty$, то E называется конечным расширением поля F.

Определение 11. Последовательность расширений $F = E_0 \leqslant E_1 \leqslant \ldots \leqslant E_n = E$ называется *башней* полей.

Теорема 3 (о башне полей). Пусть в башне полей $F = E_0 \leqslant E_1 \leqslant \ldots \leqslant E_n = E$ каждое расширение E_i поля E_{i-1} — конечное, $i = 1, \ldots, n$. Тогда E — конечное расширение поля F и

$$[E : F] = [E_1 : E_0][E_2 : E_1] \ldots [E_n : E_{n-1}] \tag{1}$$

◄ Ясно, что достаточно доказать (1) для $n = 2$ и воспользоваться индукцией по n. Итак, рассмотрим башню $F \leqslant E_1 \leqslant E$. Пусть $e_1, \dots e_n$ — базис E_1 над F, $f_1, \dots, f_m$ — базис E над E_1. Покажем, что $B = \{f_i e_j : \ i = 1, \dots, m, \ j = 1, \dots n\}$ — базис E над F. Действительно, пусть $a \in E$. Тогда существуют $\lambda_1, \dots, \lambda_m \in E_1$, такие, что $a = \lambda_1 f_1 + \dots + \lambda_m f_m$. Далее, запишем $\lambda_i = \mu_{i,1} e_1 + \dots + \mu_{i,n} e_n$, $i = 1, \dots, n$, $\mu_{i,j} \in F$. Подставляя и раскравая скобки, получим $a = \sum_{i,j} \mu_{i,j} f_i e_j$, т. е. B — система образующих линейного пространства E над F. Проверим линейную независимость системы B. Допустим, что $\sum_{i,j} \mu_{i,j} f_i e_j = 0$, $\mu_{i,j} \in F$. Перепишем это соотношение в виде $\sum_i (\sum_j \mu_{i,j} e_j) f_i = 0$. Тогда при любом $i = 1, \dots, m$, $\sum_j \mu_{i,j} e_j \in E_1$, значит, из линейной независимости $f_1, \dots, f_m$ над E_1, следует, что $\sum_j = \mu_{i,j} e_j = 0$. А уже из линейной независимости $e_1, \dots, e_n$ следует, что $\mu_{i,j} = 0$ при всех $j = 1, \dots, n$.►

Теорема 4 (о присоединении корня многочлена к полю). Пусть F — поле, $f(x)$ — многочлен положительной степени с коэффициентами из F. Тогда существует расширение E поля F, содержащее некоторый корень многочлена $f(x)$.
Пример: $\mathbb{C}$ — расширение поля $\mathbb{R}$, в котором многочлен $x^2 + 1$ имеет корень.
◄ Очевидно, что если многочлен $f(x)$ разлагается на множители положительной степени, то достаточно построить расширение, в котором хотя бы один из этих множителей имел бы корень. Поэтому будем считать $f(x)$ неприводимым многочленом. Рассмотрим идеал $I = (f) = f(x)F[x]$ кольца $F[x]$, состоящий из многочленов, кратных $f(x)$. Пусть $\pi : F[x] \to F[x]/I = E$ — канонический гомоморфизм. Поскольку $F \leqslant F[x]$ (элементы поля — константы), и ни одна константа не лежит в I, ограничение π на F задает изоморфизм между F и $\pi(F)$. Мы отождествим элементы $a \in F$ и $\pi(a) = a + I \in E$, таким образом, будем считать, что $F \leqslant E$. Пусть $E \ni g(x) + I \neq 0$. Это означает, что $g(x)$ не делится на $f(x)$, но $f(x)$ неприводим, поэтому $(f(x), g(x)) = 1$ и существуют многочлены $u(x)$ и $v(x)$, для которых $u(x)f(x) + v(x)g(x) = 1$. Но тогда $v(x)g(x) = 1 - u(x)f(x) \in 1 + I$, значит $v(x) + I = (g(x) + I)^{-1}$ в E. Следовательно, E — поле, и E — расширение F. Положим $\alpha = \pi(x) \in E$. Если $f(x) = a_0 + a_1 x + \dots + a_n x^n$, то $f(\alpha) = a_0 + a_1 \pi(x) + \dots + a_n \pi(x)^n = \pi(a_0 + a_1 x + \dots + a_n x^n) = \pi(f(x)) = 0$, так как $f(x) \in I$. ►

Определение 12. Расширение $E = F[x]/(f)$, где $f(x)$ — неприводимый многочлен, называется *простым алгебраическим расширением* поля F. Обозначение $E = F(\alpha)$, где $\alpha = x + (f)$ — корень $f(x)$ в E.

Замечание 4. Если $E = F(\alpha)$, то $[E : F] = \deg f(x)$.

◄ Если $\deg f(x) = n$, то $1, \alpha, \dots, \alpha^{n-1}$ образуют базис E над F. Это вытекает из того, что любой многочлен $g(x) \in F[x]$ можно записать в виде $g(x) = f(x)q(x) + r(x)$, где $\deg r(x) < n$, и ни один многочлен степени меньше n не делится на $f(x)$. ►

Определение 13. Расширение E поля F называется *полем разложения* многочлена положительной степени $f(x) \in F[x]$, если $f(x)$ разлагается на линейные множители над E, причем E — наименьшее подполе в E, содержащее F и все корни $f(x)$.
Построение поля разложения: разлагаем $f(x)$ на неприводимые множители. Если все неприводимые множители линейные, то F — поле разложения $f(x)$. Если имеются множители степени больше 1, присоединяем корень одного из них и повторяем процесс, пока не дойдем до поля разложения.

Лекция 10. Свойство минимальности простого алгебраического расширения. Свойство минимальности поля разложения. Единственность поля разложения многочлена с точностью до изоморфизма. Характеристика поля. Порядок конечного поля. Существование и единственность поля заданного примарного порядка. Теорема о строении мультипликативной группы конечного поля. Группа автоморфизмов конечного поля.

