ЛЕКЦИИ

4.09.2015г.

Группа

$(G;\cdot)$ — группа, если выполнены 3 усл:
мн-во операция

1) $a(bc)=(ab)c \quad \forall a,b,c\in G$ } полугруппа

2) $\exists e\in G: ae=ea=a \quad \forall a\in G$

3) $\forall g\in G \ \exists g^{-1}: gg^{-1}=g^{-1}g=e$

4) $ab=ba \quad \forall a,b\in G \Rightarrow$ абелева группа

$(G;+)$

вместо e пишут 0; вместо g

$H\subset G$ наз-ся подгруппой, если H само является группой относит. операции в G.

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

2) $e_H=e_G \quad , e\in H$

3) $a\in H \Rightarrow a^{-1}\in H$

Порядок элемента группы.

а) $a^n\neq e \quad \forall n\in\mathbb{N} \Rightarrow O(a)=\infty$

б) $\exists n$, т.ч. $a^n=e \Rightarrow O(a)=\min\{n>0, a^n=e\}$

Т [Если $O(a)=\infty$, то $a^k=a^l \Leftrightarrow k=l$.]

Т [Если $O(a)=n<\infty$, то $a^k=a^l \Leftrightarrow k\equiv l \pmod{n}$] $a^{-1}=a^{n-1}$

Т $\left[O(a)=n \Rightarrow O(a^k)=\frac{n}{НОД(k,n)} \right]$

ПРИМЕРЫ

① $(\mathbb{Z};+) \supset \underset{\text{подгр. кратных } n}{n\mathbb{Z}}$

② $(\mathbb{C};+) \supset (\mathbb{R};+) \supset (\mathbb{Z};+)$

K – поле; $K^* = K \setminus \{0\}$

③ $(K^*;\cdot)$

$U: \{z : |z|=1\}$

④ $(\mathbb{C}^*;\cdot) \supset U \supset \{\sqrt[\infty]{1}\} \supset \{\sqrt[n]{1}\}$

⑤ $\mathbb{C}^* \supset \mathbb{R}^* \supset \mathbb{R}_+$

⑥ $(\underset{\text{невыр. матрицы над полем } K}{GL(n,K)};\cdot) \supset \underset{\text{спец. } \{A \mid \det A=1\}}{SL(n,K)}$

⑦ $GL(n,\mathbb{R}) \supset SL(n,\mathbb{R})$

$\cup$

$\underset{\text{ортог. матр.}}{O(n)} \supset \underset{\text{спец. ортог.}}{SO(n)}$

Ортогональная:

$A^{-1} = A^T$

$A^{-1} = \overline{A^T}$ – унит.

⑧ $GL(n,\mathbb{C}) \supset SL(n,\mathbb{C})$

$\cup$

$\underset{\text{унитарн. матр.}}{U(n)} \supset \underset{\text{спец. унит.}}{SU(n)}$

⑨ S_n – симметрическая группа (перестановок)

$\cup$

A_n – знакопеременная

Для $n=4$: $V_4 \subset A_4 \subset S_4$

$\{e, (12)(34), (13)(24), (14)(23)\}$

$|M|$ – число элементов мн-ва M.

⑩ V – векторное пр-во над полем

$(V;+)$ – группа

Если $L \subset V$ – подпр-во, то L – подгруппа (абелева)

⑩а $V = \langle e_1, .., e_n \rangle$ над $\mathbb{R}$

$G = \{ \underset{k_i \in \mathbb{Z}}{k_1 e_1 + .. + k_n e_n} \}$ – подгруппа решетка (не зам. подпр-вом)

Циклическая группа

$(G;\cdot)$

Фиксим $a \in G$ и рассматриваем $\{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$

$|\langle a \rangle| = O(a)$.

G – циклическая группа, если $\exists\, a$, т.ч. $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

a – порождающий элемент

ПРИМЕРЫ

① $(\mathbb{Z};+)$

② $\sqrt[n]{1} = \langle \xi \rangle$, где ξ – первообр. корень n-й степени из 1; $|\sqrt[n]{1}| = n$.

