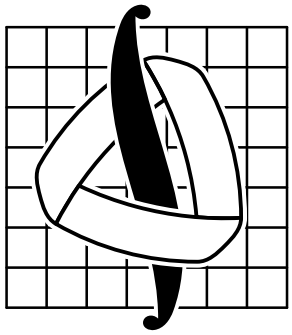
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
имени М.В.ЛОМОНОСОВА

Механико–математический факультет

Кафедра Высшей алгебры



# Курс лекций по высшей алгебре

Лектор — Эрнест Борисович Винберг

Летописец — Бибиков Павел Витальевич (группа 212)

II курс, 2 поток, отделение математики (2006 – 2007 гг.)

Лекция 1.

## 1. Определение и примеры групп.

*Группой* называется множество $G$ с операцией умножения, удовлетворяющей условиям

1) $(ab)c = a(bc)$ (*ассоциативность*),

2) $\exists\, e$ (*единица*) : $ae = ea = a \quad \forall\, a \in G$,

3) $\forall a \in G \ \exists\, a^{-1} \in G$ (*обратный элемент*) : $aa^{-1} = a^{-1}a = e$.

Группа $G$ называется *коммутативной* (или *абелевой*), если $ab = ba \ \ \forall a, b \in G$.

*Аддитивной группой* называется множество $G$ с операцией сложения, удовлетворяющей условиям

1) $(a + b) + c = a + (b + c)$ (*ассоциативность*)

2) $\exists\, 0$ (*нуль*) : $a + 0 = 0 + a = a \ \ \forall a \in G$

3) $\forall a \in G \ \exists (-a) \in G$ (*противоположный элемент*) : $a + (-a) = (-a) + a = 0$.

Обычно аддитивная группа предполагается абелевой: $a + b = b + a \ \ \forall a, b \in G$.

Подмножество $H$ группы $G$ называется *подгруппой*, если

1) $ab \in H \ \ \forall a, b \in H$,

2) $a^{-1} \in H \ \ \forall a \in H$,

3) $e \in H$.

Подгруппа сама является группой относительно той же операции.

Отображение $f\colon G \to H$ называется *изоморфизмом* группы $G$ на группу $H$, если

1) $f$ биективно,

2) $f(ab) = f(a)f(b) \ \ \forall a, b \in G$.

Свойства изоморфизма: $f(e) = e$, $f(a^{-1}) = f(a)^{-1}$.

**Примеры.**

1. $\mathbb{Z}$ (по сложению) — абелева группа. По определению, всякое кольцо является абелевой группой по сложению.

2. $\mathbb{R}^+ = \mathbb{R} \setminus \{0\}$ — абелева группа по умножению. По определению, совокупность ненулевых элементов любого поля $K$ является абелевой группой по умножению и обозначается через $K^*$.

3. $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ — подгруппа в $\mathbb{C}^*$.

4. $C_n = \{z \in \mathbb{C} : z^n = 1\}$ — подгруппа в $\mathbb{T}$.

5. Векторы плоскости (или пространства) образуют абелеву группу относительно сложения. По определению, всякое векторное пространство является абелевой группой по сложению.

6. $S(X)$ — группа преобразований (биективных отображений в себя) множества $X$ (единица — $\mathrm{id}_X$). В частности, $S(\{1, 2, \ldots, n\}) = S_n$ — симметрическая группа подстановок степени $n$. Всякая подгруппа группы $S(X)$ называется *группой преобразований* множества $X$.

7. $\mathrm{Isom}\,\mathbb{E}^2$ ($\mathrm{Isom}\,\mathbb{E}^3$) — группа движений евклидовой плоскости (пространства). $\mathrm{Isom}_+\,\mathbb{E}^2$ ($\mathrm{Isom}_+\,\mathbb{E}^3$) — подгруппа собственных (сохраняющих ориентацию) движений.

8. Группа симметрий правильных многоугольников (или многогранников): $P \subset \mathbb{E}^2$ ($\mathbb{E}^3$). $\mathrm{Sym}\,P = \{g \in \mathrm{Isom}\,\mathbb{E}^2\ (\mathbb{E}^3) : gP = P\}$. $D_n$ — группа симметрий правильного $n$-угольника (*группа диэдра*). $|D_n| = 2n$. $C_n$ — это группа вращений правильного $n$-угольника. $|C_n| = n$.

9. Кристаллографические группы (группы симметрий кристаллических структур).

10. $\mathrm{GL}(V)$ — группа невырожденных линейных преобразований $n$-мерного векторного пространства над полем $K$. $\mathrm{GL}(V) \simeq \mathrm{GL}_n(K)$ — группа невырожденных матриц $n \times n$ над полем $K$.

11. $\mathrm{O}(V)$ — группа преобразований евклидова векторного пространства $V$. $\mathrm{O}(V) \simeq \mathrm{O}_n$ — группа ортогональных матриц. Отказываясь от требования положительной определенности скалярного умножения (но предполагая невырожденность), получаем группу псевдоортогональных преобразований, изоморфную $\mathrm{O}_{p,q}$ (группа псевдоортогональных матриц), где $(p, q)$ — *сигнатура* скалярного умножения (т.е. число плюсов и минусов). В частности, $\mathrm{O}_{3,1}$ — группа Лоренца.

12. $\mathrm{GL}_n(\mathbb{Z})$ — группа обратимых целочисленных матриц.

13. $K$ — поле, $f \in K[x]$ — неприводимый многочлен степени $n$; $K \subset L$ — поле разложения многочлена $f$. $\mathrm{Gal}\,L/K = \{\varphi \in \mathrm{Aut}\,L : \varphi|_K = \mathrm{id}\}$ — группа Галуа поля $L$ над $K$. $\mathrm{Gal}\,L/K \subset S_n$. Например, $\mathrm{Gal}\,\mathbb{C}/\mathbb{R} \simeq C_2$.

## 2. Циклические группы.

*Степень* элемента: $g^n = \underbrace{g \cdot \ldots \cdot g}_{n}$ при $n > 0$, $e$ при $n = 0$ и $\underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n}$ при $n < 0$. $g^m \cdot g^n = g^{m+n}$, $(g^n)^{-1} = g^{-n}$.

$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ — *циклическая группа, порожденная элементом* $g$. Если $\exists\, g \in G : G = \langle g \rangle$, то $G$ называется *циклической группой*.

Либо все $g^n$ различны, либо нет. Во втором случае они циклически повторяются с некоторым периодом $m = \operatorname{ord} g$ (*порядок элемента* $g$). $\operatorname{ord} g = \min\limits_{g^n = e}\{n > 0\}$.

**Теорема 2.1.** *1. Все бесконечные циклические группы изоморфны* $\mathbb{Z}$.

*2. Всякие конечные циклические группы порядка* $n$ *изоморфны* $C_n$. $\square$

Лекция 2.

## 3. Факторгруппа.

*Отношение* на множестве $X$ — это подмножество $\mathcal{R} \in X \times X$. Если $(x, y) \in \mathcal{R}$, то говорят, что $x$ и $y$ *находятся в отношении* $\mathcal{R}$ и пишут $x\mathcal{R}y$. Отношение $\mathcal{R}$ называется *отношением эквивалентности*, если

1) $x\mathcal{R}x \;\; \forall x \in X$ (*рефлексивность*),

2) $x\mathcal{R}y \Rightarrow y\mathcal{R}x$ (*симметричность*),

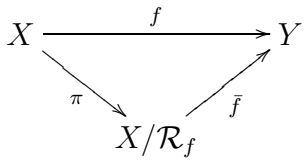
3) $x\mathcal{R}y \;\&\; y\mathcal{R}z \Rightarrow x\mathcal{R}z$ (*транзитивность*).

Обычно пишут $x \underset{\mathcal{R}}{\sim} y$, или просто $x \sim y$.

*Класс эквивалентности, содержащий* $x$: $\mathcal{R}(x) = [x] = \{y \in X : x \sim \sim y\}$. Классы эквивалентности задают разбиение множества $X$. Множество классов эквивалентности называется *фактормножеством* множества $X$ по отношению эквивалентности $\mathcal{R}$ и обозначается $X/\mathcal{R}$.

Есть естественное отображение $\pi\colon X \to X/\mathcal{R}$, $x \mapsto \mathcal{R}(x)$. Оно называется *отображением факторизации*.

Для любого отображения $f\colon X \to Y$ определяется отношение эквивалентности $\mathcal{R}_f$ на $X$: $x_1 \sim x_2$, если $f(x_1) = f(x_2)$. Получается следующая диаграмма:



По определению, $\bar{f}([x]) = f(x)$. $f = \bar{f} \circ \pi$, $\pi$ сюръективен, $\bar{f}$ инъективен. Это разложение называется *факторизацией* $f$.

Пусть $(X, \circ)$ — множество с операцией. Отношение эквивалентности $\mathcal{R}$ на множестве $X$ называется *согласованным с операцией* $\circ$, если $x \sim x'$, $y \sim y' \Rightarrow x \circ y \sim x' \circ y'$. Тогда на фактормножестве $X/\mathcal{R}$ можно ввести операцию $\circ$: $[x] \circ [y] = [x \circ y]$. Это определение корректно. Из определения следует, что отображение факторизации является гомоморфизмом, т.е. $\pi(x \circ y) = \pi(x) \circ \pi(y)$.

Пусть $(X, \circ)$ и $(Y, *)$ — два множества с операциями, $f\colon X \to Y$ — *гомоморфизм*, т.е. $f(x_1 \circ x_2) = f(x_1) * f(x_2) \ \ \forall x_1, x_2 \in X$. Имеем: $f = \bar{f}\pi$, где $\pi\colon X \to X/\mathcal{R}_f$, $\bar{f}([x]) = f(x)$.

**Теорема 3.1.** *$\bar{f}$ — гомоморфизм, а если $f$ сюръективен, то $\bar{f}$ — изоморфизм $X/\mathcal{R}_f$ на $Y$.*

*Доказательство.* $\bar{f}([x_1] \circ [x_2]) = \bar{f}([x_1 \circ x_2]) = f(x_1 \circ x_2) = f(x_1) * f(x_2) = \\ = \bar{f}([x_1]) * \bar{f}([x_2])$. □

Пусть $G$ — группа, $H \subset G$ — подгруппа. *Отношение сравнимости по модулю* $H$: $g_1 \equiv g_2 \pmod{H}$, если $g_1^{-1} g_2 \in H$. Это отношение является отношением эквивалентности. Классы эквивалентности имеют вид $[g] = \\ = gH = \{gh : h \in H\}$ и называются *левыми смежными классами группы $G$ по $H$*.

Аналогично, можно определить $g_1 \equiv g_2 \pmod{H}$, если $g_2 g_1^{-1} \in H$. Тогда классы эквивалентности имеют вид $[g] = Hg$ и называются *правыми смежными классами группы $G$ по $H$*.

*Инверсия* (взятие обратного элемента) в группе $G$ осуществляет биекцию между множествами левых и правых смежных классов: $(gH)^{-1} = \\ = Hg^{-1}$. Количество левых и правых смежных классов одинаково и обозначается $|G : H|$.

**Теорема 3.2** (Лагранж)**.** *Если $|G| < \infty$, то $|G| = |G : H| \cdot |H|$.* □

Подгруппа $H \subset G$ называется *нормальной*, если $\forall g \in G \ \ gH = Hg$ ($\Leftrightarrow gHg^{-1} = H$). Обозначение: $H \lhd G$.

**Примеры.**

1. $S_{n-1} \not\lhd S_n$ при $n \geqslant 3$.

2. Если $G$ абелева, то всякая ее подгруппа нормальна.

**Теорема 3.3.** *Отношение сравнимости по модулю подгруппы $H$ согласовано с операцией в $G$ тогда и только тогда. когда $H$ нормальна.*

*Доказательство.* Пусть $H \triangleleft G$, $g_1 \equiv g_1' \pmod H$, $g_2 \equiv g_2' \pmod H$. Тогда $g_1' = g_1 h_1$, $g_2' = g_2 h_2$ (где $h_1, h_2 \in H$) $\Rightarrow g_1' g_2' = g_1(h_1 g_2)h_2 = g_1(g_2 h_1')h_2 = (g_1 g_2)(h_1' h_2) \equiv g_1 g_2 \pmod H$.

Обратно, пусть отношение сравнимости согласовано с операцией. Тогда $\forall g \in G$, $h \in H \quad ghg^{-1} \equiv geg^{-1} \equiv e \pmod H \Rightarrow ghg^{-1} \in H$, т.е. $gHg^{-1} \subset H$. Аналогично, $g^{-1}Hg \subset H$. Но тогда $H \subset gHg^{-1} \Rightarrow gHg^{-1} = H$. □

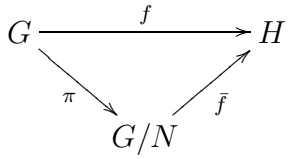
**Теорема 3.4.** *Всякое отношение эквивалентности в $G$, согласованное с операцией, есть отношение сравнимости по модулю некоторой подгруппы.*

*Доказательство.* Рассмотрим $H = [e] = \{h \in G : e \sim h\}$. Докажем, что $H$ — подгруппа: $h_1, h_2 \sim e \Rightarrow h_1 h_2 \sim e$; $h \sim e \Rightarrow e = hh^{-1} \sim eh^{-1} = h^{-1}$; $e \sim e$. Тогда $g_1 \sim g_2 \Leftrightarrow e \sim g_1^{-1} g_2 \Leftrightarrow g_1^{-1} g_2 \in H \Leftrightarrow g_1 \equiv g_2 \pmod H$. □

Т.о., если $N \triangleleft G$, то на множестве классов сравнимости по модулю $N$ определяется операция: $(g_1 N)(g_2 N) = (g_1 g_2)N$. Множество классов сопряженности обозначается $G/N$ и относительно такой операции оно является группой. Она называется *факторгруппой группы $G$ по $N$*.

Отображение факторизации $\pi\colon G \to G/N$, $g \mapsto gN$ является гомоморфизмом. Обратно, пусть $f\colon G \to H$ — гомоморфизм групп. Тогда соответствующее отношение эквивалентности $\mathcal{R}_f$ согласовано с операцией. Значит, это отношение сравнимости по модулю нормальной подгруппы $N = \{g \in G : f(g) = e\}$. Эта подгруппа называется *ядром* и обозначается как $N = \ker f$.

Имеет место следующая диаграмма:




**Теорема 3.5.** *Если $f\colon G \to H$ — гомоморфизм групп, то $\bar f\colon G/N \to H$ — гомоморфизм. Если $f$ сюръективен, то $\bar f$ — изоморфизм.* □

**Замечание.** В общем случае $G/\ker f \simeq \operatorname{Im} f$.

**Примеры.**

1. $\operatorname{sgn}\colon S_n \to \{\pm 1\}$. $\ker \operatorname{sgn} = A_n$. Т.о., $S_n/A_n \simeq \{\pm 1\}$.
2. $\det\colon \mathrm{GL}_n(K) \to K^*$. $\ker \det = \mathrm{SL}_n(K)$. Т.о., $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \simeq K^*$.
3. $f\colon \mathbb{C}^* \to \mathbb{C}^*$, $z \mapsto z^n$. $\ker f = C_n \Rightarrow \mathbb{C}^*/C_n \simeq \mathbb{C}^*$.
4. $f\colon \mathbb{C}^* \to \mathbb{R}_+^*$, $z \mapsto |z|$. $\ker f = \mathbb{T} \Rightarrow \mathbb{C}^*/\mathbb{T} \simeq \mathbb{R}_+^*$.
5. $\exp\colon \mathbb{R} \to \mathbb{R}^*$, $x \mapsto e^x$. $\ker \exp = \{0\}$, $\operatorname{Im} \exp = \mathbb{R}_+^* \Rightarrow \mathbb{R} \simeq \mathbb{R}_+^*$.
   $\exp\colon \mathbb{C} \to \mathbb{C}^*$, $z \mapsto e^z$. $\ker \exp = 2\pi i\mathbb{Z}$, $\operatorname{Im} \exp = \mathbb{C}^* \Rightarrow \mathbb{C}/2\pi i\mathbb{Z} \simeq \mathbb{C}^*$ (также $\mathbb{C}/\mathbb{Z} \simeq \mathbb{C}^*$).
6. Линейное отображение $f\colon K^n \to K^m$, $(x_1, \ldots, x_n) \mapsto (y_1, \ldots, y_n)$, $y_i = \sum\limits_{j=1}^{n} a_{ij}x_j$, $i = 1, \ldots, m$. $\ker f$ — множество решений системы однородных линейных уравнений $\sum\limits_{j=1}^{n} a_{ij}x_j = 0$. $b = (b_1, \ldots, b_m) \in K \Rightarrow f^{-1}(b)$ либо пуст, либо класс сопряженности $\pmod{\ker f}$, т.е. $f^{-1}(b) = x_0 + \ker f$. С другой стороны, $f^{-1}(b)$ есть множество решений системы $\sum\limits_{j=1}^{n} a_{ij}x_j = b_i$ $(i = 1, \ldots, m)$.
7. $f\colon S_4 \to S_3$. $y_1 = x_1x_2 + x_3x_4$, $y_2 = x_1x_3 + x_2x_4$, $y_3 = x_1x_4 + +x_2x_3$. $\ker f = \{e, (12)(34), (13)(24), (14)(23)\} = V_4$ (*четверная группа Клейна*) $\Rightarrow S_4/V_4 \simeq S_3$.

