ЛЕКЦИИ ПО АЛГЕБРЕ

И. А. Чубаров

Настоящий курс лекций был прочитан в 2022 году
И. А. Чубаровым для слушателей вечернего отделения;
оформлен с разрешения автора М. С. Тимошик.

Лекция 1

Систематика алгебраических структур

1.1 Структуры с одной бинарной операцией

Определение 1.1. *На X задана бинарная операция $\star$, если $\forall x_1, x_2 \in X$ выполнено $(x_1, x_2) \mapsto x_1 \star x_2 \in X$.*

Название	**Аксиомы**	**Примеры**
Группоид	—	$X = V_3$ - геометрические векторы, $\bar{a} \star \bar{b} := [\bar{a}, \bar{b}]$; $X = \mathbb{N}, x \star y = x^y$
Полугруппа	1. Ассоциативность: $(x_1 \star x_2) \star x_3 = x_1 \star (x_2 \star x_3)$, $\forall x_1, x_2, x_3 \in X$	$(\mathbb{N}, +)$; $(\mathbb{N} \setminus \{1\}, \cdot)$; $(\{A_{n\times n} \mid \det A = 0\}, \cdot)$
Моноид	1. Ассоциативность. 2. $\exists e \in X$: $e \star x = x \star e = x, \forall x \in X$.	$(\mathbb{Z}, \cdot)$; $M_n(\mathbb{R}), n \geq 2$; $\{f : A \to A, (f_1 \cdot f_2)(a) = f_1(f_2)(a))\}$
Группа	1. Ассоциативность. 2. $\exists e \in X$. 3. $\forall x \in X \exists x^{-1} \in X$: $x \star x^{-1} = x^{-1} \star x = e$ 4. Коммутативность (не обязательно): $x_1 \star x_2 = x_2 \star x_1$	$(GL(n, \mathbb{R}) = \{A_{n\times n} \mid \det A \neq 0\}, \cdot)$; $(SL(n, \mathbb{R}) = \{A_{n\times n} \mid \det A = 1\}, \cdot)$; $(S_n = \{\sigma : X_n \to X_n\}, \cdot)$, биективное отображение = подстановка; $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, +)$; $(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^*, \mathbb{C}^*, \cdot)$

1.2 Структуры с двумя бинарными операциями $\{+, \cdot\}$

Название	**Аксиомы**	**Примеры**
Кольцо	1. $(X, +)$ — коммутативная группа. 2. $(X, \cdot)$ — группоид. 3. Дистрибутивность: $x_1 \cdot (x_2 + x_3) = x_1 \cdot x_2 + x_1 \cdot x_3$ $(x_2 + x_3) \cdot x_1 = x_2 \cdot x_1 + x_3 \cdot x_1$	$X = (V_3, +, [,])$ (оно является кольцом Ли) $[[x_1, x_2], x_3] +$ $+[[x_3, x_1], x_2] +$ $+[[x_2, x_3], x_1] = 0$ (тождество Якоби)
	Дополнительные требования к $\{\cdot\}$:	
Ассоциативное кольцо	Ассоциативность, т. е. $(X, \cdot)$ — это полугруппа	$(\mathbb{R}[x], +, \cdot)$ (но с 1, коммутативно) $(M_n(\mathbb{R}), +, \cdot)$ (но с E)
Кольцо с единицей	$\exists 1 \in X$: $1 \cdot x = x \cdot 1 = x, \forall x \in X$	
Ассоциативное кольцо с единицей	Ассоциативность, $\exists 1$	
Ассоциативное коммутативное кольцо с единицей	Ассоциативность, $\exists 1$, коммутативность	($\mathbb{Z}_n$ или $\mathbb{Z}, +, \cdot$)

Определение 1.2. *Пусть R (ring) — ассоциативное кольцо с 1. Элемент $x \in R$ называется обратимым, если $\exists x^{-1} \in R$ такой, что $x^{-1} \cdot x = x \cdot x^{-1} = 1$.*

Определение 1.3. *Пусть R — произвольное кольцо. Элемент $x \in R$ называется делителем нуля (обозначение: $x \mid 0$), если $x \neq 0$, и $\exists y \neq 0$ или $z \neq 0$ такие, что:*

$$\begin{cases} x \cdot y = 0 & (1) \\ z \cdot x = 0 & (2) \end{cases}$$

Если выполнено только (1), то x — левый делитель 0, а если только (2), то x — правый делитель 0.

Название	**Аксиомы**	**Примеры**
Кольцо с делением (тело)	Ассоциативное кольцо с 1, $\forall x \in R, x \neq 0 \quad \exists x^{-1} \in R$	поля; $\mathbb{Z}_p, p$ — простое $\mathbb{H}$ — гамильтоновы кватернионы
Поле K	I. $(K, +)$ — абелева группа (аддитивная группа поля) II. $(K \setminus 0 = K^*, \cdot)$ — коммутативная группа (в частности, $1 \neq 0$) III. Дистрибутивность	$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$; $\mathbb{Z}_p$; $\mathbb{R}(x)$ — рациональные дроби: $\frac{f(x)}{g(x)}$, $f(x), g(x)$ — многочлены над $\mathbb{R}$ и $g(x) \neq 0$

1.3 Подгруппы

Определение 1.4.

Подгруппа.

Пусть G — группа, $\emptyset \neq H \subseteq G$. H — подгруппа, если:

$$1)\forall h_1, h_2 \in H \quad \exists h_1 * h_2 \in H,$$
$$2)\forall h \in H \Rightarrow h^{-1} \in H.$$

Подкольцо.

Пусть $(R, +, \cdot)$ — кольцо и $S \subseteq R$. S - подкольцо, если:

$$1)(S, +) \text{ — подгруппа в } (R, +),$$
$$2)(S, \cdot) \text{ — подгруппоид (подполугруппа ...)}$$

1.4 Группы и их подгруппы

Определение 1.5. *$(G, \cdot)$ — группа, если:*

$1)\forall g_1, g_2, g_3 \in G$: $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ (*ассоциативность умножения*);
$2)\exists e \in G$: $e \cdot g = g \cdot e = g, \forall g \in G$ (e *— нейтральный элемент*);
$3)\forall g \in G\ \exists g^{-1} \in G$: $g^{-1} \cdot g = g \cdot g^{-1} = e$ (*существование обратного элемента*).
Необязательная аксиома:
$4)$*коммутативность (абелевость):* $g_1 \cdot g_2 = g_2 \cdot g_1$.

Следствия.

1) e единственен.

2) $\forall g \in G, g^{-1}$ единственен.

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

4) Обобщенная ассоциативность: произведение $g_1 \cdot g_2 \cdot \ldots \cdot g_n (n \geq 4)$ не зависит от расстановки скобок, можно доказать, что $g_1 \cdot g_2 \cdot \ldots \cdot g_n = (\ldots(((g_1 \cdot g_2) \cdot g_3) \cdot g_4 \cdot \ldots) \cdot g_n$. Например, для $n = 4$: $g_1 \cdot ((g_2 \cdot g_3) \cdot g_4) = (g_1 \cdot g_2) \cdot (g_3 \cdot g_4)$.

Доказательство. 1) Допустим, что $\exists e'$ — "другой" нейтральный элемент. Рассмотрим $e = e \cdot e' = e' \Rightarrow e = e'$.

2) Допустим, что g' и g'' два обратных к g элемента. Тогда рассмотрим: $g' \cdot g \cdot g''$. С одной стороны, $g' \cdot g \cdot g'' = g' \cdot (g \cdot g'') = g' \cdot e = g'$. С другой стороны, $g' \cdot g \cdot g'' = (g' \cdot g) \cdot g'' = e \cdot g'' = g''$. Таким образом $g' = g''$.

3) Достаточно доказать, что для $(g_1 \cdot g_2) \cdot (g_2^{-1} \cdot g_1^{-1}) = e$ имеем $g_1 \cdot (g_2 \cdot g_2^{-1}) \cdot g_1^{-1} = g_1 \cdot e \cdot g_1^{-1} = e$; точно также и в другом порядке. □

Определение 1.6. *Пусть $a \in G, m$ — целое число. Тогда*

$$a^m = \begin{cases} \underbrace{a \cdot a \cdot \ldots \cdot a}_{m}, & \text{если } m > 0 \\ e, & \text{если } m = 0 \\ (a^{-m})^{-1}, & \text{если } m < 0. \end{cases}$$

Теорема 1.1. *1)* $a^m \cdot a^n = a^{m+n}, m, n \in \mathbb{Z}$; *2)* $(a^m)^p = a^{mp}$

Доказательство. Очевидно. □

1.5 Подгруппы

Определение 1.7. *Пусть* G *— группа, тогда* $\emptyset \neq H \subseteq G$ *— подгруппа в* G*, если:*

$$1)\forall h_1, h_2 \in H \Rightarrow h_1 \cdot h_2 \in H \text{ и}$$
$$2)\forall h \in H \Rightarrow h^{-1} \in H.$$

Заметим, что если $h \in H \Rightarrow h^{-1} \in H \Rightarrow h \cdot h^{-1} = e_G \in H$, т. е. H содержит нейтральный элемент всей группы G, и e_G будет нейтральным элементом в H. Стандартное обозначение: $H \leqslant G$ будет обозначать, что H — подгруппа в G (возможно, что $H = G$). Для $H \neq G$ применяется обозначение $H < G$.

Теорема 1.2.
1) Если H_1, H_2 *— подгруппы в* G*, то* $H_1 \cap H_2$ *— тоже подгруппа.*
2) $H_1 \cdot H_2 = \{h_1 \cdot h_2 \mid h_1 \in H_1, h_2 \in H_2\}$ *(не всегда является подгруппой).*
3) Если $H_1 \cdot H_2 = H_2 \cdot H_1$*, (т. е.* $\{h_1 \cdot h_2 \mid h_1 \in H_1, h_2 \in H_2\} = \{h_2' \cdot h_1' \mid h_1' \in H_1, h_2' \in H_2\}$*), то* $H_1 \cdot H_2$ *— подгруппа в* G*.*

Доказательство. 1) $H_1 \cap H_2 = \{g \in G \mid g \in H_1, H_2 \Rightarrow e_G \in H_1 \cap H_2$, т. к. $e_G \in H_1$ и $e_G \in H_2$.
i) $\forall a, b \in H_1 \cap H_2 \Rightarrow a \cdot b \in H_1$ и $H_2 \Rightarrow a \cdot b \in H_1 \cap H_2$;
ii) если $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ и $a \in H_2 \Rightarrow a^{-1} \in H_1$ и $a^{-1} \in H_2 \Rightarrow a^{-1} \in H_1 \cap H_2$.
2) Рассмотрим группу $G = SL(2, \mathbb{Z}_2) =$

$$\left\{e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, d = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, f = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right\}$$

Рассмотрим $H_1 = \{E, a\}, H_2 = \{E, b\} \Rightarrow H_1 \cdot H_2 = \{E, a, b, a \cdot b = f\}$ — подгруппа ли это? $f^{-1} = f^2 = d \notin H_1 \cdot H_2$ — не подгруппа.
3) Пусть $H_1 \cdot H_2 = H_2 \cdot H_1$.
i) $(h_1 \cdot h_2) \cdot (h_1' \cdot h_2') = h_1 \cdot (h_2 \cdot h_1') \cdot h_2' = h_1 \cdot (h_1'' \cdot h_2'') \cdot h_2' = (h_1 \cdot h_1'') \cdot (h_2'' \cdot h_2') \in H_1 \cdot H_2$.
ii) $(h_1 \cdot h_2)^{-1} = h_2^{-1} \cdot h_1^{-1} \in H_2 \cdot H_1 = H_1 \cdot H_2 \Rightarrow h_2^{-1} \cdot h_1^{-1} = h_1' \cdot h_2' \in H_1 \cdot H_2 \Rightarrow (h_1 \cdot h_2)^{-1} \in H_1 \cdot H_2$.
Таким образом $H_1 \cdot H_2$ — подгруппа в G. □

1.6 Циклические подгруппы и группы

Определение 1.8. *Пусть* G *— группа,* $a \in G$*. Рассмотрим* $\langle a \rangle \overset{опр.}{=} \{a^k \mid k \in \mathbb{Z}\}$.

Теорема 1.3. *Множество* $\langle a \rangle$ *с соответствующим умножением является подгруппой в* G*.*

Доказательство. i) $\forall k, l \in \mathbb{Z}$, $a^k a^l = a^{k+l} \in \langle a \rangle$, ii) $(a^k)^{-1} = a^{-k} \in \langle a \rangle$. $\square$

Определение 1.9. *Подгруппа $\langle a \rangle$ называется циклической подгруппой, порожденной элементом a, при этом сам элемент a называется порождающим элементом этой подгруппы.*

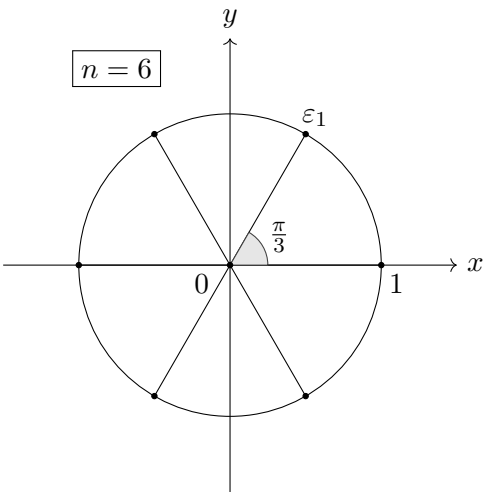
Если $\exists a \in G$ такой, что $\langle a \rangle = G$, т. е. $G = \{a^k \mid k \in \mathbb{Z}\}$, то G — циклическая группа, порожденная элементом a.

Примеры. 1) $\mathbb{Z}_n, n \in \mathbb{N}$ — группа по сложению классов вычетов по модулю n.

Для $k \in \mathbb{Z}$ обозначим $\bar{k} = \{k + nt \mid t \in \mathbb{Z}$ — все целые числа, равноостаточные с k, рассматриваемые как один элемент множества $\mathbb{Z}_n$.

Сложение: $\bar{k} + \bar{l} = \overline{k+l}$, т. к. $(k + nt_1) + (l + nt_2) = k + l + n(t_1 + t_2)$.

Возьмем $a = \bar{1}$, тогда для $\forall k\colon 0 \leqslant k \leqslant n-1, ka = \bar{1} + \cdots + \bar{1} = \bar{k} \Rightarrow \mathbb{Z}_n = \langle \bar{1} \rangle$.



2) $(\mathbb{Z}, +) = \langle 1 \rangle$.

3) $U_n = \sqrt[n]{1} = \{\cos(\frac{2\pi k}{n}) + i \sin(\frac{2\pi k}{n}) \mid k = 0, \ldots, n-1\}$. Обозначим $\varepsilon_1 = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n}) \Rightarrow \varepsilon_k = \cos(\frac{2\pi k}{n}) + i \sin(\frac{2\pi k}{n}) = \varepsilon_1^k$ (по формуле Муавра) $\Rightarrow U_n = \langle \varepsilon_1 \rangle$[1].

1.7 Циклические группы

Теорема 1.4. *В циклической группе любая подгруппа является циклической.*

Доказательство.

Дано: $G = \langle a \rangle$, т. е. $\forall g \in G\ \exists k \in \mathbb{Z}\colon g = a^k$. Пусть $H \leqslant G$ — подгруппа ($|H| \geqslant 1$) $\Rightarrow \forall h \in H\ \exists l \in \mathbb{Z}\colon h = a^l$. Выберем $b = a^q$, где $q = \min\{l \in \mathbb{N} \mid a^l \in H\}$ (заметим, что если $a^l \in H$ и $l \leq 0$, то $(a^l)^{-1} = a^{-l} \in H$ и $-l \geqslant 0$)[2].

Покажем, что $\forall h \in H\ \exists m \in \mathbb{Z}$ такие, что $h = b^m$, т. е. $H = \langle b \rangle$.

[1] На приведенном выше рисунке $n = 6$.

[2] В любом непустом множестве натуральных чисел найдется единственное наименьшее число.

Пусть $h = a^l$. Разделим l с остатком на q: $l = p \cdot q + r, p \in \mathbb{Z}, 0 \leqslant r < q$, тогда $h = a^l = (a^q)^p \cdot a^r$, здесь $h \in H, a^q \in H$ по выбору $q \Rightarrow (a^q)^p \in H \Rightarrow a^r = h \cdot (a^{qp})^{-1} \in H$, но $r < q \Rightarrow r = 0$, значит, $h = b^p$. $\square$

Лекция 2

Определение 2.1. *Пусть* $(G_1, \cdot)$ *и* $(G_2, \star)$ *— группы. Отображение* $\varphi\colon G_1 \to G_2$ *называется гомоморфизмом групп (*G_1 *в группу* G_2*), если:*

$$\forall a, b \in G_1 \Rightarrow \varphi(a \cdot b) = \varphi(a) \star \varphi(b).$$

Это отображение φ *называется изоморфизмом, если* φ *биективно (взаимно однозначно). Группы называются изоморфными, если существует изоморфизм* $\varphi\colon G_1 \to G_2$.

Теорема 2.1. *Любые две циклические группы одинакового порядка изоморфны между собой. Точнее, если* G_1 *и* G_2 *— циклические группы с одинаковым количеством элементов, т. е.* $|G_1| = |G_2|$, *то они изоморфны (либо* $|G_1| = |G_2| = n$, *либо обе бесконечны).*

Доказательство. Докажем, что если $|G| = \infty$, то $G \cong \mathbb{Z}$ (по сложению), а если $|G| = n$, то $G \cong \mathbb{Z}_n$ (по сложению).

Т. к. группа G циклическая, то $\forall g \in G\ \exists k \in \mathbb{Z}\colon g = a^k$, где a — порождающий элемент.

Пусть $|G| = \infty$, тогда любой элемент g записывается в виде a^k единственным образом: если $a^k = a^l, k > l$, то $a^{k-l} = e$, обозначим $m = k - l$, тогда все элементы группы G содержатся среди $e = a^0, a, a^2, \ldots, a^{m-1}$, потом степени периодически повторяются $\Rightarrow k = l$.

Определим отображение $\varphi\colon \mathbb{Z} \to G$ формулой $\varphi(k) = a^k$. По доказанному, это отображение взаимно однозначно. Кроме того, φ — гомоморфизм: $\varphi(k+l) = a^{k+l} = a^k \cdot a^l = \varphi(k) \cdot \varphi(l) \Rightarrow$ Утверждение верно. Таким образом, φ — изоморфизм: $\mathbb{Z} \cong G$.

Пусть теперь $|G| = n$, т. е. $G = \{e = a^0, a, a^2, \ldots, a^{n-1}\}$ $(a^n = e)$. Тогда посмотрим, при каком условии $a^k = a^l, k > l \Rightarrow a^{k-l} = e \Rightarrow (k-l) \vdots n$. В самом деле, разделим $k-l$ с остатком на n: $k-l = nq+r, 0 \leqslant r < n \Rightarrow a^{k-l} = e = a^{nq+r} = (a^n)^q \cdot a^r = a^r \Rightarrow a^r = e$. По определению порядка элемента a $r \leqslant n$ только если $r = 0 \Rightarrow k - l = n$, то есть $k = l + nq$, то есть k и l сравнимы по модулю n (принадлежат одному классу вычетов по модулю n).

Но группа $\mathbb{Z}_n$ определялась, как группа классов вычетов $\bar{0} = \{nq \mid q \in \mathbb{Z}\}$, $\bar{1} = \{1 + nq \mid q \in \mathbb{Z}\}$, $\ldots$, $\overline{n-1} = \{n - 1 + nq \mid q \in \mathbb{Z}\}$ с правилом сложения: $\bar{k} + \bar{l} \overset{\text{опр.}}{=} \overline{k+l}$, то есть, если число из класса $\bar{k}$ имеет вид $a = k + nq$, а число из

класса $\bar{l}$ имеет вид $b = l + np$, $q, p \in \mathbb{Z}$, то число $a + b = k + l + n(q + p)$ принадлежит классу числа $k + l$.

Определим $\varphi\colon \mathbb{Z}_n \to G, \varphi(\bar{k}) = a^k$, тогда φ — искомый изоморфизм по доказанному выше. □

2.1 Некоторые примеры групп

(1) Группы чисел по сложению (аддитивные группы).

$$\mathbb{Z} \subset \mathbb{Q} = \left\{ \frac{m}{n}, m \in \mathbb{Z}, n \in \mathbb{N} \right\} \subset \mathbb{R} \subset \mathbb{C},$$

где каждая группа, кроме $\mathbb{C}$, является подгруппой во всех группах, записанных правее.

(2) Группы чисел по умножению (мультипликативные группы).

$$\mathbb{Z}^* = \{1, -1\} \subset \mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \subset \mathbb{R}^* = \mathbb{R} \setminus \{0\} \subset \mathbb{C}^* = \mathbb{C} \setminus \{0\},$$

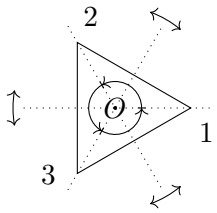
где каждая группа, кроме $\mathbb{C}^*$, является подгруппой во всех группах, записанных правее.

(3) $\mathbb{Z}_n$ — группа классов вычетов целых чисел по модулю n. Это циклическая группа. Любой класс $\bar{k} = \underbrace{\bar{1} + \cdots + \bar{1}}_{k}, 1 \leqslant k \leqslant n - 1$, так что $\bar{1}$ — порождающий элемент этой группы.

Группы (1) – (3) являются абелевыми группами.

(4) Группа диэдра D_n всех движений плоскости[1], которые переводят в себя некоторый правильный n-угольник.

2.1.1 Группа правильного треугольника



O – центр $\triangle$

Треугольник $\triangle$ можно повернуть вокруг точки O на углы $\alpha = 0, \frac{2}{3}\pi (= 120°)$ и $-\frac{2}{3}\pi = \frac{4}{3}\pi (= 240°)$. Повороты образуют группу C_3 — группу вращений треугольника. Можно делать симметрии относительно высот (осей симметрии). Относительно оси, проходящей через вершину (1): (1) → (1), (2) ↔ (3). Таких симметрий тоже 3.

$$D_3 = \{e, a = R_0^{\frac{2}{3}\pi}, a^2 = a^{-1} = R_0^{-\frac{2}{3}\pi}, s_1, s_2, s_3 - \text{симметрии}\}.$$

[1] Движение — преобразование плоскости, которое сохраняет расстояния между точками и, следовательно величины углов между отрезками.

В общем случае группа D_n состоит из n поворотов вокруг центра на углы $\frac{2\pi k}{n}, k = 0, 1, \ldots, n-1$ — это группа вращений C_n и n симметрий относительно осей.

Задача. Доказать, что $D_3 \cong S_3$ всех подстановок множества $\{1, 2, 3\}$.

Решение. Вспомним определение группы S_3. S_3 — множество всевозможных подстановок, т. е. биективных отображений $\{1, 2, 3\} \to \{1, 2, 3\}$. Любое отображение σ можно задать таблицей:

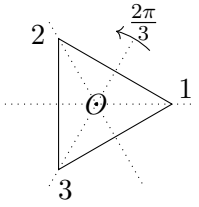
$$\begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix}, \text{ где } i_1 = \sigma(1), i_2 = \sigma(2), i_3 = \sigma(3).$$

Т. к. числа (i_1, i_2, i_3) — произвольная перестановка чисел $(1, 2, 3)$, то таких подстановок столько же, сколько перестановок, т. е. $3! = 6$.

Запишем их все:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \underbrace{\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{\text{циклические подстановки длины 3}},$$

$$\underbrace{\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}_{\text{транспозиции}}.$$



Установим соответствия: $R_0^{\frac{2}{3}\pi} \leftrightarrow \sigma_2, R_0^{-\frac{2}{3}\pi} \leftrightarrow \sigma_1$. Симметриям соответствуют транспозиции, например, $s_1 \leftrightarrow \sigma_4$, и так далее. Кроме этого, композиция движений отвечает произведению соответствующих подстановок, т. е. установлен изоморфизм.

(5) Симметрическая группа S_n — группа всех подстановок степени n, на множестве $X_n = \{1, 2, \ldots, n\}$. Любая подстановка $\sigma\colon X_n \to X_n$ задаётся таблицей:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ i_1 & i_2 & \cdots & i_k & \cdots & i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(k) & \cdots & \sigma(n) \end{pmatrix}.$$

Операция в S_n — композиция (= произведение) отображений, т. е. если $X_n \xrightarrow{\sigma} X_n \xrightarrow{\tau} X_n$, то $(\tau \cdot \sigma)(i) = \tau(\sigma(i))$. Эта операция ассоциативна; $\exists$ "единица" — тождественное отображение; для любого $\sigma \in S_n$ $\exists$ обратное σ^{-1} такое, что если $y = \sigma(x)$, то $\sigma^{-1}(y) = x$. Получается группа.

Вспомним правило перемножения подстановок, записанных как таблица. Подстановка (перестановка из 2-й строки) *чётная*, если в ней есть чётное число инверсий, *нечётная*, если число инверсий нечётно.

Знак подстановки $\operatorname{sign}(\sigma) \overset{\text{опр.}}{=} (-1)^{inv(\sigma)}$, где $inv(\sigma)$ — число инверсий, поэтому $\operatorname{sign}(\sigma) = 1$, если σ чётная, и $\operatorname{sign}(\sigma) = -1$, если σ нечётная.

Свойство: $\operatorname{sign}(\sigma \cdot \tau) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau)$.[2]

Обозначение: Множество $A_n \overset{\text{опр.}}{=} \{\sigma \in S_n \mid \sigma - \text{ чётная}\}$ является подгруппой в S_n. В самом деле: $\sigma, \tau \in A_n \Rightarrow \sigma \cdot \tau \in A_n$; $\sigma^{-1} \in A_n$. Группа A_n называется знакопеременной группой. Кроме того:

$$|S_n| = n!, \quad |A_n| = \frac{1}{2}n!$$

2.2 Смежные классы по подгруппе. Теорема Лагранжа

Определение 2.2. *Пусть G — группа, $H \leqslant G$ — некоторая подгруппа в G. Множество элементов $gH = \{gh \mid h \in H\}$ называется левым смежным классом по подгруппе H, порожденным элементом g.*

Аналогично, определяется $Hg = \{hg \mid h \in H\}$ — правый смежный класс.

Лемма 2.1.

1. Пусть G — группа, $H \leqslant G$ — некоторая подгруппа в G. Тогда:

$$\begin{aligned} g_1H = g_2H &\quad \Leftrightarrow \quad g_2^{-1}g_1 \in H, \\ Hg_1 = Hg_2 &\quad \Leftrightarrow \quad g_1^{-1}g_2 \in H. \end{aligned}$$

2. Если aH и bH — различные, то $aH \cap bH = \emptyset$. Аналогичное утверждение выполнено для правых смежных классов.

Доказательство.

1. Докажем утверждение для левых смежных классов. Поскольку $g_1H = g_2H$, то $\exists h_1, h_2 \in H\colon g_1h_1 = g_2h_2$. Умножим последнее равенство слева на g_2^{-1}, а справа на h_1^{-1}:

$$g_2^{-1}\cdot \mid g_1h_1 = g_2h_2 \mid \cdot h_1^{-1} \Rightarrow g_2^{-1}g_1h_1 = h_2 \Rightarrow g_2^{-1}g_1 = h_2h_1^{-1} \in H.$$

Обратно: пусть $\exists h_0 \in H$ такой, что $g_2^{-1}g_1 = h_0 \Rightarrow g_1 = g_2h_0$. Умножая на произвольный $h \in H \Rightarrow g_1h = g_2(h_0h), h_0h \in H \Rightarrow g_1H = g_2H$.

2. Допустим, что $c \in aH \cap bH$, и покажем, что $aH = bH$. По условию существуют $h_1, h_2 \in H$ такие, что $c = ah_1 = bh_2 \Rightarrow b^{-1}ah_1 = h_2 \Rightarrow b^{-1}a = h_2h_1^{-1} \in H$, а по пункту 1 это значит, что $aH = bH$ — противоречие условию $\Rightarrow aH \cap bH = \emptyset$. □

Теорема 2.2 (Теорема Лагранжа)**.**

1. Если $H \leqslant G$, то группа G разбивается как на попарно непересекающиеся левые смежные классы: $G = \bigsqcup\limits_{i \in I} g_iH$, так и на попарно непересекающиеся правые смежные классы: $G = \bigsqcup\limits_{i \in I} Hg_i'$. Причем количества левых и правых смежных классов одинаковы и равны мощности множества I.

2. $\forall g \in G, |gH| = |Hg| = |H|$ (равенство порядков, если H конечная, либо равенство мощностей).

[2] Будем использовать как известное.

Следствие 2.1 (Арифметическая теорема Лагранжа)**.**
Если $|G| < \infty$ *и* $H \leqslant G$, *то* $|H|$ *делит* $|G|$.

Доказательство. 1. Любой элемент $g \in G$ принадлежит классу gH $(g = g \cdot e)$ и классу $Hg \Rightarrow G = \bigcup\limits_{g \in G} gH = \bigcup\limits_{g' \in G} Hg'$. Если в каждом классе (левом) выбрать по одному элементу (представителю своего класса) и как-либо занумеровать их, наберутся элементы g_i, и тогда $g_iH \cap g_jH = \emptyset, i \neq j$ — первое разбиение.

Аналогично, можно выбрать и занумеровать элементы g'_k в разных правых классах, тогда $Hg_k \cap Hg_l = \emptyset, k \neq l$ — второе разбиение. Установим взаимно однозначное соответствие между классами $gH \leftrightarrow Hg^{-1}$ (если $g_1H \cap g_2H = \emptyset$, то $Hg_1^{-1} \cap Hg_2^{-1} = \emptyset$) это покажет, что представителей правых классов $\{g'\}$ столько же, сколько и левых.

Рассмотрим $\tau\colon G \to G, \tau(g) = g^{-1}$ — это биекция, $\tau^{-1}(g^{-1}) = g$, т. е. $\tau = \tau^{-1} \Rightarrow$ биективное отображение $\bar{\tau}\colon gH \mapsto Hg^{-1}; \tau\colon gh \mapsto (gh)^{-1} = h^{-1}g^{-1} \in Hg^{-1}$.

2. Чтобы доказать, что $|gH| = |H|$, рассмотрим отображение $f_l\colon G \to G, f_l(x) = gx, \forall x \in G (g$ — фиксировано). Отображение f_l является биекцией, т. к. $f_l^{-1}(y) = g^{-1}y, \forall y \in G$. При биекции мощности сохраняются. Для $|Hg| = |H|$ надо рассмотреть $f_r\colon G \to G, f_r(x) = xg, \forall x \in G$. □

Доказательство следствия. Пусть $|G| < \infty, H < G \Rightarrow$ т. к. G содержит конечное число элементов, то и множество смежных классов конечно, т. е. $|I| = r \in \mathbb{N}$.

Имеем: $G = \bigsqcup\limits_{i=1}^{r} g_iH$, и т. к. классы попарно не пересекаются, то $|G| = \sum\limits_{i=1}^{r} |g_iH| = \sum\limits_{i=1}^{r} |H| = r\,|H|$, т. е. $\frac{|G|}{|H|} = r$ — число смежных классов.

Аналогично, $G = \bigsqcup\limits_{i=1}^{r} Hg'_i \Rightarrow |G| = \sum\limits_{i=1}^{r} |Hg'_i| = \sum\limits_{i=1}^{r} |H| = r\,|H|$. Таким образом r — количество как левых, так и правых смежных классов, r называется *индексом* подгруппы в группе G, и обозначается как: $r = |G : H|$. □

Вопрос. Есть ли в группе S_4 подгруппа порядка 9?

$|S_4| = 24 \not\vdots 9$.

Ответ: нет.

Вопрос. Верна ли "обратная теорема": если $|G| = n$, и m делит n, то в G существует подгруппа H порядка m?

Это заведомо верно, если G — циклическая: если $G = \langle a \rangle$, то $b = a^{\frac{n}{m}}$ порождает подгруппу порядка m, т. к. $b^m = e$, но $b^k \neq e$, где $1 \leqslant k < m$. обдумайте!

2.3 Нормальные подгруппы и факторгруппы

Вообще говоря, $gH \neq Hg$.

Определение 2.3. *Подгруппа* $N < G$ *называется нормальной подгруппой группы* G *(или нормальной в* G*), если:*

$$\forall g \in G,\ gN = Ng. \tag{2.1}$$

Удобно это равенство умножить справа на g^{-1} и получить равносильное условие:

$$gNg^{-1} = N. \tag{2.2}$$

Примеры.

(1) Группа $S_3 = \{(1,2,3),(1,3,2),(1,2),(1,3),(2,3),e\}$.[3] Рассмотрим следующие подгруппы в S_3:

$$A_3 = \{(1,2,3),(1,3,2),e\} \text{ и } H = \{(1,2),e\}.$$

1) Вычислим смежные классы по $N = A_3$.

Один класс — это $N = e \cdot N = N \cdot e$.

$(1,2)N = \{(1,2)\cdot(1,2,3),(1,2)\cdot(1,3,2),(1,2)\cdot e\} = \{(2,3),(1,3),(1,2)\}$

$(1,2)\cdot(1,2,3) = (1)\cdot(2,3) = (2,3), (1,2)\cdot(1,3,2) = (1,3)$.

Очевидно, что $N\cdot(1,2) = \{(2,3),(1,3),(1,2)\} = (1,2)\cdot N$, и это показывает, что $N = A_3$ — нормальная подгруппа.