Т $\left[\text{Если } |G| = n < \infty, \text{ то } G \text{ – циклическая} \Leftrightarrow \Leftrightarrow \exists\, a \in G\ O(a) = n;\ G = \langle a \rangle_n \right]$

$G=\langle a\rangle_n$; $\langle a^k\rangle = G \Leftrightarrow \underset{\text{взаимно просты}}{(k;n)=1}$

Число разных порождающих равна $\varphi(n)$

$G=\langle a\rangle_\infty$, a, a^{-1} — только 2 порождающих эл-та

(T) [Всякая подгр. цикл. группы является цикл.]

$\langle a\rangle_\infty$

$\langle a^k\rangle$, $k=0,1,\dots$ — получаем разные подгруппы, и это все подгруппы.

Подгруппы находятся в биективном соответствии:

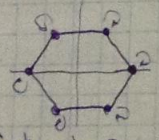
$\forall\, d|n\ \exists!$ подгр.: $\langle a^{\frac{n}{d}}\rangle_d$

Группы Диедра.

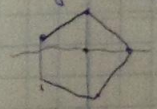
$\underset{\text{ортогональ. преобраз.}}{\overset{\text{подмножество}}{O(2)}} \subset \underset{\text{собств. орт. преобр.}}{SO(3)}$ n — фикс. нат. число

D_n — орт. преобр., сохр. правильный n-угольник с центром в начале координат.

$n=6$:



a — поворот на угол $\frac{2\pi}{n}$



$D=\begin{cases} a^k, & k=0,\dots,n-1 \\ \text{отражений относительно } n \text{ осей} \end{cases}$

$|D_n| = 2n$.

Пусть b — фикс. отражение

$a^k b$, $k=0,\dots,n-1$

$D_n = \{a^k b^\varepsilon \mid k=0,\dots,n-1,\ \underset{\text{обороты}}{\varepsilon=0}, \underset{\text{отраж.}}{1}\}$

$ba^k = a^{-k}b$.

$a^n=e$; $b^2=e \Rightarrow a^{k_1}b^{\varepsilon_1}a^{k_2}b^{\varepsilon_2} = a^{l}b^{\xi}$

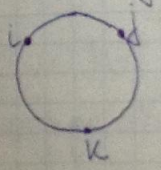
$\langle a\rangle \subset D_n$

Группа кватернионов

$Q_8 = \{\pm 1; \pm i, \pm j; \pm k\}$

При умножении знаки меняются как обычно

$+1$ — единица группы.



Определим операцию пр-ния:

$ij=k$ $\quad ji=-kj=-k$ $\quad i^2=j^2=k^2=-1$

$jk=i$ $\quad kj=-jk=-i$

$ki=j$ $\quad ik=-ki=-j$

1) Проверяем ассоциативность перебором небольшого числа случаев.

2) $e=1$ — единица

3) $i^{-1}=-i$ — обратный

4) Группа не абелева

D_4 — также не абелева.

Группы D_4 и Q_8 не изоморфны.

Разложение группы на смежные классы по подгруппе

$(G;\cdot)$ – группа

A, B – подмножества

Определяем их произведение.

$AB = \{ab \mid a \in A,\ b \in B\} \subset G$ – операция на подмножествах

$A(BC) = (AB)C$

$\{e\}$ – мн-во из одного эл-та (единица полугруппы)

Получаем полугруппу с единицей

$A^{-1} = \{a^{-1} \mid a \in A\}$ обр.