Лекция 3.

## 4. Прямые произведения групп.

Говорят, что группа $G$ *разлагается в прямое произведение своих подгрупп* $G_1, \ldots, G_k$, если

1) каждый элемент $g \in G$ единственным образом представляется в виде $g = g_1 \ldots g_k$, где $g_i \in G_i$,

2) при $i \neq j$ $g_ig_j = g_jg_i$ $\forall g_i \in G_i, g_j \in G_j$.

Правило умножения: $(g_1 \dots g_k)(g'_1 \dots g'_k) = (g_1 g'_1) \dots (g_k g'_k)$.
Обозначение: $G = G_1 \times \dots \times G_k$.

**Свойства.**

1. $G_i \cap G_j = \{e\}$ при $i \neq j$: $g \in G_i \cap G_j \Rightarrow g = e \dots \overset{i}{g} \dots e = e \dots \overset{j}{g} \dots e \Rightarrow g = e$.

2. $G_i \lhd G$: $h \in G_i$, $g_1, \dots, g_k \in G$, $g = g_1 \dots g_k \Rightarrow$

$$ghg^{-1} = (g_1 e g_1^{-1}) \dots (g_i h g_i^{-1}) \dots (g_k e g_k^{-1}) = g_i h g_i^{-1} \in G_i.$$

**Лемма 4.1.** *Если* $G', G'' \in G$, $G', G'' \lhd G$ *и* $G' \cap G'' = \{e\}$, *то* $g'g'' = g''g' \ \ \forall g' \in G', g'' \in G''$.

*Доказательство.* $g'g''g'^{-1}g''^{-1} \in G' \cap G'' = \{e\} \Rightarrow g'g''g'^{-1}g''^{-1} = e$. □

**Теорема 4.1.** *Пусть* $G_1, G_2 \lhd G$, $G_1 \cap G_2 = \{e\}$, $G_1 G_2 = G$. *Тогда* $G = G_1 \times G_2$.

*Доказательство.* 1) Любой элемент $g \in G$ представляется в виде $g = g_1 g_2$ (где $g_1 \in G_1, g_2 \in G_2$) по условию теоремы. Докажем, что такое представление единственно. $g = g_1 g_2 = g'_1 g'_2 \Rightarrow G_1 \ni g_1'^{-1} g_1 = g'_2 g_2^{-1} \in G_2 \Rightarrow g_1'^{-1} g_1 = g'_2 g_2^{-1} = e \Rightarrow g_1 = g'_1$, $g_2 = g'_2$.
2) $\forall g_1 \in G_1, g_2 \in G_2 \ \ g_1 g_2 = g_2 g_1$ по лемме 4.1. □

**Примеры.**

1. Разложение векторного пространства в прямую сумму подпространств: $V = V_1 \oplus \dots \oplus V_k$ есть разложение аддитивной группы в прямую сумму подгрупп.

2. $\mathbb{C}^* = \mathbb{R}_+^* \times \mathbb{T}$, т.е. $z = r(\cos\varphi + i \sin\varphi)$.

3. $\mathrm{GL}_n^+(\mathbb{R})$ — группа вещественных матриц с положительным определителем; $\mathrm{GL}_n^+(\mathbb{R}) = \mathrm{SL}_n(\mathbb{R}) \times \{\lambda E\}$, где $\lambda \in \mathbb{R}_+$.

Пусть $G_1, \dots, G_k$ — произвольные группы. *Внешним произведением групп* $G_1, \dots, G_k$ называется прямое произведение множеств $G_1, \dots, G_k$ с операцией умножения $(g_1, \dots, g_k)(g'_1, \dots, g'_k) = (g_1 g'_1, \dots, g_k g'_k)$. Это также группа, обозначаемая $G_1 \times \dots \times G_k$. Если группа $G$ разлагается в прямое произведение подгрупп $G_1, \dots, G_k$, то $G \simeq G_1 \times \dots \times G_k$ (внешнее прямое произведение): $g = g_1 \cdot \dots \cdot g_k \leftrightarrow (g_1, \dots, g_k)$.

**Примеры.**

1. $K^* \times \ldots \times K^* = (K^*)^n$ изоморфна группе невырожденных диагональных матриц порядка $n$.

## 5. Абелевы группы[1].

Пусть $A$ — абелева группа. $\forall a \in A$, $\forall k \in \mathbb{Z}$ определен элемент $ka \in A$.

**Свойства.**

1. $k(a+b) = ka + kb$,
2. $(k+l)a = ka + la$,
3. $(kl)a = k(la)$,
4. $1 \cdot a = a$.

*Линейная комбинация* элементов $a_1, \ldots, a_n \in A$ есть элемент $k_1a_1 + \ldots + k_na_n$ $(k_1, \ldots, k_n \in \mathbb{Z})$. Совокупность всех линейных комбинаций элементов $a_1, \ldots, a_n$ есть наименьшая подгруппа, содержащая $a_1, \ldots, a_n$. Она называется подгруппой, *порожденной* $a_1, \ldots, a_n$ и обозначается как $\langle a_1, \ldots, a_n \rangle$. Если $\langle a_1, \ldots, a_n \rangle = A$, то говорят, что группа $A$ *порождается* элементами $a_1, \ldots, a_n$. Группа, порожденная конечным числом элементов, называется *конечно-порожденной*. В частности, группа, порожденная одним элементом, — это циклическая группа.

Элементы $a_1, \ldots, a_n$ называются *линейно зависимыми*, если существуют числа $k_1, \ldots, k_n \in \mathbb{Z}$, не все равные 0, такие, что $k_1a_1 + \ldots + k_na_n = 0$. В противном случае $a_1, \ldots, a_n$ называются *линейно независимыми*. Линейно независимая система элементов, порождающих группу $A$, называется *базисом группы* $A$. Не всякая конечно порожденная абелева группа обладает базисом, например, группа $\mathbb{Z}_m$ не обладает базисом.

Конечно порожденная абелева группа, обладающая базисом, называется *свободной*. Если $\{e_1, \ldots, e_n\}$ — базис группы $A$, то

$$A = \langle e_1 \rangle \oplus \ldots \oplus \langle e_n \rangle \simeq \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} = \mathbb{Z}^n.$$

[1] В этой теме все рассматриваемые подгруппы считаются аддитивными, если не оговорено противное.

**Теорема 5.1.** *Все базисы свободной абелевой группы равномощны.*

*Доказательство.* Пусть $\{e_1, \ldots, e_n\}$ и $\{e'_1, \ldots, e'_m\}$ — два базиса. Предположим, что $m > n$. Имеем $(e'_1, \ldots, e'_m) = (e_1, \ldots, e_n) \underset{n\times m}{C}$. Можно рассматривать $C$ как матрицу над $\mathbb{Q}$. Т.к. $m > n$, то столбцы линейно зависимы над $\mathbb{Q}$, а значит, и над $\mathbb{Z}$. Но тогда $e'_1, \ldots, e'_m$ линейно зависимы в $A$ — противоречие. □

Число элементов базиса свободной абелевой группы называется ее *рангом* и обозначается $\operatorname{rk} A$.

Опишем все базисы свободной абелевой группы. Пусть $\{e_1, \ldots, e_n\}$ — базис и $(e'_1, \ldots, e'_n) = (e_1, \ldots, e_n)C$.

**Теорема 5.2.** $\{e'_1, \ldots, e'_n\}$ — *базис* $\Leftrightarrow \det C = \pm 1$.

*Доказательство.* 1) Пусть $\det C = \pm 1$. Тогда $C^{-1}$ целочисленна и $(e_1, \ldots$ $\ldots, e_n) = (e'_1, \ldots, e'_n)C^{-1} \Rightarrow e'_1, \ldots, e'_n$ порождают $A$. Т.к. столбцы матрицы $C$ линейно независимы, то $\{e'_1, \ldots, e'_n\}$ линейно независимы.

2) Пусть $\{e'_1, \ldots, e'_n\}$ — базис. Тогда $(e_1, \ldots, e_n) = (e'_1, \ldots, e'_n)D$, где $D$ — целочисленная матрица $\Rightarrow (e_1, \ldots, e_n) = (e_1, \ldots, e_n)CD \Rightarrow CD = E$ $\Rightarrow \det C \cdot \det D = 1 \Rightarrow \det C = \pm 1$. □

## Лекция 4.

**Теорема 5.3.** *Всякая подгруппа $N$ свободной абелевой группы $L$ ранга $n$ есть свободная абелева группа ранга не больше $n$.*

*Доказательство.* Индукция по $n$.

$n = 1 \Rightarrow L \simeq \mathbb{Z}$. Будем считать, что $L = \mathbb{Z}$. Если $N = \{0\}$, то $N$ — свободная абелева группа ранга 0. Если $N \neq \{0\}$, то $N$ содержит положительные числа, и $k$ — наименьшее из них. Докажем, что $N = k\mathbb{Z}$. Пусть $m \in N$, тогда $m = qk + r$, $0 \leqslant r < k$. Тогда $r = m - qk \in N \Rightarrow$ $r = 0$.

Пусть теперь $\{e_1, \ldots, e_n\}$ — базис $L$ и $L_1 = \langle e_1, \ldots, e_{n-1}\rangle$. Тогда $L_1$ — это свободная абелева группа ранга $n - 1$. Рассмотрим группу $N_1 = N \cap$ $\cap L_1 \subset L_1$. По предположению индукции $N_1$ — свободная абелева группа ранга $m \leqslant n - 1$. Пусть $\{f_1, \ldots, f_m\}$ — базис $N_1$. Если $N = N_1$, то все

доказано. Если $N \neq N_1$, то рассмотрим последние координаты всех элементов из $N$ в базисе $\{e_1, \ldots, e_n\}$ группы $L$. Они образуют ненулевую подгруппу в группе $\mathbb{Z}$. Значит, она имеет вид $k\mathbb{Z}$. Пусть $f_{m+1} \in N$ имеет последнюю координату $k$. Тогда $\{f_1, \ldots, f_m, f_{m+1}\}$ — базис $N$. $\square$

**Замечание.** $\operatorname{rk} N = n \not\Rightarrow N = L$. Например, $k\mathbb{Z} \subsetneqq \mathbb{Z}$ при $k > 1$ и $\operatorname{rk} k\mathbb{Z} = \operatorname{rk} \mathbb{Z} = 1$.

Пусть $\mathbb{E}^n$ — $n$-мерное евклидово векторное пространство, $\{e_1, \ldots, e_n\}$ — его базис. Тогда $L = \left\{ \sum\limits_{i=1}^{n} k_i e_i : k_i \in \mathbb{Z} \right\}$ — свободная абелева группа ранга $n$ с базисом $\{e_1, \ldots, e_n\}$. Такие подгруппы называются *решетками в* $\mathbb{E}^n$.

Подмножество $A \subset \mathbb{E}^n$ *дискретно*, если в любом ограниченном подмножестве $K \subset \mathbb{E}^n$ имеется лишь конечное число точек из $A$ (по-другому: у $A$ нет предельных точек). Очевидно, что всякая решетка является дискретным подмножеством.

**Теорема 5.4.** *Всякая дискретная подгруппа $L$ в $\mathbb{E}^n$, порождающая $\mathbb{E}^n$ как векторное пространство, является решеткой.*

*Доказательство.* Существует базис $\{e_1, \ldots, e_n\}$ пространства $\mathbb{E}^n$, содержащийся в $L$. Пусть $L_0$ — решетка, порожденная этим базисом. Ясно, что $L_0 \subset L$.

Докажем, что $L_0$ — подгруппа конечного индекса в $L$. Рассмотрим параллелепипед $P = \left\{ \sum\limits_{i=1}^{n} x_i e_i : 0 \leqslant x_i \leqslant 1 \right\}$. Тогда $\forall x \in L \;\; \exists\, k_1, \ldots, k_n \in \in \mathbb{Z} : x - (k_1 e_1 + \ldots + k_n e_n) \in P$. Это означает, что каждый смежный класс $L$ по $L_0$ содержит элемент из $P$. По условию дискретности $L \cap P$ конечно, а значит, $|L : L_0| = d < \infty$.

$|L/L_0| = d \Rightarrow dL \subset L_0$. Т.о., $L_0 \subset L \subset d^{-1}L_0$. $d^{-1}L_0$ есть свободная абелева группа ранга $n$ с базисом $\{d^{-1}e_1, \ldots, d^{-1}e_n\}$. По теореме 5.3 $L$ — свободная абелева группа ранга $n$. Всякий базис группы $L$ содержит $n$ элементов и порождает $\mathbb{E}^n$, а значит, является базисом $\mathbb{E}^n$. $\square$

*Кристаллической структурой в* $\mathbb{E}^3$ называется конечный набор дискретных подмножеств $A_1, \ldots, A_k \subset \mathbb{E}^3$ со следующим свойством: существует такой базис $\{e_1, e_2, e_3\}$ пространства $\mathbb{E}^3$, то $A_i + e_j = A_i$, $i = = 1, \ldots, k$, $j = 1, 2, 3$. Рассмотрим группу $L = \{a \in \mathbb{E}^3 : t_a A_i = A_i, i = = 1, \ldots, k\}$. По теореме 5.4 это решетка.

Группа симметрий кристаллической структуры $A = \{A_1, \ldots, A_k\}$ — это группа $\Gamma = \operatorname{Sym} A = \{g \in \operatorname{Isom} \mathbb{E}^3 : gA_i = A_i, i = 1, \ldots, k\}$. Такие группы называются *кристаллографическими*.

*Группа симметрий направлений в кристаллической структуре* — это группа $G = d\Gamma = \{dg : g \in \Gamma\} \subset \mathrm{O}_3$.

**Теорема 5.5.** *Группа $G$ конечна и может содержать повороты или зеркальные повороты только на углы $0, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}, \pi$.*

*Доказательство.* Пусть $L = \{a \in \mathbb{E}^3 : t_a \in \Gamma\}$ — решетка и $\{e_1, e_2, e_3\}$ — базис этой решетки. Тогда $\forall a \in \mathbb{E}^n$, $\forall \gamma \in \operatorname{Isom} \mathbb{E}^n \quad \gamma t_a \gamma^{-1} = t_{d\gamma(a)} \Rightarrow d\gamma(a) \in \Gamma$. Т.о., $\forall g \in G \quad gL = L$, т.е. в базисе $\{e_1, e_2, e_3\}$ $g$ записывается целочисленной матрицей. Значит, $G$ — дискретное подмножество в пространстве всех матриц. Но $G \subset \mathrm{O}_3$ — ограниченное подмножество (в ортонормированном базисе все матричные элементы по модулю не больше 1). Значит, $|G| < \infty$. Далее, $\forall g \in G \quad \operatorname{tr} g \in \mathbb{Z}$. Но в некотором ортонормированном базисе $g$ записывается матрицей $\begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & \pm 1 \end{pmatrix} \Rightarrow$ $\operatorname{tr} g = 2\cos\varphi \pm 1 \Rightarrow 2\cos\varphi \in \mathbb{Z} \Rightarrow |\cos\varphi| = \{\frac{1}{2}, 1\}$. □

## Лекция 5.

*Элементарные преобразования базисов*:
1) $e_i' = e_i + ce_j$ $(c \in \mathbb{Z})$, $e_k' = e_k$ при $k \neq i$,
2) $e_i' = e_j$, $e_j' = e_i$, $e_k' = e_k$ при $k \neq i, j$,
3) $e_i' = -e_i$, $e_k' = e_k$ при $k \neq i$.