2) $H = \{(1,2),e\}$. Рассмотрим левые классы: $H, (1,2,3)H$ и $(1,3,2)H$.

$(1,2,3)H = \{(1,2,3),(1,2,3)\cdot(1,2) = (1,3)\}, (1,3,2)H = \{(1,3,2),(2,3)\}$.

С другой стороны:

$H(1,2,3) = \{(1,2,3),(1,2)\cdot(1,2,3) = (2,3)\} \Rightarrow (1,2,3)H \neq H(1,2,3)$, т. е. H не является нормальной подгруппой в G.

(2) $UT_2(A), A = \mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ — унитреугольные (unitriangular) матрицы 2-го порядка:

$$X = \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}, X_1\cdot X_2 = \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & a+b\\ 0 & 1\end{pmatrix}$$

$UT_2(\mathbb{Z}) \cong (\mathbb{Z},+); UT_2(\mathbb{Q}) \cong (\mathbb{Q},+); UT_2(\mathbb{R}) \cong (\mathbb{R},+); UT_2(\mathbb{C}) \cong (\mathbb{C},+)$.

Определим отображение $\varphi\colon \mathbb{Z} \to UT_2(\mathbb{Z}), \varphi(a) = \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$ — это изоморфизм, для которого $\varphi^{-1}\left(\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\right) = a$.

Задача. Доказать, что в группе $G = T_2(A)$, группе верхнетреугольных матриц, подгруппа $N = UT_2(A)$ является нормальной подгруппой.

Д.З.	55.20, 56.16 (а), 56.26, 56.37 (а, в, г, д)[4]

[3] Мы используем здесь не табличную, а циклическую запись подстановок.

[4] Здесь и далее по тексту номера задач указаны для задачника "Сборник задач по алгебре" под ред. А. И. Кострикина — М.: МЦНМО — 2009 г.

Лекция 3

3.1 Дальнейшие примеры нормальных подгрупп. Факторгруппы.

Напоминание. Пусть G — группа, $N \leqslant G$ — подгруппа в G. N — нормальная подгруппа в G, если $\forall g \in G$:

$$gN = Ng \Longleftrightarrow gNg^{-1} = N \quad \text{(обозначение: } N \lhd G)$$

Термин: gNg^{-1} — подгруппа, сопряженная с N с помощью элемента $g \in G$. Индекс подгруппы N в G — количество смежных классов по N.

Теорема 3.1. *Если подгруппа H имеет индекс 2 в G, то $H \lhd G$.*

Доказательство. Имеем: $G = H \bigsqcup gH = H \bigsqcup Hg$, для $\forall g \in G \setminus H$. Берем произвольное $g \in G$; если $g \in H$, то $gH = Hg = H$; если $g \notin H$, то, по условию, $gH = G \setminus H$ и $G \setminus H = Hg$, то есть $gH = Hg$ (при этом $gH \cap H = \emptyset$ и $H \cap Hg = \emptyset$). $\square$

Пример 1. $G = S_n = \left\{ \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \right\}$. Здесь $i_1 = \sigma(1), i_2 = \sigma(2)$, и т. д., причём все $i_1, i_2, \dots, i_n$ различные, так что $(i_1, i_2, \dots, i_n)$ — некоторая перестановка чисел $(1, 2, \dots, n)$.

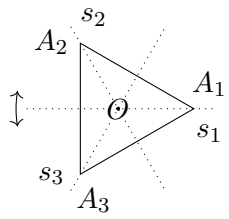
Подмножество чётных подстановок A_n — знакопеременная группа степени n. $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$

Из теоремы Лагранжа следует, что индекс $|S_n : A_n| = \frac{|S_n|}{|A_n|} = 2$. По теореме 3.1, $A_n \lhd S_n$.

Пример 2. $G = D_n$ — группа диэдра степени n.

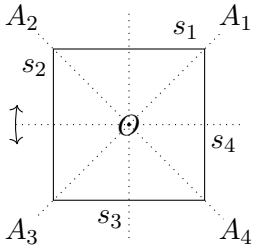
D_n — группа всех поворотов плоскости вокруг центра данного правильного n-угольника и симметрий относительно осей симметрии этого n-угольника, при которых этот многоугольник совмещается с самим собой.

$\boxed{n=3}$



$\angle A_1OA_2 = \angle A_2OA_3 = \angle A_3OA_1 = \frac{2\pi}{n} = \frac{2\pi}{3}$, Углы поворота будут: $\frac{2\pi}{3}, \frac{4\pi}{3}, 0$. Оси симметрии: OA_1, OA_2, OA_3. s_1 — симметрия относительно оси OA_1, тогда $A_2 \leftrightarrow A_3$, $A_1 \leftrightarrow A_1$. $D_3 = \{E, r_\alpha, \alpha = \frac{2\pi}{3}, \frac{4\pi}{3}; s_1, s_2, s_3\}$ — всего $6 = 2 \cdot 3$ элементов.

$\boxed{n=4}$



D_4 — группа квадрата. $D_4 = \left\{r_O^\alpha, \alpha = \frac{2\pi}{4}k = \frac{\pi k}{2}, k = 0,1,2,3; s_1, s_2, s_3, s_4 \text{ — осевые симметрии}\right\}$ s_1 – симметрия относительно диагонали A_1A_3, s_2 — симметрия относительно диагонали A_2A_4, s_3 и s_4 — симметрии относительно средних линий.

Рассмотрим множество поворотов $C_4 = \left\{e, r_O^{\pi/2}, r_O^{\pi}, r_O^{3\pi/2} = r_O^{-\pi/2}\right\}$ — группа вращений квадрата. Это циклическая группа с порождающим элементом $r_O^{\pi/2}$ (поворот на угол $\frac{\pi}{2}$).

Общий случай. Полная группа симметрий правильного $n-$угольника $D_n = \{r_O^\alpha, \alpha = \frac{2\pi}{n}k, k = 0,1,2,\ldots,n-1; s_1, s_2, \ldots, s_n$ — осевые симметрии$\}$. Порядок группы $|D_n| = 2n$, а повороты образуют подгруппу вращений $C_n = \{r_O^\alpha, \alpha = \frac{2\pi}{n}k, k = 0,1,2,\ldots,n-1\} = \langle r_O^{\frac{2\pi}{n}} \rangle$. Т. к. $|D_n| = 2n, |C_n| = n$, то $|D_n : C_n| = \frac{2n}{n} = 2$, и по теореме 3.1 $C_n \lhd D_n$.

3.2 Факторгруппа группы по нормальной подгруппе

Пусть G — группа, $N \lhd G$. Знаем, что $G = \bigsqcup\limits_{i\in I} g_iN = \bigsqcup\limits_{i\in I} Ng_i$. Обозначим через $\bar{g} = gN$ и будем рассматривать $\bar{g}$ как один элемент "укрупненного" множества G/N — множества смежных классов группы G по N (каждый смежный класс — один элемент).

Знакомый пример: $G = \mathbb{Z}, N = n\mathbb{Z}, G/N = \bar{0}, \bar{1}, \ldots, \overline{n-1}$.

Определим на множестве G/N операцию, согласованную с операцией на G. Пусть операция — умножение. Рассмотрим $(g_1N)(g_2N) = \{(g_1n_1)(g_2n_2) \mid n_1, n_2$ — любые элементы из $N\}$. $(g_1n_1)(g_2n_2) = g_1(n_1g_2)n_2 = (g_1g_2)(g_2^{-1}n_1g_2)n_2 = (g_1g_2)(n_1'n_2) \in g_1g_2N$, т. к. $N \lhd G, g_2^{-1}n_1g_2 = n_1' \in N$. На этом основании определим, что произведение[1]:

$$\overline{g_1} \cdot \overline{g_2} = \overline{g_1g_2}.$$

Проверка корректности этого определения.

Пусть g_1' и g_2' — другие представители своих классов, т. е. $g_1N = g_1'N$ и $g_2N = g_2'N$, это значит, что $\overline{g_1} = \overline{g_1}'$, $\overline{g_2} = \overline{g_2}'$.

Покажем, что $g_1g_2N = g_1'g_2'N$, т. е. результат операции не зависит от выбора элементов в классах. $g_1' = g_1n_1, g_2' = g_2n_2 \Rightarrow g_1'g_2' = (g_1n_1)(g_2n_2) = (g_1g_2)(g_2^{-1}n_1g_2)n_2 = (g_1g_2)(n_1'n_2) \in g_1g_2N$.

Значит, при любом $n \in N$

$$(g_1'g_2')n = (g_1g_2)(n_1'n_2n) \Rightarrow g_1'g_2'N = g_1g_2N,$$

что и утверждалось.

Теорема 3.2. *Множество G/N с определенной выше операцией является группой.*

Доказательство. 1) Ассоциативность.

$$(\overline{g_1} \cdot \overline{g_2}) \cdot \overline{g_3} = \overline{g_1g_2} \cdot \overline{g_3} = \overline{(g_1g_2)g_3} = \overline{g_1(g_2g_3)} = \overline{g_1} \cdot \overline{g_2g_3} = \overline{g_1} \cdot \overline{g_2} \cdot \overline{g_3}$$

— верно

2) Единица: $\bar{e} = H$ — класс самой подгруппы, т. к. $\bar{e} \cdot \bar{g} = \overline{eg} = \bar{g}$ — верно (справа — аналогично).

3) Обратный элемент: $(\bar{g})^{-1} = \overline{g^{-1}}$. В самом деле, $\bar{g} \cdot \overline{g^{-1}} = \overline{gg^{-1}} = \bar{e}$, а в пункте 2) проверено, что это единица. □

Замечание. 1) Если группа G абелева, то и факторгруппа G/N будет абелевой, т. к. если $g_1g_2 = g_2g_1$, то $\overline{g_1g_2} = \overline{g_2g_1}$, т. е. $\overline{g_1} \cdot \overline{g_2} = \overline{g_2} \cdot \overline{g_1}$.

2) Если G абелева, то любая подгруппа в G — нормальна.

К семинару. Найти факторгруппу G/N будет означать: а) выяснить, из каких элементов состоят смежные классы; б) установить изоморфизм группы G/N с какой-либо известной группой.

Примеры.

58.32 (а) $G = (\mathbb{C}, +), N = (\mathbb{R}, +)$: $\forall z = x + iy \in \mathbb{C}$, а числа вида $z = x + i \cdot 0$ — подмножество действительных чисел.

Решение. Изучим классы вида $z_0 + \mathbb{R}$, где $z_0 = x_0 + iy_0$, тогда $z_0 + \mathbb{R} = \{z_0 + x \mid x \in \mathbb{R}\} = \{(x_0 + x) + iy_0\}$ (если x меняется, то $x_0 + x$ — любое действительное число). Таким образом, $[z_0] = z_0 + \mathbb{R}$ состоит из всех чисел, у которых мнимая часть y_0 — общая для всех $\Rightarrow z_0 + \mathbb{R} = iy_0 + \mathbb{R}$ — прямая, параллельная оси $\Re(z)$, проходящая через точку $(0, y_0)$. Вся плоскость разбивается на параллельные прямые.

[1] В точности как с группой $(\mathbb{Z}_n, +)$: $\bar{k} + \bar{l} = \overline{k+l}$.

Покажем, что $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$. Определим $\phi(x+iy) = y$. Т. к. $[x+iy] = iy+\mathbb{R}$, то ϕ можно рассматривать как отображение $\phi([x+iy]) = y, \phi\colon \mathbb{C}/\mathbb{R} \to \mathbb{R}$, и это гомоморфизм, т. к. $[x_1+iy_1]+[x_2+iy_2] = [x_1+x_2+i(y_1+y_2)] = [i(y_1+y_2)] \to y_1+y_2$. Вследствие описания смежных классов как прямых, $\phi\colon \mathbb{C}/\mathbb{R} \to \mathbb{R}$ — биекция. Поэтому $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$.

58.32 (в) Пусть $G = \mathbb{C}^*$ группа ненулевых комплексных чисел по умножению, $N = U = \{z \in \mathbb{C} \mid |z| = 1\}$.

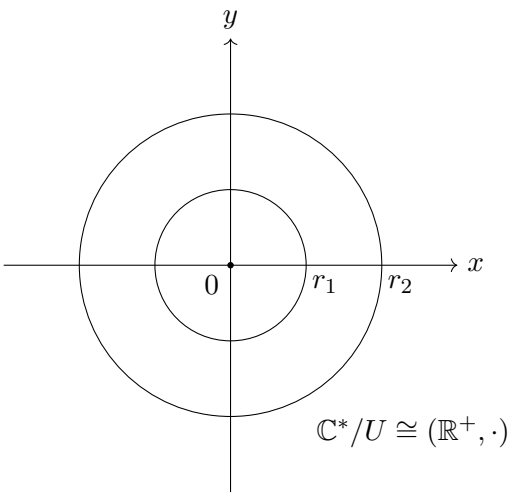
а) Описать смежные классы $\mathbb{C}^*/U$,

б) Показать, что $\mathbb{C}^*/U \cong \mathbb{R}^+$, группа положительных действительных чисел.

Решение.

а) Возьмём $z_0 \neq 0, z_0 = |z_0|(\cos\phi_0 + i\sin\phi_0)$. Определим z_0U для любого $u = \cos\phi + i\sin\phi, \phi \in \mathbb{R} \Rightarrow z_0u = |z_0|\cdot|u|(\cos(\phi_0+\phi) + i\sin(\phi_0+\phi))$. Когда ϕ принимает все возможные значения, то $\phi_0+\phi$ — тоже $\Rightarrow$ все числа из смежного класса z_0U имеют одинаковый модуль $|z_0|$, а угол — произвольный, т. е. z_0U — вся окружность $S = \{z \in \mathbb{C} \mid |z| = |z_0|\}$.

б) Заметим, что каждая такая окружность радиуса r пересекает ось x в единственной точке $x = r > 0$. Поэтому отображение $f\colon \mathbb{C}^*/U \to \mathbb{R}^+$ определим формулой $f(z_0U) = |z_0| = r$ — это биекция, и т. к. $|z_1 \cdot z_2| = |z_1|\cdot|z_2|$, то f и гомоморфизм, т. е. f — изоморфизм, значит $\mathbb{C}^*/U \cong \mathbb{R}^+$.



3.3 Гомоморфизмы. Теорема о гоморфизме

Пусть G, H — группы с операциями $\cdot$ в G и $*$ в H.

Определение 3.1. *Отображение $\phi\colon G \to H$ называется гомоморфизмом группы G в группу H, если $\forall g_1, g_2 \in G$:*

$$\phi(g_1 \cdot g_2) = \phi(g_1) * \phi(g_2).$$

При этом множество $\phi(H) = \operatorname{Im}\phi = \{\phi(g) \mid g \in G\}$ называется образом группы G под действием ϕ, а ядро ϕ определяется как $\operatorname{Ker}\phi = \{g \in G \mid \phi(g) = e_H\}$.

Теорема 3.3.

1) $\phi(e_G) = e_H$;

2) $\phi(g^{-1}) = \phi(g)^{-1} \in H$;

3) $\operatorname{Ker}\phi$ *— нормальная подгруппа в* G;

4) $\operatorname{Im}\phi$ *— подгруппа в* H.

Доказательство. 1) Пусть $\phi(e_G) = h$. Запишем: $e_G \cdot e_G = e_G \Rightarrow \phi(e_G) * \phi(e_G) = \phi(e_G)$, или $h * h = h \mid *h^{-1} \Rightarrow h * (h * h^{-1}) = h = h * h^{-1} = e_H \Rightarrow h = e_H$ ч. т. д.

2) Рассмотрим $\phi(g) * \phi(g^{-1}) = \phi(g \cdot g^{-1}) = \phi(e_G) = e_H \Rightarrow \phi(g^{-1})$ — обратный к $\phi(g)$.

3) Покажем, что $\operatorname{Ker}\phi$ — подгруппа в G. Ясно, что $e_G \in \operatorname{Ker}\phi$, в силу 1). Пусть $g_1, g_2 \in \operatorname{Ker}\phi$; тогда $\phi(g_1 \cdot g_2) = \phi(g_1) * \phi(g_2) = e_H * e_H = e_H \Rightarrow g_1 \cdot g_2 \in \operatorname{Ker}\phi$.

Пусть $g \in \operatorname{Ker}\phi$; вычислим $\phi(g^{-1}) = \phi(g)^{-1} = e_H^{-1} = e_H \Rightarrow g^{-1} \in \operatorname{Ker}\phi$.

Проверим, что $\operatorname{Ker}\phi$ — нормальная подгруппа в G. Пусть $x \in \operatorname{Ker}\phi, g$ — любой элемент из G. Вычислим $\phi(g \cdot x \cdot g^{-1}) = \phi(g) * \phi(x) * \phi(g)^{-1} = \phi(g) * \phi(g)^{-1} = e_H \Rightarrow g \cdot x \cdot g^{-1} \in \operatorname{Ker}\phi$.

4) $\operatorname{Im}\phi$ — подгруппа в H. Во-первых, $e_H \in \operatorname{Im}\phi$. Далее, если $h_1 = \phi(g_1), h_2 = \phi(g_2) \Rightarrow h_1 * h_2 = \phi(g_1) * \phi(g_2) = \phi(g_1 \cdot g_2) \Rightarrow h_1 * h_2 \in \operatorname{Im}\phi$.

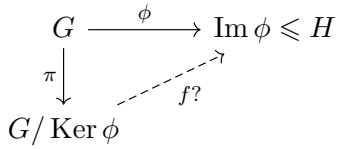
Замкнутость относительно обращения. Пусть $h = \phi(g)$, тогда по 2) $h^{-1} = \phi(g^{-1}) \in \operatorname{Im}\phi$. □

Замечание. Для любых группы G и подгруппы $N \lhd G$ существует группа $\bar{G}$ и сюръективный гомоморфизм $\pi\colon G \to \bar{G} = G/N$ с ядром N. Определим $\pi(g) = gN \equiv \bar{g}$. Любой элемент $\bar{g} = gN$, тогда $\bar{g} = \pi(g)$, гомоморфизм:$\pi(g_1 \cdot g_2) = \overline{g_1 g_2} = \overline{g_1} * \overline{g_2} = \pi(g_1) * \pi(g_2)$.

Термин: π — канонический гомоморфизм G на G/N.

Теорема 3.4 (Основная теорема о гомоморфизме)**.** *Пусть* $\phi\colon (G, \cdot) \to (H, *)$ *— гомоморфизм групп, тогда* $\operatorname{Im}\phi \cong G/\operatorname{Ker}\phi$.

Доказательство. Рассмотрим диаграмму групп из теоремы и соответствующих гомоморфизмов:



и построим отображение f так, чтобы эта диаграмма стала коммутативной. Для этого определим:

$$f(g \operatorname{Ker}\phi) = f(\bar{g}) \overset{\text{опр.}}{=} \phi(g).$$

1. Проверка корректности определения. Пусть $g_1 \operatorname{Ker}\phi = g \operatorname{Ker}\phi \Rightarrow g_1 = gx, x \in \operatorname{Ker}\phi \Rightarrow \phi(g_1) = \phi(g) * \phi(x) = \phi(g) * e_H = \phi(g)$.

2. Проверка того, что f — гомоморфизм, т. е. $f(\overline{g_1} \cdot \overline{g_2}) = f(\overline{g_1 g_2}) = \phi(g_1 g_2) = \phi(g_1) * \phi(g_2) = f(\overline{g_1}) * f(\overline{g_2})$.

3. Проверка того, что f — биекция.

$\forall h \in \operatorname{Im}\phi\ \exists g \in G\colon \phi(g) = h$, но $\phi(g) = f(\bar{g}) = h$, то есть f — сюръекция.

f инъективно: допустим, что $f(\overline{g_1}) = f(\overline{g_2})$, то есть $\phi(g_1) = \phi(g_2) \Rightarrow g_1^{-1}g_2 \in \operatorname{Ker}\phi$ $\Rightarrow g_1 \operatorname{Ker}\phi = g_2 \operatorname{Ker}\phi$, то есть $\overline{g_1} = \overline{g_2}$. □

Для решения задач на доказательство изоморфизма укажем *метод, как доказать изоморфизм* $G/N \cong H$. Для этого надо построить сюръективный гомоморфизм $\phi\colon G \to H$ так, чтобы $\operatorname{Ker}\phi = N$, тогда $G/\operatorname{Ker}\phi \cong H$ — будет доказано.

Лекция 4

4.1 Некоторые теоремы, которые вытекают из теоремы о гомоморфизме

Теорема 4.1 (Теорема о соответствии подгрупп при гомоморфизмах)**.**

Пусть $\phi\colon G \to H$ *— сюръективный гомоморфизм (эпиморфизм) групп. Тогда имеют место взаимно-однозначные соответствия между множествами подгрупп:*

1. $\{K \leqslant H\}$ *и* $\{N \leqslant G\}$*, где* $\operatorname{Ker}\phi \leqslant N$*, а также*

2. $\{K \lhd H\}$ *и* $\{N \lhd G\}$*, где* $\operatorname{Ker}\phi \leqslant N$*.*

Доказательство. 1. Знаем, что если $N \leqslant G$, то $\phi(N)$ — подгруппа в H. Возьмем произвольную подгруппу $K \leqslant H$ и рассмотрим её полный прообраз при отображении ϕ, $\phi^{-1}(K) = \{g \in G \mid \phi(g) \in K\}$. Заметим, что $\operatorname{Ker}\phi = \phi^{-1}(e_H) \leqslant= N$. Надо доказать, что отображения $\phi\colon N \to \phi(N)$ и $\phi^{-1}\colon K \to \phi^{-1}(K)$ взаимно обратные. Рассмотрим $\phi(\phi^{-1}(K)) = F = \{h \in H \mid \exists g \in G \phi(g) = h\}$, но $g \in \phi^{-1}(K)$, а это значит, что $\phi(g) = k, k \in K$.

Отсюда следует, что $\phi(\phi^{-1}(K)) = K$, таким образом $K \leftrightarrow \phi^{-1}(K)$ будет биекцией.

2. Если $N \lhd G$, то $\phi(N) \lhd H$, поэтому для $\forall h \in H, h = \phi(g)$ и для некоторого $g \in G$; $h\phi(N)h^{-1} = \{h\phi(n)h^{-1} = \phi(gng^{-1})\} \subseteq \phi(N) = \{\phi(n) \mid n \in N\}$. $\Rightarrow \phi(N) \lhd H$.

Аналогично, если $K \lhd H$, то $\phi^{-1}(K) \lhd G$, и соответствие даёт биекцию между $K \lhd H$ и $\phi^{-1}(K) \lhd G$, причем, по построению, $\operatorname{Ker}\phi \leqslant \phi^{-1}(K)$. □

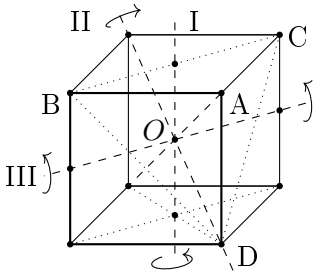
Пример применения

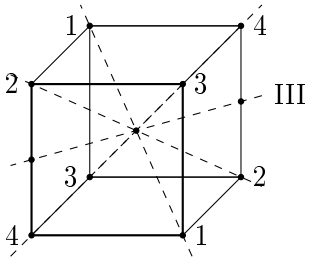
Доказать, что в группе S_4 имеется подгруппа порядка 8. Или, что тоже самое, в группе вращений куба имеется подгруппа порядка 8, поскольку эти две группы изоморфны.

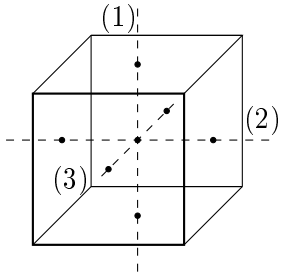
Группа вращений куба (октаэдра) состоит из поворотов трёхмерного евклидова пространства вокруг таких осей, чтобы после поворота куб совместился с собой.

Допустимы повороты вокруг осей типа I (проходящие через центры противоположных граней) на углы $\frac{\pi}{2}k, k = 0, 1, 2, 3$. Повороты вокруг осей типа II (диагоналей куба)[1]. Повороты вокруг осей типа III на угол π.

Общее число поворотов: $1 — id$, $3 \cdot 3 = 9$ поворотов I типа, $2 \cdot 4 = 8$ поворотов II типа, $1 \cdot 6 = 6$ поворотов III типа, итого $1 + 9 + 8 + 6 = 24 = |S_4|$.







Устроим гомоморфизм из группы куба (она же октаэдра) $\mathbb{O} \to S_4$. Любой поворот куба вызывает некоторую перестановку этих четырёх диагоналей. Например, поворот вокруг вертикальной оси на $\frac{\pi}{2}$ против часовой стрелки переводит $1 \to 2 \to 3 \to 4 \to 1$. Ему можно сопоставить цикл длины четыре: $(1234) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. Поворот на π вокруг указанной оси III-го типа $2 \leftrightarrow 4, 1 \leftrightarrow 3$, ему можно сопоставить $(13)(24) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$. И так для всех поворотов. Разным поворотам будут соответствовать разные подстановки $\Rightarrow \mathbb{O} \cong S_4$.

[1] $ABCD$ — правильная пирамида, её высота лежит на этой диагонали $\Rightarrow$ углы поворота $\frac{2\pi}{3}l, l = 0, 1, 2$.

Построим гомоморфизм $\phi\colon \mathbb{O} \cong S_4 \to S_3$. Любой поворот куба вызывает перестановку трех осей куба типа I. Например, поворот вокруг оси (1) на $\frac{pi}{2}$ меняет местами (2) и (3), оставляя неподвижной ось (1), то есть ему соответствует транспозиция $(23) = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$. Образы для всех остальных перестановок находятся аналогично. Найдем $\operatorname{Ker}\phi$. Поскольку $S_3 \cong S_4/\operatorname{Ker}\phi$, (6=24/4), то

$\operatorname{Ker}\phi = \{e, 3$ поворота вокруг осей (1), (2), (3) на $\pi\} \cong V_4$. Таким образом, $S_4/V_4 \cong S_3$. В группе S_3 есть три подгруппы порядка 2: $K_1 = \{e,(12)\}$, $K_2 = \{e,(13)\}$, $K_3 = \{e,(23)\}$. Каждая из подгрупп $\phi^{-1}(K_1), \phi^{-1}(K_2), \phi^{-1}(K_3)$ в группе S_4 имеет порядок 8.

Теорема 4.2 (Первая теорема об изоморфизме)**.**
Пусть $H < G, N \lhd G$, тогда NH — подгруппа в G, причем $NH/N \cong H/(H\cap N)$.

Доказательство. Нужно доказать, что NH — подгруппа. Рассмотрим отображение $\phi\colon NH \longrightarrow H/(H\cap N)$. Любой элемент $g = nh \overset{\phi}{\mapsto} h(H\cap N), n \in N, h \in H$.

Допустим, что $\phi(g_1) = \phi(n_1h_1) = h_1(H\cap N)$. Значит, $h(H\cap N) = h_1(H\cap N) \Rightarrow h_1^{-1}h \in (H\cap N)$. Тогда $h_1 = h\cdot n_2, n_2 \in H\cap N$ $n_1h_1 = n_1hn_2 = h\underbrace{h^{-1}n_1hn_2}_{\tilde{n}_2\in N} = h\tilde{n}_2$ даёт тот же смежный класс по $H\cap N$. Так как $\operatorname{Ker}\phi = \{nh \mid h(H\cap N) = H\cap N\} = N$, по основной теореме получен нужный изоморфизм. □

4.2 Центр группы

Определение 4.1. *Пусть G — группа. Тогда центр группы G определяется как множество $Z(G) = \{z \in G \mid zg = gz, \forall g \in G\}$.*

Теорема 4.3. *Центр группы — нормальная подгруппа в G.*

Доказательство. Это подгруппа: $e \in G$ принадлежит $Z(G)$; если $z_1, z_2 \in Z(G)$, то $z_1z_2 \in Z(G)$, поскольку $\forall g \in G, g(z_1z_2) = (gz_1)z_2 = (z_1g)z_2 = z_1(gz_2) = z_1(z_2g) = z_1z_2g$ — верно.

Для $z \in Z(G)$ имеем $zg = gz \Rightarrow (zg)^{-1} = (gz)^{-1} \Rightarrow g^{-1}z^{-1} = z^{-1}g^{-1}$; любой элемент $a \in G$ можно представить в виде $a = (a^{-1})^{-1}$, поэтому, если g — любой элемент, то и g^{-1} — любой элемент группы G, пусть $g^{-1} = a \Rightarrow az^{-1} = z^{-1}a$. Нормальность: $\forall z \in Z(G), \forall g \in G$ нужно показать, что $gzg^{-1} \in Z(G)$: $g(zg^{-1}) = g(g^{-1}z) = (gg^{-1})z = z \in Z(G)$. □

Примеры.
(1) $G = D_4$ — группа квадрата.
$D_4 = \{e, \underbrace{a, a^2, a^3 = a^{-1}}_{\text{повороты}}, \underbrace{s_1, s_2, s_3, s_4}_{\text{симметрии}}\}$.

Можно показать, что для любой симметрии $sas^{-1} = a^{-1}(s^{-1} = s)$. Рассмотрим $sa^2s^{-1} = (sas^{-1})(sas^{-1}) = a^{-2} = a^2$, т. к. $a^4 = e, a^2a^2 = e \Rightarrow (a^2)^{-1} = a^2$. Таким образом, $a^2 \in Z(D_4)$ (это поворот на π, т. е. центральная симметрия).

Элементы e и a^2 — единственные элементы из центра $D_4 \Rightarrow Z(D_4) = \{e, a^2\}$.

(2) Пусть $G = GL_n(\mathbb{R})$ — невырожденные вещественные матрицы порядка n с операцией умножения. Заметим, что $H = \{\lambda E \mid \lambda \neq 0\}$ — подгруппа скалярных матриц содержится в $Z(G)$, так как $(\lambda E)A = A(\lambda E) = \lambda A, \forall \lambda \neq 0$ (λE — скалярная матрица).

Задача. Доказать (хотя бы для $n = 2$), что $Z(GL_n) = \{\lambda E \mid \lambda \neq 0\}$.

Теорема 4.4. *Факторгруппа $G/Z(G)$ для неабелевой группы G не может быть циклической.*

Доказательство. Допустим, что $G/Z(G)$ — циклическая, и покажем, что G — абелева. Группа G разбивается на смежные классы по $Z(G) \overset{\text{обозн.}}{=} Z$, то есть $G = \bigcup\limits_{i \in I} g_i Z$ $\Rightarrow \forall g \in G$ представим в виде: $g = g_i z_i$ для некоторого i. Возьмем другой элемент $g' = g_j z_j$. Дано, что $G/Z(G)$ – циклическая $\Rightarrow \exists a \in G$ такой, что все смежные классы имеют вид $a^k Z$. Значит $g = a^i z_i, g' = a^j z_j \Rightarrow gg' = (a^i z_i)(a^j z_j) = a^i(z_i a^j) z_j = a^i(a^j z_i) z_j = a^{i+j} z_i z_j = (a^j z_j)(a^i z_i) = g'g \Rightarrow gg' = g'g$. $\square$

Задача. Доказать, что группа порядка p^2 (p — простое число) абелева.

Решение. Обозначим эту группу через G. Если в G существует элемент порядка p^2, то G циклическая $\Rightarrow$ абелева. Пусть $\nexists$ элемента порядка $p^2 \Rightarrow \forall g \in G, g^p = e$ ($\text{ord}(g) \mid |G| = p^2 \Rightarrow \text{ord}(g) = 1, p$; рассматриваем случай, когда $\text{ord}(g) \neq p^2$).

Покажем, что $Z(G) > \{e\}$. Возьмем $g_0 \in G$ и рассмотрим всевозвозможные элементы вида gg_0g^{-1} — сопряженные с g_0.

Их количество — делитель $|G| = p^2$. Если $g_0 \in Z(G)$, то $gg_0g^{-1} = g_0, \forall g \in G$. Если $g_0 \ni Z(G)$, посмотрим, при каком условии $g_1 g_0 g_1^{-1} = g_2 g_0 g_2^{-1} \Rightarrow (g_2^{-1} g_1) g_0 (g_1^{-1} g_2) = g_0$. Но $g_1^{-1} g_2 = (g_2^{-1} g_1)^{-1} \Rightarrow$ элемент $g_2^{-1} g_1$ оставляет элемент g_0 неподвижным. Обозначим $C = \{g \in G \mid gg_0g^{-1} = g_0\}$ — это подгруппа в G. Если $C = G$, то $g_0 \in Z(G)$, иначе $|C| = p : C \geq \langle g_0 \rangle$ порядка p, но $G > C$.

В таком случае $\left|\{gg_0g^{-1}\}\right| = \frac{|G|}{|C|} = p$.

Вся группа G разбивается на сопряженные подмножества: $G = \underbrace{\{e\} \bigsqcup \{z_1\} \bigsqcup \ldots \bigsqcup \{z_k\}}_{k} \underbrace{\bigsqcup K_1 \bigsqcup \ldots \bigsqcup K_r}_{\text{по } p \text{ элементов } \vdots p} \Rightarrow k = |Z(G)| \vdots p$.

Итак, если G неабелева, но $|Z(G)| = p$, тогда $|G/Z(G)| = p$, а любая группа простого порядка p — циклическая $\Rightarrow G/Z(G)$ – циклическая $\Rightarrow G$ абелева. Получается противоречие.