Теорема 1 (о минимальности простого алгебраического расширения). Пусть $\varphi : F \to L$ — гомоморфизм поля F в поле L, $f(x)$ — неприводимый многочлен над F и $E = F[x]/(f)$ — соответствующее простое алгебраическое расширение. Для любого многочлена $g(x) = b_0 + b_1x + \ldots + b_mx^m$ положим $g^\varphi(x) = \varphi(b_0) + \varphi(b_1)x + \ldots + \varphi(b_m)x^m \in L[x]$. Если многочлен $f^\varphi(x)$ имеет корень в L, то существует продолжение $\tilde{\varphi} : E \to L$ гомоморфизма φ на поле E.

◀ Пусть α — корень $f(x)$ в E, а β — корень многочлена $f^\varphi(x)$ в L, причем $\deg f(x) = n$. Используем предыдущее замечание и проверим, что отображение $\tilde{\varphi}(a_0 + a_1\alpha \ldots + a_{n-1}\alpha^{n-1}) = \varphi(a_0) + \varphi(a_1)\beta + \ldots + \varphi(a_{n-1})\beta^{n-1}$ (где $a_0, \ldots, a_{n-1}$ — произвольные элементы поля F) — гомоморфизм. Достаточно заметить, что $\tilde{\varphi}(\alpha^k) = \beta^k$ при всех $k \geqslant 0$. Если $i + j < n$, это видно из определения $\tilde{\varphi}$, иначе запишем $x^k = f(x)q(x) + r(x)$, где $\deg r(x) < n$. Тогда $(x^k)^\varphi = f^\varphi(x)a^\varphi(x) + r^\varphi(x)$. Имеем $\alpha^k = r(\alpha)$ и $\beta^k = r^\varphi(\beta) = \tilde{\varphi}(\alpha^k)$.▶

Теорема 2 (о минимальности поля разложения). Пусть $\varphi : F \to L$ — гомоморфизм поля F в поле L, $f(x)$ — произвольный многочлен положительной степени над F и E — поле разложения многочлена $f(x)$. Если многочлен $f^\varphi(x)$ разлагается на линейные множители над L, то существует продолжение $\tilde{\varphi} : E \to L$ гомоморфизма φ на поле E.

◀ Построим продолжение $\tilde{\varphi}$, последовательно используя теорему 1. Если все неприводимые множители $f(x)$ линейны, то $E = F$ и $\tilde{\varphi} = \varphi$. Выберем неприводимый множитель положительной степени $p(x)$ многочлена $f(x)$. Ясно, что $p(x)$ имеет корень, скажем, α_1, в E, значит, по теореме 1, имеется подполе $E_1 \leqslant E$, изоморфное $F[x]/(p)$. Но $f(x) = p(x)g(x)$, $f^\varphi = p^\varphi(x)g^\varphi(x)$ и многочлен $p^\varphi(x)$ имеет корень в L. По теореме 1, существует продолжение φ_1 гомоморфизма φ на E_1. Далее разложим $f(x)$ над E_1: $f(x) = (x - \alpha_1)f_1(x)$, где $\deg f_1(x) < \deg f(x)$. Применим те же построения к $f_1(x) \in E_1[x]$ и т.д. ▶

Теорема 3 (о единственности поля разложения). Поле разложения многочлена $f(x) \in F[x]$ единственно в том смысле, что если E_1, E_2 — два поля разложения, то существует изоморфизм $\psi : E_1 \to E_2$, тождественный на F.

◀ Применим предыдущую теорему к тождественному вложению F в E_1. Получим гомоморфизм $\psi : E_1 \to E_2$, тождественный на F. Поскольку $f(x)$ разлагается на линейные множители над E_1, он разлагается на линейные множители над $\psi(E_1)$, поэтому $\psi(E_1)$ содержит все корни многочлена $f(x)$ в E_2 и по определению поля разложения совпадает с E_2.▶

Определение 1. *Характеристикой* поля F называется порядок элемента 1 в аддитивной группе $(F, +)$, если этот порядок конечен, и число 0, если 1 — элемент бесконечного порядка. Обозначение: $\operatorname{char} F$.
Пример: $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$.

Теорема 4. Если F — поле и $p = \operatorname{char} F > 0$, то p — простое число.

◄ По определению, $p \cdot 1 = 0$. Если $p = ab$, где $a < p$ и $b < p$, то по определению порядка элемента группы, $a \cdot 1 \neq 0$. Но тогда $b \cdot 1 = (a \cdot 1)^{-1}(a \cdot 1)(b \cdot 1) = (a \cdot 1)^{-1}(p \cdot 1) = 0$, и $p|b$, противоречие. ►

Замечание 1. Здесь мы впервые использовали то, что в теле (в частности, в поле) нет делителей нуля: если $ab = 0$, то $a = 0$ или $b = 0$.

Теорема 5. Пусть p — простое число (до конца лекции). Тогда кольцо вычетов $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ — поле.

◄ Если $p \nmid n$, то $(p, n) = 1 \Rightarrow \exists u, v \in \mathbb{Z} : \ up + vn = 1 \Rightarrow [v][n] = [1]$ в $\mathbb{Z}_p$.►

Теорема 6. Поле F характеристики $p > 0$ содержит подполе F_0, изоморфное $\mathbb{Z}_p$ (его называют *простым подполем* в F).

◄ $F_0 =< 1 >$ в группе $(F, +)$.►

Теорема 7 (о числе элементов конечного поля). Пусть F — поле из $q < \infty$ элементов. Тогда $q = p^n$, где $p = \operatorname{char} F$ — простое число, и $n \geqslant 1$.