Прямоугольная матрица $C = (c_{ij})$ размера $m \times n$ называется *диагональной*, если $c_{ij} = 0$ при $i \neq j$. Обозначение: $C = \operatorname{diag}(c_{11}, \ldots, c_{pp})$, $p = \min\{m, n\}$.

**Лемма 5.1.** *Всякую целочисленную матрицу $C$ размера $m \times n$ с помощью целочисленных элементарных преобразований строк и столбцов можно привести к виду* $\operatorname{diag}(u_1, \ldots, u_p)$ *($p = \min\{m, n\}$), где $u_i \in \mathbb{Z}$, $u_i \geqslant 0$ и $u_i \mid u_{i+1}$ при $i = 1, \ldots, p-1$.*

*Доказательство.* Если $C = 0$, то доказывать нечего. Если $C \neq 0$, то путем элементарных преобразований строк и столбцов можно добиться, чтобы $c_{11} > 0$. Далее будем минимизировать $c_{11}$.

Если $c_{i1}$ не делится на $c_{11}$, то разделим с остатком: $c_{i1} = qc_{11} + r$, $0 < r < c_{11}$ и, вычитая из $i$-й строки 1-ю, умноженную на $q$, получим $r$ на месте $i, 1$. Переставив 1-ю и $i$-ю строки, получим $r$ на месте $(1, 1)$.

Аналогично, если $c_{1j}$ не делится на $c_{11}$, то с помощью целочисленных элементарных преобразований столбцов можно также уменьшить $c_{11}$.

Пусть все элементы 1-й строки и 1-го столбца делятся на $c_{11}$. Тогда с помощью целочисленных элементарных преобразований строк и столбцов их можно сделать нулями, т.е. привести $C$ к виду

$$\begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix}$$

Предположим теперь, что $c_{ij}$ $(i, j \geqslant 2)$ не делится на $c_{11}$. Прибавив к 1-й строке $i$-ю строку, мы не изменим $c_{11}$, но получим, что $c_{1j}$ не делится на $c_{11}$ и придем к рассмотренной ранее ситуации.

В конце концов

$$C = \begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{p2} & \cdots & c_{pp} \end{pmatrix}$$

где всякий элемент матрицы

$$C_1 = \begin{pmatrix} c_{22} & \cdots & c_{2p} \\ \vdots & \ddots & \vdots \\ c_{p2} & \cdots & c_{pp} \end{pmatrix}$$

делится на $c_{11} = u_1$. Далее, делая то же самое с матрицей $C_1$, свойство делимости на $u_1$ сохранится, и мы приведем матрицу $C$ к требуемому виду. □

**Теорема 5.6.** *Для всякой подгруппы $N$ свободной абелевой группы $L$ существует такой базис $\{e_1, \ldots, e_n\}$ группы $L$ и такие натуральные числа $u_1, \ldots, u_m$ $(m \leqslant n)$, что $\{u_1e_1, \ldots, u_me_m\}$ — базис $N$ и $u_i \mid u_{i+1}$ при $i = 1, \ldots, m-1$.*

*Доказательство.* Пусть $\{e_1, \ldots, e_n\}$ — произвольный базис группы $L$ и $\{f_1, \ldots, f_m\}$ — базис $N$. Тогда $(f_1, \ldots, f_m) = (e_1, \ldots, e_n) \underset{n\times m}{C}$ ($C$ — целочисленная матрица). При элементарных преобразованиях базиса группы $L$ $(e'_1, \ldots, e'_n) = (e_1, \ldots, e_n)U$ ($U$ — элементарная матрица) $\Rightarrow (f_1, \ldots, f_m) = = (e'_1, \ldots, e'_n)U^{-1}C$, т.е. в $C$ происходят целочисленные элементарные преобразования строк.

При элементарных преобразованиях базиса подгруппы $N$ получаем: $(f'_1, \ldots, f'_m) = (f_1, \ldots, f_m)V \Rightarrow (f'_1, \ldots, f'_m) = (e_1, \ldots, e_n)CV$, т.е. в $C$ происходят целочисленные элементарные преобразования столбцов.

По лемме 5.1 матрицу $C$ можно таким образом привести к виду $C = = \operatorname{diag}(u_1, \ldots, u_m)$. Т.к. $\operatorname{rk} C = m$, то $u_i \neq 0$ и $f_i = u_1 e_i$, $i = 1, \ldots, m$. □

**Теорема 5.7.** *Всякая конечно порожденная абелева группа $A$ разлагается в прямую сумму циклических групп.*

*Доказательство.* Пусть $A = \langle a_1, \ldots, a_n \rangle$. Рассмотрим гомоморфизм

$$\varphi\colon \mathbb{Z}^n \overset{\text{на}}{\to} A, \quad (k_1, \ldots, k_n) \mapsto k_1 a_1 + \ldots + a_n e_n.$$

Пусть $N = \ker \varphi$, тогда $A \simeq \mathbb{Z}^n/N$. По теореме 5.6 существуют базис $\{e_1, \ldots, e_n\}$ группы $\mathbb{Z}^n$ и натуральные числа $u_1, \ldots, u_m$ ($m \leqslant n$), такие, что $\{u_1 e_1, \ldots, u_m e_m\}$ — базис $N$ и $u_i \mid u_{i+1}$ при $i = 1, \ldots, m-1$.

Рассмотрим гомоморфизм

$$\psi\colon \mathbb{Z}^n \overset{\text{на}}{\to} \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m} \oplus \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n-m},$$

$$l_1 e_1 + \ldots + l_n e_n \mapsto ([l_1]_{u_1}, \ldots, [l_m]_{u_m}, l_{m+1}, \ldots, l_n).$$

$\ker \psi = \langle u_1 e_1, \ldots, u_m e_m \rangle = N$. Следовательно,

$$A \simeq \mathbb{Z}^n/N \simeq \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m} \oplus \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n-m}.$$

□

**Замечание.** 1) На самом деле мы доказали, что $A$ разлагается в прямую сумму циклических групп порядков $u_1, \ldots, u_m, \infty$, где $u_i \mid u_{i+1}$.

2) Если $A$ конечна, то слагаемых $\mathbb{Z}$ нет.

**Лемма 5.2.** *Если $n = kl$, $(k, l) = 1$, то $\mathbb{Z}_n \simeq \mathbb{Z}_k \oplus \mathbb{Z}_l$.*

*Доказательство.* Нужно доказать, что группа $\mathbb{Z}_k \oplus \mathbb{Z}_l$ циклическая, т.е. что в ней есть элемент порядка $n$. Таким элементом является $([1]_k, [1]_l)$. В самом деле, $m([1]_k, [1]_l) = ([m]_k, [m]_l) = 0 \Leftrightarrow k, l \mid m \Leftrightarrow n \mid m$. Следовательно, $\operatorname{ord}([1]_k, [1]_l) = n$. □

**Теорема 5.8.** *Если $n = p_1^{k_1} \dots p_s^{k_s}$ ($p_1, \dots, p_s$ — различные простые числа), то $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}}$.*

*Доказательство.* По лемме 5.2

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2} \dots p_s^{k_s}} \simeq \dots \simeq \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}}.$$

□

**Примеры.**

1. $\mathbb{Z}_{60} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 = \langle [15] \rangle \oplus \langle [20] \rangle \oplus \langle [12] \rangle$. Например, $[1] = -[15] - -[20] + 3 \cdot [12]$.

Группа называется *примарной*, если ее порядок есть степень простого числа.

**Теорема 5.9.** *Всякая конечно порожденная абелева группа $A$ разлагается в прямую сумму примарных и бесконечных циклических групп, причем число слагаемых и набор порядков определены однозначно.*

*Доказательство.* 1) Существование такого разложения следует из теорем 5.2 и 5.3.

2) Покажем единственность числа слагаемых и наборов их порядков. Пусть $A = \langle a_1 \rangle_{p_1^{k_1}} \oplus \dots \oplus \langle a_s \rangle_{p_s^{k_s}} \oplus \langle a_{s+1} \rangle_\infty \oplus \dots \oplus \langle a_{s+t} \rangle_\infty$ (среди чисел $p_1, \dots, p_s$ могут быть одинаковые).

Рассмотрим *подгруппу кручения* $\operatorname{Tor} A = \{a \in A : \operatorname{ord} a < \infty\}$. Ясно, что $\operatorname{Tor} A = \langle a_1 \rangle_{p_1^{k_1}} \oplus \dots \oplus \langle a_s \rangle_{p_s^{k_s}}$ и $A/\operatorname{Tor} A \simeq \mathbb{Z}^t$. Т.к. определение $\operatorname{Tor} A$ не зависит от разложения, то и число $t$ не зависит от разложения.

Рассмотрим *подгруппу $p$-кручения* $\operatorname{Tor}_p A = \{a \in A : p^k a = 0\}$. Ясно, что $\operatorname{Tor} A$ — сумма тех $\langle a_i \rangle_{p_i^{k_i}}$, для которых $p_i = p$. Т.к. определение $\operatorname{Tor}_p A$ не зависит от разложения, то и $\bigoplus\limits_{p_i = p} \langle a_i \rangle_{p_i^{k_i}}$ не зависит от разложения.

Т.о., доказательство теоремы сводится к случаю, когда $A$ — примарная группа.

3) Случай примарной группы: $A = \langle a_1 \rangle_{p^{k_1}} \oplus \ldots \oplus \langle a_r \rangle_{p^{k_r}}$ $(k_1 \leqslant \ldots \leqslant k_r)$, $|A| = p^k$, $k = k_1 + \ldots + k_r$.

Докажем индукцией по $k$, что набор $(k_1, \ldots, k_r)$ определен однозначно. При $k = 1$ это очевидно. Предположим, что утверждение верно для групп порядка $p^l$, $l \leqslant k$. Пусть $k_1 = \ldots = k_s = 1$, $k_{s+1} > 1$.

Рассмотрим подгруппу $pA = \{pa : a \in A\}$. Ясно, что

$$pA = \langle pa_s \rangle_{p^{k_{s+1}-1}} \oplus \ldots \oplus \langle pa_r \rangle_{p^{k_r-1}}.$$

По предположению индукции (для $pA$) набор $(k_{s+1} - 1, \ldots, k_r - 1)$ определен однозначно. Значит, набор $(k_{s+1}, \ldots, k_r)$ определен однозначно.

Число $s$ определяется из равенства $s + k_{s+1} + \ldots + k_r = k$. □

## Лекция 6.

**Замечание.** Сами слагаемые разложения, о которых идет речь в теореме, вообще говоря. не определены однозначно. Например, $\langle a_1 \rangle_2 \oplus \langle a_2 \rangle_2 = \langle a_1 + a_2 \rangle_2 \oplus \langle a_2 \rangle_2$. Вообще. если $G = \mathbb{Z}_p^r$, то $G$ можно рассматривать как $r$-мерное векторное пространство над $\mathbb{Z}_p$, и разложение $G$ в прямую сумму циклических подгрупп — это разложение векторного пространства в сумму одномерных подпространств.

*Экспонентой* конечной группы $G$ называется н.о.к. порядков всех своих элементов. Обозначение: $e(G)$. Ясно, что $e(G) \mid |G|$ и что $g^{e(G)} = e \ \ \forall g \in G$.

Вообще говоря, элемента порядка $e(G)$ не существут: $e(S_3) = 6$, но элементов порядка 6 в $S_3$ нет.

**Теорема 5.10.** *В любой конечной абелевой группе $A$ существует элемент порядка $e(A)$.*

*Доказательство.* $A = \langle a_1 \rangle_{u_1} \oplus \ldots \langle a_m \rangle_{u_m} \oplus$, где $u_i \mid u_{i+1}$ $(i = 1, \ldots, m-1)$. $e(A) = u_m = \operatorname{ord} a_m$. □

**Теорема 5.11.** *Мультипликативная группа $F^*$ любого конечного поля $F$ циклическая.*

*Доказательство.* $|F| = q \Rightarrow |F^*| = q - 1$. Докажем, что $e(F^*) = q - 1$. $\forall x \in F^* \;\; x^{e(F^*)} - 1 = 0 \Rightarrow q - 1 \leqslant e(F^*) \Rightarrow e(F^*) = q - 1$. По теореме 5.10 $\exists\, a \in F^* : \operatorname{ord} a = q - 1 \Rightarrow F^* = \langle a \rangle$. □

Пусть $p$ — нечетное простое число. $\mathbb{Z}_p^* = \langle a \rangle_{p-1}$.

Элемент $c \in \mathbb{Z}_p^*$ называется *квадратичным вычетом*, если он является квадратом в $\mathbb{Z}_p^*$. $c = a^k$ — квадратичный вычет $\Leftrightarrow$ $k$ четно.

**Примеры.**

1. $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, $1, 2, 4$ — квадратичные вычеты, $3, 5, 6$ — квадратичные невычеты.

**Теорема 5.12.** *Уравнение* $x^2 + 1$ *имеет корень в* $\mathbb{Z}_p^* \Leftrightarrow p \equiv 1 \pmod 4$.

*Доказательство.* $-1$ — единственный элемент порядка 2 в $\mathbb{Z}_p^*$. Если $\mathbb{Z}_p^* = \langle a \rangle$, то $-1 = a^{\frac{p-1}{2}} \Rightarrow -1$ — квадратичный вычет $\Leftrightarrow \frac{p-1}{2}$ четно. □

## 6. Действия групп.

Пусть $S(X)$ — группа всех преобразований множества $X$. *Действием группы $G$ на множестве $X$* называется всякий гомоморфизм $\alpha\colon G \to S(X)$: $\alpha(gh) = \alpha(g)\alpha(h) \Rightarrow \alpha(e) = \mathrm{id}$, $\alpha(g^{-1}) = \alpha(g)^{-1}$. Обозначения: $G \overset{\alpha}{:} X$, $\alpha(g)x = gx$; условие гомоморфизма: $(gh)x = g(hx)$. $\ker\alpha \triangleleft G$ — *ядро неэффективности действия* $\alpha$. Если $\ker\alpha = \{e\}$, то действие *эффективно*.

$\operatorname{Im}\alpha$ — группа преобразований множества $X$. По теореме о гомоморфизме $\operatorname{Im}\alpha \simeq G/\ker\alpha$.

Если $G : X$, то $G$ действуют

1) на любом инвариантном подмножестве $Y \subset X$,

2) на множестве всех подмножеств множества $X$.

**Примеры.**

1. $\operatorname{Isom}\mathbb{E}^2 : \mathbb{E}^2 \Rightarrow \operatorname{Isom}\mathbb{E}^2$ действует на множестве треугольников.

Если $G : X$ и $H \subset G$ — подгруппа, то $H : X$.

Действие $G : X$ определяет отношение эквивалентности: $x \underset{G}{\sim} y$, если $\exists\, g \in G : y = gx$. Классы эквивалентности называются *орбитами* данного действия. Класс эквивалентности $x$ обозначается как $Gx = \{gx :$

$g \in G\}$. Действия с одной орбитой называются *транзитивными*. Число точек в орбите называется ее *длиной* и обозначается $|Gx|$.

*Стабилизатор элемента* $x$ — это $G_x = \{g \in G : gx = x\}$.

**Теорема 6.1.** *Пусть* $G : X$. *Тогда* $G_{gx} = gG_xg^{-1}$.

*Доказательство.* $h \in G_x \Rightarrow (ghg^{-1})(gx) = g(hx) = gx \Rightarrow ghg^{-1} \in G_{gx}$.
$h \in G_{gx} \Rightarrow (g^{-1}hg)x = g^{-1}(gx) = x \Rightarrow g^{-1}hg \in G_x$. □

**Примеры.**

1. $\mathrm{SO}_2 : \mathbb{E}^2$, $G_o = \mathrm{SO}_2$, $G_p = \{e\}$, $p \neq o$.
2. $\mathrm{GL}_n(\mathbb{C}) : \mathrm{GL}_n(\mathbb{C})$, $A \circ X = AXA^{-1}$. Ядро неэффективности есть $\{\lambda E : \lambda \in \mathbb{C}^*\}$. $A \sim B \Leftrightarrow A$ и $B$ имеют одну и ту же жорданову форму.
3. $\mathrm{GL}_n(\mathbb{C}) : L_n(\mathbb{C})$, $A \circ X = AXA^t$.
4. $S_4 : \{1,2,3,4\} \rightsquigarrow V_4 : \{1,2,3,4\}$. Действие $V_4 : \{1,2,3,4\}$ транзитивно, стабилизаторы тривиальны.