Полугр. будет группой, если будет мн-во из одного эл-та

$(AB)^{-1} = B^{-1}A^{-1}$

$(ab)^{-1} = b^{-1}a^{-1}$

Если $H \subset G$ – подгруппа

$g \in G$ $\{g\}$. $gH = \{gh \mid h \in H\}$ – левый смежный класс

$Hg = \{hg \mid h \in H\}$ – правый смежный класс

(Т) [Кол-во левых и правых смежных классов совпадает]

{ Строим биекцию. Рассм: $\varphi: g \mapsto g^{-1}$

{ $(gH)^{-1} = H^{-1}g^{-1} = Hg^{-1}$

Индекс подгруппы = число левых ~~=~~ правых смежных классов

$(G:H)$ – индекс подгр. H по группе G

1) $g \in gH \Longrightarrow G = \bigcup_{\text{по всем } g} gH$

2) $g_1 \in gH \Longrightarrow g_1H = gH$

3) либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \varnothing$.

$G = \bigcup gH$ – разбиение на попарно непересекающиеся множества

4) $|gH| = |H|$

(Т) [Если $|G| < \infty$ $H \subset G$; $|G| = |H|(G:H)$]

Лагранжа

(СЛ) [$O(a) = |\langle a \rangle| \overset{\text{т. Лагранжа}}{\Longrightarrow} O(a)$ явл. делителем порядка группы (в случае конечной группы)]

(СЛ) [Всякая группа простого порядка является циклической.]

ОПР Подгруппа наз-ся нормальной, если её левые и правые смежные классы совпадают, т.е.

$gH = Hg \quad \forall g \in G$

(Т) [Следующие условия равносильны:

1) $gH = Hg \quad \forall g \in G$ (опр)

2) $gHg^{-1} = H \quad \forall g \in G$

3) $gHg^{-1} \subset H \quad \forall g \in G$]

$1 \Rightarrow 2$
Умнож. 1) справа на g^{-1}
$2 \Rightarrow 1$
Умножаем 2) справа на g
$3 \Rightarrow 2$
$g^{-1}Hg \subseteq H$
Справа на g^{-1}, слева на g $\Rightarrow H \subseteq gHg^{-1}$ $\Big\} \Rightarrow g^{-1}Hg = H$ ■

ПРИМЕРЫ

① В абелевой группе всякая подгр. нормальная (т.к. умножение слева и справа одно и тоже)

② $\underline{H\text{-нормальная}, H \subseteq G \underset{\text{обозн.}}{\Rightarrow} H \triangleleft G}$
$(G:H) = 2 \Rightarrow H \triangleleft G$
Примеры может быть H и $G \setminus H$.

③ S_3-группа $\supset H = \langle (1\,2) \rangle$ – ненормальная подгруппа

④ $A_n \triangleleft S_n$

⑤ $V_4 \triangleleft S_n$

⑥ $H \triangleleft G$
$H \subset K \subset G \Rightarrow H \triangleleft K$
$K \subset G$ – любая $\Rightarrow (H \cap K) \triangleleft K$

⑦ $SL(n,K) \triangleleft GL(n,K)$ – из правила умнож. определителей

⑧ $\langle a \rangle_n \triangleleft D_n$, причем если $n > 2$, то $\langle b \rangle$ не явл. нормальной
подгруппа всех отражений

Задача Доказать, что в Q_8 не абелевой группе все подгруппы нормальные
(Почти все подгруппы имеют индекс 2)

Гомоморфизмы групп
$(G;\cdot) \xrightarrow{f} (\Gamma;\cdot)$ – группы
f – гомоморфизм двух групп, если оно сохраняет операцию, т.е. $f(ab) = f(a)f(b)$ $\forall a,b \in G$
Св-ва гомоморфизмов
1) $f(e_G) = e_\Gamma$
2) $f(a^{-1}) = (f(a))^{-1}$
3) Если $a \in G$, $O(a) = n < \infty$ то $O(f(a)) \mid O(a)$

Изоморфизм – биективный гомоморфизм (сохраняются все св-ва операций группы).
Если f – гомоморфизм, то $\operatorname{Im} f$ – подгр. в Γ
$G = \langle a \rangle$, $f: G \mapsto \Gamma$
f однозначно задается образом порождающего элемента, т.к. $f(a^k) = f(a)^k$
В) Какие эл-ты можно переводить порождающий?
1) $G = \langle a \rangle_\infty$, тогда в качестве $f(a)$ выбираем любой $b \in \Gamma$
$f(a^k) = b^k$ и получаем гомоморфизм.