◄ Поле F — конечномерное линейное пространство над простым подполем F_0. Пусть $[F : F_0] = n$. Тогда $|F| = |F_0^n| = p^n$.►

Теорема 8 (о существовании и единственности поля заданного примарного порядка). Пусть p — простое число, $n \geqslant 1$ и $q = p^n$. Тогда существует единственное с точностью до изоморфизма поле F такое, что $|F| = q$. Точнее, поле F изоморфно полю разложения многочлена $x^q - x$ над $\mathbb{Z}_p$.

◄

Лемма. Если F — поле характеристики $p > 0$, то отображение $\sigma : F \to F$, определенное по правилу $\sigma(a) = a^p \ \forall a \in F$. является гомоморфизмом. В случае конечного поля F гомомрфизм σ является изоморфизмом и называется *автоморфизмом Фробениуса*.

◄ Очевидно, что $\sigma(1) = 1^p = 1$ и $\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b) \ \forall a, b \in F$. Запишем $(a + b)^p = a^p + \sum\limits_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p$. Простой множитель p не входит в разложение знаменателя дроби $\binom{p}{i} = \dfrac{p}{i!(p-i)!}$. Значит, $p \Big| \binom{p}{i}$, и $\binom{p}{i} a^{p-i} b^i = 0$ при $i = 1, \ldots, p-1$. Итак, $\sigma(a+b) = \sigma(a)+\sigma(b)$, значит, σ — гомоморфизм. Если $|F| < \infty$, то из $|\sigma(F)| = |F|$ следует, что $\sigma(F) = F$, т.е. σ — автоморфизм.►

Пусть F — произвольное поле из $q = p^n$ элементов. Заметим, что если $a = 0$, то $a^q - a = 0 - 0 = 0$. Если же $a \in F^*$, то $a^{q-1} = 1$ по теореме Лагранжа, так как $|F^*| = q - 1$. Пусть теперь E — поле разложения многочлена $f(x) = x^q - x$. Заметим, что формальная производная $f'(x) = (p^n)x^{q-1} - 1 = -1$ не имеет корней в E, поэтому многочлен $f(x)$ не имеет в E кратных корней. Значит, число корней многочлена $f(x)$ в E равно q. С помощью доказанной выше леммы легко проверить, что множество корней $f(x)$ — подполе в E. Это подполе содержит $\mathbb{Z}_p$, так как $a^p = a$ для любого $a \in \mathbb{Z}_p$, по доказанному выше. Значит, по определению поля разложения, E совпадает с множеством корней $f(x)$, т.е. $|E| = q$. Изоморфизм полей F и E следует из

теоремы 3.►
Поле из q элементов обозначается $\mathbb{F}_q$ или $\mathrm{GF}(q)$.

Теорема 9 (о строении мультипликативной группы конечного поля). Если F — конечное поле, то F^* — циклическая группа.

◄ F^* — конечная абелева группа, поэтому $F^* \cong \mathbb{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_s}}$, где $p_1, \ldots, p_s$ — простые числа. Ясно, что $|F^*| = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$. Если, скажем, $p_1 = p_2$, и $k_1 \leqslant k_2$, то $a^m = 1$ для любого $a \in F^*$ и $m = p_2^{k_2} \ldots p_s^{k_s} < q-1$. Иными словами, многочлен $x^m - 1$ имеет более m корней, что невозможно. Значит, все простые числа $p_1, \ldots, p_s$ различны, и утверждение следует из китайской теоремы об остатках (теорема 4.2).►
Похожими рассуждениями можно доказать следующий факт:

Теорема 10. Если $F = \mathrm{GF}(q)$, и $q = p^n$, p — простое, то группа автоморфизмов поля F — циклическая группа порядка n, порождённая автоморфизмом Фробениуса σ.

◄ (Факультативно)►
Сначала заметим, что автоморфизмы $\sigma^0, sig, \ldots, sig^{n-1}$ различны (если $\sigma^k = \sigma^l$, где $0 \leq k < l < n$, то все элементы поля F — корни многочлена $x^{p^l} - x^{p^k}$, степень которого меньше q). С другой стороны, $a^q = a$ для любого $a \in F$, т.е. σ^n — тождественный автоморфизм. Осталось заметить, что $F = \mathrm{GF}(p)(\alpha)$, где α — корень некоторого неприводимого многочлена $f(x)$ степени n над $\mathrm{GF}(p)$, и любой автоморфизм поля F однозначно определяется образом α, который также должен быть корнем $f(x)$. Значит, число автоморфизмов не больше n.

Лекция 11. Алгебры над полем. Алгебраические элементы. Конечномерные алгебры с делением над полем $\mathbb{C}$. Коммутативные конечномерные алгебры с делением над полем $\mathbb{R}$. Тело кватернионов, его базис, структурные константы. Теорема Фробениуса.

Определение 1. *Алгеброй* над полем F называется кольцо A, которое одновременно является линейным пространством над F, причем операции сложения кольца и пространства совпадают, а операции умножения удовлетворяют соотношению

$$\forall a, b \in A,\ \lambda \in F:\ (\lambda a)b = a(\lambda b) = \lambda(ab). \tag{1}$$

Алгебра, являющаяся телом, называется *алгеброй с делением.*
Все рассматриваемые ниже в этой лекции алгебры — ассоциативные алгебры с единицей. Отождествим каждый элемент $\lambda \in F$ с элементом $\lambda \cdot 1 \in A$, т.е. будем считать, что $F \leqslant A$.

Определение 2. Пусть A — алгебра над полем F. Элемент $a \in A$ называется *алгебраическим*, если существует ненулевой многочлен $f(x) \in F[x]$, такой, что $f(a) = 0$. Многочлен наименьшей степени с таким свойством (для определённости можно считать, что его старший коэффициент равен 1) называется *минимальным многочленом* элемента a и обозначается $\mu_a(x)$. (вспомним курс линейной алгебры)

Теорема 1. Если A — алгебра с делением, и a — алгебраический элемент алгебры A, то $\mu_a(x)$ — неприводимый многочлен.