## Лекция 7.

**Теорема 6.2.** *Если группа* $G$ *конечна, то* $|Gx| = |G : G_x|$.

*Доказательство.* Рассмотрим отображение $G/G_x \to Gx$, $gG_x \mapsto gx$. Это определение корректно: $\forall h \in G_x \ \ (gh)x = g(hx) = gx$. Построенное отображение сюръективно по определению орбиты. Оно также инъективно: $g_1x = g_2x \Rightarrow (g_2g_1^{-1})x = x$, т.е. $g_2g_1^{-1} \in G_x \Rightarrow g_1G_x = g_2G_x$. □

Пусть $P$ — выпуклый многогранник. *Флагом* многогранника $P$ назовем тройку $\{v, e, f\}$, где $v$ — вершина, $e$ — ребро, содержащее $v$, $f$ — грань, содержащая $e$. $P$ — *правильный многогранник*, если $\mathrm{Sym}\, P$ действует транзитивно на множестве флагов.

Пусть $V$ — множество вершин многогранника $P$. Рассмотрим действие $\mathrm{Sym}\, P : V$. Это транзитивное действие. По теореме 6.2 $|\mathrm{Sym}\, P| = |V| \cdot |(\mathrm{Sym}\, P)_v|$.

Пусть $E_v$ — множество ребер, выходящих из $v$. Действие $(\operatorname{Sym} P)_v : E_v$ транзитивно $\Rightarrow$ по теореме 6.2 $|(\operatorname{Sym} P)_v| = |E_v| \cdot 2$.

Окончательно получаем, что

$$|\operatorname{Sym} P| = 2(\text{число вершин})(\text{степень вершины}).$$

Для куба $|\operatorname{Sym} P| = 48$, для икосаэдра $|\operatorname{Sym} P| = 120$.

$G \underset{l}{:} G$, $l(g)x = gx$ — действие группы на себе:

$$l(g_1g_2)x = g_1(g_2x) = l(g_1)l(g_2)x.$$

Это действие транзитивно. Стабилизатор тривиален.

Если $H \subset G$ — подгруппа, то орбитами $H$ будут правые смежные классы $Hx$.

Аналогично, $G \underset{r}{:} G$, $r(g)x = xg^{-1}$:

$$r(g_1g_2)x = x(g_1g_2)^{-1} = xg_2^{-1}g_1^{-1} = r(g_1)r(g_2)x.$$

Орбиты подгруппы — левые смежные классы $xH$.

$G \underset{a}{:} G$, $a(g)x = gxg^{-1}$:

$$a(g_1g_2)x = g_1g_2xg_2^{-1}g_1^{-1} = a(g_1)a(g_2)x.$$

$\forall x \in G \;\; a(g)$ — автоморфизм группы $G$:

$$a(g)(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = (a(g)x)(a(g)y).$$

Эквивалентные элементы называются *сопряженными*, т.е. $x$ и $y$ сопряжены, если $\exists\, g \in G : gxg^{-1} = y$. Орбиты — *классы сопряженности*. Обозначение: $C(x)$.

Стабилизатор элемента $x$ называется *централизатором элемента* $x$ и обозначается $Z(x)$. По определению, $Z(x) = \{g \in G : gx = xg\}$. Ядро неэффективности — *центр* $Z(G)$ *группы* $G$.

**Следствие 6.1.** *Если $G$ конечна, то* $|C(x)| = \frac{|G|}{|Z(x)|}$. $\square$

**Примеры.**

1. $G = S_n$. Пусть $\sigma = (i_1 \dots i_k)(j_1 \dots j_l) \dots$ — разложение на независимые циклы, $\tau \in S_n$. Если $\sigma(p) = q$, то $\tau\sigma\tau^{-1}(\tau(p)) = \tau(q)$. Следовательно, $\tau\sigma\tau^{-1} = (\tau(i_1) \dots \tau(i_k))(\tau(j_1) \dots \tau(j_l)) \dots$ Т.о., сопряженные подстановки характеризуются тем, что наборы длин независимых циклов в их разложениях совпадают.

   Рассмотрим $S_4$: $e$ —1, $(ij)$ — 6, $(ij)(kl)$ — 3, $(ijk)$ — 8, $(ijkl)$ — 6.

   Докажем, что $Z(S_n) = \{e\}$. Пусть $\tau \in Z(S_n) \Rightarrow$

   $$\tau(ij)\tau^{-1} = (\tau(i)\tau(j)) = (ij) \ \ \forall i, j,$$

   т.е. $\tau$ сохраняет любую пару $\{i, j\} \Rightarrow \tau = e$, т.к. любой элемент из $\{1, 2, \dots, n\}$ есть пересечение двух пар.

2. $G = \mathrm{GL}_n(\mathbb{C})$. $A$ и $B$ сопряжены тогда и только тогда. когда они имеют одну и ту же жорданову форму. $Z(\mathrm{GL}_n(\mathbb{C})) = \{\lambda E : \lambda \in \mathbb{C}^*\}$.

Рассмотрим действие группы $G$ на множестве своих подгрупп сопряжениями: $a(g)H = gHg^{-1}$. Эквивалентные подгруппы называются *сопряженными*, т.е. $H_1$ и $H_2$ сопряжены, если $\exists\, g \in G : gH_1g^{-1} = H_2$. Орбита называется *классом сопряженной подгруппы*. Стабилизатор подгруппы $H$ называется ее *нормализатором* и обозначается $N(H)$. Т.о., $N(H) = \{g \in G : gHg^{-1} = H\}$. Очевидно, что $H \lhd N(H)$.

**Теорема 6.3.** *Если $G$ конечна, то число подгрупп, сопряженных $H$, делит $|G : H|$.*

*Доказательство.* По теореме 6.2 это число равно

$$|G : N(H)| = \frac{|G|}{|N(H)|} = \frac{|G|}{|H|} : \frac{|N(H)|}{|H|}$$

и делит $\frac{|G|}{|H|} = |G : H|$. □

**Теорема 6.4.** *Центр примарной конечной группы нетривиален.*

*Доказательство.* Пусть $|G| = p^k$, $k \in \mathbb{N}$. Разложим $G$ на классы сопряженности, тогда $G = Z \sqcup C(x_1) \sqcup \dots \sqcup C(x_s)$. $\forall i = 1, \dots, s \ \ |C(x_i)| = p^l$, $l \in \mathbb{N} \Rightarrow p \mid |C(x_i)| \Rightarrow p \mid |Z| \Rightarrow Z \neq \{e\}$. □

**Следствие 6.2.** *Всякая группа порядка $p^2$ абелева.*

*Доказательство.* Пусть $|G| = p^2$, $Z = Z(G)$. Предположим, что $|Z| = p$. Тогда $|G : Z| = p$, и значит, $G/Z$ — циклическая группа. Пусть $aZ$ — ее порождающий элемент $\Rightarrow \forall g \in G \;\; gZ = (aZ)^k = a^k Z \Rightarrow g = a^k z$, $z \in Z$ $\Rightarrow G$ абелева — противоречие. □

## 7. Теоремы Силова.

Пусть $|G| = p^k m$, где $p$ простое, $p \nmid m$.

*Силовской $p$-подгруппой группы $G$* называется всякая подгруппа порядка $p^k$. Если $G$ абелева, то ее единственная силовская $p$-подгруппа есть подгруппа $p$-кручения $\mathrm{Tor}_p G$.

**Теорема 7.1.** *Силовские $p$-подгруппы существуют.*

**Теорема 7.2.** *Все силовские $p$-подгруппы сопряжены. Более того, всякая $p$-подгруппа содержится в некоторой силовской $p$-подгруппе.*

**Теорема 7.3.** *Число силовских $p$-подгрупп сравнимо с 1* $\pmod p$.

**Примеры.**

1. $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. Силовские 2-подгруппы: $V_4 \subset A_4 \subset A_5$ — 5; 3-подгруппы: $\langle (ijk) \rangle$ — 10; 5-подгруппы: $\langle (i_1 \dots i_5) \rangle$ — 6.

## Лекция 8.

*Доказательство теоремы 7.1.* Доказывать будем индукцией по $|G|$. Если $|G| = 1$, то утверждение тривиально.

Пусть $|G| = n > 1$ и для всех групп порядка меньше $n$ утверждение верно. $G = Z \sqcup C(x_1) \sqcup \dots \sqcup C(x_s)$, $|C(x_i)| > 1$. Рассмотрим два случая.

1) $\exists\, i : p \nmid |C(x_i)|$. $|C(x_i)| = \frac{|G|}{|Z(x_i)|} \Rightarrow p^k \mid |Z(x_i)|$. Но $|Z(x_i)| < n$, поэтому по предположению индукции существует силовская $p$-подгруппа в $Z(x_i)$. Она будет силовской $p$-подгруппой в $G$.

2) $\forall i \quad p \mid |C(x_i)|$. Тогда $p \mid |Z|$. Пусть $|Z| = p^{k_0} m_0$, где $0 < k_0 \leqslant k$ и $p \nmid m_0$, и пусть $Z_0 = \mathrm{Tor}_p Z$ (силовская $p$-подгруппа в $Z$). Имеем $|Z_0| = p^{k_0}$. Рассмотрим $G/Z_0$ и канонический гомоморфизм $\pi\colon G \to G/Z_0$. Имеем $|G/Z_0| = p^{k-k_0} m$. По предположению индукции в $G/Z_0$ существует силовская $p$-подгруппа $S_1$, $|S_1| = p^{k-k_0}$. Тогда $\pi^{-1}(S_1) = S$ имеет порядок $|S_1| \cdot |Z_0| = p^k$ и является силовской $p$-подгруппой в $G$. □

*Доказательство теоремы 7.2.* Пусть $S$ — какая-то силовская $p$- подгруппа и $H$ — какая-то $p$-подгруппа. Рассмотрим $H : G/S$, $h \circ gS = hgS$. Длина каждой нетривиальной орбиты делится на $p$ (т.к. она делит $|H| = p^l$). Но $|G/S| = |G : S|$ не делится на $p$. Значит, существуют неподвижные точки, т.е. $\exists\, g \in G : H \subset gSg^{-1}$. Т.о., $H$ содержится в силовской $p$-подгруппе $gSg^{-1}$. Если же $|H| = p^k$, то $H = gSg^{-1}$. □

*Доказательство теоремы 7.3.* Пусть $S$ — какая-то силовская $p$-подгруппа и $C(S)$ — множество всех подгрупп, сопряженных с $S$, т.е. по теореме множество всех силовских $p$-подгрупп. Рассмотрим действие $S : C(S)$ сопряжениями. Длина каждой нетривиальной орбиты делится на $p$. Найдем все тривиальные орбиты, т.е. неподвижные точки данного действия. Если $S_1 \in C(S)$ — неподвижная точка, то $S \subset N(S_1) = \{g \in G : gS_1g^{-1} = S_1\}$. Но тогда $S$ и $S_1$ — силовские $p$-подгруппы в $N(S_1)$ и по теореме они сопряжены в $N(S_1)$. Т.к. $S_1 \lhd N(S_1)$, то $S_1 = S$.

Итак, для действия $S : C(S)$ имеется единственная неподвижная точка, а именно сама подгруппа $S$. Следовательно, $|C(S)| \equiv 1 \pmod p$. □

**Примеры.**

1. $|G| = pq$, где $p > q$ — различные простые числа. Тогда число силовских $p$-подгрупп $N_p \equiv 1 \pmod p$ и $N_p \mid q \Rightarrow N_p = 1$, т.е. силовская $p$-подгруппа нормальна и единственна. Обозначим ее $G_p$. Тогда $|G_p| = p \Rightarrow G_p \simeq \mathbb{Z}_p$ и $G_p$ — циклическая. Далее, $N_q \equiv 1 \pmod q$ и $N_q \mid p$. Если $p \not\equiv 1 \pmod q$, то $N_q = 1$, т.е. силовская $q$-подгруппа $G_q$ также единственна и нормальна. Т.к. $G_p \cap G_q = \{e\}$, то $G_p \cdot G_q = G$ и, значит, $G = G_p \times G_q$, т.е. $G$ — циклическая.

2. $|G| = 45 = 3^2 \cdot 5$. $N_3 \equiv 1 \pmod 3$ и $N_3 \mid 5 \Rightarrow N_3 = 1$. $N_5 \equiv 1 \pmod q$ и $N_5 \mid 9 \Rightarrow N_5 = 1$. $G = G_3 \times G_5$. $G_5$ циклическая, $G_3$ абелева $\Rightarrow G$ абелева.

## 8. Полупрямые произведения групп.

Группа $G$ разлагается в *полупрямое произведение своих подгрупп* $N$ *и* $H$, если

1) $N \triangleleft G$,

2) $N \cap H = \{e\}$,

3) $NH = G$, т.е. $\forall g \in G \;\; g = nh$, где $n \in N$, $h \in H$.

Из этих условий следует, что представление $g = nh$ единственно: $g = n_1h_1 = n_2h_2 \Rightarrow N \ni n_2^{-1}n_1 = h_2h_1^{-1} \in H \Rightarrow n_1 = n_2$, $h_1 = h_2$. Обозначение: $G = N \leftthreetimes H = H \rightthreetimes N$.

**Примеры.**

1. $S_n = A_n \leftthreetimes \langle(12)\rangle$.

2. $S_4 = V_4 \leftthreetimes S_3$.

3. $D_n = C_n \leftthreetimes \langle r\rangle$, $r \in D_n$ — отражение.

4. $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \leftthreetimes \{\mathrm{diag}(1, \ldots, \lambda)\}$.

5. $\mathrm{GA}(S) = N \leftthreetimes \mathrm{GA}(S)_o$.

Правило умножения: $(n_1h_1)(n_2h_2) = (n_1(h_1n_2h_1^{-1}))(h_1h_2)$. В частности, отображение $G \to H$, $nh \mapsto h$, является гомоморфизмом, и по теореме о гомоморфизме $G/N \simeq H$.

Отображение $N \to N$, $n \mapsto hnh^{-1}$ является автоморфизмом группы $N$. Обозначим его через $\alpha(h)$. Отображение $\alpha\colon H \to \mathrm{Aut}\, N$ является гомоморфизмом. Оно определяет структуру полупрямого произведения. В частности, это произведение является прямым $\Leftrightarrow$ $\alpha$ тривиален: $\alpha = \mathrm{id} \;\; \forall h \in H$.

*Внешнее полупрямое произведение групп* $N$ *и* $H$ определяется гомоморфизмом $\alpha\colon H \to \mathrm{Aut}\, N$. Тогда $G = N \times H$, $(n_1, h_1)(n_2, h_2) = (n_1(\alpha(h_1)n_2), h_1h_2)$. Выполнены все аксиомы группы: $e = (e_N, e_H)$ и $(n, h)^{-1} = (\alpha(h^{-1})n^{-1}, h^{-1})$.

Опишем полупрямые произведения циклической группы. Для этого пишем группу автоморфизмов циклической группы.

**Теорема 8.1.** *Всякий автоморфизм циклической группы* $\langle a\rangle_n$ *имеет вид* $\varphi_k(x) = x^k$, *где* $(k, n) = 1$.

*Доказательство.* Пусть $\varphi \in \mathrm{Aut}\langle a\rangle_n$, $\varphi(a) = a^k$. Тогда $\forall x = a^m \;\; \varphi(x) = \varphi(a)^m = a^{km} = x^k$.

$\ker\varphi = \{a^m : n \mid km\}$. Если $(k,n) = 1$, то $\ker\varphi = \{e\}$. Если $(k,n) = d > 1$, то $\ker\varphi = \langle a^{\frac{n}{d}}\rangle \neq \{e\}$. Т.о., если $\varphi \in \mathrm{Aut}\langle a\rangle_n$, то $(k,n) = 1$.

Обратно, пусть $(k,n) = 1$ . Рассмотрим $\varphi_k\colon \langle a\rangle_n \to \langle a\rangle_n$, $\varphi_k(x) = x^k$. Это гомоморфизм: $(xy)^k = x^k y^k$ и $\ker\varphi_k = \{e\} \Rightarrow \mathrm{Im}\,\varphi_k = \langle a\rangle_n \Rightarrow \varphi_k \in \in \mathrm{Aut}\langle a\rangle_n$. □

**Следствие 8.1.** $\mathrm{Aut}\langle a\rangle_n \simeq \mathbb{Z}_n^*$.

*Доказательство.* Автоморфизмы нумеруются элементами этого кольца: $\mathbb{Z}_n^* \to \mathrm{Aut}\langle a\rangle_n$, $[k]_n \mapsto \varphi_k$. Это гомоморфизм: $\varphi_{kl} = \varphi_k\varphi_l$, и он биективен $\Rightarrow$ он изоморфизм. □

Т.о., полупрямое произведение $\langle a\rangle_n \leftthreetimes \langle b\rangle_m$ задается гомоморфизмом $\alpha\colon \langle b\rangle_m \to \mathrm{Aut}\langle a\rangle_n \simeq \mathbb{Z}_n^*$, определяющийся образом $b$: $\alpha(b) = [k]_n$, $k^m \equiv 1 \pmod n$.