4.3 Системы порождающих в группах

Пусть G — группа, $S \subset G$. Скажем, что S — *система порождающих для группы G*, если любой элемент $g \in G$ можно представить в виде:

$$g = s_1^{\pm 1} \cdot s_2^{\pm 1} \cdot \ldots \cdot s_k^{\pm 1}, \text{ где } s_i \in S, k = 1, 2, \ldots .$$ Обозначение: $G = \langle s \rangle$.

Простейший случай: $S = \{a\}$, тогда G — циклическая группа.

Примеры.

(1) $G = D_n = \{e, a, a^2, \ldots, a^{n-1}, s_1, s_2, \ldots, s_n\}$ (a — поворот вокруг центра O на угол $\frac{2\pi}{n}$, $s_1, s_2, \ldots, s_n$ — осевые симметрии)

Для любой симметрии s, $sas^{-1} = sas = a^{-1}$. Обозначим s_1 за b и покажем, что $S = \{a, b\}$, т. е. $D_n = \langle a, b\rangle$.

Рассмотрим элементы $b, ab, a^2b, \ldots, a^{n-1}b$. Покажем, что это симметрии. Для этого надо убедиться, что $\forall k = 1, \ldots, n-1$ $(a^kb)^2 = e$. Действительно, $(a^kb)(a^kb) = a^k(ba^kb^{-1}) = a^ka^{-k} = e$.

(2) $G = S_n$ — симметрическая группа степени n. Очевидно, что систему порождающих в S_n составляют все транспозиции, т. к. любую подстановку можно разложить в произведение транспозиций.

3.14 (1) Показать, что транспозиции $(1,2), (1,3), \ldots, (1,n)$ составляют систему порождающих для S_n. Для этого достаточно выразить любую транспозицию через $(1,2), (1,3), \ldots, (1,n)$.

Задача 1. Доказать, что если $|G| = 4$, то $G \cong \mathbb{Z}_4$ или $G \cong \mathbb{V}_4$.

Решение. Пусть $|G| = 4$. По теореме Лагранжа, $\forall g \in G, \operatorname{ord}(g) = |\langle g\rangle|$ делит $|G| \Rightarrow \operatorname{ord}(g) = 4, 2$ или 1, при $g = e$. Если $\exists a, \operatorname{ord}(a) = 4$, то $\langle a\rangle = G$ — группа циклическая, изоморфная $\mathbb{Z}_4$. Если $\forall g \in G, g \neq e, \operatorname{ord}(g) = 2$, то есть $g^2 = e$, то G содержит $\{e, a, b, ab = ba\}$ — подгруппа в $G \Rightarrow G = \{e, a, b, ab = ba\}$ $\Rightarrow G \cong V_4$, а именно, можно положить, что $a \leftrightarrow (1,2)(3,4), b \leftrightarrow (1,3)(2,4) \Rightarrow ab \leftrightarrow (1,2)(3,4)(1,3)(2,4) = (2,3)(1,4)$.

Задача 2. Доказать, что если $|G| = 6$, то $G \cong \mathbb{Z}_6$ или $G \cong D_3 \cong S_3$.

Решение. Пусть $|G| = 6$. По теореме Лагранжа $\operatorname{ord}(g) = 6, 3, 2$ или 1, при $g = e$. Если $\exists a \in G, |a| = 6$, то $\langle a\rangle = G$, G — циклическая, $\cong \mathbb{Z}_6$.

Пусть $\nexists$ элемента порядка 6. Покажем, что $\exists a \in G, \operatorname{ord}(a) = 2$. От противного, допустим, что $\forall g \neq e, g^2 \neq e$, т. е. $|g| \neq 2$, тогда $g^{-1} \neq g$, и вся группа G состоит из $\{e, g, g^{-1}, h, h^{-1}$ и т. д. $\}$, т. е. $|G|$ нечётный $\Rightarrow$ противоречие.

Покажем, что $\exists b \in G, \operatorname{ord}(b) = 3$. Допустим, что $\forall g \in G, g^2 = e$, тогда группа G будет абелевой (если $g, h \in G, g \neq h$, тогда $(gh)^2 = e \Rightarrow (gh)^{-1} = gh$, но $(gh)^{-1} = h^{-1}g^{-1} = hg \Rightarrow gh = hg$). В этом случае $\{e, a, b, ab = ba\}$ — подгруппа в G из 4-х элементов, чего не может быть поскольку 4 не делит 6 (противоречие со следствием из т. Лагранжа).

Итак, в G есть a порядка 2 и b порядка 3. Либо $ab = ba$, и тогда $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b) = 6$, и G циклическая, что не так в данном случае по предположению $\Rightarrow$ либо $ab = b^{-1}a$, и мы можем установить изоморфизм с D_3, $a \leftrightarrow s$ — симметрия, $b \leftrightarrow R_0^{2\pi/3}$. В самом деле, $\langle b\rangle$ содержит половину элементов группы $G \Rightarrow \langle b\rangle \lhd G \Rightarrow aba^{-1} = b^2 = b^{-1}$.

Д.З.	3.14 (2), 58.11, 58.20 (в)

Лекция 5

5.1 Прямые произведения (прямые суммы) подгрупп и групп

5.1.1 Прямые произведения подгрупп

Определение 5.1. *Пусть G — группа, H_1, H_2 — подгруппы. G называется прямым произведением подгрупп H_1, H_2 (обозначение: $H_1 \times H_2$), если:*

1. *$G = H_1 \cdot H_2$, т. е. $\forall g \in G\ \exists h_1 \in H_1$ и $h_2 \in H_2$ такие, что $g = h_1 h_2$.*

2. *Для $\forall g$ такие h_1 и h_2 единственные (например, единственное разложение $e = e \cdot e$, т. к. $e \in H_1$ и $e \in H_2$).*

3. *$\forall h_1 \in H_1, h_2 \in H_2$: $h_1 h_2 = h_2 h_1$ (сами подгруппы H_1 и H_2 могут быть некоммутативными).*

Отметим, что если операция в G — сложение (коммутативная операция), то часто говорят, что G — прямая сумма подгрупп $G = H_1 \oplus H_2$; условие 3 в этом случае излишне.

Утверждение 5.1. *Если $G = H_1 \times H_2$, то i) $H_1 \lhd G, H_2 \lhd G$ и ii) $H_1 \cap H_2 = \{e\}$.*

Доказательство. i) $\forall g = h_1 h_2$, если $\tilde{h}_1 \in H_1$, рассмотрим $g\tilde{h}_1 g^{-1} = h_1 h_2 \tilde{h}_1 (h_1 h_2)^{-1} = h_1 h_2 \tilde{h}_1 h_2^{-1} h_1^{-1} = (h_1 \tilde{h}_1)(h_2 h_2^{-1}) h_1^{-1} = h_1 \tilde{h}_1 h_1^{-1} \in H_1$, доказали, что H_1 нормальна в G, для H_2 аналогично.

ii) Пусть $h \in H_1 \cap H_2$ и $h \neq e$. Тогда для h имеем два различных разложения: $h = \underbrace{h}_{\in H_1} \cdot \underbrace{e}_{\in H_2} = \underbrace{e}_{\in H_1} \cdot \underbrace{h}_{\in H_2}$ – противоречит определению $\Rightarrow h = e$. □

Пример. Пусть $G = V_4 = \{e, a = (1,2)(3,4), b = (1,3)(2,4), c = (1,4)(2,3)\}$. Рассмотрим $H_1 = \{e, a\}, H_2 = \{e, b\}$, тогда $G = H_1 \times H_2$.

$$H_1 \cdot H_2 = \{e, eb = b, ae = a, ab = c\} = G,$$

$$H_1 \cap H_2 = \{e\}$$

и $h_1 h_2 = h_2 h_1, \forall h_1 \in H_1, \forall h_2 \in H_2$, так как G абелева.

5.1.2 Прямое произведение групп

Пусть G_1, G_2 некоторые группы. Рассмотрим $G = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2 = G_1 \times G_2\}$ — декартово произведение множеств G_1, G_2.

Пусть в G_1 операция $\cdot$, а в G_2 операция $*$.

Определим операцию на множестве пар покомпонентно:

$$(g_1, g_2) \circ (g_1', g_2') \overset{\text{опр.}}{=} (g_1 \cdot g_1', g_2 * g_2').$$

Получится группа.

1. Ассоциативность: возьмем ещё (g_1'', g_2''), рассмотрим $\big((g_1, g_2) \circ (g_1', g_2')\big) \circ (g_1'', g_2'') = (g_1 \cdot g_1', g_2 * g_2') \circ (g_1'', g_2'') = \big((g_1 \cdot g_1') \cdot g_1'', (g_2 * g_2') * g_2''\big) \overset{\text{acc.}}{=} \big(g_1 \cdot (g_1' \cdot g_1''), g_2 * (g_2' * g_2'')\big) = (g_1, g_2) \circ \big((g_1', g_2') \circ (g_1'', g_2'')\big)$.

2. Единица $e = (e_1, e_2)$.

3. $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$, т. к. $(g_1, g_2) \circ (g_1^{-1}, g_2^{-1}) = (g_1 \cdot g_1^{-1}, g_2 * g_2^{-1}) = (e_1, e_2) = e$.

Установим соответствие двух прямых произведений — внутреннего (подгрупп) и внешнего (групп).

Пусть $G = G_1 \times G_2$ — внешнее прямое произведение групп G_1, G_2, то есть $\forall g \in G$: $g = (g_1, g_2), g_1 \in G_1, g_2 \in G_2$.

Рассмотрим в G два подмножества:

$$H_1 = \{(g_1, e_2) \mid g_1 \in G_1\} \text{ и } H_2 = \{(e_1, g_2) \mid g_2 \in G_2\}.$$

Тогда H_1 и H_2 подгруппы в G, причем $H_1 \cong G_1, H_2 \cong G_2$; в самом деле, $(g_1, e_2) \leftrightarrow g_1 \in G_1$ и $(e_1, g_2) \leftrightarrow g_2 \in G_2$.

Покажем, что $G = H_1 \times H_2$ — прямое произведение этих подгрупп $\forall g = (g_1, g_2) = (g_1, e_2) \circ (e_1, g_2)$ и если $= (g_1', e_2) \circ (e_1, g_2') \Rightarrow g_1 = g_1', g_2 = g_2'$ — единственность.

Наконец, $(g_1, e_2) \circ (e_1, g_2) = (g_1, g_2) = (e_1, g_2) \circ (g_1, e_2)$, то есть все три условия из определения 5.1 выполнены.

Вывод: $G = G_1 \times G_2 \cong H_1 \times H_2$ (во втором случае — прямое произведение подгрупп группы G).

5.1.3 Распространение понятия прямого произведения подгрупп (и групп) на случай $n \geqslant 2$

Определение 5.2. *Пусть $H_1, H_2, \ldots, H_n$ — подгруппы в группе G.*

$$G = H_1 \times H_2 \times \cdots \times H_n,$$

если

1. $\forall g = h_1 \cdot h_2 \cdots h_n, h_i \in H_i, i = 1, \ldots, n$.
2. *Разложение из п. 1 единственно.*
3. $\forall h_i \in H_i, h_j \in H_j (i \neq j)$: $h_i h_j = h_j h_i$.

Определение 5.3. *Пусть $G_1, G_2, \ldots, G_n$ — группы. Образуем прямое произведение групп $G = G_1 \times G_2 \times \cdots \times G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i, 1 \leqslant i \leqslant n\}$ с операцией $(g_1, \ldots, g_n) \circ (g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n')$.*

Также, как для $n = 2$, если в прямом произведении $G = G_1 \times G_2 \times \cdots \times G_n$ рассмотреть подгруппы: $H_i = \{e_1, \ldots, g_i, \ldots, e_n\} \cong G_i, g_i \in G_i$, то $G = H_1 \times H_2 \times \cdots \times H_n$ — прямое произведение подгрупп.

Например, $\mathbb{Z}^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{Z}, i = 1, \ldots, n\}$ и операция — покоординатное сложение, т. е. $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z} = \mathbb{Z}^n$.

Примеры.

(1) Доказать, что группа $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$, $\mathbb{R}$ — подгруппа действительных чисел $z = x + i \cdot 0$, и $i\mathbb{R}$ подгруппа чисто мнимых чисел $z = 0 + i \cdot y$.

Решение. $(\mathbb{C}, +)$ — коммутативная группа и $\forall z = x + iy$ $(x, y \in \mathbb{R})$ единственным образом.

(2) $(\mathbb{C}^*, \cdot)$ — группа комплексных чисел $\neq 0$ с операцией умножения.

Доказать, что $\mathbb{C}^* = \mathbb{R}^+ \times U$, где $\mathbb{R}^+ = \{x > 0\}, U = \{z \in \mathbb{Z} \mid |z| = 1\}$.

Решение. $\forall z \in \mathbb{C}, z \neq 0$: $z = r \cdot (\cos\phi + i \sin\phi)$ — единственным образом (если $\phi \in [0, 2\pi]$), где $r = |z| > 0, |\cos\phi + i\sin\phi| = 1$.

(3) Показать, что $\mathbb{Z}$ нельзя представить в виде прямой суммы двух ненулевых подгрупп.

5.1.4 Абелевы группы с конечным числом порождающих

Определение 5.4. *Пусть A — абелева группа с операцией $+$. Скажем, что элементы $a_1, \ldots, a_n$ порождают группу A, если $\forall a = \sum\limits_{i=1}^{n} k_i a_i, k_i \in \mathbb{Z}$, где*

$$k_i a_i = \begin{cases} a_i + \cdots + a_i, & \text{если } k_i > 0; \\ -(a_i + \cdots + a_i), & \text{если } k_i < 0; \\ 0, k_i = 0. \end{cases}$$

Скажем, что элементы $a_1, \ldots, a_n$ линейно независимы над $\mathbb{Z}$ (в целочисленном смысле), если из того, что $k_1 a_1 + \cdots + k_n a_n = 0 \Rightarrow k_1 = \ldots = k_n = 0$.

Элементы $e_1, \ldots, e_n$ образуют базис группы A, если:

1) $e_1, \ldots, e_n$ линейно независимы над $\mathbb{Z}$;

2) $\forall a \in A$ существуют целые $k_1, \ldots, k_n$ такие, что $a = \sum\limits_{i=1}^{n} k_i a_i$.

Определение 5.5. *Абелева группа F называется свободной группой ранга n, если в F существует базис из n элементов.*

Лемма 5.1. *Если в группе F существует базис из n элементов, то все базисы в F состоят из n элементов.*

Доказательство. Пусть $\exists e'_1, \ldots, e'_m$ в F с $m > n$, тогда $e'_1, \ldots, e'_m$ линейно зависимы (и значит не могут служить базисом).

Рассмотрим разложения элементов $e'_1, \ldots, e'_m$ по исходному базису: $e'_j = \sum\limits_{i=1}^{n} c_{ij} e_i, \forall j, 1 \leqslant j \leqslant m$ $(c_{ij} \in \mathbb{Z})$.

Запишем линейную комбинацию $\sum\limits_{j=1}^{m} \lambda_j e'_j = 0 \in A$, $\lambda_j \in \mathbb{Z}$. Надо показать, что существуют λ_j не все $= 0$.

$$\sum_{j=1}^{m} \lambda_j \sum_{i=1}^{n} c_{ij} e_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} c_{ij} \lambda_j \right) e_i = 0 \Rightarrow \sum_{j=1}^{m} c_{ij} \lambda_j = 0, 1 \leqslant j \leqslant n.$$

В этой системе количество неизвестных $>$ количества уравнений $\Rightarrow$ эта система имеет $\neq 0$ решение: $\lambda_i = \frac{p_i}{q_i} \in \mathbb{Q}$, тогда $\sum\limits_{j=1}^{m} \frac{p_j}{q_j} e'_j = 0$, где не все $p_j \in \mathbb{Z}$ равны 0.

Умножим это равенство на общий знаменатель q всех дробей, и тогда получим $\sum\limits_{j=1}^{m} \tilde{p}_j e'_j = 0$, где $\tilde{p}_j = \frac{p_j q}{q_j} \in \mathbb{Z}$ не все $= 0$.

Таким образом базис в F не может содержать больше, чем n элементов. Но если бы нашелся базис с $m < n$ элементов: $e'_1, \ldots, e'_m$, то его можно было бы взять за исходный базис, а тогда по лемме элементы $e_1, \ldots, e_n$, (т. к. $m < n$) будут линейно зависимыми. Получается противоречие $\Rightarrow m = n$. □

5.1.5 Сравнение свойств абелевых групп и векторных пространств

Векторное пространство	Абелева группа
1) Если $0 \neq U \subseteq V, \dim V = n$, то $\dim U \leqslant n$. Если $\dim U = \dim V$, то $U = V$	Если F — свободная аб. гр., $\operatorname{rk} F = n$ и $0 \neq H \leqslant F$, то H — свободна, причем $\operatorname{rk} H \leqslant \operatorname{rk} F$ (теорема о свободе) Из того, что $\operatorname{rk} H = \operatorname{rk} F \not\Rightarrow H = F$ Контрпример: $F = \mathbb{Z}, H = 2\mathbb{Z}$, $F \neq H$, но $\operatorname{rk} F = \operatorname{rk} H = 1$
2) Любую линейно независимую систему векторов $e_1, \ldots, e_r (r < n)$ из V можно дополнить до базиса пространства V	2) Не всегда верно. Пример. $F = \mathbb{Z}^2, H = \{(n, 2m)\}$ Вектор $(0, 2)$ нельзя дополнить до базиса в F
	3) Справедлива т. н. теорема о согласованных базисах

Теорема 5.1 (Теорема о свободе)**.**

Если $F = F_n$ — свободная абелева группа ранга n, H — её ненулевая подгруппа, то H свободна и $\operatorname{rk} H = r \leqslant n$.

Доказательство. Индукция по $n = \operatorname{rk} F$. Случай $n = 0$ не рассматриваем.

База. Если $n = 1$, то $F = \langle e_1 \rangle$ циклическая группа, т. е. $F = \{te_1 \mid t \in \mathbb{Z}\}$. H — её подгруппа $\Rightarrow$ H тоже циклическая, то $H = \langle d_1 e_1 \rangle = \{td_1 e_1 \mid t \in \mathbb{Z}, d_1 \in \mathbb{N}\} \Rightarrow$ $\operatorname{rk} H = 1$ и d_1 то самое число.

Пусть $n > 1, \{e_1, \ldots, e_n\}$ базис в F и для подгрупп в группах ранга меньшего, чем n теорема верна.

Сделаем шаг индукции. Рассмотрим $F_1 = \langle e_1, \ldots, e_{n-1} \rangle$ ранга $n-1$ (она состоит из "векторов", у которых n-я координата равна нулю) и рассмотрим $H_1 = H \cap F_1$. Либо $H_1 = 0 \Rightarrow H \leqslant \langle e_1 \rangle$, и этот случай уже рассмотрен при $n = 1$, либо $H_1 \neq 0$, тогда она по предположению индукции имеет ранг $m \leqslant n-1$.

Если $H_1 = H$, то $\operatorname{rk} H = m \leqslant n-1 < n$ — верно.

Теперь пусть подгруппа $H_1 < H$. По предположению $H = \{k_1 e_1 + \cdots + k_{n-1} e_{n-1} + k_n e_n\}$, $k_i \in \mathbb{Z}$. Множество последних координат $K = \{k_n \in \mathbb{Z}\}$ для элементов из H — это подгруппа в $\mathbb{Z}$. Группа K — циклическая. Пусть k — наименьшее натуральное число в K, а $f_{m+1} = k_1 e_1 + \cdots + k_{n-1} e_{n-1} + k e_n$. Если $\{f_1, \ldots, f_m\}$ базис в H_1, то $\{f_1, \ldots, f_{m+1}\}$ базис в H, $\operatorname{rk} H = m+1 \leqslant n$. □

Д.З.	60.1, 60.2 (а), 60.8, 60.5 (а,б)

Лекция 6

Теорема 6.1 (Теорема о согласованных базисах)**.**

Если $F = F_n$ — свободная абелева группа ранга n и H — подгруппа ранга $r \leqslant n$, то в F существует базис $e'_1, \ldots, e'_n$ и существуют натуральные числа $d_1, \ldots, d_r$ такие, что $d_1e'_1, \ldots, d_re'_r$ — базис в H, причем $d_1 \mid d_2, d_2 \mid d_3, \ldots, d_{r-1} \mid d_r$.

Замечание. В теореме о согласованных базисах можно добиться того, чтобы каждое $d_i (1 \leqslant i \leqslant r-1)$ делило d_{i+1}, и тогда эти $d_1, \ldots, d_r$ однозначно определены по H.

Необходимые сведения о целочисленных матрицах

Пусть $C = (c_{ij})$ матрица размеров $n \times r, c_{ij} \in \mathbb{Z}$ (в нашем случае $n \geqslant r$). Матрица C считается диагональной, если $c_{ij} = 0$ для $i \neq j$.

Целочисленные элементарные преобразования

I. Прибавление к строке (или к столбцу) другой строки (столбца), умноженой на целое число.

II. Перестановка двух строк (или столбцов).

III. Умножение строки (или столбца) на -1.

Теорема 6.2 (Теорема Смита)**.**

Любую целочисленную матрицу C размера $n \times r$ и ранга $r \leqslant n$ элементарными целочисленными преобразованиями строк и столбцов можно привести к диагональному виду:

$$C \sim \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix},$$

причем $d_1 \mid d_2, d_2 \mid d_3$ и так далее $d_{r-1} \mid d_r$.

Без доказательства.

Доказательство теоремы о согласованных базисах. В данном случае, когда $F = \langle e_1, \ldots, e_n \rangle, H = \langle h_1, \ldots, h_r \rangle, \forall h_j = \sum\limits_{i=1}^{n} c_{ij} e_i$. Из этих c_{ij} составим матрицу:

$$C = \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1r} \\ c_{21} & c_{22} & \ldots & c_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{nr} \end{pmatrix}.$$

Отследим, что происходит с матрицей C при заменах базиса $(e_1, \ldots, e_n)$ и базиса $(h_1, \ldots, h_r)$.

Допустим, что $e' = (e'_1, \ldots, e'_n)$ — новый базис в F, S — матрица перехода от базиса $e = (e_1, \ldots, e_n)$ к базису e'. Столбцы S — столбцы новых базисных элементов в старом базисе.

По определению $e' = eS_{e \to e'}$. Матрица S целочисленная, причем матрица обратного перехода $S_{e' \to e}$ также целочисленная и $S_{e' \to e} = S^{-1}_{e \to e'}$.

Запишем: $S_{e \to e'} \cdot S_{e' \to e} = E \Rightarrow |S_{e \to e'}| \, |S_{e' \to e}| = |E| = 1 \Rightarrow |S_{e \to e'}| = |S_{e' \to e}| = \pm 1$.

Аналогично, пусть $T = T_{h \to h'}$ — матрица перехода от базиса $h = (h_1, \ldots, h_r)$ к базису $h' = (h'_1, \ldots, h'_r) \Rightarrow T$ — целочисленна, $|T| = \pm 1$.

Рассмотрим исходное равенство:

$$h = eC, \tag{6.1}$$

более подробно: $(h_1, \ldots, h_r) = (e_1, \ldots, e_n)C$.

Имеем: $e' = eS, h' = hT$ — подставим эти выражения в 6.1, умножив его предварительно справа на матрицу T, получим $h' = hT = (eC)T = e(CT)$.

Теперь выразим базис e из равенства $e' = eS \Rightarrow e = e'S^{-1}$, получим:

$$h' = (e'S^{-1})(CT) = e'(S^{-1}CT). \tag{6.2}$$

Равенство 6.2 показывает, что $C' = S^{-1}CT$.

Умножение матрицы C на матрицу слева приводит к преобразованию её строк, а справа — к преобразованию столбцов.

Пользуясь теоремой Смита, можем найти такие матрицы S^{-1} и T — целочисленные с $\det = \pm 1$, что:

$$C' = \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix},$$

и тогда $e'_1, \ldots, e'_n$ а также $h'_1, \ldots, h'_r$ — новые базисы, причём $h'_j = d_j e'_j, j = 1, \ldots, r$.

Таким образом, доказательство теоремы о согласованных базисах получается из теоремы Смита. $\square$

Пример. (Э. Б. Винберг, “Курс алгебры” — М.: МЦНМО, 2021 — с. 346–349, с. 379)

$$C = \begin{pmatrix} 2 & 6 & 2 \\ 2 & 3 & 4 \\ 4 & 2 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 6 & 2 \\ 0 & -3 & 2 \\ 0 & -10 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & -3 & 2 \\ 0 & -10 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 10 & 0 \end{pmatrix},$$

$c_{11} > 0$ наименьшее (по модулю) в матрице C.

С помощью элементарных преобразований строк и столбцов будем пытаться уменьшить c_{11}. $c_{22} = -3$ не делится на 2.

Прибавим 2-ю строку к 1-й строке:

$$\rightsquigarrow \begin{pmatrix} 2 & 3 & 2 \\ 0 & 3 & 2 \\ 0 & 10 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 1 & 0 \\ 0 & 3 & 2 \\ 0 & -10 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 0 \\ 3 & 0 & 2 \\ 10 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & -6 & 2 \\ 0 & -20 & 0 \end{pmatrix} \rightsquigarrow$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 2 \\ 0 & 20 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 6 \\ 0 & 0 & 20 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 20 \end{pmatrix},$$

$d_1 = 1, d_2 = 2, d_3 = 20$.

В общем виде алгоритм будет сформулирован позднее.

6.0.1 Структура произвольных абелевых групп с конечным числом порождающих

Пусть A — абелева группа (по сложению) с порождающими элементами $a_1, \ldots, a_n$, то есть для $\forall a \in A$ найдутся целые числа $k_1, \ldots, k_n$ такие, что $a = \sum\limits_{i=1}^{n} k_i a_i$ (такое разложение может не быть единственным).

Рассмотрим свободную абелеву группу F ранга n с базисом $e_1, \ldots, e_n$; элементы f из F разлагаются по базису единственным образом. Построим отображение:

$$\phi\colon F \to A$$

по формуле $\phi\big(\sum\limits_{i=1}^{n} k_i e_i\big) = \sum\limits_{i=1}^{n} k_i a_i$. Поскольку ϕ — сюръективный гомоморфизм групп, то по теореме о гомоморфизме $A \cong F/\operatorname{Ker}\phi$.

Итак, $A \cong F/\operatorname{Ker}\phi$.

Если $\operatorname{Ker}\phi = \{0\}$, то $A \cong F$ и сама является свободной абелевой группой ранга n.

Считаем, что $A \neq 0$, так что $n \geqslant 1$, значит, $\operatorname{Ker}\phi < F$, обозначим $H = \operatorname{Ker}\phi$.

По теореме H — свободная группа некоторого ранга $r \geqslant 1$, и по теореме о согласованных базисах: $\langle e'_1\rangle \oplus \cdots \oplus \langle e'_r\rangle \oplus \langle e'_{r+1}\rangle \oplus \cdots \oplus \langle e'_n\rangle$, $\langle h'_1\rangle \oplus \cdots \oplus \langle h'_r\rangle = \langle d_1 e'_1\rangle \oplus \cdots \oplus \langle d_r e'_r\rangle$. Из теоремы о гомоморфизме вытекает

Лемма 6.1 (Лемма о факторизации по прямым слагаемым). *Пусть* $F = F_1 \oplus \cdots \oplus F_n, H < F, H = H_1 \oplus \cdots \oplus H_n$, *где* $H_i \trianglelefteq F_i, i = 1, \dots n$ *(прямые суммы подгрупп), тогда* $F/H \cong F_1/H_1 \oplus F_2/H_2 \oplus \cdots \oplus F_n/H_n$ *(здесь прямая сумма внешняя).*

Доказательство. Построим гомоморфизм $\phi\colon F \to F_1/H_1 \oplus F_2/H_2 \oplus \cdots \oplus F_n/H_n$ $\forall f = f_1 + \cdots + f_n (f_i \in F_i, 1 \leqslant i \leqslant n)$.

$\phi(f) = (f_1 + H_1, f_2 + H_2, \dots, f_n + H_n)$ — так выглядит любой элемент из группы $F/H \cong F_1/H_1 \oplus \cdots \oplus F_n/H_n \Rightarrow \phi$ — сюръективное отображение; $\phi(f + f') = \phi((f_1 + f_1') + \cdots + (f_n + f_n')) = ((f_1 + f_1') + H_1, \dots, (f_n + f_n') + H_n) = (f_1 + H_1, f_2 + H_2, \dots, f_n + H_n) + (f_1' + H_1, f_2' + H_2, \dots, f_n' + H_n) = \phi(f) + \phi(f') \Rightarrow (F_1/H_1) \oplus \cdots \oplus (F_n/H_n) \cong F/\operatorname{Ker}\phi$. $\operatorname{Ker}\phi \cong \{f = f_1 + \cdots + f_n \mid (f_1 + H_1, f_2 + H_2, \dots, f_n + H_n) = (\bar{0}, \dots, \bar{0})\}$, то есть $f_i \in H_i$ $\Rightarrow \operatorname{Ker}\phi = H = H_1 \oplus \cdots \oplus H_n$.

Лемма доказана. □

В нашем случае:

$$F = \langle e_1' \rangle \oplus \cdots \oplus \langle e_r' \rangle \oplus \langle e_{r+1}' \rangle \oplus \cdots \oplus \langle e_n' \rangle,$$
$$H = \langle d_1 e_1' \rangle \oplus \cdots \oplus \langle d_r e_r' \rangle \oplus \{0\} \oplus \cdots \oplus \{0\}.$$

По лемме:

$$F/H \cong \langle e_1' \rangle / \langle d_1 e_1' \rangle \oplus \cdots \oplus \langle e_r' \rangle / \langle d_r e_r' \rangle \oplus \langle e_{r+1}' \rangle / \{0\} \oplus \cdots \oplus \langle e_n' \rangle / \{0\} \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-r}.$$

Теорема 6.3 (Основная теорема о строении конечнопорожденных абелевых групп). *Любая конечнопорожденная абелева группа изоморфна прямой сумме циклических групп, частично конечно, частично бесконечных.*

Единственность. Количество r конечных циклических и количество $(n - r)$ бесконечных циклических слагаемых, а также порядки $d_1, \dots, d_r (d_i \mid d_{i+1}, 1 \leqslant i \leqslant r - 1)$ однозначно определены по группе A.

Пример

60.52 (а) $A = \langle x_1, x_2, x_3 \rangle$ — свободная абелева группа с базисом x_1, x_2, x_3, $B = \langle y_1, y_2, y_3 \rangle$, где:

$$\begin{cases} y_1 = 7x_1 + 2x_2 + 3x_3 \\ y_2 = 21x_1 + 8x_2 + 9x_3 \\ y_3 = 5x_1 - 4x_2 + 3x_3 \end{cases}$$

1) Построить согласованные базисы и найти d_1, d_2, d_3.

2) Определить $A/B \cong$?

Решение.

$C = \begin{pmatrix} 7 & 2 & 3 \\ 21 & 8 & 9 \\ 5 & -4 & 3 \end{pmatrix}$ надо привести к диагональному виду.

Находим $c_{12} = 2$ — наименьший по модулю элемент.

$$C \rightsquigarrow \begin{pmatrix} 2 & 7 & 3 \\ 8 & 21 & 9 \\ -4 & 5 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 7 & 3 \\ 0 & -7 & -3 \\ 0 & 19 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 1 & 1 \\ 0 & -7 & -3 \\ 0 & 19 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 & 2 \\ -3 & -7 & 0 \\ 9 & 19 & 0 \end{pmatrix} \rightsquigarrow$$

нужно, чтобы на c_{11} делились все элементы матрицы

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ -3 & -4 & 6 \\ 9 & 10 & -18 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & -6 \\ 0 & 10 & -18 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 2 \\ 0 & 10 & 8 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 8 & 10 \end{pmatrix} \rightsquigarrow$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

$d_1 = 1, d_2 = 2, d_3 = 6 \Rightarrow$

$A/B \cong \langle e_1' \rangle / \langle e_1' \rangle \oplus \langle e_2' \rangle / \langle 2e_2' \rangle \oplus \langle e_3' \rangle / \langle 6e_3' \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$

6.0.2 Строение конечных абелевых групп

Теорема 6.4. *Конечная абелева группа представима в виде прямой суммы:*

$$A \cong \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{k_n}},$$

где $p_1, p_2, \ldots, p_n$ — простые числа, $k_1, k_2, \ldots, k_n$ — натуральные числа.

Определение 6.1. *Группа H называется примарной, если существует простое число p такое, что $|H| = p^n$, $n \geqslant 1$. Если p указано, то H называется p-примарной.*

Словесная формулировка теоремы: конечная абелева группа представляется в виде прямой суммы примарных циклических групп.

Частный случай: A — циклическая группа порядка $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ — каноническое разложение на простые множители. Тогда:

$$A \cong \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{\alpha_r}}.$$

Доказательство. По условию и основной теореме $A \cong \mathbb{Z}_{d^1} \oplus \mathbb{Z}_{d^2} \oplus \cdots \oplus \mathbb{Z}_{d^r}$; если $d_i = p_1^{\alpha_{1i}} p_2^{\alpha_{2i}} \cdots p_{si}^{\alpha_s}, i = 1, \ldots, r, \alpha_{1i}, \ldots, \alpha_{si} \geqslant 0$, то $A \cong \mathbb{Z}_{p_1^{\alpha_{11}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{\alpha_{1r}}} \oplus \mathbb{Z}_{p_2^{\alpha_{21}}} \oplus \cdots \oplus \mathbb{Z}_{p_2^{\alpha_{2r}}} \oplus \cdots$ до s. □

Пример. Пусть $n = 300 = 2^2 \cdot 3 \cdot 5^2$.

$$A = \mathbb{Z}_{300} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{5^2}.$$

Дополнение. *Теорема единственности.* Если $A \cong \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{k_s}}, B \cong \mathbb{Z}_{q_1^{l_1}} \oplus \cdots \oplus \mathbb{Z}_{q_t^{l_t}}$. $A \cong B \Leftrightarrow t = s, p_i = q_i$ (с точностью до нумерации) и $k_i = l_i, 1 \leqslant i \leqslant s$.