◀ Предположим противное. Пусть $\mu_a(x) = f(x)g(x)$ и $\deg f(x) < \deg \mu_a(x)$, $\deg g(x) < \deg \mu_a(x)$. Тогда $u = f(a) \neq 0$, но $ug(a) = 0 \Rightarrow g(a) = 0$ — противоречие.▶

Теорема 2. Любая конечномерная алгебра с делением над $\mathbb{C}$ изоморфна $\mathbb{C}$.

◀ Пусть A — указанная алгебра. Неприводимые многочлены над $\mathbb{C}$ имеют степень 1, поэтому для любого элемента $a \in A$ можно записать $\mu_a(x) = x - \lambda$, где $\lambda \in \mathbb{C}$. Имеем $0 = \mu_a(a) \Rightarrow a = \lambda$. Таким образом, $A = \mathbb{C}$.▶

Теорема 3. Любая коммутативная конечномерная алгебра с делением над $\mathbb{R}$ изоморфна либо $\mathbb{R}$, либо $\mathbb{C}$.

◀ Пусть A — указанная алгебра, $a \in A$. Если $\deg \mu_a(x) = 1$, то, как показано выше, $a \in \mathbb{R}$. Допустим, что $a \in A \setminus \mathbb{R}$. Тогда $\mu_a(x) = x^2 + \alpha x + \beta$, причем $\alpha^2 - 4\beta < 0$. Выделяем полный квадрат: $x^2 + \alpha x + \beta = (x + \alpha/2)^2 + \beta - \alpha^2/4$. Положим $\gamma = \sqrt{\beta - \alpha^2/4} \in \mathbb{R}$, $i = (a + \alpha/2)/\gamma$. Тогда $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ — подалгебра в A. Поскольку алгебра A коммутативна, выполняется (1) для любого $\lambda \in \mathbb{C}$. Итак, A — конечномерная алгебра с делением над $\mathbb{C}$, значит, $A = \mathbb{C}$. ▶

Определение 3. *Алгеброй кватернионов* называется четырехмерная алгебра $\mathbb{H}$ над $\mathbb{R}$ с базисом $1, i, j, k$, элементы которого удовлетворяют соотношениям

$$\begin{gathered} ij = k,\ jk = i,\ ki = j \\ ji = -k,\ kj = -i,\ ik = -j \\ i^2 = j^2 = k^2 = -1 \end{gathered} \tag{2}$$

Ассоциативность алгебры $\mathbb{H}$ и то, что $\mathbb{H}$ есть алгебра с делением, можно проверить непосредственно, а можно указать следующее матричное представление алгебры $\mathbb{H}$. Рассмотрим множество $\mathcal{H}$ матриц вида $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$, где z, w — произвольные комплексные числа. Легко видеть, что $\mathcal{H}$ — алгебра над $\mathbb{R}$ (но не над $\mathbb{C}$!), и если $A = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \neq 0$, то $\det A = |z|^2 + |w|^2 > 0$ и $A^{-1} = \dfrac{1}{|z|^2+|w|^2} \begin{pmatrix} \overline{z} & -w \\ \overline{w} & z \end{pmatrix} \in \mathcal{H}$. В $\mathcal{H}$ имеется базис E, $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Легко проверяются соотношения между I, J, K, аналогичные (2). Значит, $\mathbb{H} \cong \mathcal{H}$, и $\mathbb{H}$ — ассоциативная алгебра с делением над $\mathbb{R}$.

Теорема 4 (теорема Фробениуса). Любая конечномерная некоммутативная алгебра с делением над $\mathbb{R}$ изоморфна $\mathbb{H}$.

◀ Пусть A — алгебра с указанными свойствами. Как доказательстве теоремы 3, найдем элемент $i \in A$, удовлетворяющий условию $i^2 = -1$. Тогда $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ — подалгебра в A, и A можно рассматривать как векторное пространство над $\mathbb{C}$. Рассмотрим $\mathbb{C}$-линейный оператор на A: $\mathcal{A}(a) = ai \ \forall a \in A$. Легко видеть, что $\mathcal{A}(1) = 1i = i1$, значит, 1 — собственный вектор оператора $\mathcal{A}$ с собственным значением i. Далее, $\mathcal{A}^2(a) = ai^2 = -a$, значит, минимальный многочлен оператора $\mathcal{A}$ делит многочлен $x^2 + 1$. Поэтому минимальный многочлен оператора $\mathcal{A}$ не имеет кратных корней, его матрица в некотором базисе диагональна, и линейное пространство A представляется в виде прямой суммы $A = A_+ \oplus A_-$, где $A_+ = \{a : \ \mathcal{A}(a) = ia\}$, $A_- = \{a : \ \mathcal{A}(a) = -ia\}$. Заметим, что $a \in A_+ \Leftrightarrow ai = ia$, $ai = ia \Rightarrow a^{-1}i = ia^{-1} \Rightarrow a^{-1} \in A_+$, $a, b \in A_+ \Rightarrow abi = aib = iab \Rightarrow ab \in A_+$. Получаем, что A_+ — конечномерная алгебра с делением над $\mathbb{C}$, значит, по теореме 2, $A_+ = \mathbb{C}$. Если $A_- = 0$, то $A = A_+ = \mathbb{C}$ — коммутативная алгебра, что противоречит условию. Значит, существует ненулевой элемент $b \in A_-$. Заметим, что отображение $\mathcal{B} : A_- \to A$, заданное умножением справа на b (т.е. $\mathcal{B}(a) = ab$) переводит A_- в A_+ и имеет нулевое ядро: $abi = -aib = -(-iab) = iab$ при $a \in A_-$. Поэтому $\dim_{\mathbb{C}} A_- = 1$. В частности, $b^2 \in A_+ = \mathbb{C}$, т.е. $b^2 = \alpha + \beta i, \ \alpha, \beta \in \mathbb{R}$. Но тогда $b^2 b = \alpha b + \beta ib$, $bb^2 = b(\alpha + \beta i) = \alpha b - \beta ib$. Поскольку $b^2 b = bb^2$, получаем $\beta = 0$. При этом $\alpha < 0$, иначе получили бы невозможное равенство $(b - \sqrt{\alpha})(b + \sqrt{\alpha}) = 0$. Значит, полагая $j = b/\sqrt{-\alpha}$, получаем элемент j, удовлетворяющий условиям $j^2 = -1$ и $ij = -ji$. Положим $k = ij$. Остальные соотношения (2) проверяются с использованием уже полученных, например: $k^2 = ijij = i(-ij)j = -i^2 j^2 = -1$ (не забываем о некоммутативности!). Поскольку $1, j$ — базис A над $\mathbb{C}$, $1, i, j, k$ — базис A над $\mathbb{R}$.▶