2) $G = \langle a \rangle_n$

$f(a) = b$, то $b^n = e_r$ можно брать точно такие

Проверка корректности: $f(a^k) = b^k$

V, W – два векторных пр-ва

$V \xrightarrow{f} W$ – линейное отображение, т.е.:

1) $f(a+b) = f(a) + f(b) \quad \forall a, b \in V$

2) $f(\lambda a) = \lambda f(a) \quad \forall \lambda \in K, \forall a \in V$

$\Rightarrow$

$\Rightarrow$ линейное отображение – это гомоморфизм групп по сложению.

Ядро гомоморфизма

f – гомоморфизм, тогда $\operatorname{Ker} f \overset{\text{опр}}{=} \{a \in G : f(a) = e\}$

[(Ядро лин. отобр. – подпростр.). Ядро любого отображения групп является нормальной подгруппой]

$f(ab) = f(a)f(b) = ee = e \Rightarrow ab \in \operatorname{Ker} f$

$f(a^{-1}) = f(a)^{-1} = e^{-1} = e \Rightarrow a^{-1} \in \operatorname{Ker} f$

} подгруппа

Возьмем $a \in \operatorname{Ker} f$, $g \in G$, тогда

$f(gag^{-1}) = f(g)\underbrace{f(a)}_{e}f(g^{-1}) = e_r \Rightarrow gag^{-1} \in \operatorname{Ker} f$

$\Rightarrow$ по 3-му условию явл. нормальной. ■

ПРИМЕРЫ ГОМОМОРФИЗМОВ И ЯДЕР

① $S_n \xrightarrow{f} (\{\pm 1\}; \cdot)$

$f(\pi) = \operatorname{sgn}(\pi) \qquad \operatorname{Ker} f = A_n$ ← четные перестановки

② $GL(n, K) \xrightarrow{f} (K^*, \cdot)$

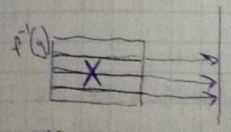
$f(a) = \det(A) \qquad \operatorname{Ker} f = \underset{\det = 1}{SL(n, K)}$

③ $(\mathbb{C}^*; \cdot) \xrightarrow{f} (\mathbb{R}^*, \cdot)$

$f(z) = |z| \qquad \operatorname{Ker} f = U$ – единичная окружность

Строение гомоморфизмов групп

$X \xrightarrow{f} Y$ Разбиение на полные прообразы



$y \in \operatorname{Im} f \subset Y$

Как устроено это разбиение при рассмотрении гомоморфизма групп?

Ⅰ [f задает разбиение группы G на смежные классы по ядру в случае гомоморфизма групп]

$y \in \operatorname{Im} f$

$f^{-1}(y)$ – смежный класс по $\operatorname{Ker} f = H$

$y = f(g_0)$, $g_0 \in G$

$f^{-1}(y) \overset{?}{=} g_0 H$ Раз $H \mapsto 1$

$f(g_0 H) = f(g_0) = y$

Имеем, что $g_0H \subseteq f^{-1}(y)$

Обратно, $\forall g \in f^{-1}(y)$. $f(g) = y$

$f(g_0^{-1}g) = \underbrace{f(g_0^{-1})}_{y^{-1}} \cdot \underbrace{f(g)}_{y} = y^{-1}y = e$

$g_0^{-1}g \in H \Rightarrow g \in g_0H \Rightarrow f^{-1}(y) \subseteq g_0H$

$f^{-1}(y) = g_0H$ ■

Пусть дана нормальная подгруппа $H \triangleleft G$.

Можно ли построить гомоморфизм, чтобы H была Ker

(T) [Подгруппа нормальна $\Leftrightarrow$ является ядром некоторого гомоморфизма]

При этом гр-ма G должна разбиться на смежные классы по H.

Построим группу, сост. из смежных классов по H.