Пример.

60.42 (б) Изоморфны ли группы $\mathbb{Z}_6 \oplus \mathbb{Z}_{36}$ и $\mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$?

Решение. Пусть $A = \mathbb{Z}_6 \oplus \mathbb{Z}_{36} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2} (6 = 2 \cdot 3, 36 = 2^2 \cdot 3^2)$. $B = \mathbb{Z}_{12} \oplus \mathbb{Z}_{18} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} (12 = 2^2 \cdot 3, 18 = 2 \cdot 3^2)$. По теореме единственности $A \cong B$.

6.0.3 Разбор задач

60.39 (ж) Найти с точностью до изоморфизма все абелевы группы порядка 36.

Решение. $36 = 2^2 \cdot 3^2$. Если $|A| = 36$, то из основной теоремы следует, что $A \cong B \oplus C, |B| = 2^2, |C| = 3^2$. B и C можно разложить в прямую сумму циклических групп: $B \cong \mathbb{Z}_4$ или $\mathbb{Z}_2 \oplus \mathbb{Z}_2$; $C \cong \mathbb{Z}_9$ или $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Нужно собрать вместе слагаемые из B и из C:

$$\left.\begin{array}{ccc} \mathbb{Z}_4 \oplus \mathbb{Z}_9 & \text{или} & \mathbb{Z}_4 \oplus \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 & \text{или} & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \end{array}\right\} 4 \text{ варианта}$$

Задача. Сколько существует неизоморфных абелевых групп порядка 600?

Решение. $600 = 2^3 \cdot 3 \cdot 5^2 \Rightarrow A \cong B \oplus C \oplus D, |B| = 2^3, |C| = 3, |D| = 5^2$.

$|A| = |B| \cdot |C| \cdot |D|$

$$B \cong \left[\begin{array}{ll} \mathbb{Z}_{2^3} = B_1 & B \cong \mathbb{Z}_{2^{n_1}} \oplus \mathbb{Z}_{2^{n_2}} \oplus \mathbb{Z}_{2^{n_3}} \quad \Rightarrow \\ \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 = B_2 & |B| = 2^{n_1} \cdot 2^{n_2} \cdot 2^{n_3} = 2^{n_1+n_2+n_3} = 2^3 \quad \Rightarrow \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 = B_3 & n_1 + n_2 + n_3 = 3\,(3 = 3+0+0, 3 = 2+1) \end{array}\right.$$

$$C \cong \mathbb{Z}_3; D \cong \left[\begin{array}{l} \mathbb{Z}_{5^2} = D_1 \\ \mathbb{Z}_5 \oplus \mathbb{Z}_5 = D_2 \end{array}\right.$$

$$A \cong B_i \oplus C \oplus D_j, 1 \leqslant i \leqslant 3, 1 \leqslant j \leqslant 2 - \text{всего 6 групп.}$$

Замечание. Сколько существует неизоморфных абелевых групп порядка p^n, p — простое число, n — натуральное число?

$$A \cong \mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_k}};$$
$$|A| = p^{n_1} \cdot p^{n_2} \cdot \cdots \cdot p^{n_k} = p^{n_1+n_2+\cdots+n_k} = p^n, \text{ значит, } \sum_{i=1}^{k} n_i = n.$$

Ответ: число таких групп равно числу разбиений n на натуральные слогаемые (k не фиксировано, порядок слагаемых не играет роли) $P(n)$, формула для него неизвестна.

60.44 (а) Доказать, что $A = \langle a \rangle_2 \oplus \langle b \rangle_2 \cong V_4$.

Решение. $A = \{0, a, b, a+b\}, V_4 = \{e, g, h, k \mid g^2 = h^2 = k^2 = e, gh = hg = k\}$. Определим гомоморфизм ϕ: $A \to V_4, a \mapsto g, b \mapsto h$. Покажем, что это изоморфизм групп.

1) доказательство инъективности отображения ϕ:

$c + d = 0 \Leftrightarrow c = 0, d = 0 \Leftrightarrow c = 2n_1 a, d = 2n_2 b \Leftrightarrow \phi(c) = \phi(2n_1 a) = \phi(a)^{2n_1} = g^{2n_1} = (g^2)^{n_1} = e^{n_1} = e, \phi(d) = \phi(2n_2 b) = \phi(b)^{2n_2} = h^{2n_2} = (h^2)^{n_2} = e^{n_2} = e \Leftrightarrow \phi(c+d) = \phi(c)\phi(d) = e \cdot e$.

2) доказательство сюръективности отображения ϕ:

так как $\phi(a+a) = \phi(b+b) = \phi((a+b)+(a+b)) = 0$, то $|\phi(A)| = 4 = |V_4|$.

60.42 (в) Изоморфны ли группы $\mathbb{Z}_6 \oplus \mathbb{Z}_{36}$ и $\mathbb{Z}_9 \oplus \mathbb{Z}_{24}$?

Решение. $|\mathbb{Z}_6 \oplus \mathbb{Z}_{36}| = 6 \cdot 36 = 216$; $|\mathbb{Z}_9 \oplus \mathbb{Z}_{24}| = 9 \cdot 24 = 216$ — равны.

Представим эти группы в виде суммы примарных циклических групп: $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$, $36 = 2^2 3^2 \Rightarrow \mathbb{Z}_{36} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2} \Rightarrow \mathbb{Z}_6 \oplus \mathbb{Z}_{36} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2}$.

Для второй группы $\mathbb{Z}_9 \oplus \mathbb{Z}_{24}$: $9 = 3^2$ — уже степень 3, раскладывать не надо. $24 = 2^2 \cdot 3 \Rightarrow \mathbb{Z}_{24} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3$, в целом $\mathbb{Z}_9 \oplus \mathbb{Z}_{24} \cong \mathbb{Z}_{3^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3$, но в первой группе есть элементы порядка 2 и 2^2, а во второй группе есть элементы порядка $2^3 \Rightarrow$ неизоморфны.

60.53 Пусть A — свободная абелева группа с базисом x_1, x_2, x_3, B — её подгруппа с базисом $y_1 = x_1 + x_2 + 4x_3, y_2 = 2x_1 - x_2 + 2x_3$. В группе A/B рассмотреть смежный класс $(x_1 + 2x_3) + B = \bar{y}_3$, если обозначить $y_3 = x_1 + 2x_3$. Найти порядок элемента $\bar{y}_3$, т. е. наименьшее число $k \in \mathbb{N}$ такое, что $a\bar{y}_3 = \bar{0} \Leftrightarrow k(x_1 + 2x_3) \in B$.

Решение. Составим матрицу из координат y_1, y_2, y_3:

$$C = \begin{pmatrix} 1 & 1 & 4 \\ 2 & -1 & 2 \\ 1 & 0 & 2 \end{pmatrix}.$$

Преобразования строк этой матрицы означают вычисление линейных комбинаций y_1, y_2, y_3.

$$C \xrightarrow{(1)+(2)} \begin{pmatrix} 3 & 0 & 6 \\ 2 & -1 & 2 \\ 1 & 0 & 2 \end{pmatrix}.$$

Видно, что $y_1 + y_2 = 3y_3 \Rightarrow$ если умножить y_3 на 3, то $3y_3 \in B \Rightarrow$ порядок элемента $\bar{y}_3$ равен 3.

Д.З.	60.39 (з), 60.42 (в, г), 60.44 (а), 60.52 (е, к)

Лекция 7

7.1 Коммутаторы и коммутант

Пусть G — произвольная группа.

Определение 7.1. *Коммутатор элементов g_1, g_2 — это элемент группы $g \in G$, определяемый через выражение:*

$$g \overset{обозн.}{=} [g_1, g_2] \overset{опр.}{=} g_1 g_2 g_1^{-1} g_2^{-1}.$$

Утверждение 7.1. *Для любых $g_1, g_2 \in G$ верно:*

$$g_1 g_2 = g_2 g_1 \text{ (коммутируют)} \Leftrightarrow [g_1, g_2] = e.$$

Доказательство.

$\Rightarrow$

Пусть $g_1 g_2 = g_2 g_1 \mid \cdot g_1^{-1} \Rightarrow g_1 g_2 g_1^{-1} = g_2 \mid \cdot g_2^{-1} \Rightarrow g_1 g_2 g_1^{-1} g_2^{-1} = e$ — верно, $[g_1, g_2] = e$.

$\Leftarrow$

Дано, что $g_1 g_2 g_1^{-1} g_2^{-1} = e \mid \cdot g_2 \Rightarrow g_1 g_2 g_1^{-1} = g_2 \mid \cdot g_1 \Rightarrow g_1 g_2 = g_2 g_1$. □

Обозначим $K(G)$ множество всех коммутаторов в G:

$$K(G) = \{[g, h] \mid g, h \in G\} \subseteq G.$$

Замечание 7.1. *$K(G)$ может не быть группой, поскольку существуют такие группы G, в которых $[g_1, h_1] \cdot [g_2, h_2]$ не является коммутатором.*

Определение 7.2. *Коммутантом группы G называется подгруппа в G, порожденная всеми коммутаторами:*

$$G' \overset{опр.}{=} \langle [g, h] \mid g, h \in G \rangle$$

Утверждение 7.2. *Для любых $g, h \in G$ верно:*

$$[h, g] = [g, h]^{-1}.$$

Доказательство.

$$[h,g] = hgh^{-1}g^{-1} = (ghg^{-1}h^{-1})^{-1}.$$

□

Это позволяет дать определение коммутанта в виде:

$$G' = \{[g_1,h_1]\cdot[g_2,h_2]\cdots[g_k,h_k] \mid g_i,h_i \in G, k = 1,2,\ldots\}$$

Теорема 7.1. *Для любой группы G*

1. *G' — нормальная подгруппа в G ($G' \lhd G$).*
2. *G/G' — абелева группа.*
3. *Если $N \lhd G$ такая, что G/N абелева группа, то $G' \leqslant N$.*

Пункт 3 означает, что коммутант — самая маленькая нормальная подгруппа в G, факторгруппа по которой абелева.

Доказательство.

1. G' — подгруппа по построению. Достаточно доказать, что если $a \in G'$, то $\forall g \in G, gag^{-1} \in G'$.

Если $a = [g_1,h_1]$, то $gag^{-1} = g(g_1h_1g_1^{-1}h_1^{-1})g^{-1} = (gg_1g^{-1})(gh_1g^{-1})(gg_1^{-1}g^{-1})(gh_1^{-1}g^{-1}) = [gg_1g^{-1}, gh_1g^{-1}] \in K(G)$.

В общем случае

$$a = [g_1,h_1]\cdot[g_2,h_2]\cdots[g_k,h_k] \Rightarrow$$
$$gag^{-1} = [gg_1g^{-1}, gh_1g^{-1}]\cdot[gg_2g^{-1}, gh_2g^{-1}]\cdots[gg_kg^{-1}, gh_kg^{-1}] \in G'$$
$$(\text{можно доказать индукцией по } k) \Rightarrow G' \lhd G.$$

2. $G/G' = \{gG' \mid g \in G\}$.

$[gG', hG'] \overset{\text{опр.}}{=} [g,h]G' = G' = \bar{e}$ в факторгруппе. $[g,h] \in G' \Rightarrow G/G'$ — абелева.

3. По условию $[gN, hN] = [g,h]N = N = \bar{e} \Rightarrow [g,h] \in N \Rightarrow G' \subseteq N$.

□

7.1.1 Коммутанты некоторых групп

(1) Группа кватернионов: $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$, причём

$[i,j] = i\cdot j\cdot(i^{-1})\cdot(j^{-1}) = i\cdot j\cdot(-i)\cdot(-j) = (ij)^2 = k^2 = -1$. Также $[i,k] = i\cdot k\cdot(i^{-1})\cdot(k^{-1}) = i\cdot j\cdot(-k)\cdot(-k) = (ik)^2 = (-j)^2 = -1$, и $[j,k] = -1$ (проделать самостоятельно) $\Rightarrow Q_8' = \{1,-1\}$.

Определим, чему изоморфна $Q_8/Q_8' = Q_8/\{1,-1\}$: она порядка 4, поэтому либо $\cong \mathbb{Z}_4$, либо $\cong V_4$.

Покажем, что $Q_8/\{1,-1\} \cong V_4$. Для этого покажем, что в факторгруппе все элементы $\bar{g} = gQ_8'$ дают $\bar{g}^2 = \bar{e}^2$.

К примеру, $(iQ_8')^2 = i^2 Q_8' = -Q_8' = Q_8'$, то есть $\bar{i}^2 = \bar{e}^2$, и так для остальных классов.[1]

(2) Группа диэдра: $D_n = \langle a, b \mid a^n = e, b^2 = e; bab^{-1} = a^{-1} \rangle$.

Решение. Вычислим $[a,b] = aba^{-1}b^{-1} = a(\underbrace{ba^{-1}b^{-1}}_{(a^{-1})^{-1}=a}) = a^2 \in D_n' \Rightarrow$ вся циклическая подгруппа $\langle a^2 \rangle = \{e, a^2, a^4, \ldots\}$ (все четные степени): $\langle a^2 \rangle \leqslant D_n'$.

Пусть $n = 3$, то есть $G = D_3$ — группа треугольника: $a = R_0^{2\pi/3}, a^2 = R_0^{4\pi/3} = R_0^{-2\pi/3} \Rightarrow \langle a^2 \rangle = \langle a \rangle$ — вся группа вращений $C_3 \Rightarrow D_3' = C_3$.

Пусть $n = 4$ — группа квадрата. $a = R_0^{\pi/2}, a^2 = R_0^{\pi}$ — центральная симметрия $\Rightarrow |\langle a \rangle| = 4$, то $\left|\langle a^2 \rangle\right| = 2, \langle a^2 \rangle = \{E, -E\}$ порядка 2.

Заметим, что $\frac{|D_4|}{|\langle a^2 \rangle|} = \frac{8}{2} = 4$, группа порядка 4 — абелева $\Rightarrow \langle a^2 \rangle \geqslant G'$, а раньше мы показали, что $\langle a^2 \rangle \leqslant G' \Rightarrow \langle a^2 \rangle = G'$ имеет порядок 2.

В общем случае: $C_n = \langle a \rangle, a = R_0^{2\pi/n}; \langle a^2 \rangle = \langle a \rangle = C_n$, если n нечетно, так как $\left|\langle a^2 \rangle\right| = |\langle a \rangle| = n$; а при четном n, $\langle a^2 \rangle$ — повороты на четные углы $\frac{2\pi}{n} \cdot 2k$, $\left|\langle a^2 \rangle\right| = \frac{n}{2} = m, (n = 2m)$ и $\left|D_n / \langle a^2 \rangle\right| = \frac{2n}{m} = \frac{4m}{m} = 4 \Rightarrow D_n / \langle a^2 \rangle$ — абелева, и $D_n' = \langle a^2 \rangle$ имеет порядок m.

7.1.2 Коммутант группы S_n

Теорема 7.2. *При $n \geqslant 3$, $S_n' = A_n$ — знакопеременная группа, то есть группа четных подстановок из S_n.*

Доказательство является следствием следующих двух лемм.

Лемма 7.1. *Если $\sigma, \tau \in S_n$, то $[\sigma, \tau]$ — четная подстановка.*

Доказательство. Напомним, что любая подстановка разлагается в произведение транспозиций: $\sigma = (i_1, j_1) \cdots (i_k, j_k)$. В этом случае знак σ, $\operatorname{sign}(\sigma) = (-1)^k \Rightarrow \operatorname{sign}(\sigma_1 \sigma_2) = \operatorname{sign}(\sigma_1) \cdot \operatorname{sign}(\sigma_2)$.

Тогда $\operatorname{sign}([\sigma, \tau]) = \operatorname{sign}(\sigma) \operatorname{sign}(\tau) \operatorname{sign}(\sigma^{-1}) \operatorname{sign}(\tau^{-1})$. Но $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma^{-1})$: если $\sigma = (i_1, j_1) \cdots (i_k, j_k)$, то $\sigma^{-1} = (i_k, j_k) \cdots (i_1, j_1) \Rightarrow \operatorname{sign}(\sigma^{-1}) = (-1)^k = \operatorname{sign}(\sigma)$ Значит, $\operatorname{sign}([\sigma, \tau]) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\sigma^{-1}) \cdot \operatorname{sign}(\tau) \cdot \operatorname{sign}(\tau^{-1}) = 1 \Rightarrow [\sigma, \tau]$ — четная $\Rightarrow S_n' \leqslant A_n$.

Лемма 7.2. *Группа $A_n, n \geqslant 3$ порождается циклами длины 3.*

Доказательство. Любая четная подстановка имеет вид:

$$\sigma = (i_1, j_1)(i_2, j_2) \cdots (i_{2k-2}, j_{2k-2})(i_{2k}, j_{2k}) =$$
$$= \big((i_1, j_1)(i_2, j_2)\big) \cdots \big((i_{2k-2}, j_{2k-2})(i_{2k}, j_{2k})\big).$$

Вычислим произведение любых двух транспозиций:

[1] Между прочим, в данном случае $Q_8' = \{1, -1\} = Z(Q_8)$ — центр, а факторгруппа неабелевой группы по центру не может быть циклической.

i) $i_2 = j_1$, а i_1, i_2, j_2 различные, тогда

$$(i_1, j_1)(i_2, j_2) = (i_2, j_2, i_1);$$

ii) Все i_1, i_2, j_1, j_2 различные (значит, $n \geqslant 4$).

Запишем $(i_1, j_1)\underbrace{(j_1, i_2)(j_1, i_2)}_{e}(i_2, j_2) = \big((i_1, j_1)(j_1, i_2)\big)\big((j_1, i_2)(i_2, j_2)\big) =$ это произведение двух циклов длины 3 $\Rightarrow$ все σ — произведение циклов длины 3. $\square$

Пусть i_1, j_1, j_2 различные:

$$[(i_1, j_1), (j_1, j_2)] = (i_1, j_1)(j_1, j_2)(i_1, j_1)(j_1, j_2) = (j_1, i_1, j_2)$$
$$i_1 \leftarrow j_1 \leftarrow j_2 \leftarrow j_2 \leftarrow j_1$$
$$j_2 \leftarrow j_2 \leftarrow j_1 \leftarrow i_1 \leftarrow i_1$$

Для любого цикла σ длины 3 можно так подобрать две транспозиции τ_1 и τ_2, чтобы $[\tau_1, \tau_2] = \sigma \Rightarrow S'_n \geqslant A_n \Rightarrow S'_n = A_n$. $\square$

7.1.3 Коммутанты высших порядков. Разрешимые группы

Определение 7.3. *Второй коммутант:* $G'' \overset{опр.}{=} (G')'$ *(сам* G' *— первый коммутант).*

В общем случае, рекурсивно определяются дальнейшие коммутанты: третий коммутант $G''' \overset{опр.}{=} (G'')'$ *и так далее, то есть, если уже построен* n*-ый коммутант* $G^{(n)}$*, то* $G^{(n+1)} \overset{опр.}{=} (G^{(n)})', n = 1, 2, \ldots$.

Получаем вложенную цепочку подгрупп:

$$G = G^{(0)} \geqslant G' \geqslant G'' \geqslant \ldots \geqslant G^{(n)} \geqslant G^{(n+1)} \geqslant \ldots.$$

Определение 7.4. *Группа* G *называется разрешимой, если* $\exists n \in \mathbb{N}$ *такое, что* $G^{(n)} = \{e\}$.

Примеры.

1) Если G — абелева, то $G' = \{e\}$, так что G разрешима.

2) $G = D_n \Rightarrow D'_n = \langle a^2 \rangle$ — циклическая $\Rightarrow$ абелева $\Rightarrow D''_n = \{e\}$, так что D_n разрешима.

Уточнение. Если считать, что n — наименьшее с условием $G^{(n)} = \{e\}$, то n — ступень разрешимости группы G.

По определению G разрешима ступени n, если включения строгие:

$$G = G^{(0)} > G' > G'' > \ldots > G^{(n-1)} > G^{(n)} = \{e\}.$$

Например, D_n, $n \geqslant 3$, разрешима ступени 2.

Теорема 7.3. *Для любого $k \geqslant 1$, k-й коммутант $G^{(k)} \lhd G$.*

Доказательство. Индукция по k.

`База:` $k = 1$. $G' \lhd G$ — свойство G', которое было доказано ранее.

`Индуктивный переход:` Допустим, что доказано, что $G^{(k)} \lhd G$ для некоторого фиксированного k. Докажем утверждение для $G^{(k+1)}$.

Поскольку любой $h \in G^{(k+1)}$ — произведение коммутаторов вида $[a, b]$, где $a, b \in G^{(k)}$, то для доказательства утверждения достаточно проверить, что для $\forall g \in G$ $g[a, b]g^{-1} \in G^{(k+1)}$. Однако, несложно убедиться, что:

$$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}],$$

где по предположению индукции $gag^{-1}, gbg^{-1} \in G^{(k)}$, и поэтому $ghg^{-1} \in G^{(k+1)}$, $\forall h \in G^{(k+1)}$. □

Замечание 7.2. *В ряду нормальных подгрупп:*

$$G = G^{(0)} \rhd G' \rhd G'' \rhd \ldots \rhd G^{(k)} \rhd G^{(k+1)} \rhd \ldots$$

факторгруппы абелевы $G^{(k)}/G^{(k+1)}$, так как $G^{(k+1)} = (G^{(k)})'$.

Теорема 7.4 (Основная теорема о разрешимых группах)**.**

1. Если группа G разрешима, $\forall H < G \Rightarrow H$ — разрешима.

2. Если группа G разрешима, $N \lhd G \Rightarrow G/N$ — разрешима.

3. Признак разрешимости. Если группа G имеет разрешимую нормальную подгруппу $N \lhd G$ такую что G/N — разрешима, то G — разрешима.

Доказательство.

1. Очевидно, что $\forall k = 1, 2, \ldots, H^{(k)} \leqslant G^{(k)}$, поэтому если $G^{(n)} = \{e\}$, то и $H^{(n)} = \{e\}$, то есть H разрешима.

2. Покажем, что $(G/N)^{(k)} = (G^{(k)}N)/N, k = 1, 2, \ldots$. Если это уже доказано, и $G^{(n)} = \{e\}$, то $(G/N)^{(n)} = (G^{(n)}N)/N = \{\bar{e}\}$.

$$(G/N)' = \langle [gN, hN] \rangle = [gN, hN] = [g, h]N \subseteq G'N \Rightarrow$$
$$\text{можно рассмотреть } (G'N)/N.$$

Используем канонический гомоморфизм $\pi\colon G \overset{\text{на}}{\to} G/N, \pi(g) = gN$.

При этом $\pi(G') = (G/N)'$, а по теореме о соответствии подгрупп, $\pi^{-1}\big((G/N)'\big) = G/N$.

Для $k > 1$ — индукция по k.

Лемма 7.3. *Если $\phi\colon G \to H$ — сюръективный гомоморфизм, то $\forall k = 1, 2, \ldots$: $\phi(G^{(k)}) = H^{(k)}$.*

Доказательство леммы. Индукция по k.

`База.` $k = 1$: $\phi(G') = H' = \langle [h_1, h_2] \mid h_1, h_2 \in H \rangle$. Так как ϕ — сюръективное отображение $\Rightarrow \exists g_1 \in G, \phi(g_1) = h_1$, $\exists g_2 \in G, \phi(g_2) = h_2$, тогда $[h_1, h_2] = h_1 h_2 h_1^{-1} h_2^{-1} = \phi(g_1)\phi(g_2)\phi(g_1)^{-1}\phi(g_2)^{-1} = \phi(g_1)\phi(g_2)\phi(g_1^{-1})\phi(g_2^{-1}) = \phi(g_1 g_2 g_1^{-1} g_2^{-1}) = \phi([g_1, g_2])$.

Таким образом любой коммутатор $[h_1, h_2]$ — образ некоторого коммутатора в группе $G \Rightarrow H' = \langle [h_1, h_2] \rangle = \langle \phi([g_1, g_2]) \rangle \Rightarrow \phi(G') = H'$.

`Предположение индукции.` Пусть для k уже доказано, что $\phi(G^{(k)}) = H^{(k)}$, докажем, что $\phi(G^{(k+1)}) = H^{(k+1)}$. Применим лемму с $k = 1$ и с $G^{(k)}, H^{(k)}$ вместо G, H, и тогда $\phi(G^{(k+1)}) = \phi((G^{(k)})') = (H^{(k)})' = H^{(k+1)} \Rightarrow$ по принципу индукции доказали для всех k. □

Возврат к доказательству п. 2. По условию, $G^{(n)} = \{e\}$.

Обозначим за $H = G/N$ и $\phi\colon G \to H, \phi(g) = gN$ — канонический гомоморфизм.

По лемме $\phi(G^{(n)}) = H^{(n)}$, но так как $G^{(n)} = \{e\}$, то $\phi(G^{(n)}) = \{\bar{e}\} = H^{(n)} \Rightarrow H$ — разрешима.

3. Пусть $m \in \mathbb{N}$ таково, что $N^{(m)} = \{e\}$ (т. к. N разрешима) и $p \in \mathbb{N}$ таково, что $(G/N)^{(p)} = \{\bar{e}\}$ (в факторгруппе $G/N, \bar{e} = eN = N$ как один элемент).

Докажем, что $G^{(m+p)} = \{e\}$. Так как $(G/N)^{(p)} = \{\bar{e}\}$, а по лемме $(G/N)^{(p)} = \phi(G^{(p)}) \Rightarrow G^{(p)} \subseteq N \Rightarrow (G^{(p)})^{(m)} \subseteq N^{(m)} = \{e\} \Rightarrow G^{(m+p)} = \{e\}$. □

Утверждение 7.3. *Пусть A, B — группы, $A \times B = \{(a, b) \mid a \in A, b \in B\}$. Тогда $(A \times B)' = A' \times B'$.*

Доказательство. По определению $(A \times B)' = \langle [(a_1, b_1), (a_2, b_2)] \mid a_i \in A, b_i \in B \rangle$.

Вычислим поэтому:

$$\begin{aligned}[(a_1, b_1), (a_2, b_2)] &= (a_1, b_1)(a_2, b_2)(a_1, b_1)^{-1}(a_2, b_2)^{-1} = \\ &= (a_1, b_1)(a_2, b_2)(a_1^{-1}, b_1^{-1})(a_2^{-1}, b_2^{-1}) = \\ &= (a_1 a_2 a_1^{-1} a_2^{-1}, b_1 b_2 b_1^{-1} b_2^{-1}) = ([a_1, a_2], [b_1, b_2]) \in A' \times B'.\end{aligned}$$

Таким образом произвольный коммутатор из $(A \times B)'$ принадлежит $A' \times B'$, но A' порождается коммутаторами $[a_1, a_2]$, а B' порождается коммутаторами $[b_1, b_2] \Rightarrow$ они порождают всю группу $A' \times B'$. □

Обобщение 7.1. *Для $\forall k \in \mathbb{N}$, $(A \times B)^{(k)} = A^{(k)} \times B^{(k)}$.*

Следствие 7.1. *Если A и B разрешимы, то $A \times B$ тоже разрешима.*

Доказательство. Допустим, что $A^{(m)} = \{e_1\}, B^{(p)} = \{e_2\}$. Положим $n = \max(m, p)$, тогда $A^{(n)} = \{e_1\}$ и $B^{(n)} = \{e_2\} \Rightarrow (A \times B)^{(n)} = A^{(n)} \times B^{(n)} = \{e_1\} \times \{e_2\} = \{e\} (e = (e_1, e_2), e_1 \in A, e_2 \in B)$. □

62.7 (б) Найти коммутант группы A_4.

Решение. A_4 неабелева $\Rightarrow e \neq A_4' \lhd A_4$.

В A_4 есть нормальная подгруппа $V_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \lhd A_4$, $|V_4| = 4, |A_4| = \frac{1}{2}4! = 12 \Rightarrow |A_4/V_4| = 3$, группа порядка 3 абелева $\Rightarrow$
по пункту 3 теоремы о свойствах коммутанта $A_4' \leqslant V_4$.

Значит коммутант представляет собой нормальную подгруппу, которая содержится в V_4. Однако ни одна из подгрупп второго порядка не является нормальной в A_4. В самом деле, вычислим, например:

$$(1,2,3)(1,2)(3,4)(1,2,3)^{-1} = (1,2,3)(1,2)(3,4)(3,2,1) = (1,4)(2,3) \text{ и}$$
$$(1,3,2)(1,2)(3,4)(1,3,2)^{-1} = (1,3,2)(1,2)(3,4)(1,2,3) = (1,3)(2,4),$$
$$\text{т. е. оба этих элемента} \neq e,$$

а это означает, что для любой подгруппы $H < V_4$, $|H| = 2$, существует элемент $\sigma \in A_4$ такой, что $\sigma H \sigma^{-1} \neq H$. В нашем примере, если $H = \{e, (1,2)(3,4)\}$, то для $\sigma = (1,2,3)$ $\sigma H \sigma^{-1} = \{e, (1,4)(2,3)\} \neq H$, а $\sigma^{-1} H \sigma = \{e, (1,3)(2,4)\} \neq H$.

Окончательно делаем вывод, что $A_4' = V_4$.

Д.З.	62.3, 62.6, 62.7 (б, в), 62.12 (а, б, в) (в том числе определить ступень разрешимости)

Лекция 8

8.1 Действия групп на множествах

Пусть X — непустое множество. Обозначим $S_X = \{\, \sigma \colon X \to X \,\}$, σ — биективное отображение (т. е. перестановка на X), с операцией композиции: $(\sigma_2 \circ \sigma_1)(x) = \sigma_2(\sigma_1(x))$, $\forall x \in X, \sigma_1, \sigma_2 \in S_X$. Множество S_X является группой, в ней e — тождественное преобразование, и $\forall \sigma \in S_X$, σ^{-1} — обратное отображение.

Определение 8.1. *Скажем, что группа G действует на множестве X, если задан гомоморфизм*

$$\rho : G \to S_X.$$

Это значит, что любому $g \in G$ сопоставлено биективное отображение $\rho(g)$ на X, причем $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2), \forall g_1, g_2 \in G$.

Из этого следует, что $\rho(e) = id$ — тождественное преобразование на X, то есть $\forall x \in X, id(x) = x$. Тогда $\rho(G) \leqslant S_X, \rho(G)$ — группа перестановок, отвечающая группе G. По теореме о гомоморфизме:

$$\rho(G) \cong G/\operatorname{Ker}\rho.$$

Если $\operatorname{Ker}\rho = \{e\}$, то действие ρ называется *эффективным*.

Термины. Орбита точки $x \in X$ — это множество

$$Orb(x) = \{\, y = \rho(g)(x) \mid g \in G \,\} \subseteq X.$$

Сокращённая запись действия элемента $g \in G$: $\rho(g) \cdot x$ или ещё короче $g \cdot x$, также возможно обозначение $G(x)$.

Стабилизатор точки $x \in X$ — это множество

$$St(x) = \{\, g \in G \mid \rho(g) \cdot x = x \,\} = G_x.$$

Теорема 8.1. *Стабилизатор G_x точки $x \in X$ — подгруппа в G.*

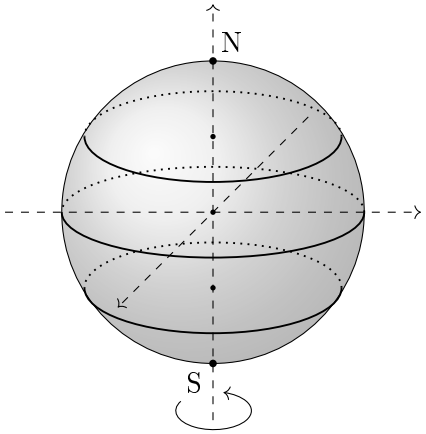
Доказательство. $e \in G_x$; $\forall g_1, g_2 \in G_x, \rho(g_1 g_2) \cdot x = \rho(g_1)(\rho(g_2) \cdot x) = \rho(g_1) \cdot x = x \Rightarrow g_1 g_2 \in G_x$; $\forall g \in G_x g^{-1} g \cdot x = x \Rightarrow id \cdot x = x = g^{-1} \cdot x$. □

Примеры.

(1) Пусть X — сфера $R = 1$: $x^2 + y^2 + z^2 = 1$. N и S — северный и южный полюса. G — группа поворотов пространства вокруг оси Oz.

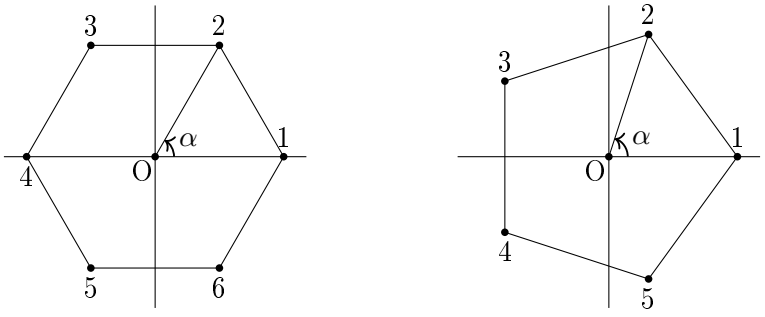
$$G = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \cong SO(2).$$

Орбиты точек этой сферы: $\{N\}$ и $\{S\}$ — неподвижные, их орбиты состоят из одной точки. Остальные орбиты — это окружности — параллели точек.