Лекция 12. Представления групп. Примеры. Эквивалентность представлений, условие эквивалентности представлений в матричной записи. Подпредставления и инвариантные подпространства, прямые суммы представлений. Неприводимые представления. Вполне приводимые представления. Теорема Машке.

Определение 1. Пусть G — группа, F — поле, V — линейное пространство над F. *Представлением* группы G в пространстве V называется произвольный гомоморфизм $\rho : G \to \mathrm{GL}(V)$ группы G в группу обратимых линейных операторов на пространстве V. *Размерностью* представления ρ называется размерность соответствующего пространства V. Обозначение: $\dim \rho$.
Примеры: тождественное отображение $\mathrm{GL}(V)$ или любой ее подгруппы в $\mathrm{GL}(V)$, мономиальное представление S_n (оператор $\rho(\sigma)$ задается на базисе $e_1, \ldots, e_n$ так: $\rho(\sigma)(e_i) = e_{\sigma(i)}$).

Определение 2. *Гомоморфизмом* представления $\rho_1 : G \to \mathrm{GL}(V_1)$ в представление $\rho_2 : G \to \mathrm{GL}(V_2)$ называется линейное отображение $f : V_1 \to V_2$, удовлетворяющее условию

$$\forall g \in G : \ f\rho_1(g) = \rho_2(g)f. \tag{1}$$

Обозначение $f : \rho_1 \to \rho_2$.

Определение 3. *Изоморфизм* представлений — гомоморфизм, заданный изоморфизмом соотвествующих линейных пространств. Изоморфные представления называют также *эквивалентными.*
В случае представления размерности $n < \infty$ имеется изоморфизм $\mathrm{GL}(V) \cong \mathrm{GL}(n, F)$, поэтому представление можно рассматривать как гомоморфизм группы G в группу обратимых матриц $\mathrm{GL}(n, F)$ порядка n (матричная форма представления).

Теорема 1 (условие эквивалентности представлений в матричной форме). Представления $\rho_1 : G \to \mathrm{GL}(n, F)$ и $\rho_2 : G \to \mathrm{GL}(n, F)$ эквивалентны $\Leftrightarrow$ существует обратимая матрица C, такая, что

$$\forall g \in G : \ \rho_2(g) = C\rho_1(g)C^{-1}. \tag{2}$$

◀ Любой изоморфизм n-мерных пространств задается умножением на обратимую матрицу, и обратно. Подставляя в (1) умножение на C вместо применения f, получаем $C\rho_1(g) = \rho_2(g)C$, откуда и следует (2).▶

Определение 4. Пусть $\rho : G \to \mathrm{GL}(V)$ — представление группы G. Подпространство $U \subseteq V$ называется *инвариантным* относительно ρ, если

$$\forall g \in G : \ \rho(g)(U) \subseteq U. \tag{3}$$

Замечание 1. Из (3) следует, что $\rho(g^{-1})(U) \subseteq U$, поэтому $\rho(g)(U) = U$ для любого $g \in G$.

Определение 5. Пусть $\rho : G \to \mathrm{GL}(V)$ — представление группы G, и U — инвариантное подпространство в V. Представление $\rho_U : g \mapsto \rho(G)|_U$ называется *подпредставлением* представления ρ.

Замечание 2. Если $f : \rho_1 \to \rho_2$ — гомоморфизм представлений, т.е. линейное отображение $f : V_1 \to V_2$ соответствующих пространств, то $f(V_1)$ — инвариантное подпространство в V_2, а

$\ker f$ — инвариантное подпространство в V_1.

Замечание 3. Пусть U — инвариантное подпространство относительно представления $\rho : G \to \mathrm{GL}(V)$. Пусть $e_1, \ldots, e_k$ — базис U, $e_{k+1}, \ldots, e_n$ — его дополнение до базиса V. Тогда матрица любого оператора $\rho(g)$ в этом базисе имеет блочно-треугольный вид $\begin{pmatrix} \rho_U(g) & * \\ 0 & * \end{pmatrix}$.

Определение 6. Пусть $\rho : G \to \mathrm{GL}(V)$ — представление группы G, $U_1, \ldots, U_s$ — инвариантные подпространства в V, $\rho_i = \rho_{U_i}$ при $i = 1, \ldots, s$ причем $V = U_1 \oplus \ldots \oplus U_s$. Тогда представление ρ называется прямой суммой подпредставлений $\rho_1, \ldots, \rho_s$. Обозначение: $\rho = \rho_1 \oplus \ldots \oplus \rho_s$.

Замечание 4. Если $\rho = \rho_1 \oplus \ldots \oplus \rho_s$, то в подходящем базисе матрица каждого оператора $\rho(g)$ имеет блочно-диагональный вид $\begin{pmatrix} \rho_1(g) & 0 & \cdots & 0 \\ 0 & \rho_2(g) & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & \rho_s(g) \end{pmatrix}$.