## Лекция 9.

Таким образом, полупрямое произведение $\langle a\rangle_n \underset{k}{\leftthreetimes} \langle b\rangle_m$ определяется образом $\varphi_k \in \mathrm{Aut}\langle a\rangle_n$ элемента $b$. При этом должны выполняться следующие условия: $(k,n) = 1$ и $k^m \equiv 1 \pmod n$. Произведение будет прямым $\Leftrightarrow k \equiv 1 \pmod n$.

Отсюда получается следующая формула умножения: $(a^p b^s)(a^q b^t) = = a^p(b^s a^q b^{-s})(b^s b^t) = a^{p+k^s q} b^{s+t}$.

**Примеры.**

1. Группа диэдра $D_n = \langle a\rangle_n \leftthreetimes \langle b\rangle_2$. Поскольку $bab^{-1} = a^{-1}$, то $k = -1$ и $D_n = \langle a\rangle_n \underset{-1}{\leftthreetimes} \langle b\rangle_2$.

**Замечание.** Может быть так, что $\langle a\rangle_n \underset{k}{\leftthreetimes} \langle b\rangle_m \simeq \langle a\rangle_n \underset{k'}{\leftthreetimes} \langle b\rangle_m$ при $k \not\equiv k' \pmod n$ при другом выборе порождающего элемента группы $\langle b\rangle_m$. А именно, при замене $b$ на $b' = b^s$, где $(s,m) = 1$, $k$ заменяется на $k^s$.

Рассмотрим группу порядка $pq$, где $p > q$ — простые.

**Теорема 8.2.** *1) Если $p \not\equiv 1 \pmod q$, то всякая группа порядка $pq$ циклическая.*

*2) Если $p \equiv 1 \pmod q$, то существуют ровно две неизоморфные группы порядка $pq$: одна циклическая, другая неабелева.*

*Доказательство.* Пусть $G_p = \langle a\rangle_p$ — силовская $p$-подгруппа, $G_q = \langle b\rangle_q$ — силовская $q$-подгруппа. Тогда $G_p \lhd G$, $G_p \cap G_q = \{e\}$, $G_p \cdot G_q = G \Rightarrow G = \langle a\rangle_p \underset{k}{\rtimes} \langle b\rangle_q$, где $(k, p) = 1$ и $k^q \equiv 1 \pmod p$, т.е. $[k]^q = 1$ в $\mathbb{Z}_p^*$.

1) $p \not\equiv 1 \pmod q$. Тогда в $\mathrm{Aut}\langle a\rangle_p \simeq \mathbb{Z}_p^*$ (циклическая группа порядка $p-1$) нет элементов порядка $q \Rightarrow [k]_p = 1$, т.е. $G = \langle a\rangle_p \times \langle b\rangle_q \Rightarrow G$ циклическая.

2) $p \equiv 1 \pmod q$. Тогда в $\mathrm{Aut}\langle a\rangle_p \simeq \mathbb{Z}_p^*$ есть единственная циклическая подгруппа порядка $q$, скажем, $\langle \varphi_k\rangle_q$. Либо $[k]_p = 1$, и тогда $G$ циклическая, либо $[k]_p \neq 1$, и тогда для любого $[l]_p = [k]_p^s$ (где $(s, q) = 1$) заменяя $b$ на $b' = b^s$, перейдем от $k$ к $l$. В этом случае $G \simeq \langle a\rangle_p \underset{k}{\rtimes} \langle b\rangle_q \simeq$ $\simeq \langle a\rangle_p \underset{l}{\rtimes} \langle b'\rangle_q$. □

## 9. Разрешимые группы.

Пусть $G$ — группа. *Коммутатор элементов $x, y \in G$* — это элемент $(x; y) = xyx^{-1}y^{-1}$.

**Свойства.**

1. $(x; y) = e \Leftrightarrow xy = yx$,
2. $(y; x) = (x; y)^{-1}$.

*Коммутант группы $G$* — это подгруппа $G' = (G; G)$, порожденная всеми коммутаторами, т.е. совокупность всех произведений вида $(x_1; y_1) \cdot \ldots \cdot (x_n; y_n)$. $G$ абелева $\Leftrightarrow G' = \{e\}$.

Если $\varphi\colon G \to H$ — гомоморфизм группы $G$ на группу $H$, то $\varphi(G') = H'$.

**Теорема 9.1.** *Коммутант $G'$ группы $G$ — это наименьшая нормальная подгруппа, фактор по которой абелев.*

*Доказательство.* 1) Докажем, что $G' \triangleleft G$. Коммутант $G'$ инвариантен относительно всех автоморфизмов группы $G$, и, в частности, относительно внутренних автоморфизмов $a(g)$, $g \in G \Rightarrow G' \triangleleft G$.

2) Докажем минимальность. Пусть $N \triangleleft G$ и $\pi\colon G \to G/N$ — канонический гомоморфизм. Тогда $G/N = A$ — абелева $\Leftrightarrow A' = \{e\} \Leftrightarrow \pi(G') = \{e\}$ $\Leftrightarrow G' \subseteq N$. □

**Примеры.**

1. $S_3' \subset A_3$, но $S_3' \neq \{e\}$, т.к. $S_3$ неабелева $\Rightarrow S_3' = A_3$.
2. $S_4' \subset A_4$, $S_4' \neq \{e\}$ и $S_4' \supset S_3' = A_3 \Rightarrow S_4'$ содержит все тройные циклы $\Rightarrow |S_4'| \geqslant 9 \Rightarrow S_4' = A_4$.
3. $V_4 \triangleleft A_4$, $A_4/V_4$ циклическая порядка $3 \Rightarrow A_4' \subset V_4$, $A_4' \neq \{e\}$. Пусть $A_4' \ni (12)(34)$. Но все произведения двух нетривиальных транспозиций сопряжены в $A_4 \Rightarrow A_4' = V_4$.

**Лемма 9.1.** *При любом $n$ $A_n$ порождается тройными циклами, а при $n \geqslant 5$ — также произведениями пар независимых транспозиций.*

*Доказательство.* Т.к. группа $S_n$ порождается транспозициями, то группа $A_n$ порождается произведениями пар транспозиций. Но $(ij)(jk) =$ $= (ijk)$, $(ij)(kl) = (ijk)(jkl)$. Значит, $A_n$ порождается тройными циклами. Аналогично, при $n \geqslant 5$ $(ij)(jk) = [(ij)(lm)][(jk)(lm)]$, и $A_n$ порождается произведениями пар независимых транспозиций. □

**Теорема 9.2.** *$S_n' = A_n$, при $n \geqslant 5$ $A_n' = A_n$.*

*Доказательство.* $S_n' \subset A_n$, $S_n' \supset S_3' = A_3 \Rightarrow S_n'$ содержит все тройные циклы $\Rightarrow S_n' = A_n$.

При $n \geqslant 5$ $A_n' \supset A_4 = V_4 \Rightarrow A_n'$ содержит все произведения пар независимых транспозиций $\Rightarrow A_n' = A_n$. □

**Замечание.** Все произведения пар независимых транспозиций сопряжены не только в $S_n$ но и в $A_n$: $\forall\, i,j,k,l$ $(ij)(kl) = \tau((12)(34))\tau^{-1}$. Если $\tau$ четна, то все доказано. Если $\tau$ нечетна, то заменим $\tau$ на $\tau' = \tau(12)$. Тогда $\tau'((12)(34))\tau'^{-1} = \tau((12)(34))\tau^{-1}$.

**Лемма 9.2.** *Группа $\mathrm{SL}_n(K)$ порождается элементарными матрицами первого типа.*

*Доказательство.* Пусть $\det A = 1$. Докажем, что матрицу $A$ можно привести к $E$ с помощью элементарных преобразований строк первого типа. Вначале сделаем $a_{11} = 1$. Если $a_{i1} \neq 0$, то добавим к первой строке $i$-ю строку с подходящим коэффициентом.

Если все $a_{i1} = 0$ при $i > 1$, то $a_{11} \neq 0$ и, прибавив ко второй строке первую, придем к предыдущему случаю.

Пусть теперь $a_{11} = 1$. Вычитаем из всех строк первую с подходящими коэффициентами, получаем, что $a_{i1} = 0$ при $i > 1$.

Аналогично $A$ приводится к унитреугольному виду. Дальше — обратный ход метода Гаусса. □

## Лекция 10.

**Теорема 9.3.** *При* $|K| > 3$ $\mathrm{GL}_n(K)' = \mathrm{SL}_n(K) = \mathrm{SL}_n(K)'$.

*Доказательство.* Во-первых, $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \simeq K^*$ — абелева, поэтому $\mathrm{GL}_n(K)' \subset \mathrm{SL}_n(K)$.

Во-вторых, $\left(\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{smallmatrix}\right);\left(\begin{smallmatrix}1 & c\\ 0 & 1\end{smallmatrix}\right)\right) = \left(\begin{smallmatrix}1 & (\lambda^2-1)c\\ 0 & 1\end{smallmatrix}\right)$. Если $|K| > 3$, то беря $\lambda \neq \neq 0, \pm 1$ и подходящее $c$, можно получить любую матрицу вида $\left(\begin{smallmatrix}1 & a\\ 0 & 1\end{smallmatrix}\right)$.

$\forall\, n \geqslant 2$, $\forall\, i, j \in \{1, \ldots, n\}$, $i \neq j$ имеется вложение $\mathrm{SL}_2(K) \hookrightarrow \mathrm{SL}_n(K)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & a & \cdots & c & \\ & & & \vdots & \ddots & \vdots & \\ & & & d & \cdots & b & \\ & & & & & & 1 \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix}$$

Из предыдущего вычисления следует, что $E + aE_{ij} \in SK_n(K)'$. По лемме 9.2 получаем, что $\mathrm{SL}_n(K) = \mathrm{SL}_n(K)$. Т.к. $\mathrm{GL}_n(K)' \supset \mathrm{SL}_n(K)' = = \mathrm{SL}_n(K)$ и $\mathrm{GL}_n(K)' \subset \mathrm{SL}_n(K)$, то $\mathrm{GL}_n(K)' = \mathrm{SL}_n(K)$. □

*Кратные коммутанты* $G^{(n)}$ определяются по индуктивному правилу: $G^{(0)} = G$, $G^{(1)} = G'$, $G^{(n+1)} = (G^{(n)})'$. Если $\varphi\colon G \overset{\text{на}}{\to} H$, то $\varphi(G^{(n)}) = = H^{(n)}$. Отсюда следует, что $\forall\, n \;\; G^{(n)} \lhd G$.

Группа $G$ называется *разрешимой*, если $\exists\, n \in \mathbb{N} : G^{(n)} = \{e\}$.

**Примеры.**

1. $S_n$ разрешима $\Leftrightarrow n \leqslant 4$ ($S_4^{(3)} = \{e\}$, $S_3^{(2)} = \{e\}$, $S_2' = \{e\}$).
2. $\mathrm{GL}_n(K)$ не разрешима при $n \geqslant 2$ и $|K| > 3$.

**Свойства.**

1. $G$ разрешима $\Rightarrow$ всякая подгруппа $H \subset G$ и всякая факторгруппа $G/N$ разрешима: $G^{(n)} = \{e\} \Rightarrow H^{(n)} = \{e\}$; пусть $\pi\colon G \to G/N$ — канонический гомоморфизм, тогда $(G/N)^{(n)} = \pi(G^{(n)}) = \pi(e) = e$.
2. Если нормальная подгруппа $N \triangleleft G$ и факторгруппа $G/N$ разрешимы, то и группа $G$ разрешима: пусть $N^{(k)} = \{e\}$ и $(G/N)^{(l)} = \{e\}$, тогда $\pi(G) = (G/N)^{(l)} = \{e\} \Rightarrow G^{(l)} \subset N \Rightarrow G^{l+k} \subset N^{(k)} = \{e\}$.

**Теорема 9.4.** *Всякая $p$-примарная конечная группа разрешима.*

*Доказательство.* Индукция по $n$. При $n = 1$ — очевидно. Пусть $n > 1$, тогда $Z(G) \neq \{e\}$ — абелева (а значит, и разрешимая), $G/Z(G)$ разрешима по предположению индукции. □

**Теорема 9.5.** *Группа $\mathrm{B}_n(K)$ треугольных матриц порядка $n$ над полем $K$ разрешима.*

*Доказательство.* Рассмотрим гомоморфизм $\varphi\colon \mathrm{B}_n(K) \to (K^*)^n$:

$$\begin{pmatrix} \lambda_1 & * & * \\ \vdots & \ddots & * \\ 0 & \cdots & \lambda_n \end{pmatrix} \mapsto (\lambda_1, \ldots, \lambda_n),$$

причем группа $(K^*)^n$ абелева. $\ker\varphi = \mathrm{U}_n(K)$. Если $\mathrm{U}_n(K)$ разрешима, то и $\mathrm{B}_n(K)$ разрешима.

Докажем разрешимость группы $\mathrm{U}_n(K)$ индукцией по $n$. При $n = 1$ — очевидно. При $n > 1$ рассмотрим гомоморфизм $\psi\colon \mathrm{U}_n(K) \to \mathrm{U}_{n-1}(K)$,

$$\begin{pmatrix} 1 & * & * & \vdots \\ \vdots & \ddots & * & \vdots \\ 0 & \cdots & 1 & \vdots \\ \cdots & 0 & \cdots & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & * & * \\ \vdots & \ddots & * \\ 0 & \cdots & 1 \end{pmatrix}.$$

Очевидно, что

$$\ker\psi = \begin{pmatrix} 1 & \cdots & 0 & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & a_{n-1} \\ \cdots & 0 & \cdots & 1 \end{pmatrix} \simeq (K^*)^{n-1}$$

—абелева группа. $\mathrm{U}_n(K)/\ker\psi \simeq \mathrm{U}_{n-1}(K)$ — разрешима по предположению индукции. Значит, $\mathrm{U}_n(K)$ разрешима. □

## 10. Простые группы.

Группа $G$ называется *простой*, если она не содержит нетривиальных нормальных подгрупп.

Простая группа $G$ разрешима $\Leftrightarrow$ $G$ — циклическая группа простого порядка.

Существуют некоммутативные простые группы.

**Лемма 10.1.** *Если $G$ — конечная группа и $p \mid |G|$, то существует элемент $g \in G$ порядка $p$.*

*Доказательство.* Возьмем нетривиальную силовскую $p$-подгруппу $S \subset$ $\subset G$. Тогда $\forall\, g \in S, g \neq e$ $\operatorname{ord} g = p^k$ и $\operatorname{ord} g^{p^{k-1}} = p$. □

**Теорема 10.1.** *Группа $A_5$ проста.*

*Доказательство.* Поскольку $|A_5| = 2^2 \cdot 3 \cdot 5$, то все элементы, не равные $e$, имеют порядок 2, 3 или 5. Пусть $N$ — нетривиальная нормальная подгруппа.

1) Если $2 \mid |N|$, то по лемме 10.1 $N$ содержит элемент порядка $2 \Rightarrow N$ содержит все транспозиции вида $(ij)(kl) \Rightarrow N = A_5$ — противоречие.

2) Если $3 \mid |N|$, то по лемме 10.1 $N$ содержит тройной цикл $\Rightarrow N$ содержит все тройные циклы $\Rightarrow N = A_5$ — противоречие.

3) Если $|N| = 5$, то $N = \langle (ijklm) \rangle$ — силовская 5-подгруппа. Но в $A_5$ силовская 5-подгруппа не единственна, а значит, не нормальна — противоречие. □

**Замечание.** Можно доказать, что не существует некоммутативных простых групп порядка меньше 60. Более того. всякая группа порядка меньше 60 разрешима. Группа $\mathrm{PSL}_n(K) = \mathrm{SL}_n(K)/\{\lambda E : \lambda^n = 1\}$ проста, кроме случая $n = 2$, $|K| = 2, 3$.