(2) Рассмотрим правильный n-угольник. $G = D_n$ — группа диэдра. X — множество вершин этого многоугольника, т. е. $X = \{1, 2, 3, \ldots, n\}$. Орбита точки 1: $R_0^{\frac{2\pi}{n}}(1) = 2, R_0^{\frac{2\pi}{n}}(2) = 3, \ldots, R_0^{\frac{2\pi}{n}}(n) = 1$. Значит, все точки $1, 2, 3, \ldots, n$ циклически переставляются и образуют одну орбиту.

Стабилизатор вершины: $G_{\{i\}} = \{id, S_i\}, S_i$ — симметрия относительно оси, проходящей через i-ю вершину.



Определение 8.2. *Действие ρ группы G на множестве X называется транзитивным, если $X = Orb\{x_0\}$ для некоторой точки x_0.*

Это значит, что $\forall x \in X\ \exists g \in G$ такой, что $x = g \cdot x_0$.

Утверждение 8.1. *Действие транзитивно тогда и только тогда, когда для любых точек x и $y \in X$ $\exists g \in G$: $g \cdot x = y$.*

Доказательство. Пусть $X = Orb(x_0) \Rightarrow$ для $x \in X$ $\exists g_1 \in G$: $x \overset{(1)}{=} g_1 \cdot x_0$, для $y \in X$ $\exists g_2 \in G$: $y \overset{(2)}{=} g_2 \cdot x_0$; надо найти $g \in G$, чтобы $g \cdot x = y$.

Из (1) $\Rightarrow x_0 = g_1^{-1} \cdot x$, подставим x_0 в (2): $y = g_2 \cdot (g_1^{-1} \cdot x) = (g_2 \cdot g_1^{-1}) \cdot x \Rightarrow g = g_2 \cdot g_1^{-1}$.

Обратно: возьмем x_0 вместо x, x вместо $y \Rightarrow \exists g \in G$: $g \cdot x_0 = x$. $\Rightarrow Orb(x_0) = X$. □

Теорема 8.2. *Пусть G действует на множестве $X \neq \emptyset$. Тогда выполнены следующие утверждения:*

1. *Если $Orb(x_1)$ и $Orb(x_2)$ различные орбиты, то $Orb(x_1) \cap Orb(x_2) = \emptyset$.*
2. *Множество X — объединение попарно непересекающихся орбит:*

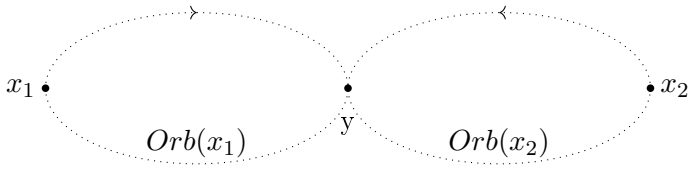
$$X = \bigsqcup_{i \in I} Orb(x_i), \text{ где } \{x_i\} \text{ — полная система представителей орбит.}$$

3. *Имеется биекция: $Orb(x_0) \leftrightarrow G/G_{x_0} = \{gG_{x_0} \mid g \in G\}$.*

Доказательство.

1. От противного. Допустим, что $\exists y \in Orb(x_1) \cap Orb(x_2) \Rightarrow \exists g_1 \in G$: $y = g_1 \cdot x_1$ и $\exists g_2 \in G$: $y = g_2 \cdot x_2 \Rightarrow g_1 \cdot x_1 = g_2 \cdot x_2 \Rightarrow x_2 = (g_2^{-1} g_1) x_1$, то есть $x_2 \in Orb(x_1) \Rightarrow Orb(x_2) \subseteq Orb(x_1)$.

Наоборот, $x_1 = (g_1^{-1} g_2) x_2 \Rightarrow x_1 \in Orb(x_2) \Rightarrow Orb(x_1) \subseteq Orb(x_2) \Rightarrow Orb(x_1) = Orb(x_2)$ — вопреки условию, что они различные.



2. Очевидно, $\forall x \in X, x \in Orb(x)$, а именно $x = e \cdot x (e \in G) \Rightarrow X = \cup_{x \in X} Orb(x)$, чтобы получить непересекающиеся орбиты, нужно в этом разложении оставить только различные орбиты.

3. Нужно установить биекцию $Orb(x_0) \overset{f}{\to} G/G_{x_0}$.

Сначала допустим, что $y = g_1 \cdot x_0 = g_2 \cdot x_0 \Leftrightarrow (g_2^{-1} g_1) \cdot x_0 = x_0 \Leftrightarrow g_2^{-1} g_1 \in G_{x_0} \Leftrightarrow g_1 G_{x_0} = g_2 G_{x_0}$ [$g_2^{-1} g_1 \in G_{x_0} \to g_2^{-1} g_1 = h \in G_{x_0} \Rightarrow g_1 = g_2 h \mid \cdot h' \in G_{x_0} \Rightarrow g_1 h' = g_2 h h' \Rightarrow g_1 G_{x_0} \subseteq g_2 G_{x_0}$, и обратно $g_2 = g_1 h^{-1} \mid \cdot h' \in G_{x_0} \Rightarrow g_2 h' = g_2 h^{-1} h' \Rightarrow g_2 G_{x_0} \subseteq g_1 G_{x_0} \Rightarrow g_1 G_{x_0} = g_2 G_{x_0}$]

Это показывает, что надо определить $f(y) = gG_{x_0}$, где g — такой элемент, что $g \cdot x_0 = y$. И это отображение биективно.

Сюръективность: $\forall g \in G$ класс $gG_{x_0} = f(y)$, где $y = g \cdot x_0$.

Инъективность: если $f(y_1) = f(y_2)$, то $g_1 G_{x_0} = g_2 G_{x_0} \Rightarrow g_1 \cdot x_0 = g_2 \cdot x_0 \Rightarrow y_1 = y_2$. □

Иллюстрация п. 1 теоремы. Теорема о разложении подстановки в произведение непересекающихся циклов и единственность такого разложения.

Для доказательства берем подстановку $\sigma \in S_n, \sigma \neq e$.

Рассмотрим действие группы $G = \langle\sigma\rangle = \{e, \sigma, \sigma^2, \ldots, \sigma^{l-1}\}, \sigma^l = e$ на множестве $X = \{1, 2, \ldots, n\}$. Орбита $Orb(i) = \{i, \sigma(i), \sigma^2(i), \ldots, \sigma^{l-1}(i)\} = \{i_1 = i, i_2 = \sigma(i_1), i_3 = \sigma(i_2), \ldots, i_l = \sigma(i_{l-1})\}$. По пункту 1 теоремы 8.2 $X = \bigsqcup\limits_{i \in X} Orb(i)$ — это разбиение единственно, оно не зависит от алгоритма.

Теперь рассмотрим случай, когда $X = \{x_1, x_2, \ldots, x_n\}$, так что $|X| = n$, и группа G конечная ($|G| = m$).

Следствие 8.1. *Если группа G действует на непустом множестве X, и $x_0 \in G$ некоторая точка этого множества, тогда:*

1. $|Orb(x_0)| = |G/G_{x_0}| = \frac{|G|}{|G_{x_0}|}$.

2. *Формула орбит:* $|X| = \sum\limits_{i \in I} Orb(x_i) = \sum\limits_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$, *где r — количество орбит.*

57.3 (а) Пусть $V = \mathbb{R}^3, G = \{A \in M_{3\times3}(\mathbb{R}^3) \mid A^T = A^{-1}\}$, и действие G на V задаётся так: если $A \in G, X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3$, то $X \mapsto A \cdot X$. Найти стабилизаторы G_X.

Преобразование A сохраняет длины всех векторов (и потому углы). $|A \cdot X_O| = |X_O|$, орбита — сфера с центром $O, R = |X_O|$. $G_X = \{A \in G \colon A \cdot X = X\}$, т. е. G_X состоит из матриц, для которых X собственный вектор с $\lambda = 1$.

Выберем в пространстве ортонормированный базис $\vec{e}_1, \vec{e}_2, \vec{e}_3$, приняв за $\vec{e}_3$ вектор X. В этом базисе матрица оператора A будет иметь вид:

$$A' = \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} (\det A' = 1), \text{ либо } A'' = \begin{pmatrix} \cos\alpha & \sin\alpha & 0 \\ \sin\alpha & -\cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} (\det A'' = -1).$$

Если $O(2) = \{(B) \colon B^T = B^{-1}\}$ 2-го порядка, то $G_X = \left\{ \left(\begin{array}{cc|c} & & 0 \\ & B & 0 \\ \hline 0 & 0 & 1 \end{array} \right) \right\}, B \in O(2)$.

(i) B имеет вид A' или $A'' \Rightarrow G_X \cong O(2)$.

(ii) $|A| = 1 \Rightarrow G_X = \{A'\}, G_X \cong SO(2) = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \right\}$.

Д.З.	57.1 (а, б), 57.3, 57.8, 57.9 (а)

Лекция 9

9.0.1 Некоторые типичные действия, связанные с группой G

(1) $X = G$, действие группы G на себе левыми умножениями (левое регулярное действие группы G на себе).

Определение 9.1. $l_g(x) = g \cdot x \quad (\forall g \in G, \forall x \in X = G)$.[1]

Это действие, так как $(g_1 g_2)x = g_1(g_2 x) \Rightarrow l_{g_1 g_2} = l_{g_1} \cdot l_{g_2}$.

Оно транзитивное: для $\forall x, y \in X = G$ найдем элемент $g \in G$ такой, что $g \cdot x = y : g = yx^{-1}$.

Оно регулярное: это означает, что если $g \neq e$, то для $\forall x \in X, l_g(x) \neq x$. (то есть $\forall g \neq e$ не имеет неподвижных точек) $\Rightarrow$ эффективное. Если $gx = x \mid \cdot x^{-1} \Rightarrow g = e$.

Теорема 9.1 (Теорема Кэли)**.**
Любая группа G изоморфна транзитивной подгруппе группы S_X на некотором множестве X.

Доказательство. Возьмём $X = G$. На нём G будет действовать левыми умножениями: $g(x) = g \cdot x$.

Обозначим $l_g(x) = gx$. Было показано, что $l_{g_1 g_2} = l_{g_1} \cdot l_{g_2}$, т. е. $l \colon G \to S_X$ — гомоморфизм, причем ядро $\operatorname{Ker} l = \{g \in G \mid gx = x, \forall x \in G\} = e$ $gx = x \mid \cdot x^{-1} \Leftrightarrow g = e \Rightarrow l(G) \cong G$, а G действует транзитивно. □

(2) Действие группы G на множестве $G/H = \{xH \mid x \in G\}$ левых смежных классов по H.

Действие $l_g^H(xH) = g(xH) = (gx)H$ — левыми умножениями (Если $H = \{e\}$, это будет пример 1).

Это тоже действие: $l_{g_1 g_2}^H = l_{g_1}^H \cdot l_{g_2}^H$, так как $(g_1 g_2)(xH) = \big((g_1 g_2)x\big)H = \big(g_1 \cdot (g_2 x)\big)H = g_1(g_2 x)H = \big(l_{g_1}^H \cdot l_{g_2}^H\big)(xH)$.

Это действие транзитивное: $\forall x, y \in G\ \exists g \in G\ g(xH) = yH$, т. к. $g(xH) = (gx)H = yH$, то можно найти элемент $g \in G$, чтобы $y = gx \Rightarrow g = yx^{-1}$. Все смежные классы составляют одну орбиту.

[1] Точка — это умножение в G.

Определим стабилизатор (стационарную подгруппу) смежного класса xH, то есть множество $G_{xH} = \{g \in G \mid gxH = xH\}$. Для этого умножим слева на x^{-1} равенство $gxH = xH$:

$$(x^{-1}gx)H = H \Leftrightarrow x^{-1}gx \in H \Leftrightarrow g \in xHx^{-1}.$$

Ответ: $G_{xH} = xHx^{-1}$ (подгруппа, сопряженная с H посредством x). В частности, для $x = e$ остается H.

(3) Действие группы на себе сопряжениями. Пусть $X = G$, для $\forall x \in X$ и $\forall g \in G$ определим $A_g(x) = gxg^{-1}$ (сопряженный с x посредством g).

Орбита любого элемента x, $Orb(x) = \{gxg^{-1} \mid \forall g \in G\}$ — класс элементов, сопряженных с $x \in G$.

Обозначим $K(x)$ — класс элементов, сопряженных с x в G.

Основная теорема о разбиении множества на орбиты относительно группы преобретёт формулировку:

Теорема 9.2.

1. Любая группа G разбивается на попарно непересекающиеся классы сопряженных элементов:

$$G = \bigsqcup_{i \in I} K(x_i) \quad (K(x_i) \cap K(x_j) = \emptyset \text{ при } i \neq g).$$

2. [Предварительно введём термин. Для любого $x \in X = G$ стабилизатор элемента x равен $St(x) = G_x = \{g \in G \mid gxg^{-1} = x\} = C_G(x)$ — централизатор элемента x в G.]

$$K(x) \leftrightarrow G/C_G(x)$$

(множество левых смежных классов группы G по централизатору элемента x.)

Следствие 9.1. *Если G конечная ($|G| < \infty$), то $|K(x)| = \frac{|G|}{|C_G(x)|}$.*

Доказательство. $|K(x)| = |G/C_G(x)| = \frac{|G|}{|C_G(x)|}$. □

Следствие 9.2. $K(x) = \{x\} \Leftrightarrow x \in Z(G)$, *т. е. x — центральный элемент группы G.*

Доказательство. $K(x) = \{gxg^{-1} \mid \forall g \in G\}$, значит $gx = xg$ для $\forall g \in G$, т. е. $x \in Z(G)$. □

Следствие 9.3 (Формула классов)**.** *Пусть $Z(G)$ — объединение одноэлементных орбит. Тогда:*

$$G = Z(G) \cup \big(\bigcup_j K(x_j)\big),$$

где $x_j \notin Z(G)$ и поэтому $|K(x)| > 1$.

Для случая, когда $|G| < \infty$, получается:

$$|G| = |Z(G)| + \sum_{j=1}^{s} |K(x_j)| = |Z(G)| + \sum_{j=1}^{s} \frac{|G|}{|C_G(x_j)|}. \tag{9.1}$$

Задачи.

(1) Пусть $H < G$ конечного индекса $n \in \mathbb{N}$ ($n = |G/H|$ — количество смежных классов по H). Доказать, что существует нормальная подгруппа $N \lhd G$ индекса, делящегося на $n!$.

Идея: использовать действие группы G левыми умножениями на множестве $X = G/H$.

Решение. Действие $l_g^H(xH) = (gx)H$ задает гомоморфизм $l^H \colon G \to S_X$, $X = G/H, |X| = n$, поэтому $S_X \cong S_n$, $\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$.

В таком случае группа подстановок, отвечающая G, есть $l^H(G) \leqslant S_n$ и по теореме Лагранжа $\left|l^H(G)\right|$ делит $|S_n| = n!$.

По теореме о гомоморфизме $l^H(G) \cong G/\operatorname{Ker} l^H$, в качестве N можно взять $N = \operatorname{Ker} l^H$, т. к. $\left|l^H(G)\right| = \left|G/\operatorname{Ker} l^H\right|$ = индекс подгруппы N в G.

Определим ядро действия G на смежных классах по H. $g \in \operatorname{Ker} l^H \Leftrightarrow$ для $\forall x \in G$ $gxH = xH \Leftrightarrow g \in xHx^{-1}$.

Таким образом, $g \in \operatorname{Ker} l^H \Leftrightarrow g \in \bigcap\limits_{x \in G} xHx^{-1}$, так что:

$$N = \bigcap_{x \in G} xHx^{-1}$$

(термин: N — сердцевина H, N — наибольшая нормальная подгруппа группы G, содержащейся в H).

(2) Определить классы сопряжённых элементов в группах D_3 и D_4.

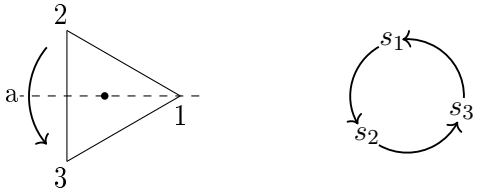
Решение. $\underline{n = 3.}$ $D_3 = \{e, a, a^2 = a^{-1}; s_1, s_2, s_3\} = \{e\} \cup \{a, a^{-1}\} \cup \{s_1, s_2, s_3\}$. Вспомним, $sas^{-1} = a^{-1}$, т. е. $\{a, a^{-1}\}$ — класс сопряженных элементов.

Упражнение: Доказать, что $\left|gxg^{-1}\right| = |x|$.

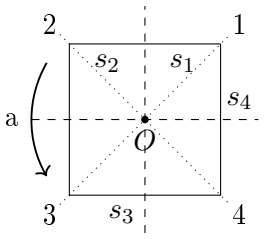
Проверим, что все симметрии сопряжены:

$$as_1a^{-1} = s_2, \text{ т. к. } 1 \overset{a^{-1}}{\mapsto} 3 \overset{s_1}{\mapsto} 2 \overset{a}{\mapsto} 3 \text{ т. е. } 1 \mapsto 3.$$

$$as_2a^{-1} = s_3, \text{ т. к. } 1 \overset{a^{-1}}{\mapsto} 3 \overset{s_2}{\mapsto} 1 \overset{a}{\mapsto} 2 \text{ т. е. } 1 \mapsto 2.$$



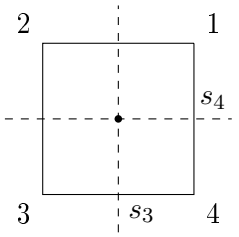
$\underline{n = 4.}$ $D_4 = \{e, a, a^2, a^3 = a^{-1}; s_1, s_2, s_3, s_4\}$, $a = R_O^{\pi/2}$, s_1, s_2 — симметрии относительно диагоналей, проходящих через вершины 1 и 2, s_3 и s_4 — симметрии относительно средних линий.



$a^2 = R_O^\pi$ — центральная симметрия; $\{e, a^2\} = Z(D_4)$.

Т. е. $\{e\}$ и $\{a^2\}$ отдельные классы. Для любой симметрии $s, sas^{-1} = a^{-1}$, т. е. $\{a, a^{-1}\}$ — отдельный класс. Рассмотрим $as_1a^{-1} = s_2$, и наоборот $\Rightarrow \{s_1, s_2\}$ — отдельный класс. $1 \overset{a^{-1}}{\to} 4 \overset{s_1}{\to} 2 \overset{a}{\to} 3 \Rightarrow 1 \leftrightarrow 3$

$as_3a^{-1} = s_4$, $1 \overset{a^{-1}}{\to} 4 \overset{s_3}{\to} 3 \overset{a}{\to} 4 \Rightarrow 1 \leftrightarrow 4$, т. е. $\{s_3, s_4\}$ — отдельный класс.



Итого: $D_4 = \{e\} \cup \{a^2\} \cup \{a, a^{-1}\} \cup \{s_1, s_2\} \cup \{s_3, s_4\}$ — 5 классов сопряженности.

Обобщение: если n нечетно, $n = 2m + 1$, то $Z(D_n) = \{e\}$. $D_n = \{e\} \cup \{s_1, \ldots, s_n\} \bigcup\limits_{k=1}^{\frac{n-1}{2}} \{a^k, a^{-k}\}$ (если $n = 2m + 1 \Rightarrow \frac{n-1}{2} = m$)

Если n чётно, $n = 2m$, то $Z(D_n) = \{e, a^n\}$, симметрии образуют два класса: $\{s_1, \ldots, s_m\}$ — относительно больших диагоналей; $\{s_{m+1}, \ldots, s_n\}$ — относительно средних линий, и $\{a^k, a^{-k}\}, k = 1, \ldots, m-1, D_n = \{e\} \cup \{s_1, \ldots, s_n\} \cup \{a^m\} \bigcup\limits_{k=1}^{m-1} \{a^k, a^{-k}\}$.

9.1 Теоремы Силова (Sylow)

Пусть G — группа, $|G| = p^n m$, p — простое число, $n \geqslant 1, m > 1$, т. е. $p^n \mid |G|$, $p^{n+1} \nmid |G|$.

Определение 9.2. *Подгруппа $P < G$ называется силовской p-подгруппой группы G, если $|P| = p^n$.*

Введем обозначение: $Syl_p(G)$ — множество всех силовских p-подгрупп в G.

Теорема 9.3 (Первая теорема Силова)**.** *Силовские p-подгруппы в G существуют, т. е. $Syl_p(G) \neq \emptyset$.*

Теорема 9.4 (Вторая теорема Силова)**.**

1. *Любая p-подгруппа $H < G$ содержится в некоторой силовской p-подгруппе.*
2. *Все силовские p-подгруппы группы G сопряжены между собой, т. е. $\forall P_1, P_2 < G, |P_1| = |P_2| = p^n$ $\exists g \in G$ такой, что $P_2 = gP_1g^{-1}$.*

Введем обозначение: $N_p(G) = |Syl_p(G)|$ — количество силовских p-подгрупп в G.

Теорема 9.5 (Третья теорема Силова)**.** $N_p(G) \equiv 1 \pmod p$, *т. е.* $N_p(G) = 1+kp, k \in \mathbb{N} \cup 0$.

Следствие 9.4 (из 2-й теоремы)**.** $N_p(G) \mid m$, *где* $|G| = p^n m, m > 1$.

Следствие 9.5. $N_p(G) = 1 \Leftrightarrow P \lhd G$, *т. е.* $Syl_p(G) = \{P\}$.

Доказательство теоремы 1. Если G абелева, то она разлагается в прямое произведение $G = P \times Q$, где $|P| = p^n, |Q| = m$. А именно, $P = \{g \in G \mid \exists l : g^{p^l} = e\}$ (множество всех p-элементов), данное утверждение вытекает из основной теоремы о строении конечных абелевых групп.

Если G неабелева, проведем индукцию по $|G|$.

Рассмотрим разбиение G на классы сопряженных элементов. По формуле классов из предыдущего §: $|G| = |Z(G)| + \sum_{j=1}^{s} |K(x_j)|$. Возможны два случая.

1-й случай. $|Z(G)| \vdots p$, так что $|Z(G)| = p^{n_1} m_1, n_1 \geqslant 1, p \not| m_1$. Так как $Z(G)$ абелева группа, то $\exists Z_1 < Z(G), |Z_1| = p^{n_1}$ и $|Z(G)/Z_1| = p^{n-n_1} m_1$.

Если $n_1 = n$, то Z_1 уже силовская p-подгруппа в G, если $n_1 < n$,то по предположению индукции в $Z(G)/Z_1$ существует подгруппа $\bar{P}$ порядка p^{n-n_1}, а её прообраз P в группе G имеет порядок p^n.

2-й случай. $\neg |Z(G)| \vdots p$. Если допустить, что $|K(x_j)| \vdots p, \forall j$, то получилось бы, что $|Z(G)| \vdots p$ $\left(Z(G) = \left(|G| - \sum\limits_{j=1}^{s} |K(x_j)|\right) \vdots p\right)$.

Значит $\exists i, |K(x_i)| \not\vdots p$, причем $|K(x_i)| = \frac{|G|}{|C_G(x_i)|} \Rightarrow |C_G(x_i)| \vdots p^n$. Но $|C_G(x_i)| < |G|$, так как $x_i \notin Z(G)$. По предположению индукции $\exists P < C_G(x_i), |P| = p^n$, поэтому она по определению и является искомой подгруппой в G. $\square$

Доказательство теоремы 2.

i) По теореме 1 $Syl_p(G) \neq \emptyset$. Выберем одну из силовских подгрупп и обозначим ее через P.

Пусть $H < G, |H| = p^k, k \leqslant n$.

Группа G действует на множестве G/P; рассмотрим действие группы H. Тогда $G/P = \bigcup\limits_i Orb_H(x_i P)$.[2]

Либо орбита состоит из одного элемента (класса), который неподвижен относительно H, либо $|Orb_H(\bar{x})| \vdots p$, но $G/P = m$ не делится на p, то есть $\forall h \in H, hxP = xP$

[2]Орбиты относительно действия подгруппы H.

$\Rightarrow x^{-1}hx \in P \Rightarrow h = xPx^{-1}$, но $\left|xPx^{-1}\right| = |P| = p^n$, то есть xPx^{-1} тоже силовская $\Rightarrow H \leqslant xPx^{-1}$.

ii) Пусть H — другая силовская подгруппа такая, что $|H| = p^n$. По доказанному в i) $\exists x \in G\colon H \leqslant xPx^{-1}$, но $|H| = p^n = \left|xPx^{-1}\right| \Rightarrow H = xPx^{-1}$. □

Доказательство следствия 1.

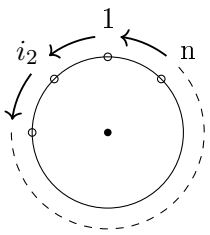
1. $N_p(G)$ делит m. $Syl_p(G)$ составляет одну орбиту при действии G сопряжениями на множестве подгрупп $\Rightarrow |Syl_p(G)| = \frac{|G|}{|St_G(P)|}$, $St_G(P) = \{g \in G \mid gPg^{-1} = P\}$ — нормализатор P в G, $P \leqslant N_G(P) \Rightarrow |N_G(P)| \vdots p^n \Rightarrow |Syl_p(G)| = \frac{p^n m}{p^n q} = r \in \mathbb{N} \Rightarrow m = rq$, то есть $r \mid m$. □

Д.З.	57.23 (а, б), 57.35 (а, б), 59.3 (а, б), 59.11 (т. Вильсона)

Лекция 10

Задачи.

27.23 (б) Если $\sigma \in S_n, \sigma = \sigma_1 \cdot \ldots \cdot \sigma_r$ — произведение независимых циклов, $\tau \in S_n, \tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdot (\tau\sigma_2\tau^{-1}) \cdot \ldots \cdot (\tau\sigma_r\tau^{-1})$; для любого цикла $(i_1, i_2, \ldots, i_l)$: $\tau(i_1, i_2, \ldots, i_l)\tau^{-1} = (\tau(i_1), \tau(i_2), \ldots, \tau(i_l))$ $\tau \in C_{S_n}(\sigma) \Leftrightarrow \tau\sigma\tau^{-1} = \sigma$.



Пусть $\sigma = (1, 2, \ldots, n)$, тогда $\tau\sigma\tau^{-1} = (\tau(1), \tau(2), \ldots, \tau(n)) = (1, 2, \ldots, n)$ $\tau =$? Это значит, что $\tau(1), \tau(2), \ldots, \tau(n)$ получены из цикла $(1, 2, \ldots, n)$ циклической перестановкой символов, то есть $\tau = \sigma^k, k = 1, 2, \ldots, n$. Это значит, что $\tau \in \langle\sigma\rangle$.

Ответ: $C_{S_n}(\sigma) = \langle\sigma\rangle$.

Замечание 10.1. *Порядок класса элементов, сопряженных с σ, равен:*

$$\frac{|G|}{|C_G(\sigma)|} = \frac{n!}{n} = (n-1)! \tag{10.1}$$

Доказательство. **Комбинаторный подсчет**. Все циклы длины n сопряжены между собой. Найдем количество циклов длины n. Любая перестановка $(j_1, \ldots, j_n)$ дает некоторый цикл; всего перестановок $n!$, но перестановки, которые отличаются друг от друга циклическим сдвигом, дают один и тот же цикл $\Rightarrow$ всего $\frac{n!}{n} = (n-1)!$ циклов, что совпадает с формулой 10.1. □

27.23 (а) $\sigma = (1, 2)(3, 4)$, $\tau\sigma\tau^{-1} = (\tau(1), \tau(2))(\tau(3), \tau(4)) = (1, 2)(3, 4)$. Это возможно, если $\tau(1) = 2, \tau(2) = 1, \tau(3) = 4, \tau(4) = 3$; либо $\tau(1) = 1, \tau(2) = 2, \tau(3) = 4, \tau(4) = 3$; либо $\tau(1) = 2, \tau(2) = 1, \tau(3) = 3, \tau(4) = 4$; либо $\tau(1) = 3, \tau(2) = 4, \tau(3) = 1, \tau(4) = 2$; либо $\tau(1) = 4, \tau(2) = 3, \tau(3) = 2, \tau(4) = 1$.

$V_4 \ni \sigma, V_4$ абелева $\Rightarrow V_4 \leqslant C_{S_4}(\sigma)$. Также $\tau = (1,2)$ и $(3,4) \in C_{S_4}(\sigma)$. Класс элементов, сопряженных с σ – это $\{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$. $\Rightarrow V_4 \cdot \langle(1,2)\rangle \leqslant C_{S_4}(\sigma)$.

$$V_4 \cdot \langle(1,2)\rangle = \{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} \cdot \{e,(1,2)\} =$$

$$= \{V_4,(3,4),(1,3)(2,4)(1,2) = (1,4,2,3),(1,4)(2,3)(1,2) = (1,3,2,4) = (1,4,2,3)^{-1}\} \overset{?}{\cong} D_4.$$

Замечание 10.2. $|S_4| = 2^3 \cdot 3$, *силовские 2-подгруппы в* S_4 *имеют порядок* 2^3. *Мы установили, что они изоморфны группе* D_4.

10.0.1 Окончание доказательств теорем Силова и их следствий

Доказательство следствия 2.

$\Rightarrow$ Пусть $P \lhd G$, для $\forall g \in G \left|gPg^{-1}\right| = |P|$, т. е. gPg^{-1} является силовской p-подгруппой. По 2-й теореме Силова $\{gPg^{-1} \mid g \in G\} = Syl_p(G)$. По условию $gPg^{-1} = P$, т. к. P нормальна в $G \Rightarrow Syl_p(G) = \{P\}$.

$\Leftarrow$ $Syl_p(G) = \{P\} \Rightarrow \forall g \in G gPg^{-1} \in Syl_p(G) \Rightarrow gPg^{-1} = P \Rightarrow P \lhd G$. □

Доказательство 3-й теоремы Силова. Выберем одну из силовских подгрупп: P, а $Syl_p(G) = \{P_1, P_2, \ldots, P_s\}$, где $s = N_p(G)$[1]. Определим действие группы P на множестве $Syl_p(G)$ сопряжениями: $\forall g \in P, P_i \mapsto gP_ig^{-1} = P_j$. Множество $Syl_p(G)$ разбивается на орбиты: $Syl_p(G) = Orb(P_1) \sqcup \ldots \sqcup Orb(P_t), t \leqslant s$.

Мы знаем, что $|P_k| = \frac{|P|}{|St_P(P_k)|}$. Либо $|P_k| = 1 (Orb(P_1) = P)$, либо $|P_k| = p^{\alpha_k}, \alpha_k \geqslant 1$, тогда $|P_k| \vdots p$. Покажем, что порядки всех остальных орбит делятся на p.

Доказательство от противного: допустим, что $gP_kg^{-1} = P_k, \forall g \in P, k > 1$. $gP_kg^{-1} = P_k \Leftrightarrow gP_k = P_kg, \forall g \in P = P_1 \Leftrightarrow P_1P_k = P_kP_1$ – это подгруппа в G, причем $|P_1P_k| = \frac{|P_1| \cdot |P_k|}{|P_1 \cap P_k|} = \frac{p^n \cdot p^n}{p^q} = p^{2n-q}$ — p-подгруппа в G, которая содержит P и P_k — вопреки допущению, что $k > 1$.

Итак, $|Syl_p(G)| = N_p(G) = 1 + \underbrace{\sum_{k=2}^{s} |Orb(P_k)|}_{\vdots p} \equiv 1 \pmod p$. □

10.0.2 Некоторые применения теорем Силова и действий

Задачи.

(1) Пусть $|G| = pq.p, q$ — простые, $p > q$. Обозначим за P силовскую p-подгруппу в G. Доказать, что $P \lhd G$.

Решение. Найдем $N_p(G)$ по 3-й теореме Силова и следствию 1.

Если $N_p(G) \equiv 1 \pmod p$, то $N_p(G) = 1 + kp, k = 0, 1, 2, \ldots$.

[1] Можно считать, что $P_1 = P$.

По следствию 1 $N_p(G)$ делит $q < p$. Если бы $k \geqslant 1$, то $N_p(G) = 1 + kp > p > q \Rightarrow q \not| (1 + kp)$. Значит $k = 0$, т. е. $N_p(G) = 1 \Rightarrow P \lhd G$ по следствию 2.

59.20 (б) Доказать, что любая группа порядка 35 абелева и даже циклическая.

Решение. $35 = 7 \cdot 5$ $N_7(G) = 1$ (см. предыдущую задачу) т. е. если $|P| = 7$, то $P \lhd G$.

$q = 5$. $N_5(G) \equiv 1 \pmod 5$, т. е. $N_5(G) = 1 + 5k, k = 0, 1, 2, \ldots$, а также $N_5(G) \mid 7 \Rightarrow k = 0$, т. е. $N_5(G) = 1$, и если обозначить эту подгруппу через $Q, |Q| = 5 \Rightarrow Q \lhd G \Rightarrow G = P \times Q, P = \langle a \rangle, Q = \langle b \rangle, |P| = 7, |Q| = 5$, и $ab = ba \Rightarrow G$ коммутативная, $|ab| = |a| \cdot |b| = 35 \Rightarrow G = \langle ab \rangle$, т. е. G циклическая.