$\Gamma = \{gH\}$ - мн-во смежных классов

Зададим операцию: $g_1H \bullet g_2H \overset{опр}{=} (g_1g_2)H$

Проверка корректности (не зависит от g_1, g_2):

$g_1H = g_1'H$, $g_2H = g_2'H \overset{?}{\Longrightarrow} (g_1g_2)H = (g_1'g_2')H$

$g_1' = g_1h_1$ $(h_1, h_2 \in H)$; $g_2' = g_2h_2$

$g_1'g_2' = (g_1h_1)(g_2h_2) = g_1g_2\underbrace{g_2^{-1}h_1g_2}_{\in H}h_2 = g_1g_2h$

Т.к. $H \triangleleft G$, то $g_2^{-1}h_1g_2 \in H$

$g_1g_2H = g_1'g_2'H$

1) Ассоциативность: т.к. определяем произведение классов, как пр-ние элементов

$g_1H[g_2H g_3H] = [g_1(g_2g_3)]H = [(g_1g_2)g_3]H = [g_1g_2H]g_3H =$
$= [g_1Hg_2H] \cdot g_3H$.

2) Роль единицы играет сама H, т.к.:

$H(gH) = (gH)H = gH$

3) $g^{-1}H$ — обратный для gH

Полученная группа наз-ся фактор-группой G по нормальной подгруппе H.

Имеется канонический изоморфизм π:

$G \xrightarrow{\pi} G/H$ $\quad \pi(g) = gH$

$\operatorname{Ker}\pi = H$. ■

Если H - ненормальна, то операцию на левых смежных классах определить (чтобы получился гомоморфизм π) нельзя, т.к. в ненормальной подгр. нет ядра.

Теорема о гомоморфизме.

(T) [Пусть дан $\forall$ f-гомоморфизм: $G \xrightarrow{f} \Gamma$, и рассмотрим фактор-группу по ядру: $G \xrightarrow{\pi} G/\operatorname{Ker} f$

Тогда $\exists!$ $\bar{f}$-гомоморфизм, т.ч. получившаяся диаграмма $G \xrightarrow{f} \Gamma$, $G \xrightarrow{\pi} G/\operatorname{Ker} f \xrightarrow{\bar{f}} \Gamma$, т.е. $f = \bar{f} \circ \pi$, и гомоморфизм $\bar{f}$ является изоморфизмом фактор-группы на образ f: $\bar{f}: G/H \longrightarrow \operatorname{Im} f$]

Лемма [$G \xrightarrow{f} \Gamma$ – гомоморфизм; $H \triangleleft G$, т.ч. $H \subseteq \operatorname{Ker} f$. И $\pi: G \xrightarrow{\pi} G/H$. Тогда $\exists!\ \bar{f}: f = \bar{f} \circ \pi$]

Определим $\bar{f}(gH)$. Т.к. $h \in \operatorname{Ker} f$, то $f(gH) = f(g)$. Причем, для равенства $f = \bar{f} \circ \pi$ единственный способ опред. $\bar{f}$: $\bar{f}(gH) = f(g)$.

$\bar{f}$ – гомоморфизм: $\bar{f}((g_1H)(g_2H)) \underset{\text{по опр.}}{=} f(g_1 g_2 H) \underset{\text{умн. смежн. кл.}}{=} f(g_1 g_2) \underset{\text{по опр. } f}{=} \bar{f}(g_1H) \cdot \bar{f}(g_2H)$ ▨

$\bar{f}$ – является изоморфизмом на образ.