## Лекция 11.
## 11. Линейные представления групп.

*Линейным представлением группы $G$ в векторном пространстве $V$* называется всякий гомоморфизм $R\colon G \to \mathrm{GL}(V)$. Пространство $V$ называется *пространством представления*, а его размерность — *размерностью представления*.

*Матричным представлением группы $G$* называется всякий гомоморфизм $R\colon G \to \mathrm{GL}_n(K)$ ($K$ — поле).

Всякую матрицу $A \in \mathrm{GL}_n(K)$ можно рассматривать как линейный оператор $X \mapsto AX$ в пространстве $K^n$. Соответственно, всякое матричное представление можно рассматривать как линейное представление в пространстве $K^n$.

Обратно, если $R\colon G \to \mathrm{GL}(V)$ — линейное представление и $e = (e_1, \dots \dots, e_n)$ — базис пространства $V$, то, записывая линейные операторы $R(g)$ матрицами в базисе $e$, получим следующее матричное представление: $R_e\colon G \to \mathrm{GL}_n(K)$.

При переходе от старого базиса к новому $e' = eC$, получаем другое матричное представление $R_{e'}$, связанное с $R_e$ формулой $R_{e'}(g) = = C^{-1}R_e(g)C$.

Линейные представления одной и той же группы $R\colon G \to \mathrm{GL}(V)$ и $S\colon G \to \mathrm{GL}(U)$ *изоморфны*, если есть такой изоморфизм $\varphi\colon V \to U$ векторных пространств, что $\forall\, g \in G \quad \varphi R(g) = S(g)\varphi$, т.е. следующая диаграмма коммутативна:

$$\begin{array}{ccc} V & \xrightarrow{R(g)} & V \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ U & \xrightarrow[S(g)]{} & U \end{array}$$

Пусть $e = (e_1, \dots, e_n)$ — базис $V$. Тогда $\varphi(e) = (\varphi(e_1), \dots, \varphi(e_n))$ — базис $U$. Условие коммутативности диаграммы означает, что $R_e(g) = = S_{\varphi(e)}(g)\ \ \forall\, g \in G$.

**Примеры.**

1. $G = \mathbb{R}$, $R_1(t) = \left(\begin{smallmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{smallmatrix}\right)$, $R_2(t) = \left(\begin{smallmatrix}\operatorname{ch} t & \operatorname{sh} t\\ \operatorname{sh} t & \operatorname{ch} t\end{smallmatrix}\right)$, $R_3(t) = \left(\begin{smallmatrix}e^t & 0\\ 0 & e^{-t}\end{smallmatrix}\right)$, $R_4(t) = \left(\begin{smallmatrix}1 & t\\ 0 & 1\end{smallmatrix}\right)$. $R_2 \simeq R_3$.

2. $G = S_4$, $R_1\colon S_4 \xrightarrow{\sim} \operatorname{Sym} T \subset \mathrm{GL}(\mathbb{E}^3)$, $R_2\colon S_4 \xrightarrow{\sim} \operatorname{Sym}_+ K \subset \mathrm{GL}(\mathbb{E}^3)$. $\det R_2(g) \equiv 1 \ \ \forall\, g$, $\det R_1(g) \neq 1$ при $g \notin A_4 \Rightarrow R_1 \not\simeq R_2$.

3. $G = S_3$, $R\colon S_3 \xrightarrow{\sim} \operatorname{Sym} \triangle \subset \mathrm{GL}(\mathbb{E}^2)$.

4. $G = S_4$, $S\colon S_4 \to S_3 \xrightarrow{\sim} \operatorname{Sym} \triangle \subset \mathrm{GL}(\mathbb{E}^2)$.

5. Одномерные представления — гомоморфизмы $G \to K^*$. В частности, $\det\colon \mathrm{GL}_n(K) \to K^*$, $\operatorname{sgn}\colon S_n \to \{\pm 1\}$.

6. Тривиальные представления: $I\colon G \to \mathrm{GL}(V)$, $I(g) = \mathcal{E} \ \ \forall\, g \in G$.

*Расширение поля* $K \subset L$ (например, $\mathbb{R} \subset \mathbb{C}$), $R\colon G \to \mathrm{GL}_n(K) \subset \subset \mathrm{GL}_n(L)$.

*Сумма представлений* $R\colon G \to \mathrm{GL}(V)$ и $S\colon G \to \mathrm{GL}(U)$ — это представление $R + S\colon G \to \mathrm{GL}(V \oplus U)$, определяемое по следующим формулам: $(R+S)(g)(v,u) = (R(g)v, S(g)u)$ или $(R+S)(g) = \begin{pmatrix} R(g) & 0\\ 0 & S(g)\end{pmatrix}$.

**Примеры.**

1. Пусть $R_3\colon \mathbb{R} \to \mathrm{GL}(\mathbb{R})$, тогда оно является суммой двух представлений $t \mapsto e^t$, $t \mapsto e^{-t}$.

Пусть $R\colon G \to \mathrm{GL}(V)$ — некоторое представление Подпространство $U \subset V$ называется *инвариантным относительно представления* $R$, если оно инвариантно относительно всех операторов $R(g)$, $g \in G$, т.е. $R(g)u \in U \ \ \forall\, u \in U, g \in G$. В матричной форме (в базисе пространства $V$, согласованным с $U$) это означает, что $R(g) = \left(\begin{smallmatrix}* & *\\ 0 & *\end{smallmatrix}\right) \ \ \forall\, g \in G$.

Если $U$ инвариантно, то можно рассматривать ограничение представления $R$ на $U$: $R_U(g)u = R(g)u \ \ \forall\, u \in U$. В матричной форме $R(g) = \begin{pmatrix} R_U(g) & *\\ 0 & *\end{pmatrix}$.

Если $V = U \oplus W$, $U$, $W$ — инвариантные подпространства, то $R(g) = \begin{pmatrix} R_U(g) & 0\\ 0 & R_W(g)\end{pmatrix}$, т.е. $R \simeq R_U + R_W$.

Линейное представление $R\colon G \to \mathrm{GL}(V)$ называется *неприводимым*, если в $V$ нет нетривиальных инвариантных подпространств.

Линейное представление $R\colon G \to \mathrm{GL}(V)$ называется *вполне приводимым*, если для всякого инвариантного подпространства $U \subset V$ существует инвариантное дополнительное подпространство $W \subset V$.

Всякое неприводимое представление вполне приводимо.

Всякое одномерное представление неприводимо.

Неприводимое представление может стать приводимым после расширения поля.

**Примеры.**

1. $G = \mathbb{R}$. Представление $R_1$ неприводимо над $\mathbb{R}$, но разлагается в сумму двух одномерных представлений над $\mathbb{C}$: $R_1 = \left(\begin{smallmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{smallmatrix}\right)$ в базисе $(e_1 - ie_2, e_1 + ie_2)$.

   Представление $R_3$ разлагается в сумму двух одномерных над $\mathbb{R}$.

   Представление $R_4$ приводимо, но не вполне приводимо.

2. $G = S_4$. Представления $R_1$ и $R_2$ неприводимы, т.к. у них повороты на 120° вокруг осей, проходящих через вершины, не имеют 1-мерных инвариантных подпространств.

## Лекция 12.

**Теорема 11.1.** *Ограничение вполне приводимого представления на инвариантное подпространство $U$ также вполне приводимо.*

*Доказательство.* Пусть $U_1 \subset U$ — инвариантное подпространство. Тогда существует инвариантное подпространство $V_2 \subset V$: $V = U_1 \oplus V_2$. Рассмотрим инвариантное подпространство $U_2 = V_2 \cap U$. Докажем, что $U = U_1 \oplus U_2$.

1) $U_1 \cap U_2 \subset U_1 \cap V_2 = 0$.

2) $\forall\, u \in U \;\; u = u_1 + u_2$, где $u_1 \in U_1$, $u_2 \in V_2$. Но $u_2 = u - u_1 \in U \Rightarrow u_2 \in U_2$. □

**Теорема 11.2.** *Линейное представление $R\colon G \to \mathrm{GL}(V)$ является вполне приводимым $\Leftrightarrow$ оно раскладывается в сумму неприводимых представлений.*

*Доказательство.* 1) Пусть $R$ вполне приводимо. Пусть $0 \neq V_1 \subset V$ — минимальное инвариантное подпространство. Тогда $R|_{V_1} = R_1$ неприводимо. Существует инвариантное дополнение — подпространство $V_1'$: $V = V_1 \oplus V_1'$. Пусть $0 \neq V_2 \subset V_1'$ — минимальное инвариантное подпространство и $V_2'$ — инвариантное дополнительное подпространство: $V_1' = V_2 \oplus V_2'$. Тогда $R|_{V_2} = R_2$ неприводимо, и т.д. В конце концов мы получим сумму минимальных инвариантных подпространств: $V = V_1 \oplus \ldots \oplus V_s$. Это означает, что $R = R_1 + \ldots + R_s$, где $R_i = R|_{V_i}$ — неприводимые представления.

2) Обратно, пусть $R$ разлагается в сумму неприводимых представлений. Это означает, что пространство $V$ разлагается в прямую сумму минимальных инвариантных подпространств: $V = V_1 \oplus \ldots \oplus V_s$.

Пусть $U \subset V$ — инвариантное подпространство. Будем искать дополнительное инвариантное подпространство в виде суммы некоторых из $V_1, \ldots, V_s$. Для всякого $I \subset \{1, \ldots, s\}$ положим $V_I = \bigoplus\limits_{i \in I} V_i$. Пусть $I$ — максимальное подмножество, для которого $U \cap V_I = 0$. Докажем, что $V = U \oplus V_I$. По построению $U \cap V_I = 0$. $\forall\, j \notin I \quad U \cap V_{I \cup \{j\}} \neq 0$, т.е. $\exists\, u \in U : u = \sum\limits_{i \in I} v_i + v_j$, где $v_i \in V_I$, $v_j \in V_j$. Тогда $v_j = u - \sum\limits_{i \in I} v_i \in U \oplus V_i$. Значит, $V_j \cap (U \oplus V_i) \neq 0$. Т.к. $V_j$ — минимальное инвариантное подпространство, то $V_j \subset U \oplus V_I$. Значит, $V = U \oplus V_I$. □

**Примеры.**

1. $G = \mathbb{Z}$, $R\colon \mathbb{Z} \to \mathrm{GL}(V)$, $R(1) = \mathcal{A} \in \mathrm{GL}(V) \Rightarrow R(k) = \mathcal{A}^k$. Т.о., представление $R$ определяется однозначно линейным оператором $\mathcal{A}$. Обратно, $\forall\, \mathcal{A} \in \mathrm{GL}(V)$ формула $R(k) = \mathcal{A}^k$ определяет линейное представление группы $\mathbb{Z}$.

   Если $R$ — комплексное представление группы $\mathbb{Z}$, то его неприводимость означает, что $\dim V = 1$, а полная приводимость — что $R$ есть сумма одномерных представлений, т.е. матрица оператора $\mathcal{A}$ приводится к диагональному виду.

**Теорема 11.3.** *Всякое линейное представление $R\colon G \to \mathrm{GL}(V)$ конечной группы $G$ над полем характеристики 0 вполне приводимо.*

*Доказательство.* Пусть $U \subset V$ — инвариантное подпространство и $W \subset$ $\subset V$ — дополнительное подпространство к $U$: $V = U \oplus W$. Пусть $\mathcal{P}$ —

проектор на $U$ параллельно $W$, т.е. $\forall\, v = u + w$, где $u \in U$, $w \in W$ $\mathcal{P}v = u$. Рассмотрим *усреднение* проектора $\mathcal{P}$ по группе $G$:

$$\mathcal{P}_0 = \frac{1}{|G|} \sum_{g \in G} R(g)\mathcal{P}R(g)^{-1}.$$

Докажем некоторые свойства оператора $\mathcal{P}_0$.

1) $\forall\, u \in U \quad \mathcal{P}_0 u = u$: т.к. $R(g)^{-1}u \in U$, то $\mathcal{P}R(g)^{-1}u = R(g)^{-1}u$ и $\mathcal{P}_0 u = \frac{1}{|G|} \sum\limits_{g \in G} R(g)R(g)^{-1}u = u$.

2) $\forall\, v \in V \quad \mathcal{P}_0 v \in U$: т.к. $\mathcal{P}R(g)^{-1}v \in U$, то

$$\mathcal{P}_0 v = \frac{1}{|G|} \sum_{g \in G} R(g)\mathcal{P}R(g)^{-1}v \in U.$$

Положим $W_0 = \ker \mathcal{P}_0$. Тогда

1) $U \cap W_0 = 0$.

2) $U + W_0 = V$: $\forall\, v \in V \quad v = \mathcal{P}_0 v + (v - \mathcal{P}_0 v)$.

Таким образом, $V = U \oplus W_0$. Покажем, что $W_0$ инвариантно. Пусть $w \in W_0$, $h \in G$. Тогда

$$\begin{aligned}
\mathcal{P}_0 R(h)w &= \frac{1}{|G|} \sum_{g \in G} R(g)\mathcal{P}R(g)^{-1}R(h)w = \\
&= \frac{1}{|G|} R(h) \sum_{g \in G} (R(h)^{-1}R(g))\mathcal{P}(R(g)^{-1}R(h))w = \\
&= \frac{1}{|G|} R(h) \sum_{g \in G} R(h^{-1}g)\mathcal{P}R(h^{-1}g)^{-1}w = \\
&= \frac{1}{|G|} R(h) \sum_{g \in G} R(g)\mathcal{P}R(g)^{-1}w = R(h)\mathcal{P}_0 w = 0.
\end{aligned}$$

□

**Примеры.**

1. Докажем, что два трехмерных представлений группы $S_4$ неприводимы над $\mathbb{C}$.

   $R_{1,2}\colon S_4 \to \mathrm{GL}(\mathbb{E}^3)$. Если существует двумерное комплексное инвариантное подпространство, то в силу полной приводимости есть и

одномерное инвариантное подпространство, например. $\langle z = x+iy\rangle$. Тогда $\forall\, g \in G \;\; R(g)z = (\lambda + i\mu)z$, где $\lambda, \mu \in \mathbb{R}$, т.е. $R(g)x = \lambda x - \mu y$, $R(g)y = \mu x + \lambda y \Rightarrow$ вещественное подпространство $\langle x, y\rangle$ инвариантно — противоречие.

2. *Мономиальное представление группы $S_n$.* Пусть $V$ — векторное пространство с базисом $\{e_1, \ldots, e_n\}$ (т.е. $\dim V = n$). Определим представление $M\colon S_n \to \mathrm{GL}(V)$ по правилу $R(\sigma)e_i = e_{\sigma(i)}$. Подпространства $\langle e_1 + \ldots + e_n\rangle$ и $V_0 = \left\{ \sum\limits_{i=1}^{n} x_i e_i : \sum\limits_{i=1}^{n} x_i = 0 \right\}$ являются инвариантными и взаимно дополнительными. Тогда $M$ раскладывается в сумму одномерного представления и $(n-1)$-мерного представления $M_0 = M|_{V_0}$. Докажем, что оно неприводимо.

   Пусть $U \subset V_0$ — инвариантное подпространство. Возьмем $0 \neq u = \sum\limits_i x_i e_i \in U$. Т.к. мы можем переставлять координаты, то можно считать. что $X_1 \neq x_2$. Тогда $R((12))u - u = (x_2 - x_1)(e_1 - e_2) \in U \Rightarrow e_1 - e_2 \in U \Rightarrow e_i = e_j \in U \;\; \forall\, i, j \Rightarrow V_0 = U$. В частности при $n = 4$ $M_0 = R_1$.

## Лекция 13.

**Теорема 11.4** (Лемма Шура)**.** *Пусть $R\colon G \to \mathrm{GL}(V)$ — неприводимое комплексное линейное представление группы $G$. Тогда всякий линейный оператор $\mathcal{A}$ в пространстве $V$, перестановочный со всеми операторами $R(g)$ (где $g \in G$), скалярен.*

*Доказательство.* Пусть $\lambda$ — собственное значение оператора $\mathcal{A}$ и $V_\lambda = \{v \in V : \mathcal{A}v = \lambda v\}$. Тогда $V_\lambda$ инвариантно относительно всех операторов представления: $\forall\, v \in V_\lambda \quad \mathcal{A}R(g)v = R(g)\mathcal{A}v = \lambda R(g)v \Rightarrow V_\lambda = V$, т.е. $\mathcal{A} = \lambda\mathcal{E}$. □

**Следствие 11.1.** *Всякое неприводимое комплексное представление абелевой группы одномерно.*

*Доказательство.* Пусть $G$ — абелева группа и $R\colon G \to \mathrm{GL}(V)$ — неприводимое комплексное представление. Тогда

$$\forall\, g, h \in G \;\; R(g)R(h) = R(gh) = R(hg) = R(h)R(g),$$

т.е. $R(h)$ перестановочен со всеми операторами представления, и по лемме Шура $R(h)$ — скалярный оператор. $\square$

Опишем все комплексные линейные представления конечных абелевых групп.