(2) Доказать, что если группа G неабелева, то факторгруппа $G/Z(G)$ не может быть циклической группой.

Решение. Поскольку G неабелева, то $Z(G) < G$ (строго меньше) $\Rightarrow |G/Z(G)| > 1$. Допустим, что $G/Z(G)$ циклическая $\Rightarrow \exists a \in G$ такой, что $\langle aZ(G) = \bar{a} \rangle = \bar{G} = G/Z(G)$, т. е. $\forall \bar{g} = a^k Z(G) \in \bar{G}$. Возьмём $\bar{g}_1 = a^{k_1} Z(G), \bar{g}_2 = a^{k_2} Z(G) \Rightarrow \bar{g}_1 \cdot \bar{g}_2 = a^{k_1} Z(G) \cdot a^{k_2} Z(G)$. Запишем произведение поэлементно: $(a^{k_1} z_1)(a^{k_2} z_2) = a^{k_1} a^{k_2} z_1 z_2 = a^{k_1 + k_2}(z_1 z_2)$.

В другом порядке: $\bar{g}_2 \cdot \bar{g}_1 = a^{k_2} Z(G) \cdot a^{k_1} Z(G)$. Поэлементно: $g_2 \cdot g_1 = (a^{k_2} z_2)(a^{k_1} z_1) = a^{k_2} a^{k_1} z_2 z_1 = a^{k_1 + k_2}(z_1 z_2)$.

Для любых элементов группы G: $g_1 = a^{k_1} z_1, g_2 = a^{k_2} z_2$ получили, что $g_1 g_2 = g_2 g_1$, т. е. G абелева вопреки тому, что G неабелева. Противоречие.

Теорема 10.1. *Центр неединичной p-группы нетривиален, то есть если $G \neq \{e\}$ — p-группа, то $Z(G) \neq \{e\}$.*

Доказательство. Пусть $|G| = p^n, n \geqslant 1$. Рассмотрим разбиение группы G на классы сопряженных элементов:

$$G = Z(G) \sqcup K_1 \sqcup \ldots \sqcup K_s, \text{ где } |K_i > 1|.$$

$|K_i| = \frac{|G|}{|C_G(g_i)|} = p^{\alpha_i}, \alpha_i \geqslant 1 \Rightarrow |G| = p^n = |Z(G)| + \sum\limits_{i=1}^{s} p^{\alpha_i}, \alpha_i \geqslant 1 \Rightarrow |Z(G)| = \left(p^n - \sum\limits_{i=1}^{s} p^{\alpha_i}\right) \vdots p \Rightarrow |Z(G)| > 1.$ □

(3) Определить с точностью до изоморфизма все группы порядка p^2.

Решение. Дано: $|G| = p^2$, p — простое число.

По теореме $|Z(G)| > 1 \Rightarrow |Z(G)| = p^2 = |G| \Rightarrow$ либо G абелева, либо $|Z(G)| = p$, но тогда $|G/Z(G)| = p$, а любая группа порядка p циклическая. По задаче 4 G обязательно абелева, что противоречит предположению о том, что $|Z(G)| = p < |G|$.

Значит G абелева.

По теореме о классификации конечных абелевых групп $G \cong \mathbb{Z}_{p^2}$ или $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Замечание 10.3. *Известно, что количество неизоморфных групп порядков* 2^n *таково:*

$\lvert G\rvert = 2^n$	$2^3 = 8$	$2^4 = 16$	$2^5 = 32$	$2^6 = 64$	$2^7 = 128$	$2^8 = 256$	$\cdots$
$\#\{G \mid \lvert G\rvert = 2^n\}$	5	14	51	267^*	2328^*	56092^*	$\cdots$

* *- с помощью компьютера*

10.1 Простые группы

Определение 10.1. *Группа* G *называется простой, если* $|G| > 1$ *и она не имеет нетривиальных нормальных подгрупп, т. е. если* $N \lhd G$, *то либо* $N = G$, *либо* $N = \{e\}$.

Теорема 10.2. *Если* G *абелева и простая, то* $|G| = p$, *где* p *— простое число.*

Доказательство. Пусть p — простой делитель $|G|$; т. к. G абелева, то $\exists a \in G, |a| = p$. Подгруппа $H = \langle a \rangle \lhd G$, т. к. G абелева. Если G простая, то $H = G$, т. е. $|G| = p$. $\square$

Однако неабелевы простые группы не обязаны иметь простой порядок, например, существует простая группа порядка:

$$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$$

Теорема 10.3. *Знакопеременные группы* A_n *являются простыми группами при* $n \geqslant 5$.

Без доказательства.

Теорема 10.4. *В группе* $S_n, n \geqslant 3$ *две подстановки* σ *и* $\pi \Leftrightarrow$ *сопряжены* $\Leftrightarrow$ *они имеют одинаковый цикловый тип (т. е. в разложении* σ *и* π *на независимые циклы:* $\sigma = \sigma_1 \cdot \sigma_2 \cdot \ldots \cdot \sigma_r, \pi = \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_s \Rightarrow r = s$ *и сомножетели можно занумеровать так, что* σ_i *и* π_i *имеют одинаковую длину).*

Пример: $n = 9$. $\sigma = (1,2,3,4)(5,6,7)(8,9), \pi = (3,5,7,9)(2,4,6)(1,8)$ имеют тип $(4;3;2)$ здесь, $4 + 3 + 2 = 9 = n$.

Следствие 10.1. *Количество классов сопряженных элементов в* S_n *равно* $p(n)$ *— количеству разбиений числа* n *на натуральные слагаемые.*

(4) Доказать, что группа A_5 простая.

Решение. В знакопеременной группе A_5 все подстановки четные: кроме $\{e\}$, циклы длины 3 (i,j,k), циклы длины 5 (i_1,i_2,i_3,i_4,i_5), клейновские элементы $(i_1,i_2)\cdot(i_3,i_4)$.

Можно утверждать, что если $\sigma, \tau \in A_n$ сопряжены, то они имеют одинаковый цикловый тип. Обратное не всегда верно.

Определим порядки централизаторов этих элементов:

$$\pi(1,2,3)\pi^{-1} = (1,2,3) \Leftrightarrow (\pi(1),\pi(2),\pi(3)) = (1,2,3).$$

Таким образом все циклы длины 3 образуют один класс.

Подгруппа $\langle(1,2,3)\rangle = \{e,(1,2,3),(3,2,1)\}$ входит в $C_{A_5}\big((1,2,3)\big)$, но если $\pi(4) = 5, \pi(5) = 4$, то $\pi = (1,2,3)(4,5)$ или $(3,2,1)(4,5)$ — нечетная $\Rightarrow \big|C_{A_5}\big((1,2,3)\big)\big| = 3, \big|K_{A_5}\big((1,2,3)\big)\big| = \frac{|A_5|}{3} = \frac{5!/2}{3} = 20 = \big|K_{S_5}\big((1,2,3)\big)\big|$, где $K_G(x)$ обозначает количество элементов группы G, сопряженных элементу x.

Количество элементов порядка 5 вида (i_1,i_2,i_3,i_4,i_5): любая перестановка определяет некоторый цикл длины 5; всего перестановок пяти чисел 5!, но перестановки, отличающиеся циклическим сдвигом, определяют один и тот же цикл, их в итоге $\frac{5!}{5} = 4! = 24$.

Централизатор $= \langle(i_1,\ldots,i_5)\rangle = \langle a\rangle$ имеет порядок $5 \Rightarrow |K_{A_5}(a)| = \frac{|A_5|}{|\langle a\rangle|} = \frac{60}{5} = 12$ — половина от $24 \Rightarrow$ элементы порядка 5 образуют 2 класса по 12 элементов.

Элементы вида $(i_1,i_2)(i_3,i_4)$ образуют один класс.

Элементы	e	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,2,3,5,4)$
Порядки классов	1	15	20	12	12

Пусть $N \lhd A_5$. Она состоит из целых классов группы $A_5 \Rightarrow |N| = 1 + k_1 \cdot 15 + k_2 \cdot 20 + k_3 \cdot 12 + k_4 \cdot 12$ делит 60 (по т. Лагранжа).

Можно проверить, что это возможно только, если:

$$k_1 = k_2 = k_3 = k_4 = 0 \Rightarrow |N| = 1, \text{ либо}$$
$$k_1 = k_2 = k_3 = k_4 = 1 \Rightarrow N = A_5.$$

Д.З.	59.20 (в, г), 59.17, 59.22 (а, в), 59.23

Лекция 11

11.1 Кольца

11.1.1 Основные понятия и примеры

Определение 11.1. *Множество R с операциями $+$ и $\cdot$ называется кольцом, если выполняются аксиомы.*

I. Аксиомы сложения. *R — абелева группа по сложению.*

II. Аксиомы умножения. *В самом общем случае никаких ограничений не накладывается.*

Могут быть такие (необязательные) аксиомы:

1) ассоциативность умножения $(ab)c = a(bc)$ — ассоциативное кольцо.

2) $\exists 1 \in R$: $1 \cdot a = a \cdot 1 = a$ — кольцо с единицей.

3) $\forall a \in R, a \neq 0$ $\exists a^{-1} \in R$: $a^{-1} \cdot a = a \cdot a^{-1} = 1$ — кольцо с делением.[1]

4) $\forall a, b \in R$: $a \cdot b = b \cdot a$ — коммутативное кольцо.

III. Дистрибутивность. $a \cdot (b + c) = a \cdot b + a \cdot c; (b + c) \cdot a = b \cdot a + c \cdot a$.

Примеры.

1. Числовые кольца: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ (обычные сложение и умножение чисел) — ассоциативные, коммутативные и с 1.

2. Кольца матриц: $M_n(K)$ с элементами из поля K ($\mathbb{Q}, \mathbb{R}$ или $\mathbb{C}$) с операциями сложения и умножения для матриц. (n натуральное) — ассоциативные, с $1 = E$, но не коммутативные при $n \geqslant 2$.

3. Пусть K — поле, определим $R = K[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in K, n = 0, 1, 2, \ldots\}$ — кольцо многочленов от x с обычными операциями — ассоциативное, коммутативное с 1.

4. Кольцо вычетов целых чисел по модулю n: $\mathbb{Z}_n$.

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ — множество классов вычетов по модулю n. Класс числа k обозначим как $\bar{k} = \{k + tn \mid t \in \mathbb{Z}\}$. Сложение: $\bar{k} + \bar{l} = \overline{k + l}$ получается циклическая группа, $\bar{k} \cdot \bar{l} = \overline{kl}$.

Получается ассоциативное, коммутативное кольцо с $\bar{1}$.

[1] Ассоциативное кольцо с 1 и такое, что $\forall a \neq 0$ $\exists a^{-1} \in R$ по опрелению называется телом.

Примеры колец вычетов

$n = 4, \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

Таблица сложения

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

В частности, $\bar{1} + \bar{1} = \bar{2}, \bar{1} + \bar{3} = \bar{4} = \bar{0}, \bar{2} + \bar{3} = \bar{1}$.

В каждой строке и каждом столбце присутствуют все элементы без повторений. В соседних строчках элементы циклически переставляются $\Rightarrow \mathbb{Z}_4$ группа по сложению циклическая.

Таблица умножения

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

В частности, $\bar{2} \times \bar{2} = \bar{4} = \bar{0}$, $\bar{3} \times \bar{3} = \bar{1}$.

Определение 11.2. *Элемент $a \in R$ называется делителем 0, если $a \neq 0$ и $\exists b \in R, b \neq 0$ такой, что $a \cdot b = 0$ (a и b — делители 0) или $\exists c \in R, c \neq 0$ такой, что $c \cdot a = 0$ (если выполняется что-либо одно, то a — левый или правый делитель нуля).*

При $n = 6$ в $\mathbb{Z}_6$ есть делители 0: $\bar{2} \cdot \bar{3} = \bar{0}, \bar{4} \cdot \bar{3} = \bar{0}$; $\bar{5}$ — не делитель 0: $\bar{5} \cdot \bar{5} = \bar{25} = \bar{1}$.

Утверждение 11.1. *Если a — делитель 0, то в ассоциативном кольце a не может иметь обратный.*

Доказательство. От противного. Допустим, что $a \neq 0$, $\exists a^{-1}$ и $a \cdot b = 0$ для некоторого $b \in R$. Умножим равенство на a^{-1} и воспользуемся ассоциативностью кольца: $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b = 0$ — противоречит определению делителя 0. □

Замечание 11.1. *В кольце $\mathbb{Z}$ нет делителей 0, но обратимы только ± 1.*

Утверждение 11.2. *Кольцо многочленов $K[x]$ не имеет делителей 0.*

Доказательство. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, n \geqslant 0, a_0 \neq 0$, $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m, m \geqslant 0, b_0 \neq 0 \Rightarrow f(x) \cdot g(x) = a_0b_0x^{n+m} + \cdots$ (при перемножении степени складываются) $\Rightarrow f(x) \cdot g(x) \neq 0$. □

Примеры делителей 0 в кольце матриц

Пусть $n = 2$.

$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow A \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

В другом порядке:

$B \cdot A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq 0$, но для $C = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$: $C \cdot A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Теорема 11.1. *Матрица $A \in M_n(\mathbb{R})$ является делителем 0* $\Leftrightarrow \det A = 0$.

Доказательство. Если A — делитель 0, то A не имеет обратной $\Rightarrow \det A = 0$.

Обратно, допустим, что $\det A = 0 \Rightarrow \operatorname{rk} A < n \Rightarrow$ элементарными преобразованиями строк её можно привести к виду: $A' = \begin{pmatrix} \dots & \dots & \dots \\ \dots & \dots & \dots \\ 0 & \dots & 0 \end{pmatrix} \Rightarrow$ для A' можно взять матрицу $C = \begin{pmatrix} 0 & \dots & 0 & c_{1n} \\ 0 & \dots & 0 & c_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & c_{nn} \end{pmatrix} \Rightarrow C \cdot A' = 0, C \neq 0.$

Приведение матрицы A к A' с помощью элементарных преобразований строк равносильно умножению A с левой стороны на подходящие элементарные матрицы: $\exists C_1, \dots, C_k$: $\underbrace{C_k \cdot \cdot C_2 \cdot C_1}_{=S} \cdot A = A' \Rightarrow (C \cdot S)A = CA' = 0 \Rightarrow A$ — делитель 0; для умножения справа аналогично, но преобразовывать надо столбцы. □

Определение 11.3. *Элемент a кольца с 1 называется обратимым, если $\exists a^{-1} \in R$.*

Утверждение 11.3. *Если R — ассоциативное кольцо с 1, то его обратимые элементы образуют группу по умножению (эта группа — мультипликативная группа кольца R; обозн. R^*).*

Например, при $n = 4$, $\mathbb{Z}_4^* = \{\bar{1}, \bar{3}\}$.

Доказательство. Нужно доказать, что если a и b обратимы, то ab обратим: $(ab)^{-1} = b^{-1}a^{-1}, (a^{-1})^{-1} = a$. □

Задача. Выяснить при каком условии элемент $\bar{k}$ кольца $\mathbb{Z}_n$: 1) обратим, 2) является делителем 0.

Ответ: 1) обратим $\Leftrightarrow$ НОД$(k, n) = 1$,

2) делитель 0 $\Leftrightarrow$ НОД$(k, n) > 1$.

Пусть НОД$(k, n) = d > 1$, так что $k = k' \cdot d, n = n' \cdot d$, где НОД$(k', n') = 1$.

$$k \cdot n' = k' \cdot (d \cdot n') = k' \cdot n \vdots n \Rightarrow$$
$$\bar{k} \cdot \bar{n'} = \bar{0}, \bar{n'} \neq \bar{0} \Rightarrow$$
$$\bar{k} \text{ — делитель 0.}$$

Наоборот, пусть НОД$(k, n) = 1$.

Рассмотрим все произведения $\{\bar{k} \cdot \bar{1}, \bar{k}\bar{2} \cdot, \dots, \bar{k} \cdot \overline{(n-1)}\}$; эти произведения все различны если окажется, что $\bar{k} \cdot \bar{i} = \bar{k} \cdot \bar{j}, 1 \leqslant i, j \leqslant n-1 \Rightarrow \bar{k} \cdot \overline{(i-j)} = \bar{0}$ в $\mathbb{Z}_n \Rightarrow k(i-j) \vdots n$. Но k и n взаимно просты $\Rightarrow (i-j) \vdots n, |i-j| < n \Rightarrow i = j$. Это значит, что для k найдется такое i, что $\bar{k} \cdot \bar{i} = \bar{1} \Rightarrow \bar{i} = \bar{k}^{-1}$.

Пусть $n = 8, k = 7; \bar{7} \cdot \bar{1} = \bar{7}, \bar{7} \cdot \bar{2} = \bar{14} = \bar{6}, \bar{7} \cdot \bar{3} = \bar{21} = \bar{5}, \bar{7} \cdot \bar{4} = \bar{28} = \bar{4}, \bar{7} \cdot \bar{5} = \bar{35} = \bar{3}, \bar{7} \cdot \bar{6} = \bar{42} = \bar{2}, \bar{7} \cdot \bar{7} = \bar{49} = \bar{1} \Rightarrow \bar{7}^{-1} = \bar{7}$.

Другое доказательство: т. к. k и n имеют НОД $= 1$, то $\exists x, y \in \mathbb{Z}$ такие, что $kx + ny = 1 \Rightarrow \bar{k} \cdot \bar{x} + \bar{n} \cdot \bar{y} = \bar{1}$, но $\bar{n} = \bar{0}$ в $\mathbb{Z}_n \Rightarrow \bar{k} \cdot \bar{x} = \bar{1}$.

11.1.2 Области целостности и поле частных

Определение 11.4. *Скажем, что R — целостное кольцо, если R — ассоциативное, коммутативное, с $1 \neq 0$ и без делителей 0.*

Типичные примеры: $\mathbb{Z}$ и $K[x]$.

Определение 11.5. *R — поле, если R — коммутативное, ассоциативное, с $1 \neq 0$ и в котором любой ненулевой элемент обратим.*

Утверждение 11.4. *$\mathbb{Z}_n$ — поле $\Leftrightarrow$ n — простое число.*

Доказательство. $\mathbb{Z}_n$ — поле $\Leftrightarrow \forall \bar{k} \neq \bar{0}$ обратим $\Leftrightarrow \forall k, 1 \leqslant k \leqslant n-1, k$ и n взаимно просты $\Leftrightarrow n$ — простое число. □

Теорема 11.2. *Если R — целостное кольцо, то существует поле $Q(R)$, в которое R вкладывается в качестве подкольца.*

Термин: $Q(R)$ — поле частных кольца R.

Типичные примеры: $\mathbb{Z} \to Q(\mathbb{Z}) = \mathbb{Q}$.

$R = K[x] \Rightarrow Q(R)$ — поле рациональных дробей.

Обозначение: $K(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \text{— многочлены}, g(x) \not\equiv 0 \right\}$.

Конструкция поля $Q(R)$

Рассмотрим множество пар (a, b), $a, b \in R, b \neq 0$ $P = \{(a, b) \mid b \neq 0\}$. Введем на множестве P отношение: назовем пары эквивалентными, $(a_1, b_1) \sim (a_2, b_2)$, если $a_1 b_2 = b_1 a_2$.[2]

Отношение $\sim$ в самом деле является отношением эквивалентности 1) рефлексивность — $(a, b) \sim (a, b)$;

2) симметричность — $(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = a_2 b_1 \Leftrightarrow a_2 b_1 = a_1 b_2 \Leftrightarrow (a_2, b_2) \sim (a_1, b_1)$;

3) транзитивность — если $(a_1, b_1) \sim (a_2, b_2), (a_2, b_2) \sim (a_3, b_3) \Leftrightarrow (a_1, b_1) \sim (a_3, b_3)$.

Доказательство. По условию $a_1 b_2 = a_2 b_1 \mid \cdot b_3 \neq 0 \Rightarrow a_1 b_2 b_3 = a_2 b_1 b_3$. Но $a_2 b_3 = a_3 b_2$ $\Rightarrow a_1 b_2 b_3 = b_1 (a_2 b_3) = b_1 b_2 a_3 \Rightarrow a_1 b_2 b_3 - b_1 b_2 a_3 = (a_1 b_3 - b_1 a_3) b_2 = 0 \Rightarrow a_1 b_3 - b_1 a_3 = 0$ ($b_2 \neq 0$ и делителей 0 нет) $\Rightarrow a_1 b_3 = b_1 a_3$, т. е. $(a_1, b_1) \sim (a_3, b_3)$. □

Назовем дробью $\frac{a}{b}$ класс эквивалентности пары (a, b): по определению $\frac{a}{b} = \bar{(a, b)}$, тогда $Q(R) = \left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\}$.

Введем на $Q(R)$ операции "$+$" и "$\cdot$":

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} \overset{\text{опр.}}{=} \frac{a_1 b_2 + a_2 b_1}{b_1 b_2},$$
$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} \overset{\text{опр.}}{=} \frac{a_1 a_2}{b_1 b_2}.$$

Нужно было бы проверить (упражнение), что все свойства операций поля выполняются. В частности, в этом поле $\frac{0}{b} = 0, \frac{a}{1} = a \in R$, так что R — множество дробей со знаменателем 1; $1 = \frac{1}{1} \Rightarrow R \subset Q(R)$.

[2] Прототип: $\frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftrightarrow a_1 b_2 = b_1 a_2$.

11.1.3 Поля: основные понятия, примеры и простейшие свойства

Определение 11.6.

1. *Кольцо K называется полем, если это ассоциативное, коммутативное кольцо с 1, в котором любой элемент $a \neq 0$ обратим.*

   Тогда $K^* = K - \{0\} = \{a \in K \mid a \neq 0\}$ — мультипликативная группа.

2. *Если R — кольцо и $S \subseteq R$, то S называется подкольцом кольца R, если:*

   (i) $(S, +)$ — подгруппа группы $(R, +)$;

   (ii) S замкнуто относительно умножения, т. е. $\forall a, b \in S \Rightarrow ab \in S$.

3. *Если K — поле, $L \subseteq K$, то L — подполе в K, если L — подкольцо в K и L является полем.*

Пример. Пусть $L = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Покажем, что L — подполе в $\mathbb{C}$.
$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in L$;
$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1b_2 + 2b_1b_2) + (b_1a_2 + a_1b_2)\sqrt{2} \in L$.
Если a или $b \neq 0$, то $a + b\sqrt{2} \neq 0$, т. к. $\sqrt{2} \notin \mathbb{Q}$, т. е. $\sqrt{2} \neq a/b$, где $a, b \in \mathbb{Z}$.
$(a + b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in L$.

Лекция 12

Определение 12.1. *Поле K называется простым полем, если оно не имеет собственных подполей: из того, что F — подполе в K, следует, что $F = K$.*

Примеры простых полей:

- поле рациональных чисел $\mathbb{Q}$;

- $\mathbb{Z}_p$ — поле классов вычетов по модулю p, где p — простое число.

Утверждение 12.1. *Любое простое поле изоморфно $\mathbb{Z}_p$ (для некоторого простого p) или полю $\mathbb{Q}$.*

Доказательство.
1) Если $F \subseteq \mathbb{Q}, F$ — подполе, то $0, 1 \in F \Rightarrow \forall n \in \mathbb{Z}$, $n = n \cdot 1 = \pm \underbrace{(1 + \cdots + 1)}_{|n|} \in F$.

Если $m \in \mathbb{N} \cap F$, то дробь $\frac{n}{m} = n \cdot m^{-1} \in F \Rightarrow$ любое рациональное число $\in F \Rightarrow F = \mathbb{Q} \Rightarrow \mathbb{Q}$ — простое поле.

2) Если $F \subseteq \mathbb{Z}_p, F$ — подполе, то $F \ni 1$ и $(F, +) \subseteq (\mathbb{Z}_p, +)$ — подгруппа по сложению. Но $|\mathbb{Z}_p| = p$ — простое число $\Rightarrow 1 < |F| \mid p \Rightarrow F = \mathbb{Z}p \Rightarrow \mathbb{Z}_p$ — простое поле. □

Определение 12.2. *Если K и L — кольца, то отображение $\phi\colon K \to L$ — гомоморфизм кольца K в кольцо L, если:*
1) $\forall x, y \in K \quad \phi(x + y) = \phi(x) + \phi(y)$, и
2) $\forall x, y \in K \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y)$,
ϕ — изоморфизм колец, если ϕ — гомоморфизм и биекция.
Кольца K и L изоморфны, если существует изоморфизм $\phi\colon K \to L$.
В частности, эти понятия имеют смысл, если K и L – поля. В этом случае $\phi(1_K) = 1_L$.

Обозначение: K изоморфно L: $K \cong L$.

Доказательство леммы. Пусть P — простое поле. Для любого $k \in \mathbb{Z}$ рассмотрим элементы $k \cdot 1_P$. Для $k > 0$, $k \cdot 1_P = \underbrace{1 + \cdots + 1}_{k \text{ раз}}$.

Есть два варианта:

1) $\forall k \in \mathbb{N}$, $k \cdot 1 \neq 0$, тогда $\{k \cdot 1 \mid k \in \mathbb{Z}\}$ — подгруппа в группе поля P по сложению. При этом если $k \neq l$, то $k \cdot 1 \neq l \cdot 1$ (т. к. иначе $\Rightarrow k \cdot 1 - l \cdot 1 = (k-l) \cdot 1 = 0, k \neq l \Rightarrow 1 = 0$ — противоречие; в определении поля $1 \neq 0$).

Следовательно, $\big(\{k \cdot 1 \mid k \in \mathbb{Z}\}, +\big) \cong \mathbb{Z}$.

Для $m > 0, (k \cdot 1)m^{-1} \leftrightarrow \frac{k}{m} \cdot 1 \leftrightarrow \frac{k}{m} \in \mathbb{Q}$.

Таким образом в P есть подполе изоморфное полю $\mathbb{Q} \Rightarrow P$ — простое $\Rightarrow K = P \Rightarrow P \cong \mathbb{Q}$.

2) Второй вариант: $\exists n \in \mathbb{N}$ такое, что $n \cdot 1_P = \underbrace{1 + \cdots + 1}_{n} = 0$.

Выбирем минимальное из них, обозначим его за p. Покажем, что p — простое число.

Допустим, что p — составное, $p = q \cdot r, q < p, r < p$. Тогда $p \cdot 1 = (qr) \cdot 1 = (q \cdot 1)(r \cdot 1) = 0$.

Если $q \cdot 1 \neq 0$, то $(q \cdot 1)^{-1}(q \cdot 1)(r \cdot 1) = (r \cdot 1) = 0$, но $r < p$ — это противоречит минимальности $p \Rightarrow p$ — простое.

Тогда $(\langle 1 \rangle, +) = \{k \cdot 1 \mid k = 0, \ldots, p-1\} \cong \mathbb{Z}_p$ как группе по сложению. Но $\langle 1 \rangle$ подмножество в поле $P \Rightarrow$ все неравные нули элементы в ней обратимы $\Rightarrow$ в P есть подполе, состоящее из p элементов, а т. к. P — простое поле $\Rightarrow |P| = p$ и $P \cong \mathbb{Z}_p$. $\square$

Определение 12.3. *Наименьшее натуральное число p такое, что $p \cdot 1 = 0$, называется характеристикой поля K.*

Из доказательства леммы 12.1 ясно, что p — простое число и K содержит простое подполе $P \cong \mathbb{Z}_p$.

Если $\forall n \in \mathbb{N}, n \cdot 1 \neq 0$, то считается, что характеристика поля K равна 0 (т. к. только $0 \cdot 1 = 0$) $\Rightarrow K \cong \mathbb{Q}$ — простое.

Обозначение: $\operatorname{char} K$; $\operatorname{char} K = p$ либо $\operatorname{char} K = 0$.

12.0.1 Гомоморфизмы колец, идеалы и факторкольца

Определение 12.4. *Подмножество $I \subset R$ (R — кольцо) называется идеалом кольца R, если:*

1) $(I, +)$ — подгруппа аддитивной группы кольца R, $(R, +)$,

2) для $a \in I, \forall x \in R \Rightarrow xa \in I, ax \in I$.

Заметим: если I — идеал в R, то I — подкольцо в R : условие 2) из определения идеала, примененное к $x \in I$, означает, что если $x, a \in I \to xa \in I$ — входит в определение подкольца.

Обозначение идеала: $I \lhd R$.

Примеры идеалов

(1) $R = \mathbb{Z}$. Для любого $n \in \mathbb{N}$ подмножество $n\mathbb{Z} = \{nt \mid t \in \mathbb{Z}\}$ является идеалом в $\mathbb{Z}$. Действительно, $n\mathbb{Z}$ — подгруппа по сложению в $\mathbb{Z}$, и $\forall x \in \mathbb{Z}, x(nt) = n(xt) \vdots n \Rightarrow x(nt) \in n\mathbb{Z}$.

Будет показано, что любой идеал в $\mathbb{Z}$ равен $n\mathbb{Z}$ для $n = 0$ или некоторого натурального числа n.

(2) $R = K[x] = \{f(x) = a_0 + a_1x + \cdot + a_nx^n \mid n = 0, 1, 2, \ldots; a_i \in K\}$ — кольцо многочленов от x с коэффициентами из поля K.

Выберем какой-нибудь многочлен $p(x)$ и рассмотрим

$$p(x)K[x] = \{p(x)f(x), \text{ где } f(x) \text{ — произвольный многочлен}\}.$$

Тогда $p(x)K[x]$ — идеал в $K[x]$, поскольку $\forall h(x)$ в силу ассоциативности: $\big(p(x)f(x)\big)h(x) = p(x)\big(f(x)h(x)\big) \in p(x)K[x]$.

Теорема 12.1. *Если $\phi\colon R \to S$ — гомоморфизм колец, то*

1. *$\phi(R)$ — подкольцо в S;*
2. *ядро ϕ, т. е. $\operatorname{Ker}\phi = \{x \in R \mid \phi(x) = 0_S\}$ — идеал в R;*
3. *ϕ инъективно $\Leftrightarrow \operatorname{Ker}\phi = \{0\}$.*

Доказательство.

1) Для любых $y_1, y_2 \in \phi(R)$ $\exists x_1, x_2 \in R$, такие, что $\phi(x_1) = y_1, \phi(x_2) = y_2$.

$y_1 + y_2 = \phi(x_1) + \phi(x_2) = \phi(x_1 + x_2) \in \phi(R)$, а также $y_1 \cdot y_2 = \phi(x_1) \cdot \phi(x_2) = \phi(x_1x_2) \in \phi(R) \Rightarrow \phi(R)$ — подкольцо в R.

2) $\operatorname{Ker}\phi$ — подгруппа аддитивной группы кольца R и $\forall a \in \operatorname{Ker}\phi, \forall x \in R, \phi(xa) = \phi(x)\phi(a) = \phi(x) \cdot 0 = 0_R \Rightarrow \operatorname{Ker}\phi$ — идеал в R.

3) Если ϕ инъективно, то $\operatorname{Ker}\phi = \{0\}$. В самом деле, $\phi(0_R) = 0_S \Rightarrow 0_R$ – единственный элемент из R, который отображается в $0_S \Rightarrow \operatorname{Ker}\phi = \{0\}$.

Обратно, допустим, что $\phi(x_1) = \phi(x_2) \Rightarrow \phi(x_1) - \phi(x_2) = \phi(x_1 - x_2) = 0 \Rightarrow x_1 - x_2 \in \operatorname{Ker}\phi = \{0\}$ по условию $\Rightarrow x_1 = x_2$. □

12.0.2 Фактор-кольцо по идеалу

Пусть R — кольцо, $I \lhd R$.

Определение 12.5. *Фактор-кольцо $R/I = \{x + I\}$ — как группа по сложению: $(x_1 + I) + (x_2 + I) = (x_1 + x_2) + I$. Нужно ввести умножение: $(x_1 + I) \cdot (x_2 + I) = x_1 \cdot x_2 + I$. Мотивировка: раскроем скобки $x_1x_2 + \underbrace{x_1I + Ix_2 + I \cdot I}_{\subset I} \subseteq x_1x_2 + I$*

Нужно показать корректность определения, т. е. если $x_1 + I = x_1' + I$ и $x_2 + I = x_2' + I \overset{?}{\Rightarrow} x_1x_2 + I = x_1'x_2' + I$.

$$x_1' = x_1 + a_1, x_2' = x_2 + a_2, a_1, a_2 \in I$$

$$\Downarrow$$

$$x_1'x_2' = (x_1 + a_1)(x_2 + a_2) = x_1x_2 + \underbrace{x_1a_2 + a_1x_2 + a_1a_2}_{\in I}$$

$$\Downarrow$$

определение корректно.

Примеры.

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

(2) $R = \mathbb{R}[x]$ — кольцо многочленов с действительными коэффициентами от x.

$$I = (x^2+1)R = \{(x^2+1)f(x) \mid f(x) \in R\}.$$

Докажем, что $R/\big((x^2+1)R\big) \cong \mathbb{C}$ — поле комплексных чисел.

Имеем:

$$\forall f(x) = (x^2+1)q(x) + r(x) = (x^2+1)q(x) + a + bx,$$
$$\deg r(x) < 2 = \deg(x^2+1).$$

Рассмотрим далее отображение ϕ:

$$R/\big((x^2+1)R\big) \xrightarrow{\phi} \mathbb{C},$$
$$\phi\colon f(x) + I = a + bx + I \mapsto z = a + bi \in \mathbb{C}.$$

Поскольку остаток $a + bx$ определен однозначно, то ϕ — биекция.