Определение 7. Представление $\rho : G \to \mathrm{GL}(V)$ называется *неприводимым*, если V содержит ровно 2 инвариантных подпространства: $\{0\}$ и V.
Пример: одномерное представление всегда неприводимо.

Определение 8. Представление $\rho : G \to \mathrm{GL}(V)$ называется *вполне приводимым*, если оно разлагается в прямую сумму неприводимых подпредставлений.

Теорема 2 (теорема Машке). Если G — конечная группа, F — поле, причем $\mathrm{char}\, F = 0$ или $\mathrm{char}\, F \nmid |G|$, то любое представление группы G над полем F вполне приводимо.

◀ Докажем теорему для конечномерных представлений индукцией по размерности. Как отмечено выше, для одномерных представлений теорема верна. Пусть $\rho : G \to \mathrm{GL}(V)$ — представление размерности $m > 1$. Если ρ неприводимо, то утверждение выполнено. Иначе имеется инвариантное подпространство $0 \neq U \neq V$. Пусть U' — какое-то (может быть, не инвариантное) дополнение U до V, т.е. $V = U \oplus U'$, и $\pi : V \to U$ — проекция V на U. Заметим, что по условию $n = |G| \neq 0$ как элемент $n \cdot 1$ поля F. "Подправим" π до гомоморфизма $\rho \to \rho_U$: рассмотрим линейное отображение $\tilde{\pi} : V \to U$, заданное формулой

$$\tilde{\pi}(v) = \frac{1}{n} \sum_{h \in G} \rho(h) \pi \rho(h^{-1})(v). \tag{4}$$

Заметим сначала, что действительно $\tilde{\pi}(v) \in U$: $\pi\rho(h^{-1})(v) \in U \Rightarrow \rho(h)\pi\rho(h^{-1})(v) \in U$ для любого $h \in G$ в силу инвариантности U. Затем проверим, что $\tilde{\pi}$ — проектирование: при $u \in U$,

$$\tilde{\pi}(u) = \frac{1}{n} \sum_{h \in G} \rho(h) \pi \underbrace{\rho(h^{-1})(u)}_{\in U} = \frac{1}{n} \sum_{h \in G} \rho(h)\rho(h^{-1})(u) = \frac{1}{n} \sum_{h \in G} u = \frac{1}{n} nu = u.$$

Теперь проверим условие (1): если $g \in G$ и $v \in V$, то

$$\begin{aligned} \tilde{\pi}\rho(g)(v) &= \frac{1}{n} \sum_{h \in G} \rho(h)\pi\rho(h^{-1})\rho(g)(v) \\ &= \frac{1}{n} \sum_{h \in G} \rho(g)\rho(g^{-1}h)\pi\rho(h^{-1}g)(v) \overset{h=gt}{=} \frac{1}{n}\rho(g) \sum_{t \in G} \rho(t)\pi\rho(t^{-1})(v) \\ &= \rho(g) \underbrace{\tilde{\pi}(v)}_{\in U} = \rho_U(g)\tilde{\pi}(v). \end{aligned}$$

Теперь ясно, что $\tilde{\pi}(V) = U$ и $\ker\tilde{\pi} = W$ — инвариантные относительно ρ подпространства в V, причем $V = W \oplus U$: $\forall v \in V:\ v = \underbrace{(v - \tilde{\pi}(v))}_{\in W} + \underbrace{\tilde{\pi}(v)}_{\in U} \Rightarrow V = W + U$, и если $v \in W \cap U$, то $v = \tilde{\pi}(v) = 0$. Поскольку $\dim U < \dim V$ и $\dim W < \dim V$, по предположению индукции каждое из представлений ρ_U и ρ_W вполне приводимо. значит и ρ — вполне приводимое представление.▶

Лекция 13. Лемма Шура. Кратность неприводимого подпредставления, её инвариантность.

Замечание 1. Пусть $\rho_1 : G \to \mathrm{GL}(V_1)$ и $\rho_2 : G \to \mathrm{GL}(V_2)$ — неприводимые представления группы G. Тогда любой гомоморфизм представлений $f : V_1 \to V_2$ либо нулевой, либо изоморфизм.

◀ $\ker f$ — инвариантное подпространство в V_1. Значит, либо $\ker V_1 = V_1$, и тогда $f = 0$, либо $\ker f = 0$. Во втором случае $f(V_1) \cong V_1 \neq 0$, поэтому $f(V_1) = V_2$. Следовательно, отображение f сюръективно и инъективно, т.е. является изоморфизмом.▶

Определение 1. Для любых двух представлений $\rho_1 : G \to \mathrm{GL}(V_1)$ и $\rho_2 : G \to \mathrm{GL}(V_2)$ группы G над полем F множество всех гомоморфизмов ρ_1 в ρ_2 является линейным пространством над F относительно обычных операций поточечного сложения отображений и умножения отображения на скаляр. Обозначим это пространство через $\mathrm{Hom}(\rho_1, \rho_2)$. Если $\rho : G \to \mathrm{GL}(V)$, то в $\mathrm{Hom}(\rho, \rho)$ есть операция композиции отображений, и $\mathrm{Hom}(\rho, \rho)$ — алгебра над F. Эта алгебра называется *алгеброй эндоморфизмов* представления ρ и обозначается $\mathrm{End}(\rho)$.

Теорема 1 (Лемма Шура). Если ρ — неприводимое представление, то $\mathrm{End}(\rho)$ — тело.

◀ Из замечания 1 следует, что ненулевой гомоморфизм $f : \rho \to \rho$ — изоморфизм. Отображение $f^{-1} \in \mathrm{End}(\rho)$ — обратный элемент к f. ▶

В случае конечномерных комплексных представлений (т.е. при $F = \mathbb{C}$) лемму Шура можно уточнить и усилить.