Т.к. всякое представление есть сумма неприводимых, а всякое неприводимое представление одномерно, то достаточно описать одномерные представления.

Пусть $G = \langle a_1\rangle_{n_1} \times \ldots \times \langle a_s\rangle_{n_s}$. Одномерное представление есть гомоморфизм $R\colon G \to \mathbb{C}^*$. Оно определяется числами $R(a_1) = \varepsilon_1$, $\ldots$, $R(a_s) = \varepsilon_s$, т.к. $R(a_1^{k_1} \ldots a_s^{k_s})$. Далее, т.к. $a_i^{n_i} = e$, то должно быть $\varepsilon_i^{n_i} = 1$. Обратно, если $\varepsilon_1, \ldots, \varepsilon_s$ удовлетворяют этим условиям, то предыдущая формула определяет одномерное представление группы $G$. Т.о., получается $n_1 \ldots n_s = |G|$ представлений.

**Теорема 11.5.** *Пусть $R$ — это одномерное представление группы $G$ и $\pi\colon G \to G/(G,G)$ — канонический гомоморфизм. Тогда существует такое одномерное представление $\bar{R}$ группы $G/(G,G)$, что $R = \bar{R} \circ \pi$.*

*Доказательство.* Очевидно, что если $\bar{R}$ — одномерное представление группы $G/(G,G)$, то $R = \bar{R} \circ \pi$ — одномерное представление группы $G$.

Докажем, что $(G,G) \subset \ker R$: $R((g,h)) = (R(g), R(h)) = 1$. Следовательно, все элементы каждого смежного класса $g(G,G)$ при представлении $R$ переходят в одно и то же число. Значит, $\exists\, \bar{R} : G/(G,G) \to K^*$: $R = \bar{R} \circ \pi$. А именно, $\bar{R}(g(G,G)) = R(g)$.

Отображение $\bar{R}$ — гомоморфизм: $\bar{R}(g(G,G)\cdot h(G,G)) = \bar{R}(gh(G,G)) =$ $= R(gh) = R(g)R(h) = \bar{R}(g(G,G)) \cdot \bar{R}(h(G,G))$. $\square$

**Примеры.**

1. $G = S_n$, $(G,G) = A_n$, $S_n/A_n \simeq C_2$. Значит, группа $S_n$ имеет два одномерных комплексных представления: тривиальное и sgn.

2. $G = D_n = \langle a, b\rangle$, где $a$ — поворот на угол $\frac{2\pi}{n}$, $b$ — отражение. Элементы $a$ и $b$ удовлетворяют соотношениям $a^n = e$, $b^2 = e$, $(ab)^2 = e$. Значит, $(a,b) = a^2$ и $(G,G) \supset \langle a^2\rangle$. Если $n$ четно, то $\operatorname{ord} a^2 = n/2 \Rightarrow$ $|D_n/\langle a^2\rangle| = 4 \Rightarrow D_n/\langle a^2\rangle$ абелева $\Rightarrow (G,G) = \langle a^2\rangle$. Если $n$ нечетно, то $\operatorname{ord} a^2 = n \Rightarrow \langle a^2\rangle = C_n \Rightarrow (G,G) = C_n$. Т.о., группа $D_n$ имеет 4 одномерных представления, если $n$ четно, и 2, если $n$ нечетно.

Опишем все неприводимые комплексные представления группы $D_n$. Заметим, что всякий элемент группы $D_n$ представляется в виде $a^k$ или $a^k b$, причем этот вид определен однозначно с точностью до прибавления к $k$ целого кратного $n$.

Пусть $R\colon D_n \to \mathrm{GL}(V)$ — неприводимое комплексное представление, $\dim V > 1$. Положим $R(a) = \mathcal{A}$, $R(b) = \mathcal{B}$. Операторы $\mathcal{A}$ и $\mathcal{B}$ удовлетворяют соотношениям $\mathcal{A}^n = \mathcal{E}$, $\mathcal{B}^2 = \mathcal{E}$, $\mathcal{B}\mathcal{A}\mathcal{B} = \mathcal{A}^{-1}$. Обратно, формулы $R(a^k) = \mathcal{A}^k$, $R(a^k b) = \mathcal{A}^k\mathcal{B}$ определяют представление группы $D_n$ в пространстве $D_n$: $R(a^k \cdot a^l) = R(a^{k+l}) = \mathcal{A}^{k+l} = \mathcal{A}^k \cdot \mathcal{A}^l = R(a^k) \cdot R(a^l)$, $R(a^k \cdot a^l b) = \mathcal{A}^{k+l}\mathcal{B} = R(a^{k+l}b) = R(a^k) \cdot R(a^l b)$, $R(a^k b \cdot a^l) = R(a^k(ba^l b^{-1})b) = R(a^{k-l}b) = \mathcal{A}^{k-l}\mathcal{B} = \mathcal{A}^k\mathcal{B}\cdot\mathcal{A}^l = R(a^k b)\cdot R(a^l)$, $R(a^k b \cdot a^l b) = R(a^k b) \cdot R(a^l b)$.

Пусть $e \in V$ — собственный вектор оператора $\mathcal{A}$: $\mathcal{A}e = \lambda e$. Положим $f = \mathcal{B}e$. Заметим, что $e$ и $f$ не коллинеарны, т.к. иначе $\langle e\rangle$ инвариантно и $V = \langle e\rangle$ одномерно. Далее, $\mathcal{A}f = \mathcal{A}\mathcal{B}e = \mathcal{B}\mathcal{A}^{-1}e = \lambda^{-1}\mathcal{B}e = \lambda^{-1}f$, т.е. $f$ — собственный вектор оператора $\mathcal{A}$. $\mathcal{B}f = \mathcal{B}^2 e = e \Rightarrow$ подпространство $\langle e, f\rangle$ инвариантно $\Rightarrow V = \langle e, f\rangle$. В базисе $\{e, f\}$ $\mathcal{A} = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{smallmatrix}\right)$, $\mathcal{B} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0\end{smallmatrix}\right)$. При этом $\lambda^n = 1$ и $\lambda \neq \pm 1$, т.к. иначе $\lambda = \lambda^{-1}$ и подпространство $\langle e + f\rangle$ инвариантно.

Построенное таким образом неприводимое двумерное представление группы $D_n$ обозначим $R_\lambda$.

Очевидно, что $R_\lambda \simeq R_\mu \Leftrightarrow \mu = \lambda^{\pm 1}$. Т.о., получается $\frac{n-2}{2}$ двумерных неприводимых представлений при четном $n$ и $\frac{n-1}{2}$ при нечетном $n$.

## 12. Морфизмы представлений.

*Морфизмом* представления $R\colon G \to \mathrm{GL}(V)$ в представление $S\colon G \to$ $\to \mathrm{GL}(U)$ называется всякое линейное отображение $f\colon V \to U$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} V & \xrightarrow{R(g)} & V \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ U & \xrightarrow[S(g)]{} & U \end{array}$$

Все линейные отображения $f\colon V \to U$ образуют векторное пространство, а морфизмы представлений образуют в нем подпространство, обозначаемое $\mathrm{Mor}(R, S)$.

**Предложение 12.1.** $\operatorname{Mor}(R_1 + R_2, S) \simeq \operatorname{Mor}(R_1, S) \oplus \operatorname{Mor}(R_2, S)$.

*Доказательство.* Пусть $R_1 \colon G \to \mathrm{GL}(V_1)$, $R_2 \colon G \to \mathrm{GL}(V_2)$, $S \colon G \to \mathrm{GL}(U)$. Тогда $R_1 + R_2 \colon G \to \mathrm{GL}(V_1 \oplus V_2)$ и любой морфизм $f \in \operatorname{Mor}(R_1 + R_2, S)$ имеет вид

$$f((v_1, v_2)) = f_1(v_1) + f_2(v_2), \text{ где } f_1 \in \operatorname{Mor}(R_1, S),\ f_2 \in \operatorname{Mor}(R_2, S).$$

Отображение $f \mapsto (f_1, f_2)$ и есть искомый изоморфизм. □

В частности, $\operatorname{Mor}(R, R)$ есть пространство линейных операторов, перестановочных со всеми операторами представления.

Если $R$ — неприводимое комплексное представление, то по лемме Шура $\dim \operatorname{Mor}(R, R) = 1$.

**Теорема 12.1.** *Если $R, S$ — неприводимые комплексные представления, то*

$$\dim \operatorname{Mor}(R, S) = \begin{cases} 1, & \text{если } R \simeq S \\ 0, & \text{если } R \not\simeq S. \end{cases}$$

*Доказательство.* Если $R \simeq S$, то можно считать, что $R = S$ и тогда $\dim \operatorname{Mor}(R, R) = 1$.

Пусть $R \not\simeq S$ и $0 \neq f \in \operatorname{Mor}(R, S)$. Тогда $\ker f$ инвариантно $\Rightarrow$ $\ker f = 0$. Далее, $\operatorname{Im} f$ инвариантно $\Rightarrow \operatorname{Im} f = U \Rightarrow f$ — изоморфизм — противоречие. □

**Следствие 12.1.** *Пусть $R = \sum\limits_i k_i R_i$ — разложение представления $R$ в сумму неприводимых. Тогда $k_j = \dim \operatorname{Mor}(R, R_j)$.*

*Доказательство.* $\operatorname{Mor}(R, R_j) \simeq \bigoplus\limits_i k_i \operatorname{Mor}(R_i, R_j) = k_j \operatorname{Mor}(R_j, R_j) = k_j$. □

**Примеры.**

1. Найдем число 4-мерных комплексных представлений группы $D_6$. Имеется 4 одномерных и 2 двумерных неприводимых[2] комплексных представления. $4 = \underbrace{2+2}_{3} = \underbrace{2+1+1}_{2(4+6)=20} = \underbrace{1+1+1+1}_{CC_4^4=35}$, значит, всего 58 4-мерных представлений.

[2]Здесь в лекции было сказано «нетривиальных». Полагаю, это оговорка.

Лекция 14.

## 13. Регулярные представления.

Пусть $G$ — конечная группа, $A$ — векторное пространство с базисом $\{a_g : g \in G\}$ ($\dim A = |G|$). Рассмотрим представление $L\colon G \to \mathrm{GL}(A)$, $L(g)a_h = a_{gh}$. Это представление называется *регулярным*.

Для простоты будем писать просто $g$ вместо $a_g$. Тогда $L(g)h = gh$.

**Теорема 13.1.** *Кратность вхождения каждого неприводимого*[3] *комплексного линейного представления $R$ группы $G$ в регулярное представление равна* $\dim R$.

*Доказательство.* Опишем пространство $\mathrm{Mor}(L, R)$, где $R\colon G \to \mathrm{GL}(V)$ — любое представление. Пусть $f \in \mathrm{Mor}(L, R)$, $f\colon A \to V$ перестановочно с действием $G$. $f(e) = v$ однозначно определяет $f$: $f(g) = f(L(g)e) = = R(g)v$.

Обратно, $\forall\, v \in V$ определим линейное отображение $f_v\colon A \to V$ по формуле $f_v(g) = R(g)v$. Оно будет перестановочно с действием $G$:

$$f_v(L(g)h) = f_v(gh) = R(gh)v = R(g)R(h)v = R(g)f_v(h).$$

Кроме того, $f_v$ линейно зависит от $v$: $f_{v_1+v_2} = f_{v_1} + f_{v_2}$, $f_{\lambda v} = \lambda f_v$.

Т.о., $\mathrm{Mor}(L, R) \simeq V$ и $\dim \mathrm{Mor}(L, R) = \dim V$.

Если $R$ неприводимо, то по теореме 12.1 $\dim \mathrm{Mor}(L, R)$ равно кратности вхождения $R$ в $L$. □

**Следствие 13.1.** *Конечная группа имеет лишь конечное число неприводимых*[4] *комплексных представлений и сумма квадратов их размерностей равна порядку группы.* □

**Примеры.**

1. $G$ абелева: $\underbrace{1^2 + \ldots + 1^2}_{n=|G|} = n$.
2. $G = D_n$. Пусть $n$ четно $\Rightarrow \frac{n-2}{2} \cdot 2^2 + 4 \cdot 1^2 = 2n$. Пусть $n$ нечетно $\Rightarrow \frac{n-1}{2} \cdot 2^2 + 2 \cdot 1^2 = 2n$.

[3] В лекциях опять-таки было сказано «нетривиального».

[4] И здесь в лекции было «нетривиальных».

3. $G = S_4$: $1^2 + 1^2 + 2^2 + 3^2 + 3^2 = 24 = |G|$. Значит, других нетривиальных комплексных линейных представлений нет.

**Теорема 13.2** (Без доказательства)**.** *Число неприводимых комплексных линейных представлений конечной группы $G$ равно числу классов сопряженности в $G$.*

**Примеры.**

1. $G$ абелева: число неприводимых представлений равно $|G|$.
2. $G = S_4$: 5 классов сопряженности $\Rightarrow$ есть 5 неприводимых представлений.
3. $G = A_5$. $|G| = 60 = 1^2 + 3^2 + 4^2 + 34$. Число классов сопряженности равно 5 $\Rightarrow |G| = 1^2 + 3^2 + 4^2 + (\underbrace{3^2 + 5^2}_{34})$.

## 14. Линейные представления группы $\mathbb{R}$.

Рассмотрим представление $F\colon \mathbb{R} \to \mathrm{GL}(V)$ аддитивной группы $\mathbb{R}$, где $V$ — векторное пространство над полем $K = \mathbb{R}$ или $K = \mathbb{C}$. $F(t+u) = F(t) \cdot F(u) \quad \forall\, t, u \in \mathbb{R}$ (*однопараметрическая группа линейных операторов*).В матричной записи $F(t) = (F_{ij}(t))$. Потребуем, чтобы функции $F_{ij}(t)$ были непрерывно дифференцируемы.

**Теорема 14.1.** *Дифференцируемое отображение $F\colon \mathbb{R} \to \mathrm{GL}(V)$ является линейным представлением $\Leftrightarrow F'(t) = \mathcal{A}F(t)$ для некоторого оператора $\mathcal{A} \in V^*$, и $F(0) = \mathcal{E}$.*

**Замечание.** $\mathcal{A} = F'(0)$.

*Доказательство.* 1) Пусть $F$ — гомоморфизм. Тогда $\forall\, t, u \in \mathbb{R} \quad F(u + t) = F(u) \cdot F(t)$. Дифференцируя по $u$ при $u = 0$, получаем $F'(t) = F'(0) \cdot F(t) = \mathcal{A}F(t)$.

2) Обратно, пусть $F'(t) = \mathcal{A}F(t)$, $F(0) = \mathcal{E}$. Данное дифференциальное уравнение можно рассматривать как систему из $n^2$ обычных дифференциальных уравнений с $n^2$ неизвестными функциями. По общей теореме о решениях системы дифференциальных уравнений решение однозначно определяется начальным условием.

$\forall \mathcal{C} \in V^*$ рассмотрим функцию $F_{\mathcal{C}}(t) = F(t)\mathcal{C}$. Она удовлетворяет тому же уравнению: $F'_{\mathcal{C}}(t) = F'(t)\mathcal{C} = \mathcal{A}F(t)\mathcal{C} = \mathcal{A}F_{\mathcal{C}}(t)$ с начальным условием $F_{\mathcal{C}}(0) = \mathcal{C}$.

$\forall\, u \in \mathbb{R}$ рассмотрим матричную функцию $F_u(t) = F(t+u)$. Имеем: $F'_u(t) = F'(t+u) = \mathcal{A}F(t+u) = \mathcal{A}F_u(t)$. Следовательно, $F_u(t) = F(t)\mathcal{C}$, где $\mathcal{C} = F_u(0) = F(u)$.

T.o., $F(t+u) = F(t) \cdot F(u) \;\; \forall\, t, u \in \mathbb{R}$. □

В случае $\dim V = 1$ мы получаем обычное дифференциальное уравнение $f'(t) = af(t)$, $f(0) = 1$. Его решение — это экспонента: $f(t) = e^{at}$.