$\operatorname{Im} \bar{f} = \operatorname{Im} f \Rightarrow \bar{f}$ – сюръективно $G/\operatorname{Ker} f \to \operatorname{Im} f$

$\forall$ гом-м устанавл. биекцию между элементами образа и смежными классами (доказ. ранее) $\Rightarrow$

$\Rightarrow$ инъективен. ■

$f: G \to \Gamma$, $\{f^{-1}(g)\} \cong \operatorname{Im} f$; $f = \bar{f} \circ \pi$, $\forall g \in G$ $f(g) = (\bar{f} \circ \pi)(g) = \bar{f}(gH)$

Лемма (следствие) [Пусть дана $H \triangleleft G$ и дан-ы G; Γ – группы. Рассм. мн-во гомоморфизмов $G \to \Gamma$: $(\operatorname{Hom}(G;\Gamma))$, таких что $H \subseteq \operatorname{Ker} f$: $\{f \in \operatorname{Hom}(G;\Gamma) \mid H \subseteq \operatorname{Ker} f\}$; и рассм. $\{\operatorname{Hom}(G/H, \Gamma)\}$. Тогда между этими двумя мн-вами имеется биективное соответствие]

$\Leftarrow \varphi$

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[rr, bend right, "f = \bar{f} \circ \pi"'] & G/H \arrow[r, "\bar{f}"] & \Gamma \end{tikzcd}$$

$H \subseteq \operatorname{Ker} f$

$\varphi(\bar{f}) = f$

$\Rightarrow \psi$

$G \xrightarrow{f} \Gamma$, $H \subseteq \operatorname{Ker} f \Rightarrow$ по лемме $\exists!\ \bar{f}$, т.ч.

$f = \bar{f} \circ \pi \Rightarrow \psi(f) = \bar{f}$

φ и ψ – взаимно обратные отображения.

(Биективность следует из $!\ \bar{f}$ в лемме) ■

ПРИМЕРЫ ФАКТОР-ГРУПП.

$H \subset G$. Найдем фактор-группу, т.е.

1) $H \triangleleft G$

2) Дать описание разложения G на см. классы

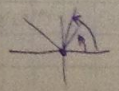
3) Описать операцию на множестве смежн. классов

4) Найти извест. ранее группу Γ, т.ч. $G/H \cong \Gamma$

$(\mathbb{C}^*; \cdot)$

① $(\mathbb{R}_+; \cdot) \subset \mathbb{C}^*$

1) абелева $\to$ норм.

2) разб. $\mathbb{C}^*$ — это разб. на мн-во лучей 

3) операция сложение углов наклона

4) биект. соотв. между мн-вом лучей и единичной окружностью

$\mathbb{C}^*/\mathbb{R}_+ \cong U$

② $U \subset \mathbb{C}^*$

1) очевидно

2) — задаются радиусом

3) умножение радиусов

4) $\mathbb{C}^*/U = \mathbb{R}_+$

В силу т. о гомоморфизме, если удастся построить

$f: G \xrightarrow[\text{сюр.}]{f} \Gamma$; $\operatorname{Ker} f = H$ $\Rightarrow$ равносильно 4 условиям.

Пример применения теоремы о гомоморфизме

③ $(\mathbb{R}^*, \cdot) \subset \mathbb{C}^*$ $\quad f: \mathbb{C}^* \to U$

$f(z) = \left(\frac{z}{|z|}\right)^2$ → сюр гом-м. ядро $= \mathbb{R}$

④ Гомоморфизм векторных пр-в.

K-поле $\quad V \xrightarrow{f} W \quad (V,+)$ — группа

$f(v_1+v_2) = f(v_1) + f(v_2)$ — f сохр. операцию сложения (явно)

$f(\lambda v) = \lambda f(v) \quad \forall \lambda \in K$ — линейное отображение

$\operatorname{Ker} f$ = Ker лин. отображения

Имеет место тер. о гомоморфизме и в этом примере

Центр группы.

Пусть имеется группа G, $n \in \mathbb{Z}$

Рассм. $f: G \to G \quad f(a) = a^n$

Если G - абелева $\Rightarrow$ f - гомоморфизм.