Теорема 2. Если ρ — неприводимое конечномерное комплексное представление, то $\mathrm{End}(\rho) = \mathbb{C}$.

◀ Вытекает из леммы Шура и теоремы 11.2.▶

Теорема 3. Пусть $\rho_1 : G \to \mathrm{GL}(V_1)$ и $\rho_2 : G \to \mathrm{GL}(V_2)$ — неприводимые конечномерные комплексные представления группы G, тогда

$$\dim \mathrm{Hom}(\rho_1, \rho_2) = \begin{cases} 0, & \text{если } \rho_1 \ncong \rho_2, \\ 1, & \text{если } \rho_1 \cong \rho_2. \end{cases} \tag{1}$$

◀ Первый вариант сразу следует из замечания 1. Во втором случае $\mathrm{Hom}(\rho_1, \rho_2)$ — линейное пространство, изоморфное $\mathrm{Hom}(\rho_1, \rho_2) \cong \mathrm{Hom}(\rho_1, \rho_1) = \mathbb{C}$, по теореме 2.▶

Теорема 4 (Единственность разложения в сумму неприводимых представлений). Пусть $\rho : G \to \mathrm{GL}(V)$ — представление, и $\rho = \rho_1 \oplus \ldots \oplus \rho_s = \rho'_1 \oplus \ldots \oplus \rho'_t$ — два разложения в прямую сумму неприводимых представлений. Тогда $s = t$ и после некоторой перестановки слагаемых $\rho_i \cong \rho'_i$, $i = 1, \ldots, s$.

◀ Пусть $V_1, \ldots, V_s$ и $V'_1, \ldots, V'_t$ — подпространства, соответствующие заданным неприводимым представлениям. Для определенности будем считать, что $s \leqslant t$, и проведем индукцию по s. Если $s = 1$, то V — неприводимое представление, значит $V = V'_1$ и $t = 1$. Выберем наибольшее подмножество $J \subseteq \{1, \ldots, t\}$, такое, что $V_1 \cap \left(\bigoplus_{j \in J} V'_j \right) = 0$. Если $V_1 \oplus \left(\bigoplus_{j \in J} V'_j \right) \neq V$, то существует хотя бы одно подпространство V'_k, которое не содержится в $V_1 \oplus \left(\bigoplus_{j \in J} V'_j \right)$. Но в

силу неприводимости ρ'_k, тогда $V_1 \oplus \left(\bigoplus\limits_{j\in J} V'_j\right) \cap V'_k = 0$, значит, $V_1 \cap \left(\bigoplus\limits_{j\in J\cup\{k\}} V'_j\right) = 0$. Это противоречит максимальности множества J. Следовательно, $V_1 \oplus \left(\bigoplus\limits_{j\in J} V'_j\right) = V$. Рассмотрим проекцию V на $V_2 \oplus \ldots \oplus V_s$. По доказанному $V_2 \oplus \ldots \oplus V_s \cong \left(\bigoplus\limits_{j\in J} V'_j\right)$. По предположению индукции $s - 1 = |J|$ и слагаемые $\rho_2, \ldots, \rho_s$ изоморфны соответствующим слагаемым из множества ρ'_j, $j \in J$. Аналогично, $\rho_1 \cong \left(\bigoplus\limits_{k\notin J} \rho'_k\right)$, значит, имеется единственный индекс $k \notin J$ и $\rho'_k \cong \rho_1$.▶

Из доказанной теоремы вытекает корректность следующего определения.

Определение 2. Пусть ρ — вполне приводимое конечномерное представление, а ρ_0 — некоторое неприводимое представление группы G. *Кратностью* неприводимого представления ρ_0 в представлении ρ называется количество слагаемых, изоморфных ρ_0, в (произвольном) разложении ρ в прямую сумму неприводимых представлений.

Лекция 14. Кратность неприводимого представления в регулярном комплексном представлении. Комплексные представления коммутативных конечных групп. Одномерные комплексные представления произвольных конечных групп.

Для частного случая комплексных представлений можно указать способ вычисления кратности, который гарантирует корректность определения.

Теорема 1. Пусть ρ — конечномерное комплексное представление, а ρ_0 — некоторое неприводимое комплексное представление группы G. Тогда кратность представления ρ_0 в ρ равна $\dim \mathrm{Hom}(\rho, \rho_0)$.

◄ Пусть $\rho = \rho_1 \oplus \ldots \oplus \rho_s$, причем $\rho_1 \cong \ldots \cong \rho_k \cong \rho_0$ и $\rho_i \ncong \rho_0$ при $i > k$, т.е. k — кратность представления ρ_0 в ρ. Тогда в силу (13.1) $\dim \mathrm{Hom}(\rho, \rho_0) = \underbrace{1 + \ldots + 1}_{k \text{ раз}} + \underbrace{0 + \ldots + 0}_{s-k \text{ раз}} = k$.►

Определение 1. Пусть G — конечная группа, F — поле. Рассмотрим пространство FG, состоящее из формальных сумм вида $\sum\limits_{h \in G} \alpha_h h,\ \alpha_h \in F$. Базис этого пространства — множество элементов вида $1h + \sum\limits_{t \neq h} 0t$, которые естественно коротко записывать просто h. На пространстве FG естественно определяется умножение, превращающее FG в алгебру (она называется *групповой алгеброй* группы G над F). *Регулярным представлением* группы G над F называется представление $\rho_{\mathrm{reg}} : G \to \mathrm{GL}(FG)$, определенное на указанном выше базисе формулой $\rho_{\mathrm{reg}}(g)(h) = gh$.

Теорема 2. Пусть $\rho : G \to \mathrm{GL}(V)$ — представление конечной группы G. Тогда $\mathrm{Hom}(\rho_{\mathrm{reg}}, \rho) \cong V$.