Отображение ϕ сохраняет сложение:

$$\begin{aligned}\phi((a_1 + b_1x + I) + (a_2 + b_2x + I)) &= \phi(a_1 + a_2 + (b_1+b_2)x + I) = \\ &= a_1 + a_2 + (b_1+b_2)i = (a_1 + b_1i) + (a_2 + b_2i) = \\ &= \phi(a_1 + b_1x + I) + \phi(a_2 + b_2x + I).\end{aligned}$$

Отображение ϕ сохраняет умножение. Действительно, поскольку:

$$\begin{aligned}&(a_1 + b_1x + I)\cdot(a_2 + b_2x + I) = \\ &\quad = a_1a_2 + b_1b_2x^2 + (b_1a_2 + a_1b_2)x + I = \boxed{\text{записав, } x^2 = (x^2+1) - 1} \\ &\quad = a_1a_2 - b_1b_2 + (b_1a_2 + a_1b_2)x + \underbrace{b_1b_2(x^2+1) + I}_{\in I},\end{aligned}$$

и т. к. $(a_1 + b_1i)\cdot(a_2 + b_2i) = a_1a_2 - b_1b_2 + (b_1a_2 + a_1b_2)i$, то окончательно получим:

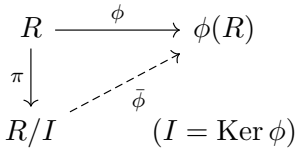
$$\phi((a_1 + b_1x + I)\cdot(a_2 + b_2x + I)) = \phi(a_1 + b_1x + I)\cdot\phi(a_2 + b_2x + I) = z_1z_2.$$

Таким образом, ϕ — гомоморфизм колец.

12.0.3 Теорема о гомоморфизме для колец

Если $\phi\colon R \to S$ — гомоморфизм колец, то $\mathrm{Im}\phi = \phi(R) \cong R/\operatorname{Ker}\phi$.

Доказательство. Учтем, что ϕ — гомоморфизм аддитивных групп, для групп теорема уже доказана: $\phi(R) \cong R/\operatorname{Ker}\phi$ — изоморфизм групп. Рассмотрим диаграмму:



где $\pi\colon R \to R/I, \pi(x) = x + I$ — канонический гомоморфизм.

Это также изоморфизм колец: $\bar{\phi}(x+I) = \phi(x) \Rightarrow \bar{\phi}((x_1+I)(x_2+I)) = \bar{\phi}(x_1x_2+I) = \phi(x_1x_2) = \phi(x_1)\phi(x_2) = \bar{\phi}(x_1+I)\bar{\phi}(x_2+I)$. □

Утверждение 12.2. *Если K — поле и $p(x)$ — многочлен, неприводимый над K, то $K[x]/p(x)K[x]$ является полем.*

И обратно, если $K[x]/p(x)K[x]$ — поле, то $p(x)$ неприводим над K.

Доказательство. Пусть $p(x)$ — неприводимый многочлен. Нужно доказать, что если $f(x) \notin p(x)K[x] = I$ (т. е. $\bar{f}(x) = f(x) + I \neq \bar{0}$), то класс $\bar{f}(x)$ обратим.

Т. к. $p(x)$ неприводимый многочлен и $f(x) \not\vdots p(x)$, то $p(x)$ и $f(x)$ взаимно простые многочлены $\Rightarrow u(x), v(x)$ такие многочлены, что:

$$u(x)f(x) + v(x)p(x) = 1 \text{ — равенство в кольце } K[x].$$

Перейдём в фактор-кольцо:

$$\overline{u(x)} \cdot \overline{f(x)} + \overline{v(x)} \cdot \underbrace{\overline{p(x)}}_{\equiv\bar{0}} = \bar{1} \quad \left(\overline{u(x)} = u(x) + I\right)$$

$$\Downarrow$$

$$\overline{u(x)} \cdot \overline{f(x)} = \bar{1}, \text{ т. е. } \overline{u(x)} = \overline{f(x)}^{-1}.$$

Обратно — от противного. Допустим, что $p(x)$ приводимый, т. е. $p(x) = g(x)h(x), \deg g(x), \deg h(x) \geqslant 1 \Rightarrow \overline{g(x)} \cdot \overline{h(x)} \overset{\text{опр.}}{=} \overline{g(x) \cdot h(x)} = \overline{p(x)} = \bar{0} \Rightarrow$ классы $\overline{g(x)} \neq 0$ и $\overline{h(x)} \neq 0$ — делители 0, которых в поле быть не может, т. к. делители 0 необратимы. □

12.0.4 Евклидовы кольца и кольца главных идеалов

Пусть R — коммутативное кольцо с 1, I — идеал в R.

Определение 12.6. *I — главный идеал, если $\exists a \in I$ такой, что $\forall y \in I$ имеет вид $y = ax$ для некоторого $x \in R$.*

Элемент a называется порождающим элементом этого идеала.

Обозначение: $I = \langle a \rangle = aR$.
Примеры.
(1) $n\mathbb{Z} = \langle a \rangle$.
(2) $(x^2+1)K[x] = \langle (x^2+1) \rangle \lhd K[x]$.

Определение 12.7. *Кольцо R называется кольцом главных идеалов, если R целостное кольцо (т. е. ассоциативное коммутативное кольцо с 1 и без делителей 0) и в R все идеалы главные.*

Определение 12.8. *Целостное кольцо R называется евклидовым кольцом, если на множестве $R \setminus \{0\}$ задана функция (норма) $N\colon R \setminus \{0\} \to \mathbb{N}_0 = \{n \in \mathbb{Z}, n \geqslant 0\}$ со свойствами:*

1. *Для любых $a, b \in R$ $(a, b \neq 0), N(ab) \geqslant N(a)$. Равенство выпоняется тогда и только тогда, когда b обратим.*
2. *Для любых $a, b \in R (b \neq 0)$ $\exists q, r \in R$ такие, что $a = bq + r$, причем $N(r) < N(b)$[1] (заметим, что если b обратим, то $r = 0$, поэтому можно считать, что b необратим).*

Из определения евклидова кольца следует, что в R можно определить понятие НОД(a, b), простого элемента и разложение элементов на простые множители.

Утверждение 12.3. *Если кольцо R евклидово, то в R все идеалы главные.*

Доказательство. Пусть $I \lhd R$; если $I = \{0\}$, то $I = \langle 0 \rangle$. Если $I \neq \{0\}$, рассмотрим множество $\{N(x) \mid x \in I, x \neq 0\} \subseteq \mathbb{N}_0$.

В нём есть наименьшее число, выберем элемент $a \neq 0$ такой, что $N(a) \leqslant N(x), \forall x \in I$. Тогда a порождает этот идеал: $\forall b \in I$ разделим b на a с остатком: $b = aq + r$. $a \in I \Rightarrow aq \in I \Rightarrow r = b - aq \in I$, но $N(r) < N(a)$ по определению деления с остатком $\Rightarrow$ противоречие с выбором $a \Rightarrow r = 0 \Rightarrow \forall b \in I \quad \exists q \in R : b = aq \Rightarrow I = \langle a \rangle$, т. е. I — главный идеал. □

Задача. Пусть K — поле. Рассмотрим кольцо $R = K[[x]]$ формальных степенных рядов от x:

$$K[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n \mid a_i \in K, i = 0, 1, \ldots, \right\}.$$

Операции над рядами.
Сложение:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n.$$

Умножение:

$$\sum_{k=0}^{\infty} a_k x^k \cdot \sum_{i=0}^{\infty} b_i x^i = \sum_{k,i} a_k b_i x^{k+i} \overset{\text{опр.}}{=} \sum_{n=0}^{\infty} c_n x^n,$$

[1] Деление с остатком.

где $c_n = \sum\limits_{k+i=n} a_k b_i = \sum\limits_{k=0}^{n} a_k b_{n-k}$ (свёртка).

Можно проверить, что с этими операциями $K[[x]]$ будет целостным кольцом.

Попробуем определить на $K[[x]]$ норму:

$$\forall f(x) = \sum_{n=0}^{\infty} a_n x^n = a_m x^m + a_{m+1} x^{m+1} + \cdots,$$
$$m \geqslant 0; a_n = 0 \text{ для } n < m$$

(например, $x^2 + x^4 + x^6 + \cdots \Rightarrow m = 2$).

Определим $N(f) = m$.

Если $N(f) = m$, $N(g) = p \Rightarrow N(f \cdot g) = m + p \geqslant N(f)$, $p = 0$ только если $g(x) = \sum\limits_{n=0}^{\infty} b_n x^n, b_0 \neq 0$.

Можно показать, что ряд $f(x) = \sum\limits_{n=0}^{\infty} a_n x^n$ обратим $\Leftrightarrow a_0 \neq 0$.

12.0.5 Об арифметике евклидовых колец

Определение 12.9. *Пусть R — целостное кольцо. Скажем, что $b \mid a$ $(a, b \in R, b \neq 0)$, если $\exists c \in R$ $a = bc$. Элемент c — общий делитель a и b, если $c \mid a$ и $c \mid b$.*

Элемент $d \in R$ — наибольший общий делитель элементов a и b, если $d \mid a$ и $d \mid b$, а для любого общего делителя c: $c \mid d$.

Элемент $p \in R$ — простой, если p — необратимый, и из того, что $c \mid p \Rightarrow c$ — обратимый или $p = c\alpha$, где α — обратимый элемент.

Далее предположим, что кольцо R евклидово.

Теорема 12.2. *В евклидовом кольце справедлива основная теорема арифметики любой необратимый элемент $a \in R$ разлагается в произведение простых элементов, причём единственным образом.*[2]

Д.З.	57.1, 63.1 (з, и, к), 63.2 (а, б), 63.3 (а, е), 63.6 (а), 61.1 (б), 64.19 (а), 66.2 (а)

[2] Что понимается под единственностью будет ясно из доказательства.

Лекция 13

13.0.1 Наибольший общий делитель в целостном кольце

Утверждение 13.1. *Если R — целостное кольцо и a, b — необратимые элементы в R, то НОД(a, b) определен с точностью до обратимости множителя: то есть если d_1, d_2 — два общих делителя элементов a, b, то $\exists \alpha$ — обратимый элемент в R такой, что $d_2 = \alpha d_1$.*

Доказательство. Считаем, что $a \neq 0, b \neq 0$. Т. к. d_1 — НОД(a, b), а d_2 — общий делитель a и b, то $d_2 \mid d_1$, т. е. $d_1 = \beta d_2, \beta \in R$.

Аналогично, т. к. $d_2 =$ НОД(a, b), а d_1 — общий делитель, то $d_1 \mid d_2 \Rightarrow \exists \alpha \in R$ такой, что $d_2 = \alpha d_1 \Rightarrow d_1 = \beta d_2 = (\beta\alpha) d_1 \Rightarrow d_1(1 - \beta\alpha) = 0$. т. к. $d_1 \neq 0$, а R не содержит делителей 0, то $(1 - \beta\alpha) = 0$, т. е. $\alpha\beta = 1 \Rightarrow \alpha$ — обратимый. $\square$

13.0.2 Алгоритм Евклида вычисления НОД(a, b) в евклидовом кольце R

Т. к. a, b необратимы, то $N(a) > 0, N(b) > 0$.

Если $b \mid a$, т. е. $a = bq, q \in R$, то НОД$(a, b) = b$.

Пусть b не делит a. Тогда разделим a на b с остатком.

1) Найдём $q, r \in R$ такие, что $a = bq + r$, где $0 < N(r) < N(b)$.

При этом НОД$(a, b) =$ НОД(b, r). В самом деле, если c — общий делитель a и b, т. е. $a = ca', b = cb' \Rightarrow r = a - bq = c(a' - b'q) \vdots c \Rightarrow c$ — общий делитель b и r. Наоборот, если $c_1 \mid b$, $c_1 \mid r$, то $b = c_1 b', r = c_1 r' \Rightarrow a = bq + r = c_1(b'q + r') \vdots c_1$. Значит, у пары (a, b) и у пары (b, r) одно и тоже множество общих делителей $\Rightarrow$ НОД$(a, b) =$ НОД(b, r).

2) Если $r \neq 0$, то разделим b на r с остатком:

$$b = rq_1 + r_2, \text{ если } r_1 = 0, \text{ то } r = \text{НОД}(b, r) = \text{НОД}(a, b).$$

3) Если $r_1 \neq 0$, то $r = r_1 q_2 + r_2$ и т. д.

При каждом делении норма остатка уменьшается $\Rightarrow$ существует число $k \in \mathbb{N}$ такое, что $r_k \neq 0$, но $r_{k+1} = 0$. Тогда НОД$(a, b) = r_k$.

Следствие 13.1. *Если НОД$(a, b) = d$, то $\exists x, y \in R$ такие, что $ax + by = d$.*

Пример

25.3 (а) Пусть $f(x) = x^4+2x^3-x^2-4x-2, g(x) = x^4+x^3-x^2-2x-2, f, g \in \mathbb{R}[x]$. Вычислить НОД$(f, g)$ и найти многочлены $u(x), v(x)$ такие, что $u(x)f(x)+v(x)g(x) = d(x) =$ НОД(f, g).

Решение:

1) Разделим f на g с остатком:

$$\begin{array}{rr|l} x^4+2x^3-x^2-4x-2 & x^4+x^3-x^2-2x-2 & \\ \hline -x^4-x^3+x^2+2x+2 & & 1 \\ \hline x^3-2x & & \end{array}$$

$\Rightarrow q = 1, r = x^3-2x \neq 0$

2) Разделим g на r с остатком:

$$\begin{array}{rr|l} x^4+x^3-x^2-2x-2 & x^3-2x & \\ \hline -x^4+2x^2 & & x+1 \\ \hline x^3+x^2-2x-2 & & \\ -x^3+2x & & \\ \hline x^2-2 & & \end{array}$$

$\Rightarrow q_1 = x+1, r_1 = x^2-2 \neq 0$

3) Разделим r на r_1 с остатком:

$$\begin{array}{rr|l} x^3-2x & x^2-2 & \\ \hline -x^3+2x & & x \\ \hline 0 & & \end{array}$$

$\Rightarrow r_2 = 0 \Rightarrow r_1 = x^2-2 =$ НОД(f, g).

Нужно найти $u(x)$ и $v(x)$. Запишем результаты шагов 1)-3): 1) $f = gq + r$, 2) $g = rq_1+r_1$, 3) $r = r_1q_2$. Из 2) выразим $r_1 = g-rq_1 = g-(f-gq)q_1 = -fq_1+g(1+qq_1) = -(x+1)f + g(x+2) = x^2-2$.

Ответ: НОД$(f, g) = x^2-2 = -(x+1)f + (x+2)g$.

13.0.3 К доказательству основной теоремы арифметики

Доказательство. Дано $a \neq 0, a \in R$ — необратимый элемент.

Возможны два случая: 1) a — простой элемент $\Rightarrow a$ уже разложен на множетели;

2) a — составной элемент $\Rightarrow a = bc$, где $N(b) < N(a)$ и $N(c) < N(a)$, т. к. b и c необратимые.

Индукция по норме a: допустим, что для элементов с нормой $< N(a)$ теорема уже доказана $\Rightarrow b = p_1 \cdot \ldots \cdot p_r$, $c = p_{r+1} \cdot \ldots \cdot p_s$, где p_i — простые $\Rightarrow a = p_1 \cdot \ldots \cdot p_s$. *Существование* разложения доказали.

Единственность. Допустим, что $a = p_1 \cdot \ldots \cdot p_s = p'_1 \cdot \ldots \cdot p'_t$, p_i, p'_j — простые. Надо доказать, что $t = s$ и простые p_i, p'_j можно занумеровать так, чтобы $p'_i = \alpha_i p_i$, α_i — обратимый, $i = 1, \ldots, s$ (т. е. p_i и p'_i ассоциированные).

Лемма 13.1. *Если $c \mid ab$ и НОД$(a,c) = 1$, то $c \mid b$.*

Доказательство. Поскольку НОД$(a,c) = 1$, то $\exists x, y \in R$ такие, что $ax + cy = 1 \mid \cdot b$ $\Rightarrow abx + bcy = b$. По условию $ab = cz$, где $z \in R \Rightarrow c(zx + by) = b \Rightarrow c \mid b$. $\square$

Рассмотрим равенство: $p_1 \cdot \ldots \cdot p_s = p'_1 \cdot \ldots \cdot p'_t$, $s > 1, t > 1 \Rightarrow p'_t \mid p_1 \cdot \ldots \cdot p_s$ Из леммы следует, что $\exists i, 1 \leqslant i \leqslant s$ такой, что $p'_t \mid p_i$, значит, $p_i = \alpha_i p'_t$ Изменим нумерацию: $i = s \Rightarrow p_1 \cdot \ldots \cdot \alpha_i p_{t-1} = p'_1 \cdot \ldots \cdot p'_{t-1}$. Количество сомножителей $s - 1$ уменьшилось, и по предположению индукции $s - 1 = t - 1 \Rightarrow s = t$.

Кроме того, p'_j можно занумеровать так, чтобы $p'_i = \alpha_i p_i, 1 \leqslant i \leqslant s$. $\square$

Следствие 13.2. *Пусть K — поле, тогда любой многочлен $f(x) \in K[x]$ степени $\geqslant 1$ можно разложить в произведение неприводимых (=простых) многочленов, причем единственным образом.*

Утверждение 13.2. *Пусть R — евклидово кольцо, $I = \langle p \rangle = \{px \mid x \in R\}$ — главный идеал, порожденный элементом p.*

Фактор-кольцо R/I является полем $\Leftrightarrow$ p — простой элемент.

Доказательство.

$(\Rightarrow)$ От противного: допустим, что $p = ab$, a, b — необратимые $\Rightarrow (a+I)\cdot(b+I) = ab + I = p + I = I = \bar{0}$ в фактор-кольце $R/I \Rightarrow \bar{a}, \bar{b}$ — делители 0, а в поле делителей 0 быть не может.

$(\Leftarrow)$ $a \notin I \Rightarrow$ НОД$(a,b) = 1 \Rightarrow ax + py = 1$. В фактор-кольце $\bar{a}\bar{x} + \bar{p}\bar{y} = \bar{1}, \bar{p} = \bar{0} \Rightarrow$ $\bar{a}\bar{x} = \bar{1} \Rightarrow \bar{x} = \bar{a}^{-1}$. $\square$

13.1 Расширения полей

Пусть k, K — поля, причем k — подполе в K: $k \subset K$. Тогда поле K называется расширением поля k.

Поле K можно рассматривать как векторное пространство над k: $\forall x, y \in K$ определены сложение $x + y \in K$ и умножение на элементы из k: $\forall x \in K, \forall \lambda \in k$ $\lambda x \in K$.

Из аксиом поля следует, что все аксиомы в определении векторного пространства для K верны.

Имеет смысл говорить о размерности K как пространства над k.

Определение 13.1. *Степенью расширения поля K над подполем k называется размерность K над k.*

Обозначение: $[K : k] = \dim_k K$ *(размерность K над k).*

Пример. $\mathbb{R} \subset \mathbb{C}$, т. к. $\forall z \in \mathbb{C} : z = 1 \cdot x + i \cdot y, x, y \in \mathbb{R}$, то $\{1, i\}$ — базис $\mathbb{C}$ над $\mathbb{R}$ как векторного пространства. Тем самым $[\mathbb{C} : \mathbb{R}] = 2$.

Термин. Если есть два расширения: $k \subset K \subset L$, то говорят, что эти три поля образуют двухэтажную башню полей. Тогда можно рассматривать степени $[K : k], [L : K], [L : k]$.

Лемма 13.2. *Если степени $[K:k]$ и $[L:K]$ конечны, то $[L:k]$ конечна и $[L:k] = [L:K]\cdot[K:k]$.*[1]

Доказательство. Пусть $[K:k] = n$, $e_1,\dots,e_n$ — базис в K, т. е. $\forall x \in K\ x = \sum\limits_{i=1}^{n} x_i e_i, x_i \in k$. Пусть $[L:K] = m$, $f_1,\dots,f_m$ — базис в L над K, т. е. $\forall y \in L$ $y \overset{(1)}{=} \sum\limits_{j=1}^{m} y_j f_j, y_j \in K \Rightarrow \exists a_{ij} \in k$ такие, что $y_j \overset{(2)}{=} \sum\limits_{i=1}^{n} a_{ij} e_i$.

Подставим (2) в (1) $\Rightarrow y = \sum\limits_{j=1}^{m} \left(\sum\limits_{i=1}^{n} a_{ij} e_i\right) f_j = \sum\limits_{i,j} a_{ij}(e_i f_j) \Rightarrow y$ — линейная комбинация элементов $e_i f_j$ — количество таких элементов равно mn.

Осталось доказать, что элементы $e_i f_j, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m$, линейно независимы.

Допустим, что $\sum\limits_{i,j} c_{ij} e_i f_j = 0, c_{ij} \in k \Rightarrow \sum\limits_{j=1}^{m} \underbrace{\left(\sum\limits_{i}^{n} c_{ij} e_i\right)}_{\in K} f_j = 0$, а т. к. $\{f_j\}$ линейно независимы над K, то $\sum\limits_{i}^{n} c_{ij} e_i = 0$, $1 \leqslant j \leqslant m$. Здесь $c_{ij} \in k$, а $\{e_i\}$ линейно независимы над $k \Rightarrow c_{ij} = 0, \forall i, j$.

Доказали, что $e_i f_j$ образуют базис L над $k \Rightarrow [L:k] = mn = [L:K]\cdot[K:k]$. $\square$

Термин. Если $[K:k] < \infty$, то расширение $k \subset K$ — расширение конечной степени (конечное расширение).

Определение 13.2. *Пусть $k \subset K$ — расширение полей. Элемент $\alpha \in K$ называется алгебраическим над полем k, если существует многочлен с коэффициентами из k степени $\geqslant 1$, корнем которого является α.*

Традиционно комплексное число z называтся алгебраическим числом, если z — корень некоторого многочлена с рациональными коэффициентами. Числа $e, \pi, 2^{\sqrt{3}}$ не являются алгебраическими.

Элемент $\beta \in K$ называется трансцендентным над k, если он не является корнем никакого многочлена с коэффициентами из k.

Расширение $k \subset K$ называется алгебраическим, если все элементы из K алгебраические над k. Расширение $k \subset K$ — трансцендентное расширение если $\exists \beta \in K$ трансцендентный над k.

Теорема 13.1. *Если $k \subset K$ — расширение конечной степени, то $k \subset K$ — алгебраическое расширение.*

Замечание 13.1. *Если $k \subset K$ алгебраическое расширение, то это не значит, что $[k:K] < \infty$.*

Например, если обозначить через $\mathbb{A}$ множество всех алгебраичеких (над $\mathbb{Q}$) элементов, то расширение $\mathbb{Q} \subset \mathbb{A}$ — алгебраическое, но $[\mathbb{A}:\mathbb{Q}]$ бесконечна (например, можно показать, что $\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{p}, \dots$ (p — простое число) линейно независимы над $\mathbb{Q}$).

[1] Похоже на умножение дробей: $\frac{L}{K}\cdot\frac{K}{k} = \frac{L}{k}$ — правило для запоминания.

Теорема 13.2. *Если $[K : k] = n$, то любой элемент $\alpha \in K$ — корень многочлена степени $\leqslant n$ с коэффициентами из k.*

Доказательство. Возьмем $\alpha \notin k$. Элементы $1, \alpha, \alpha^2, \ldots, \alpha^n$ линейно зависимы над k, т. к. $\deg_k K = n$, а их $n+1 \Rightarrow \exists a_0, a_1, \ldots, a_n \in k$: $a_0 \cdot 1 + a_1\alpha + \cdots + a_n\alpha^n = 0 \Rightarrow$ многочлен $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ имеет α своим корнем. □

Определение 13.3. *Если $\alpha \in K$ — алгебраический элемент над k, то многочлен $\mu_\alpha(x)$ называется минимальным многочленом элемента α, если $\mu_\alpha(\alpha) = 0$, но для любого многочлена $f(x) \in k[x]$ степени $< n, f(\alpha) \neq 0$.*

Утверждение 13.3. *Минимальный многочлен алгебраического элемента α неприводим над k.*

Доказательство. Если $\alpha \in k$, то минимальный многочлен $\mu_\alpha(x) = x - \alpha$. Для $\alpha \notin k, \deg \mu_\alpha(x) = n > 1$.

От противного: допустим, что $\mu_\alpha(x)$ приводим, т. е. $\mu_\alpha(x) = f(x)g(x)$. $1 \leqslant \deg f(x) < n, 1 \leqslant \deg g(x) < n \Rightarrow \mu_\alpha(\alpha) = f(\alpha)g(\alpha) = 0 \Rightarrow f(\alpha) = 0$ или $g(\alpha) = 0$. Это противоречит тому, что n — минимальная степень. □

13.1.1 Простые алгебраические расширения

Пусть $p(x)$ — многочлен степени $n \geqslant 2$ неприводимый над полем k.

Обозначим $K = k[x]/\langle p(x)\rangle, \langle p(x)\rangle = \{p(x)f(x) \mid f(x) \in k[x]\}$ — главный идеал, порожденный многочленом $p(x)$ в кольце $k[x]$.

K является полем: покажем, что если многочлен $g(x) \notin I$ то смежный класс $\overline{g(x)} = g(x) + I$ обратим в фактор-кольце $k[x]/I$.

Так как $g(x) \notin I$, то $p(x) \nmid g(x)$, и поскольку $p(x)$ неприводимый, то НОД$(g(x), p(x)) = 1 \Rightarrow$ существуют многочлены $u(x), v(x) \in k[x]$ такие, что $u(x)g(x) + v(x)p(x) = 1$.

Перейдем в фактор-кольцо: рассмотрим смежные классы $(u(x)+I)(g(x)+I) + (v(x)+I)(p(x)+I) = u(x)v(x) + v(x)p(x) + I = 1 + I = \bar{1}$ — единица в фактор-кольце $\Rightarrow g(x) + I = \overline{g(x)} = \overline{u(x)}^{-1}$. $v(x)p(x) + I = \bar{0}$, т. к. $v(x)p(x) \in I$.

Пример. Пусть $k = \mathbb{Q}, p(x) = x^2 - 2, g(x) = x^2 + x + 1$. Найти в фактор-кольце $\mathbb{Q}[x]/\langle p(x)\rangle$ класс обратный к классу $\overline{g(x)}$.

Решение. $g(x) - p(x) = x + 3 \Rightarrow g(x) = x + 3 + I$, достаточно искать для $x + 3$.

НОД$(x^2 - 2, x + 3) =?$

$x^2 - 2 = (x+3)(x-3) + 7 \Rightarrow \frac{1}{7}\big(x^2 - 2 - (x+3)(x-3)\big) = 1 =$ НОД$(x^2 - 2, x + 3) \Rightarrow$ $\overline{(x+3)} \cdot \frac{1}{7}\overline{(3-x)} = \bar{1} \Rightarrow \overline{(x+3)}^{-1} = \frac{1}{7}\overline{(3-x)}$.

Замечание 13.2. *В поле $K = k[x]/\langle p(x)\rangle$ многочлен $p(x)$ имеет корень $\alpha = x + I$, $I = \langle p(x)\rangle$, действительно $p(\alpha) = p(x) + I = I = \bar{0}$.*

Замечание 13.3. *Поле k можно отождествить с подполем в поле $K = k[x]/I$ в виде: $\forall \alpha \in k \leftrightarrow \bar{\alpha} = \alpha + I$. Это позволяет рассматривать K как расширение k.*

Термин: K — простое алгебраическое расширение поля.

13.1.2 Поле разложения многочлена

Определение 13.4. *Расширение $k \subset F$ называется полем разложения многочлена $f(x) \in k[x]$, $\deg f(x) \geqslant 1$, если в поле F многочлен $f(x)$ полностью разлагается на линейные множители: $f(x) = c(x - x_1) \cdot \ldots \cdot (x - x_n)$, $c, x_1, \ldots, x_n \in F$, но над подполем K таким, что $k \subset K \subsetneq F$, многочлен $f(x)$ не разлагается полностью на линейные множители.*

Д.З.	67.3 (а, в), 66.1, 64.55 (б), 68.41 (в)

Лекция 14

14.1 Теорема о существовании поля разложения

Теорема 14.1. *Для любого многочлена $f(x) \in K[x]$ степени $\geqslant 1$ существует поле $F \supset K$ такое, что над полем F многочлен $f(x)$ раскладывается на множители первой степени: если* $\deg f(x) = n$, *то* $f(x) = c(x-x_1)\cdot\ldots\cdot(x-x_n)$, $c, x_1, \ldots, x_n \in F$.[1]

Доказательство.

1. Если $f(x)$ неприводим над полем K, то фактор-кольцо $K_1 = K[x]/\langle f(x)\rangle$ является полем (оно содержит хотя бы один корень многочлена $f(x)$).

Поле K можно вложить как подполе в поле K_1 в виде множества смежных классов: $\forall \alpha \in K, \varphi\colon \alpha \mapsto \bar{\alpha} = \alpha + I, I = \langle f(x)\rangle$; далее надо учесть, что $\varphi(\alpha_1 + \alpha_2) = \varphi(\alpha_1) + \varphi(\alpha_2)$ и $\varphi(\alpha_1\alpha_2) = \varphi(\alpha_1)\varphi(\alpha_2)$.[2]

Замечание. Поле K_1 имеет над K степень n, базис в K_1 образует класс $\bar{1} = 1+I$, $\bar{x}, \ldots, \bar{x}^{n-1}$.

Любой класс представляется в виде:

$$a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + I = a_0\bar{1} + a_1\bar{x} + \ldots + a_{n-1}\bar{x}^{n-1},$$

единственным образом, по правилу деления с остатком.

2. В общем случае $\deg f(x) \geqslant 2$; применяем индукцию по $n = \deg f(x)$.

`База индукции:` $n = 1 \Rightarrow$ расширять не надо.

При $n \geqslant 2$ `предположение индукции:` для любого многочлена степени $< n$ поле разложения существует. Допустим, что $f(x)$ приводим, т. е. $\exists g_1(x), g_2(x)\colon f(x) = g_1(x)g_2(x), \deg g_1(x) < n, \deg g_2(x) < n$. По предположению индукции существует такое поле F, над которым $g_1(x)$ и $g_2(x)$ раскладываются на множители первой степени.

По основной теореме арифметики для многочленов (любой многочлен положительной степени раскладывается в произведение неприводимых многочленов), можно выбрать $g_1(x)$ неприводимым.

---

[1] Поле F нужно построить так, чтобы никакое промежуточное поле $L\colon K \subset L \subset F$ не содержало бы всех корней $f(x)$.

[2] $K_1 = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + I \mid a_0, a_1, \ldots, a_{n-1} \in K\}$ и поле K отождествляется с подмножеством $\{\, a_0 + I \mid a_0 \in K \,\} = \bar{K}$.

Тогда можно построить, как в пункте 1, $K_1 = K[x]/\langle g_1(x)\rangle$, вложить K в K_1 и получить расширение $K \subset K_1$, причём в поле K_1 $g_1(x)$ (и значит, $f(x)$) имеет корень x_1,

$$f(x) = (x - x_1)^{m_1} \cdot g(x), \deg g(x) < n, \text{ причём } g(x) \in K_1[x].$$

По предположению индукции для $g(x)$ существует расширение $F \supset K_1$, в котором $g(x)$ раскладывается на множители первой степени $\Rightarrow f(x)$ тоже раскладывается в F на множители первой степени. $\square$

Замечание. В случае 1, когда $f(x)$ неприводим, $k \subset K_1 = k[x]/\langle f(x)\rangle$, в поле K_1 многочлен $f(x)$ имеет корень $x_1 \in K_1$, так что $f(x) = (x - x_1)^{m_1} g(x)$, и к $g(x)$ применимо предположение индукции, как в случае 2.

Примеры.

67.13 (б) Построить поле разложения для многочлена $f(x) = x^2 - 2$ над $\mathbb{Q}$; указать его степень над $\mathbb{Q}$ и базис.

Решение. Корни $f(x)$: $x_{1,2} = \pm\sqrt{2}$ — иррациональные $\Rightarrow f(x)$ неприводим над $\mathbb{Q}$.

$$\sqrt{2} \in \mathbb{R} \quad \forall h(x) = (x^2 - 2)g(x) + a + bx, a, b \in \mathbb{Q} \Rightarrow$$
$$h(\sqrt{2}) = f(\sqrt{2})q(\sqrt{2}) + a + b\sqrt{2} = a + b\sqrt{2}.$$

Это показывает, что поле разложения $F = \{a + b\sqrt{2} \mid a + bx, a, b \in \mathbb{Q}\}$, посколку корни $f(x)$, $\pm\sqrt{2} \in F$, а меньшее поле — только $\mathbb{Q}$, которому эти корни не принадлежат.

$\dim_{\mathbb{Q}} F = 2$, т. е. степень $[F : \mathbb{Q}] = 2$, базис образуют числа 1 и $\sqrt{2}$.

(1) $f(x) = (x^2 - 2)(x^2 + 2x + 2), k = \mathbb{Q}$.

Комплексные корни: $x_{1,2} = \pm\sqrt{2}$; $x_{3,4} = -1 \pm i$.

Поле разложения F должно содержать $\sqrt{2}$ и i:

$$F = \{a + b\sqrt{2} + ci + di\sqrt{2} \mid a, b, c, d \in \mathbb{Q}\}.$$

Базис: $1, \sqrt{2}, i, i\sqrt{2}$; степень $[F : \mathbb{Q}] = 4$. Поле F можно получить в два этапа.