Экспонента — это сумма бесконечного ряда: $e^a = \sum\limits_{k=0}^{\infty} \frac{a^k}{k!}$. Можно попробовать написать такой же ряд для линейного оператора $\mathcal{A}$: $e^{\mathcal{A}} = \sum\limits_{k=0}^{\infty} \frac{\mathcal{A}^k}{k!}$. Чтобы придать смысл этому ряду, надо определить сходимость последовательности матриц.

Рассмотрим матрицы над полем $K = \mathbb{R}$ или $K = \mathbb{C}$. *Норма матрицы* $\underset{n\times n}{A} = (a_{ij})$: $\|A\| = \max\limits_i \sum\limits_j |a_{ij}|$.

**Свойства.**

1. $\|A\| \geqslant 0$, причем $\|A\| = 0 \Leftrightarrow A = 0$
2. $\sum\limits_j |a_{ij}| \leqslant \|A\|$
3. $\|A+B\| \leqslant \|A\|+\|B\|$: $\forall\, i \;\; \sum\limits_i |a_{ik}+b_{ij}| \leqslant \sum\limits_i |a_{ik}|+\sum\limits_i |b_{ij}| \leqslant \|A\|+\|B\|$.
4. $\|AB\| \leqslant \|A\| \cdot \|B\|$: пусть $C = AB = (c_{ij}) \Rightarrow \forall\, i$

$$\sum_k |c_{ik}| = \sum_k \sum_j |a_{ij}| \cdot |b_{jk}| \leqslant \sum_j |a_{ij}| \cdot \|B\| \leqslant \|A\| \cdot \|B\|.$$

Последовательность матриц $A_k$ *сходится к матрице* $A$, если $\|A - A_k\| \to 0$. Это равносильно поэлементной сходимости. Пишут: $A_k \to A$.

**Теорема 14.2** (Критерий Коши)**.** *Ряд* $\sum\limits_{k=1}^{\infty} A_k$ *сходится* $\Leftrightarrow A_{p+1} + \ldots + A_q \to 0$ *при* $p, g \to \infty$. □

**Предложение 14.1.** *Если числовой ряд* $\sum\limits_{k=1}^{\infty} \|A_k\|$ *сходится, то и матричный ряд* $\sum\limits_{k=1}^{\infty} A_k$ *сходится, причем его сумма не зависит от порядка слагаемых.*

*Доказательство.* Если ряд $\sum\limits_{k=1}^{\infty} \|A_k\|$ сходится, то $\|A_{p+1} + \ldots + A_q\| \leqslant$ $\leqslant \|A_{p+1}\| + \ldots + \|A_q\| \to 0$ при $p, q \to \infty \Rightarrow$ ряд $\sum\limits_{k=1}^{\infty} A_k$ сходится по критерию Коши, причем каждый ряд из матричных элементов сходится абсолютно $\Rightarrow$ сумма ряда не зависит от порядка слагаемых. □

**Теорема 14.3.** $\forall\, A$ *ряд* $\sum\limits_{k=1}^{\infty} \frac{A^k}{k!}$ *сходится абсолютно.*

*Доказательство.* $\sum\limits_{k=0}^{\infty} \|\frac{A^k}{k!}\| \leqslant \sum\limits_{k=0}^{\infty} \frac{\|A\|^k}{k!}$ – сходится абсолютно. □

*Экспонента матрицы* $A$: $e^A = \sum\limits_{k=1}^{\infty} \frac{A^k}{k!}$.

## Лекция 15.

$e^{C^{-1}AC} = \sum\limits_{k=0}^{\infty} \frac{C^{-1}A^kC}{k!} = C^{-1}e^AC$. Это позволяет определить экспоненту линейного оператора: $e^{\mathcal{A}}$ — это *линейный оператор с матрицей* $e^A$, где $A$ — матрица оператора $\mathcal{A}$.

**Лемма 14.1.** *Если* $AB = BA$, *то* $e^{A+B} = e^A \cdot e^B$.

*Доказательство.* Т.к. ряд $\sum\limits_{k=0}^{\infty} \sum\limits_{\substack{p,q=0 \\ p+q=k}}^{k} \frac{A^pB^q}{p!q!}$ сходится абсолютно, то суммировать можно в любом порядке $\Rightarrow$

$$e^{A+B} = \sum_{k=0}^{\infty} \frac{(A+B)^k}{k!} = \sum_{k=0}^{\infty} \sum_{\substack{p,q=0 \\ p+q=k}}^{k} \frac{C_k^p A^p B^q}{k!} =$$

$$= \sum_{k=0}^{\infty} \sum_{\substack{p,q=0 \\ p+q=k}}^{k} \frac{A^pB^q}{p!q!} = \sum_{p=0}^{\infty} \frac{A^p}{p!} \cdot \sum_{q=0}^{\infty} \frac{B^q}{q!} = e^A \cdot e^B.$$

□

**Теорема 14.4.** $\forall\, A$ *отображение* $F_A\colon t \mapsto e^{tA}$ *есть линейное представление группы* $\mathbb{R}$, *причем* $F'(0) = A$.

*Доказательство.* Нужно проверить, что $F'_A(t) = AF_A(t)$, $F_A(0) = E$. Вычислим производную $F'_A(0)$:

$$\frac{e^{tA} - E}{t} = \sum_{k=1}^{\infty} \frac{t^{k-1}A^k}{k!} = A + t\sum_{k=2}^{\infty} \frac{A^k t^{k-2}}{k!}.$$

При $|t| < 1$ ряд мажорируется числовым рядом

$$\frac{\|A\|^2}{2!} + \frac{\|A\|^3}{3!} + \ldots = C(= e^{\|A\|} - 1 - \|A\|),$$

и, следовательно, сходится, причем его сумма по норме не больше $C$. Значит, $F'_A(0) = \lim\limits_{t\to 0} \frac{e^{tA}-E}{t} = A$.

Т.к. матрицы $tA$ и $uA$ коммутируют $\forall\, t, u \in \mathbb{R}$, то $F_A(t+u) = F_A(t) \times$ $\times\, F_A(u)$. $F'_A(t) = \frac{d}{du}F_A(u+t)\big|_{u=0} = \frac{d}{du}F_A(u)\big|_{u=0} \cdot F_A(t) = AF_A(t)$. □

**Примеры.**

1. Рассмотрим 4 двумерных представления группы $\mathbb{R}$:
   $R_1(t) = \left(\begin{smallmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{smallmatrix}\right)$, $R'_1(0) = \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right) = A_1 \Rightarrow R_1(t) = e^{t\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)}$.
   $R_2(t) = \left(\begin{smallmatrix}\operatorname{ch} t & \operatorname{sh} t\\ \operatorname{sh} t & \operatorname{ch} t\end{smallmatrix}\right)$, $R'_2(0) = \left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right) = A_2 \Rightarrow R_2(t) = e^{t\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)}$.
   $R_3(t) = \left(\begin{smallmatrix}e^t & 0\\ 0 & e^{-t}\end{smallmatrix}\right)$, $R'_3(0) = \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right) = A_3 \Rightarrow R_3(t) = e^{t\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)}$.
   $R_4(t) = \left(\begin{smallmatrix}1 & t\\ 0 & 1\end{smallmatrix}\right)$, $R'_4(0) = \left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right) = A_4 \Rightarrow R_1(t) = e^{t\left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right)}$.

## 15. Идеалы и факторкольца.

Если в кольце $A$ имеется отношение эквивалентности, согласованное со сложением и умножением, то на множестве классов эквивалентности можно ввести операции сложения и умножения по формулам $[a] + [b] =$ $= [a + b]$, $[a] \cdot [b] = [ab]$.

Найдем отношения эквивалентности, согласованные с операциями. Т.к. кольцо — это абелева группа, то всякое такое отношение есть отношение сравнимости по модулю подгруппы $I$: $a \sim b \Leftrightarrow a \equiv b \pmod{I} \Leftrightarrow$ $a - b \in I$.

Найдем, какой должна быть подгруппа $I$, чтобы это отношение было согласовано с операцией умножения.

**Теорема 15.1.** *Отношение сравнимости по модулю подгруппы $I \subset A$ согласовано с умножением $\Leftrightarrow$ $I$ — идеал кольца $A$ (т.е. $AI = IA = I$).*

*Доказательство.* 1) Пусть отношение эквивалентности по модулю $I$ согласовано с умножением. Тогда $\forall\, u \in I \;\; u \equiv 0 \pmod I$, и, значит, $au \equiv$ $\equiv a \cdot 0 \equiv 0 \pmod I$, $ua \equiv 0 \cdot a \equiv 0 \pmod I$.

2) Обратно, пусть $I$ — идеал и $a \equiv a' \pmod I$, $b \equiv b' \pmod I$. Тогда $a' = a + u$, $b' = b + v$, где $u, v \in I$. Значит, $a'b' = ab + (ub + av + uv) \equiv ab \pmod I$. □

Если $I$ — идеал кольца $A$, то в факторгруппе $A/I$ можно определить операцию умножения по формуле $(a + I)(b + I) = ab + I$. Определенное таким образом умножение в $A/I$ дистрибутивно относительно сложения.

Построенное таким образом кольцо $A/I$ называется *факторкольцом кольца $A$ по идеалу $I$*.

**Примеры.**

1. $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ (кольцо вычетов по модулю $n$).

Имеется канонический гомоморфизм $\pi\colon A \to A/I$, $a \mapsto a + I$.

**Теорема 15.2** (О гомоморфизме колец)**.** *Пусть $f\colon A \to B$ — гомоморфизм колец. Тогда $\ker f = I$ — идеал кольца $A$ и $f = \bar{f} \circ \pi$, где $\pi\colon A \to A/I$ — канонический гомоморфизм, а $\bar{f}\colon A/I \to B$ — некоторый гомоморфизм. Если $f$ сюръективен. то $\bar{f}$ — изоморфизм.* □

Пусть $A$ — коммутативное ассоциативное кольцо с единицей. Тогда всякое факторкольцо также является коммутативным ассоциативным кольцом с единицей.

$\forall\, a \in A$ определим *главный идеал* $(a) = \{ua : u \in A\}$. Легко проверить, что это идеал.

**Примеры.**

1. В кольце $\mathbb{Z}$ $(n) = n\mathbb{Z}$.

*Отношение сравнимости по модулю главного идеала* $(u)$ — это то, что в 1-м семестре называлось отношением сравнимости по модулю $u$: $a \equiv b \pmod{(u)} \Leftrightarrow a - b \in (u) \Leftrightarrow a - b = cu \Leftrightarrow a \equiv b \pmod u$.

Не все идеалы являются главными.

**Примеры.**

1. В кольце $K[x,y]$ ($K$ — поле) идеал $I = \{f \in K[x,y] : f(0,0) = 0\}$ не является главным.

Целостное кольцо $A$, не являющееся полем, называется *евклидовым кольцом*, если задано отображение $N\colon A\setminus\{0\} \to \mathbb{Z}_+$ (которое называется *нормой*), удовлетворяющее условиям

1) $N(ab) \geqslant N(a)$, причем равенство достигается $\Leftrightarrow$ $b$ обратим,

2) $\forall\, a \in b,\ \forall\, b \in A \setminus \{0\}\ \ \exists\, q, r \in A : a = bq + r$ и либо $r = 0$, либо $N(r) < N(b)$.

**Теорема 15.3.** *В евклидовом кольце всякий идеал главный.*

*Доказательство.* Пусть $I$ — идеал евклидова кольца $A$. Если $I = 0$, то $I = (0)$. Если $I \neq 0$, то пусть $u \in I$ — элемент наименьшей нормы. Тогда $I \supset (u)$. Докажем, что на самом деле $I = (u)$. Пусть $a \in I$, тогда $a = qu + r$, где $r = 0$ или $N(r) < N(u)$. Но $r = a - qu \in I \Rightarrow r = 0$. □

## Лекция 16.

$a \equiv b \pmod{(u)} \Leftrightarrow a \equiv b \pmod{u}$. Т.о., факторкольцо $A/(u)$ — это то же самое, что кольцо вычетов по модулю $u$. Например, $\mathbb{Z}/(n) = \mathbb{Z}_n$.

**Теорема 15.4.** *Пусть $A$ — евклидово кольцо и $u \in A$. Тогда $A/(u)$ является полем $\Leftrightarrow$ $u$ — простой элемент.*

*Доказательство.* 1) Если $u = 0$, то $A/(u) = A$ — не поле по определению евклидова кольца.

2) Если $u$ обратим, то $(u) = A$ и $A/(u) = \{0\}$ — не поле по определению поля.

3) Если $u = v \cdot w$, где $v$ и $w$ необратимы, то $[v] \cdot [w] = 0$ в $A/(u)$. Но $[v], [w] \neq 0$, т.к. $v$ и $w$ не делятся на $u$. Значит, $A/(u)$ — не поле.

4) Пусть $u$ — простой элемент, $a \notin (u)$. Тогда $(a,u) = 1 \Rightarrow \exists\, x, y \in A : ax + uy = 1 \Rightarrow [a] \cdot [x] = 1$, т.е. $[x] = [a]^{-1}$. Значит, $A/(u)$ — поле. □

Применим эту теорему к кольцу многочленов $K[x]$ над полем $K$. Получаем, что $K[x]/(f(x))$ — поле $\Leftrightarrow$ $f(x)$ — неприводимый многочлен.

Пусть $f(x)$ — любой многочлен степени $n > 0$. Тогда для $a, b \in K$ $a \equiv b \pmod{f(x)} \Leftrightarrow a = b$. Следовательно, $K$ вкладывается в кольцо $K[x]/(f(x)) = L$. Будем отождествлять элемент $a \in K$ с $[a] \in L$. Введем обозначение: $\alpha = [x] \in L$. Тогда $f(\alpha) = [f(x)] = 0$, т.е. $\alpha$ — корень многочлена $f(x)$. Если $f(x)$ неприводим, то $L$ — поле. Говорят, что $L$ получается из $K$ *присоединением корня многочлена* $f(x)$.

В силу единственности деления с остатком в кольце $K[x]$ в каждом классе $g(x) + f(x)$ имеется единственный многочлен степени меньше $\deg f(x)$. Это означает, что каждый элемент кольца $L$ единственным образом представляется в виде $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ $(a_0, \ldots, a_{n-1} \in K)$.

Кольцо $L$ можно рассматривать как векторное пространство над $K$. Из предыдущего следует, что $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ — базис этого пространства, и, значит, $\dim_K L = n$.

**Примеры.**

1. $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$.

2. $\mathbb{Q}[x]/(x^3 - 2) = \{a_0 + a_1\alpha + a_2\alpha^2 : a_0, a_1, a_2 \in \mathbb{Q}, \alpha^3 = 2\}$. В поле $L = \mathbb{Q}[x]/(x^3 - 2)$ многочлен $x^3 - 2$ имеет ровно один корень.

Расширение $L$ поля $K$ называется *конечным*, если $\dim_K L < \infty$.

**Примеры.**

1. $\mathbb{R} \supset \mathbb{Q}$.

2. $K(x) \supset K$.

Пусть $F$ — конечное поле характеристики $p$. Тогда $\langle 1 \rangle$ (аддитивная подгруппа, порожденная 1) есть подкольцо: $(\underbrace{1 + \ldots + 1}_{k}) \cdot (\underbrace{1 + \ldots + 1}_{l}) =$ $= (\underbrace{1 + \ldots + 1}_{kl})$. Более того, это подполе, изоморфное $\mathbb{Z}_p$:

$$[k]_p \leftrightarrow \underbrace{1 + \ldots + 1}_{k}.$$

Т.о., $F \supset \mathbb{Z}_p$, и, следовательно, $|F| = p^n$.

Построим поле из $p^2$ элементов. $F = \mathbb{Z}_p[x]/(f(x))$, где $f(x) \in \mathbb{Z}_p[x]$ — неприводимый многочлен степени 2.

Если $p \neq 2$, то $\mathbb{Z}_p^*$ — циклическая группа четного порядка $p-1$. Ровно половина ее элементов являются квадратами. Пусть $a \in \mathbb{Z}_p^*$ — квадратичный невычет. Тогда $x^2 - a$ не имеет корней в $\mathbb{Z}_p$ и, следовательно, неприводим.

Если $p = 2$, то можно взять $f(x) = x^2 + x + 1$.

На самом деле, верна

**Теорема 15.5** (Без доказательства)**.** *Для любого простого $p$ и $\forall\, n \in \mathbb{N}$ существует поле из $p^n$ элементов. Более того, все такие поля изоморфны.*