◄ Рассмотрим отображение $\varphi : \mathrm{Hom}(\rho_{\mathrm{reg}}, \rho) \to V$, определенное равенством $\varphi(f) = f(e)$. Ясно, что φ — линейное отображение. Заметим, что $f(e) = 0 \Rightarrow \forall g \in G :\ f(g) = f(ge) = f\rho_{\mathrm{reg}}(g)(e) = \rho(g)f(e) = 0$, значит $f = 0$, т.е. $\ker \varphi = 0$. Для любого $v \in V$ зададим гомоморфизм $f_v : FG \to V$ на базисе FG: $f_v(h) = \rho(h)v$. Условие (12.1) проверяется непосредственно, при этом $v = \varphi(f_v)$. Значит, φ — инъективное и сюръективное линейное отображение, т. е. изоморфизм линейных пространств. ►

Теорема 3. Кратность неприводимого представления в регулярном комплексном представлении конечной группы равна его размерности.

◄ Если k — кратность неприводимого представления ρ_0 в ρ_{reg},
то $k \overset{\text{т.1}}{=} \dim \mathrm{Hom}(\rho_{\mathrm{reg}}, \rho_0) \overset{\text{т.2}}{=} \dim V$.►

Следствие. Конечная группа имеет лишь конечное число неприводимых комплексных представлений (с точностью до изоморфизма).

◄ Все такие представления изоморфны прямым слагаемым разложения регулярного представления. ►

Теорема 4. Пусть $\rho_1, \ldots, \rho_s$ — полный набор неприводимых попарно неизоморфных комплексных представлений конечной группы G, $k_i = \dim \rho_i$, $i = 1, \ldots, s$. Тогда

$$k_1^2 + \ldots + k_s^2 = |G|. \tag{1}$$

◄ Из предыдущей теоремы имеем $|G| = \dim(FG) = k_1 \dim \rho_1 + \ldots + k_s \dim \rho_s = k_1^2 + \ldots + k_s^2$.►

Теорема 5. Все неприводимые комплексные представления коммутативной конечной группы одномерны, и их число равно порядку группы.

◄ Одномерное представление — это гомоморфизм G в $\mathbb{C}^*$. Из теоремы 12.1 следует, что одномерные представления произвольной группы изоморфны тогда и только тогда, когда они совпадают. Построим $n = |G|$ одномерных представлений конечной коммутативной группы G. Группа G изоморфна прямой сумме циклических групп (теорема 4.3). Для каждого слагаемого $\mathbb{Z}_d$, входящего в эту сумму, можно отобразить [1] в любой корень степени d из 1 в $\mathbb{C}$, а таких корней d. Комбинируя всевозможные гомоморфизмы на слагаемых, получаем всего n представлений. Но тогда из (1) следует, что $k_1 = \ldots, k_n = 1$, а больше в сумме квадратов (1) слагаемых быть не может.►

Теорема 6. Число одномерных комплексных представлений конечной группы G равно $|G/G'|$.

◄ Пусть $\rho : G/G' \to \mathbb{C}^*$ — одномерное представление группы G/G', $\pi : G \to G/G'$ — канонический гомоморфизм. Тогда $\rho\pi : G \to \mathbb{C}^*$ — одномерное представление группы G. Обратно, если $\rho : G \to \mathbb{C}^*$ — одномерное представление, то $\ker \rho \supseteq G'$ (теорема 7.1, свойство 4). Следовательно, гомоморфизм $\overline{\rho} : G/G' \to \mathbb{C}^*$, такой, что $\forall g \in G, \overline{\rho}(gG') = \rho(g)$, определен корректно, и $\overline{\rho}\pi = \rho$. Тем самым установлено взаимно-однозначное соответствие между одномерными представлениями групп G и G', и можно использовать теорему 5.►

Теорема 7. Число неприводимых комплексных представлений конечной группы G равно числу классов сопряженных элементов G.

◄ Вычисление двумя способами размерности центра групповой алгебры $\mathbb{C}G$. С одной стороны, $z = \sum_{h \in G} \alpha_h h \in Z(\mathbb{C}G) \Leftrightarrow \forall g \in G,\ gz = zg \Leftrightarrow \forall g \in G,\ z = gzg^{-1} \Leftrightarrow \forall g \in G,\ \sum_{h \in G} \alpha_h h = \sum_{h \in G} \alpha_h ghg^{-1}$, откуда $\alpha_h = \alpha_{ghg^{-1}}\ \forall g, h \in G$, значит, $\dim Z(\mathbb{C}G)$ совпадает с числом классов сопряженных элементов. С другой стороны, по теореме 2 $\mathbb{C}G \cong \mathrm{End}(\rho_{\mathrm{reg}})$. Если $\rho_1, \ldots, \rho_s$ — полный набор неприводимых попарно неизоморфных комплексных представлений группы G, и $k_i = \dim \rho_i$, $i = 1, \ldots, s$, то $\mathbb{C}G \cong \mathrm{End}(\rho_{\mathrm{reg}}) \cong M_{k_1}(\mathbb{C}) \oplus \ldots \oplus M_{k_s}(\mathbb{C})$, и $\dim Z(\mathbb{C}G) = s$.►

ЛИТЕРАТУРА

1. Кострикин А.И., Введение в алгебру, М., Наука, 1977.
2. Кострикин А.И., Введение в алгебру, М., Физико-математическая литература, ч. 3: основные структуры алгебры, 2000.
3. Винберг Э.Б., Курс алгебры, М., Факториал Пресс, 2001.
4. Каргополов М.И., Мерзляков Ю.И., Основы теории групп, М., Наука, 1972.
5. Сборник задач по алгебре (под ред. Кострикин А.И.), М., Физико-математическая литература, 2001.

Предметный указатель