1. Добавление к полю $\mathbb{Q}$ числа $\sqrt{2} \Rightarrow K_1 = \{a + b\sqrt{2}\}, a, b \in \mathbb{Q}$. В поле K_1 $f(x) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2x + 2)$.

2. Добавление к полю K_1 числа $i \Rightarrow$ поле F:

$$F = \{\alpha + \beta i \mid \alpha, \beta \in K_1\}.$$

Значит, что $\alpha = a + b\sqrt{2}, \beta = c + d\sqrt{2} \Rightarrow \alpha + \beta i = a + b\sqrt{2} + c + d\sqrt{2}$. Что и утверждалось.

14.2 О строении простого расширения поля

Простое расширение поля K — поле, полученное присоединением к K корня α неприводимого многочлена $p(x)$.

Можем считать, что $\alpha \in F$ — полю разложения многочлена $p(x)$. Поле K, полученное присоединением к K элемента α, вместе с α должно содержать: $f(\alpha)$ для любого многочлена $f(x) \in K[x]$, что даст кольцо $K[\alpha] = \{ f(\alpha) \mid f(x) \in K[x] \}$. Чтобы получилось поле, нужно чтобы оно содержало все дроби $\frac{f(\alpha)}{g(\alpha)}$, где $f(x), g(x) \in K[x], g(\alpha) \neq 0$.

Поэтому поле, полученное присоединением к K элемента α, есть поле $K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \right\}$ — поле дробей для кольца $K[\alpha]$.

Утверждение 14.1. *Если α — корень неприводимого над K многочлена $p(x)$ степени n, то:*

1. *$K[\alpha] = \{f(\alpha)\}$ является полем, и, следовательно, $K[\alpha] = K(\alpha)$, и*
2. *$\dim_K K[\alpha] = n$.*

Докажем, что если $g(\alpha) \neq 0, (g(\alpha))^{-1} = h(\alpha)$, где $h(x) \in K[x]$.

Комментарий. $K \subset K[\alpha], K[\alpha] = \{a_0 + a_1\alpha + \ldots + a_n\alpha^n\}, K = \{a_0\}$. Можно рассмотреть, например, $K = \mathbb{Q}(x), K[\sqrt{2}] = \{a(x) + b(x)\sqrt{2}\}$, где $a(x) = \frac{f(x)}{g(x)}, b(x) = \frac{h(x)}{p(x)}$, $f(x), g(x), h(x), p(x)$ — многочлены с рациональными коэффициентами.

Доказательство утверждения. Так как $g(\alpha) \neq 0$, то многочлены $g(x)$ и $p(x)$ взаимно просты. Если бы у $g(x)$ и $p(x)$ был общий делитель $d(x)$, то $d(x) \mid p(x)$ — неприводимый многочлен $\Rightarrow d(x) = p(x)$, и $p(x) \mid g(x)$, т. е. $g(x) = p(x)h(x) \Rightarrow g(\alpha) = 0$ — противоречие.

Поэтому можно считать, что существуют многочлены $u(x), v(x) \in \mathfrak{K}[x]$, такие что $u(x)g(x) + v(x)p(x) = 1 \Rightarrow u(\alpha)g(\alpha) + v(\alpha)p(\alpha) = 1 \Rightarrow u(\alpha)g(\alpha) = 1$, т. к. $p(\alpha) = 0$, т. е. $u(\alpha) = (g(\alpha))^{-1} \Rightarrow \frac{f(\alpha)}{g(\alpha)} = f(\alpha)u(\alpha)$ — многочлен. □

14.3 Конечные поля

Пусть F — поле, $|F| < \infty$, тогда F содержит простое подполе $P \cong \mathbb{Z}_p$ для некоторого простого числа p. В этом случае характеристика поля F равна p, значит, если $n \vdots p$, $n \cdot 1 = \underbrace{1 + \cdots + 1}_{n=pq} = (p \cdot 1)(q \cdot 1) = 0 \cdot (q \cdot 1) = 0$.

Лемма 14.1. *Пусть F — поле характеристики p (p — простое число), тогда $\forall a, b \in F, (a + b)^p = a^p + b^p$. И вообще, $(a + b)^{p^n} = a^{p^n} + b^{p^n}$, $n \in \mathbb{N}$.*

Доказательство. По формуле бинома Ньютона,

$$(a + b)^p = a^p + C_p^1 a^{p-1}b + \ldots + C_p^k a^{p-k}b^k + \cdots + b^b.$$

Покажем, что если $1 \leqslant k \leqslant p - 1$, то $C_p^k \vdots p$. Действительно $C_p^k = \frac{p(p-1)\ldots(p-k+1)}{k!}$, и $k!$ не делится на p, а числитель делится на $p \Rightarrow C_p^k = 0$ в поле $F \Rightarrow (a + b)^p = a^p + b^p$.

Это была база индукции по n. Допустим, что уже доказано равенство $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. Тогда $(a + b)^{p^{n+1}} = ((a + b)^{p^n})^p = (a^{p^n} + b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}$. □

Лемма 14.2. *Если F — конечное поле, то $|F| = p^n$ для некоторого простого числа p и некоторого натурального числа n.*

Доказательство. Поле F можно рассматривать как векторное пространство над простым подполем $P \cong \mathbb{Z}_p$. Пусть $\dim_P F = n$. Это значит, что существует базис $e_1, e_2, \dots e_n \in F$, т. е. $\forall f = \sum\limits_{i=1}^{n} a_i e_i$, где $a_i \in P$. В координатах:

$$\forall f \leftrightarrow (a_1, \dots, a_n) \in P^n. \text{ Все } a_i = 0, \dots, p-1 \in \mathbb{Z}_p \Rightarrow$$

общее число таких строчек $\underbrace{p \cdot p \cdots p}_{n \text{ раз}} = p^n$. □

Утверждение 14.2. *Для любых простого числа p и натурального числа n существует поле из p^n элементов.*

Доказательство. Ясно, что при $n = 1$ это поле $\mathbb{Z}_p$. Если $n > 1$, заметим, что если F — поле порядка p^n, то его мультипликативная группа $F^* = F \setminus \{0\}$ имеет порядок $p^n - 1 \Rightarrow \forall x \in F^*, x^{p^n-1} = 1 \Rightarrow x^{p^n} = x$, т. е. любой элемент x поля F является корнем многочлена $h(x) = x^{p^n} - x$.

В поле разложения F многочлена $h(x)$ он имеет p^n корней, возможно, с кратностями. Покажем, что корни многочлена $h(x) = x^{p^n} - x$ все различные.

Если у $h(x)$ есть корень кратности $\alpha \geqslant 2$, то он будет и корнем $h'(x)$:

$$h(x) = (x - x_1)^\alpha g(x) \Rightarrow$$
$$h'(x) = \alpha(x - x_1)^{\alpha-1} g(x) + (x - x_1)^\alpha g'(x) = (x - x_1)^{\alpha-1}(\alpha g(x) + (x - x_1)g'(x)),$$
$$h'(x_1) = 0, \alpha \geqslant 0.$$

В данном случае $h'(x) = p^n \cdot x^{p^n-1} - 1 = -1 \neq 0 \Rightarrow$ у $h(x)$ нет кратных корней $\Rightarrow$ в поле F многочлен $h(x)$ имеет ровно p^n корней.

Обозначим $F_0 = \{\, \alpha \in F : h(\alpha) = 0 \,\}, |F_0| = p^n$. Проверим, что F_0 искомое поле. $h(0) = 0^{p^n} - 0, h(1) = 1^{p^n} - 1 = 1 - 1 = 0$, т. е. $0, 1 \in F_0$.

Если $\alpha, \beta \in F_0 \Rightarrow \alpha + \beta \in F_0$, т. к. $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta \Rightarrow \alpha + \beta$ — корень уравнения $x^{p^n} = x$.

$(\alpha\beta)^{p^n} = \alpha^{p^n} \cdot \beta^{p^n} = \alpha\beta \Rightarrow \alpha\beta$ — тоже корень этого уравнения. □

Вопрос: почему этого достаточно и не надо проверять, что $\alpha - \beta$ и α/β также принадлежат F_0?

Задачи.

(1) Построить поле из $9 = 3^2$ элементов.

(2) Построить поле из $8 = 2^3$ элементов.

Решение.

1. Найдем многочлен степени 2, не имеющий корней в $\mathbb{Z}_3$: например, $p(x) = x^2 + \bar{1}$ ($\bar{0}, \bar{1}, \bar{2}$) — не корни, т. к. $\bar{0}^2 + \bar{1} \equiv \bar{1}$, $\bar{1}^2 + \bar{1} \equiv \bar{2} \not\equiv \bar{0}$, $\bar{2}^2 + \bar{1} \equiv \bar{5} \equiv \bar{2} \pmod 3$. Тогда фактор-кольцо $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ будет полем. $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle = \{\, a + bx + \langle x^2 + 1\rangle, a, b \in \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\} \,\}$ — всего 9 элементов.

2. Поле из $8 = 2^3$ элементов. Найдем многочлен степени 3, неприводимый над $\mathbb{Z}_2$ (если $p(x)$ приводим, то $p(x) = g_1(x)g_2(x), \deg g_1(x) = 1, \deg g_2(x) = 2$.) Таким образом в $\mathbb{Z}_2$ многочлен 3–й степени $p(x)$ — неприводим $\Leftrightarrow p(x)$ он не имеет корней в $\mathbb{Z}_2$.

Поскольку $p(x) = x^3+x+1 \neq 0$ в $\mathbb{Z}_2 \Rightarrow \mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ — поле. $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle = \{\, a + bx + cx^2 + \langle x^3 + x + 1\rangle, a, b, c \in \mathbb{Z}_2 \,\}$ — всего 8 элементов.

Утверждение 14.3. *Для любого натурального $n \geqslant 1$ и любого простого числа p существует неприводимый многочлен $q(x)$ степени n, и тогда $\mathbb{Z}_p[x]/\langle q(x)\rangle$ — поле порядка p^n.*

Без доказательства.

Утверждение 14.4.

1. Если F — конечное поле, то его мультипликативная группа — циклическая.

2. Если $F_1 \subseteq F$ — подполе, причем $|F| = p^n, |F_1| = p^m$, то $m \mid n$.

Доказательство. 1. Так как группа F^* (порядка $p^n - 1$) абелева, то:

$$F^* \equiv \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \mathbb{Z}_{d_k}, \text{ где } d_1 \mid d_2, d_2 \mid d_3, \ldots d_{k-1} \mid d_k \Rightarrow \forall x \in F^*, x^{d_k} = 1.$$

Но в поле уравнение $x^{d_k} - 1 = 0$ не может иметь более, чем d_k корней, а $|F^*| = d_1 d_2 \cdots d_k = d_k$ тогда и только тогда, когда $k = 1$, а значит F^* циклическая.

2. Поле F можно рассматривать как векторное пространство над F_1; пусть при этом также его размерность равна k. Тогда:[3]

$$|F| = |F_1| = p^{mk} = p^n,$$

если $|F_1| = p^m$. Тем самым $m \mid n$. □

Д.З.	67.13 (в, г), 68.5 (а, в). Построить поле из $25 = 5^2$ элементов

[3]Сравните с доказательством леммы 14.2.

Лекция 15

15.1 Линейные представления групп

Пусть G — группа, V — векторное пространство над полем K. Обозначим группу обратимых линейных операторов на V через $GL(V) = \{\mathcal{A}\colon V \longrightarrow V\}$, где $\mathcal{A}$ — обратимый линейный оператор.

Определение 15.1. *Линейное представление группы G в пространстве V (над полем K) представляет собой гомоморфизм $\varphi\colon G \longrightarrow GL(V)$ группы G в группу обратимых линейных операторов на V (с операцией композиции операторов). Это значит, что для $\forall g_1, g_2 \in G\colon \varphi(g_1 g_2) = \varphi(g_1)\cdot\varphi(g_2)$.*[1]

Заметим для сравнения, что действие было определено как гомоморфизм

$$G \longrightarrow S_X = \{\sigma\colon X \to X \mid \sigma - \text{биекция}\},$$

где $X = V$ — векторное пространство, то $GL(V) < S_X$.

Представление подразумевает три объекта: (G, V, φ) (можно называть представлением только V или только φ).

По теореме о гомоморфизме $\varphi(G) \leqslant GL(V), \varphi(G) \cong G/\operatorname{Ker}\varphi$; если $\operatorname{Ker}\varphi = \{e\}$, то $\varphi(G) \cong G$. В этом случае представление φ называется *точным*.

Матричное представление:

$$\varphi\colon G \to GL(V) \xrightarrow{\sim} GL(n, K) = \{A\colon \det(A) \neq 0)\}, \dim V = n, e_1, \ldots, e_n - \text{базис}.$$

Пример

(1) $G = \langle a\rangle_n$ — циклическая группа порядка n. Можем сопоставить элементу a поворот плоскости вокруг т.O на угол $\alpha = \frac{2\pi k}{n}$ (мы знаем, что $\langle a\rangle \cong C_n$ группе поворотов правильного $n-$угольника); $0 \leqslant k < n$ (k фиксировано), т. е. $\varphi(a) = R_O^\alpha; \forall g \in \langle a\rangle$ имеет вид $g = a^m, 0 \leqslant m < n$.

Нужно, чтобы $\varphi(g) = (\varphi(a))^m = R_O^{m\alpha}$. Получили $\varphi\colon G \longrightarrow GL(\mathbb{R}^2)$. Матричное представление:

$$\mathcal{A}_{\varphi(a)} = \begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}, \mathcal{A}_{\varphi(a^m)} = \begin{pmatrix}\cos m\alpha & -\sin m\alpha\\ \sin m\alpha & \cos m\alpha\end{pmatrix}.$$
$$\mathcal{A} = \mathcal{A}_{\varphi(a)}; \mathcal{A}^n = \begin{pmatrix}\cos n\alpha & -\sin n\alpha\\ \sin n\alpha & \cos n\alpha\end{pmatrix} = \begin{pmatrix}\cos 2\pi k & -\sin 2\pi k\\ \sin 2\pi k & \cos 2\pi k\end{pmatrix} = E.$$

[1] Напоминание: $(\mathcal{A}\cdot\mathcal{B})(v) = \mathcal{A}(\mathcal{B}(v))$.

Так и должно было быть, т. к. $a^n = e \Rightarrow \varphi(a)^n = E$.

Обозначение: $\dim V$ — размерность представления.

Определение 15.2. *Подпространство $U \subset V$ называется инвариантным для представления φ, если $\forall g \in G$ и $\forall u \in U \Rightarrow \varphi(g)u \in U$, т. е. $\forall g \in G$, $\varphi(g)U = U$.*

Это значит, что можно рассматривать ограничение любого оператора $\varphi(g)$ на U, обозначим его как $\varphi|_U(g)\colon U \to U$, которое одновременно можно рассматривать и как представление $\varphi|_U\colon G \to GL(U)$, подпредставление группы G на инвариантном подпространстве U.

(2) Пусть $G = S_3$. Для любого $\sigma \in S_3$ рассмотрим оператор на $V = \mathbb{R}^3$,

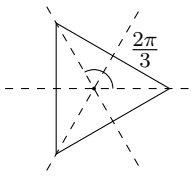
$$\varphi_\sigma\colon (x_1, x_2, x_3) \mapsto (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$$

Это линейное представление $\varphi\colon S_3 \to GL(\mathbb{R}^3)$. Например, $\varphi_{(1,2)}(x_1, x_2, x_3) = (x_2, x_1, x_3), \varphi_{(1,2,3)}(x_1, x_2, x_3) = (x_2, x_3, x_1)$. $v = (x, x, x) \to \forall \sigma \in S_3\ \varphi_\sigma(v) = v \Rightarrow U_1 = \{\,(x, x, x)\,\} = \langle (1, 1, 1)\rangle$ — инвариантное подпространство. $\varphi\restriction_{U_1} = Id(G)$ — все операторы из G оставляют все векторы из U_1 неподвижными.

Рассмотрим также $U_0 = \{\, v = (x_1, x_2, x_3)\colon x_1 + x_2 + x_3 = 0\,\}$. Поскольку $x_{\sigma(1)} + x_{\sigma(2)} + x_{\sigma(3)} = x_1 + x_2 + x_3 = 0 \Rightarrow U_0$ — инвариантное подпространство. На самом деле, $U_0 = U_1^\perp; (x_1, x_2, x_3) \cdot (1, 1, 1) = 0$, $V = U_1 \oplus U_1^\perp = U_1 \oplus U_0$.

Определение 15.3. *Представление φ группы G в пространстве V называется приводимым, если $\exists$ инвариантное подпространство $U, \{0\} \neq U \subsetneq V$. Если для любого инвариантного подпространства $U \subseteq V$ либо $U = \{0\}$, либо $U = V$, то φ (или V) называется неприводимым.*

В примере 1 с группой $G = \langle a\rangle_n$ при нечётном n и любом $k, 0 < k \leqslant n - 1$, представление будет неприводимым. Инвариантное подпространство — это инвариантная прямая. Например, при $n = 3$.



Ни одна прямая не остаётся инвариантной.

При чётном n тоже верно, если $k \neq \frac{n}{2}$ (при $k = \frac{n}{2}$ поворот задаётся матрицей $\mathcal{A} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ и поэтому соответствующая прямая переходит в себя при таком повороте).

Определение 15.4. *Представление (G, V, φ) называется вполне приводимым, если для любого инвариантного подпространства $U \subseteq V$ существует инвариантное подпространство $W \subseteq V$ такое, что $V = U \oplus W$, $\forall v = u + w; U \cap W = \{0\}$.*

Допустимы случаи, когда $U = \{0\}, W = V$ или $U = V, W = \{0\}$. Следовательно, неприводимое представление является вполне приводимым.

Подпредставление $\varphi|_U \colon U \to U$ — неприводимое, если в U уже нет нетривиальных инвариантных подпространств, т. е. U — минимальное (по включению) инвариантное подпространство.

Теорема 15.1. *Если V вполне приводимо, то V разлагается в прямую сумму неприводимых подпредставлений, т. е. минимальных инвариантных подпространств ($\dim V < \infty$).*

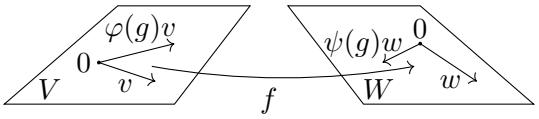
Доказательство. Индукция по $n = \dim V$.

`База:` при $n = 1, \dim V = 1 \Rightarrow V$ — неприводимо, разлагать не требуется.

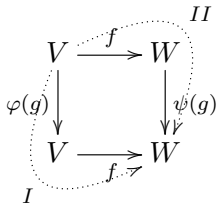
В общем случае, если $n > 1$, `предположение индукции`: пространство размерности $< n$ разлагается в прямую сумму минимальных инвариантных подпространств. Если V — неприводимо, доказывать нечего, если V — приводимо, т. е. $\exists U \subset V$, где U — инвариантное подпространство, $\{0\} \neq U \neq V$. По условию $\exists W \subset V$, где W — инвариантное подпространство, и $V = U \oplus W$ (V — вполне приводимое подпространство).

Так как $\dim U < n$ и $\dim W < n$, то предположение индукции даёт, что $\exists$ разложения $U = U_1 \oplus \ldots \oplus U_k$, $W = W_1 \oplus \ldots \oplus W_l$, где U_i, W_j — минимальные инвариантные подпространства $\Rightarrow V = U_1 \oplus \ldots \oplus U_k \oplus W_1 \oplus \ldots \oplus W_l$ — искомое разложение. $\square$

Определение 15.5. *Пусть $\varphi \colon G \to GL(V), \psi \colon G \to GL(W)$ — линейные представления группы G. Линейное отображение $f \colon V \to W$ называется гомоморфизмом представлений φ и ψ если: для $\forall g \in G, \forall v \in V, f(\varphi(g)v) = \psi(g)f(v)$.*



Изобразим диаграмму этих объектов:



Требуется, чтобы результат по стрелкам I совпадал с результатом по стрелкам II, т. е. $f \circ \varphi = \psi \circ f$.

Изоморфизм — это гомомрфизм, являющийся биекцией. Представления (φ, V) и (ψ, W) называются изоморфными, если между ними существует изоморфизм.

Обозначение: $\varphi \cong \psi$ или $V \cong W$.

Теорема 15.2 (Теорема единственности). *Если $V = U_1 \oplus \cdots \oplus U_s = W_1 \oplus \cdots \oplus W_r$ — два разложения пространства представления V на минимальные инвариантные подпространства, то $r = s$ и при подходящей нумерации $V_i \cong W_i (1 \leqslant i \leqslant s)$ как линейные представления.*

Без доказательства.

15.2 Одномерные представления

Пусть: $\dim(V) = 1, V = \langle a \rangle = \{ta \mid t \in K\}$.

Если $\mathcal{A}$ — линейный оператор на V, то $\mathcal{A}(a) = \lambda a$; для обратимости нужно, чтобы $\lambda \neq 0$. Для $\varphi\colon G \to GL(V) \cong \{\lambda \in K^*\} \cong K^*$ — мультипликативной группе поля $\Rightarrow$ можно считать, что $\varphi\colon G \to K^*$ — гомоморфизм.

Сначала рассмотрим случай, когда G — конечно порожденная абелева группа (мультипликативная). По теореме, $G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle = \langle a_1 \rangle_{d_1} \times \cdots \times \langle a_r \rangle_{d_r} \times \langle a_{r+1} \rangle_\infty \cdots \times \langle a_n \rangle_\infty$. Поэтому любое $g \in G$ записывается в виде:

$$g = a_1^{k_1} \cdot \dots \cdot a_r^{k_r} a_{r+1}^{k_{r+1}} \cdot \dots \cdot a_n^{k_n} (0 \leqslant k_i \leqslant d_i - 1, 1 \leqslant i \leqslant r; k_j \in \mathbb{Z}, j = r+1, \dots, n)$$

$$\Rightarrow \varphi(g) = \varphi(a_1)^{k_1} \cdot \dots \cdot \varphi(a_r)^{k_r} \varphi(a_{r+1})^{k_{r+1}} \cdot \dots \cdot \varphi(a_n)^{k_n}.$$

Таким образом $\varphi(g)$ однозначно определяется, если задать $\varphi(a_1), \dots, \varphi(a_n)$.

Пусть $|a_i| = d_i$, то есть $a_i^{d_i} = 1 \Rightarrow \varphi(a_i)^{d_i} = 1$ в поле $K \Rightarrow \varphi(a_i)$ — корень из 1 степени d_i в поле K, $1 \leqslant i \leqslant r$, а $a_{r+1}, \dots, a_n$ — любые не равные нулю элементы поля K.

`Обычно.` $K = \mathbb{C} \Rightarrow \{\sqrt[d]{1}\} = U_d$ — циклическая группа из d элементов:

$$\sqrt[d]{1} = \cos\left(\frac{2\pi k}{d}\right) + i \sin\left(\frac{2\pi k}{d}\right) = \varepsilon_1^k, \text{ где } \varepsilon_1 = \cos\left(\frac{2\pi}{d}\right) + i \sin\left(\frac{2\pi}{d}\right).$$

Представление $\varphi\colon \langle a_i \rangle_{d_i} \to \mathbb{C}^*$ можно построить d_i способами.

Если $G = \langle a_1 \rangle_{d_1} \times \cdots \times \langle a_r \rangle_{d_r}$, то $\varphi(g) = \varepsilon_1^{k_1} \cdot \dots \cdot \varepsilon_r^{k_r}$, где $\varepsilon_i^{k_i}$ — некоторый корень из 1 степени d_i в поле $\mathbb{C}$.

Вывод: всего имеется $d_1 \cdot d_2 \cdot \dots \cdot d_r = |G|$ одномерных представлений.

Сформулируем этот вывод в виде теоремы.

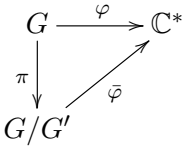
Теорема 15.3. *Конечная абелева группа G имеет $|G|$ различных одномерных представлений.*

Общий случай: G — произвольная группа.

$\varphi\colon G \to \mathbb{C}^*$ — одномерное представление. Но $\mathbb{C}^*$ — абелева группа $\Rightarrow \varphi(G) \cong G/\operatorname{Ker}\varphi$ — абелева группа.

По свойству: если $N \lhd G$ такая, что G/N абелева, то $G' \leqslant N$. Отсюда заключаем, что $\operatorname{Ker}\varphi \geqslant G'$.

Мы можем определить гомоморфизм $\bar{\varphi}\colon G/G' \to \mathbb{C}^*$ по правилу: $\bar{\varphi}(gG') = \varphi(g)$.



Здесь $\pi(g) = gG'$ — канонический гомоморфизм G на G/G'. Наоборот, если задан гомоморфизм абелевой группы $G/G' \xrightarrow{\bar{\varphi}} \mathbb{C}$, то можно определить гомоморфизм $\varphi\colon G \to \mathbb{C}^*$ по правилу: $\varphi(g) = \bar{\varphi}(gG')$.

Теорема 15.4. *Между одномерными представлениями $\varphi\colon G \to \mathbb{C}^*$ и одномерными представлениями $\bar{\varphi}\colon G/G' \to \mathbb{C}$ имеется взаимно однозначное соответствие. В частности, количество одномерных комплексных представлений конечной группы G равно $|G/G'| = |G : G'|$ — индексу коммутанта.*

(3) Определить всевозможные одномерные комплексные представления группы $A_4 = V_4$ — группы Кляйна.

$$V_4 = \{\, e, u, v, w \,\} \text{ где } u^2 = v^2 = w^2 = e, uv = w = vu \Rightarrow uw = v, vw = u.$$

т. к. $u^2 = e$, $\varphi(u)^2 = 1 = \varphi(v)^2 = \varphi(w)^2 \Rightarrow \varphi(u), \varphi(v), \varphi(w) = \pm 1$.

Составим таблицу:

	e	u	v	w
φ_1	1	1	1	$1 \cdot 1 = 1$
φ_2	1	-1	1	$(-1) \cdot 1 = -1$
φ_3	1	1	-1	$1 \cdot (-1) = -1$
φ_4	1	-1	-1	$(-1) \cdot (-1) = 1$

$w = uv \Rightarrow \varphi(w) = \varphi(uv) = \varphi(u)\varphi(v)$

В итоге:

V_4	e	u	v	w
φ_1	1	1	1	1
φ_2	1	-1	1	-1
φ_3	1	1	-1	-1
φ_4	1	-1	-1	1

(4) Найдём одномерные представления группы $G = D_4$ — группы диэдра.

$$D_4 = \{\, e, a, a^2, a^3; b, ab, a^2b, a^3b \,\}; bab^{-1} = a^{-1} \Rightarrow b^2 = e, ba^{-1}b^{-1} = a$$

Коммутант D_4:

$$D_4' = \{\, e, a^2 \,\} : [a, b] = aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = a^2 \Rightarrow$$
$$\langle a^2 \rangle \leqslant D_4' \Rightarrow \left|D_4'/\langle a^2 \rangle\right| = 4 \Rightarrow D_4'/\langle a^2 \rangle \text{ абелева } \Rightarrow D_4' \leqslant \langle a^2 \rangle \Rightarrow$$
$$D_4' = \langle a^2 \rangle.$$

Определим факторгруппу $D_4/D_4' = D_4/\langle a^2\rangle$ порядка 4. Она либо циклическая, либо изоморфна группе Кляйна.

$$D_4/\langle a^2\rangle = \{\, \langle a^2\rangle = \{\, e, a\,\}, a\langle a^2\rangle = \{\, a, a^3\,\}, b\langle a^2\rangle = \{\, b, a^2\,\}, ab\langle a^2\rangle = \{\, ab, a^3b\,\}\,\} = \{\, \bar e, \bar a, \bar b, \bar{ab}\,\}$$

$$b^2 = e, (ab)^2 = abab = a{\cdot}a^{-1} = e, a^4 = e; \bar a^2 = (a\langle a^2\rangle)(a\langle a^2\rangle) = a^2\langle a^2\rangle = \langle a^2\rangle = \{\, a^2, a^4\,\} = \bar e$$

$\Rightarrow$ все элементы факторгруппы в квадратах $= \bar e$, и $D_4/D_4' \cong V_4$. Изоморфизм $f\colon D_4/D_4' \to V_4$ задается так:

$$f(\bar e) = e, f(\bar a) = u, f(\bar b) = v, f(\bar a \cdot \bar b) = w.$$

Поэтому из таблицы для V_4 мы построим таблицу для D_4:

D_4	e	a^2	a	a^3	b	ba^2	ba	ba^3
φ_1	1	1	1	1	1	1	1	1
φ_2	1	1	-1	-1	1	1	-1	-1
φ_3	1	1	1	1	-1	-1	-1	-1
φ_4	1	1	-1	-1	-1	-1	1	1

(столбцы с номерами 1 и 2, 3 и 4, 5 и 6, 7 и 8 одинаковы)

15.2.1 Теоремы для не обязательно одномерных представлений

Теорема 15.5 (Теорема Машке)**.** *Любое конечномерное представление конечной группы G над $\mathbb{C}$ или $\mathbb{R}$ вполне приводимо.*

Теорема 15.6 (Теорема Машке для произвольного поля)**.** *Любое конечномерное представление конечной группы G над полем K характеристики 0 или p, не делящей $|G|$, вполне приводимо.*

Лемма 15.1 (Лемма Шура)**.** *Если $\varphi\colon G \to V$ и $\psi\colon G \to W$ — неприводимые представления, $f\colon V \to W$ — гомоморфизм представлений, то либо $f = 0$, либо f — изоморфизм.*

Без доказательства.

Лемма 15.2. *Пусть $\phi\colon G \to GL(V)$ — неприводимое комплексное представление группы $G, f\colon V \to V$ — такой линейный оператор, что $\forall g \in G, \phi(g)\cdot f = f\cdot\phi(g)$. Тогда f скалярный оператор, т. е. $\exists\lambda\in\mathbb{C}\colon \forall v \in V, f(v) = \lambda v$.*

Доказательство. Оператор f имеет в пространстве V собственный вектор $v_0 \neq 0, f(v_0) = \lambda v_0$. Рассмотрим собственное подпространство $V_\lambda = \{\, v \in V \mid f(v) = \lambda v\,\}$. Покажем, что V_λ инвариантно относительно любого $\phi(g), g \in G$:

$$\forall v \in V_\lambda, f(\phi(g))v = \phi(g)(f(v)) = \lambda\phi(g)v \Rightarrow \phi(g)v \in V_\lambda.$$

Так как V неприводимо, а $V_\lambda \neq \{0\}$, то $V_\lambda = V$, то есть $\forall v \in V\ f(v) = \lambda v$. $\square$

Теорема 15.7. *Любое неприводимое комплексное представление абелевой группы одномерно.*

Доказательство. Группа G абелева $\Rightarrow gh = hg, \forall g, h \in G \Rightarrow \phi(g)\phi(h) = \phi(h)\phi(g)$. Если взять в качестве оператора f оператор $\phi(h)$, то $\phi(h) = \lambda_h E$ или иначе это можно записать как $\forall v \in V, \phi(h)v = \lambda_h v$.

Если теперь взять произвольный $v_0 \in V, v_0 \neq 0$, то $\phi(h)v_0 = \lambda_h v_0, \forall h \in G \Rightarrow \langle v_0 \rangle \subset V$ — инвариантное подпространство в V, а так как V неприводимо, то $V = \langle v_0 \rangle$, то есть $\dim V = 1$. □

(5) Найти неприводимые представления абелевой группы G, имеющей порядок $|G| = 1188 = 11 \cdot 108 = 11 \cdot 6 \cdot 9 \cdot 2 = 11 \cdot 3^3 \cdot 2^2$. $G = A \oplus B \oplus C, |A| = 11, |B| = 3^3, |C| = 2^2$.

Рассмотрим случай, когда $G = \langle a \rangle_{11} \oplus \langle b \rangle_{3^2} \oplus \langle c \rangle_3 \oplus \langle d \rangle_{2^2}$. $\exp(G) = \text{НОК}(11, 3^2, 2^2) = 396$. Если запись мультипликативная, то произвольный элемент $g = a^{k_1} b^{k_2} c^{k_3} d^{k_4}, \phi(a)^{11} = 1, \phi(b)^9 = 1, \phi(c)^3 = 1, \phi(d)^4 = 1. \Rightarrow \phi(g) = \varepsilon_1^{k_1} \varepsilon_2^{k_2} \varepsilon_3^{k_3} \varepsilon_4^{k_4}, \varepsilon_1 = \sqrt[11]{1}, \varepsilon_2 = \sqrt[9]{1}, \varepsilon_3 = \sqrt[3]{1}, \varepsilon_4 = \sqrt[4]{1}, 0 \leqslant k_1 \leqslant 10, 0 \leqslant k_2 \leqslant 8, 0 \leqslant k_3 \leqslant 2, 0 \leqslant k_4 \leqslant 3$.

(6) $G = D_{10} \times A_4$. $D'_{10} = \langle a^2 \rangle$ — порядка 5. $|D_{10}/D'_{10}| = 4 \Rightarrow D_{10}/D'_{10} \cong V_4$.

$A'_4 = V_4; |A_4/V_4| = 3 \Rightarrow A_4/A'_4 \cong C_3 = \langle a \rangle, a = (1\,2\,3)V_4$.

$G' = D'_{10} \times A'_4 \cong \langle a^2 \rangle_5 \times V_4$ — порядка 20. $G/G' \cong (D_{10}/D'_{10}) \times (A_4/A'_4) \cong V_4 \times C_3$ $\Rightarrow G$ имеет 12 одномерных неприводимых представлений над $\mathbb{C}$.