$\operatorname{Ker} f = \{a : a^n = e\} = \{a^t : O(a) | n\}$ — подгруппа n-кручения

$n=2$, f - гомом $\Rightarrow$ G - абелева

Центр группы — мн-во элементов $Z(G)$, определяемое как $Z(G) = \{a \in G : ag = ga \ \forall g \in G\}$

Центр — подгруппа (проверить!); норм. подгруппой,

т.е. $H \subseteq Z(G) \subseteq G$

$H \triangleleft G$, т.к. эл-ты из H перестановочны со всеми эл-тами группы

ПРИМЕРЫ ЦЕНТРОВ

⓪ $Z(G) = G \Leftrightarrow G$ - абелева

① $Z(GL(n,K)) = \{\lambda E \mid \lambda \neq 0\}$

② $Z(SL(n,K)) = \{\lambda E \mid \lambda^n = 1\}$

③ $Z(S_n) = \{e\}$ $\quad n \geq 3$

④ $Z(A_n) = \{e\}$ $\quad n \geq 4$

⑤ $Z(Q_8) = \{\pm 1\}$

⑥ $D_n = \{a^k b^\varepsilon,\ 0 \leq k \leq n-1,\ \varepsilon = 0,1\}$

$$Z(D_n) = \begin{cases} \{e\}, & n \text{ - нечетно} \\ \langle a^{n/2} \rangle & n \text{ - четно} \end{cases}$$

Теорема о фактор-группе по центру

(Т) Фактор-группа не абелевой группы по центру не может быть циклической

Пусть $G/Z(G)$ – циклическая, т.е.
$\exists\, a \in G$, т.ч. $G/Z(G) = \langle a Z(G) \rangle$

Покажем, что $\forall$ два эл-та из G коммутируют, получив противоречие.

$a_1, a_2 \in G$

$a_1 Z(G) \overset{\text{предп.}}{=} a^k Z(G) \Rightarrow a_1 = a^k z_1$ $\quad z_1, z_2 \in Z(G)$

$a_2 Z(G) \overset{\text{предп.}}{=} a^l Z(G) \Rightarrow a_2 = a^l z_2$

$\Rightarrow a_1 a_2 = (a^k z_1)(a^l z_2) = (a^l z_2)(a^k z_1) = a_2 a_1$ (т.к. $z_1, z_2 \in Z(G)$ коммутируют с всеми элементами группы)

здесь все элементы переставились

Получим, что группа абелева, противоречие. ■

Связь между подгруппами в группе и в ее фактор-группе.

(Т) Пусть $N \triangleleft G$, G/N. Тогда имеется биективное соответствие между $\{\overline{H} \mid \overline{H} \in G/N\}$ (все подгруппы в фактор-группе по N) и всеми эл-тами $\{H : H \subseteq G,\ N \subseteq H\}$ (все подгр. в G, содержащими N)

φ ψ

При этом соотв-вии нормальные подгруппы соответствуют друг другу

$\psi(H) = H/N \subset G/N$ (подгруппа) — это взаимно обратные отображения

$\varphi(\overline{H}) = \bigcup_{gN \in \overline{H}} gN$

$H \triangleleft G \Leftrightarrow H/N \triangleleft G/N$

$\Rightarrow$ Пусть $H \triangleleft G \Rightarrow \forall\, h \in H,\ g \in G:\ ghg^{-1} \in H$

Покажем, что $\forall\, hN \in H/N;\ gN \in G/N$

$(gN)(hN)(gN)^{-1} \overset{?}{\subseteq} H/N$

$\overset{\text{опред.}}{=} (\underbrace{ghg^{-1}}_{\in H})N \subseteq H/N$

$\Leftarrow$ Аналогично (пользуемся равенством в обратную сторону). ■

Пусть дан гомоморфизм $G \xrightarrow{f} \Gamma$ (сюръективный)

Γ – гомоморфный образ группы G

На языке гомоморфизмов пред. теорема имеет вид:

(Т) Если задан сюр. гом-м f, то имеется биект. соотв. между всеми подгруппами в Γ и подгруппами в G, т.ч. $\operatorname{Ker} f \subseteq H$

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & \Gamma \\ G/\operatorname{Ker} f \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Поскольку $\bar{f}$ – биективно, можем отождествить Γ и $G/\operatorname{Ker} f$ $\Rightarrow$ подгр. в Γ то же самое что и подгр. в $\operatorname{Ker} f$.

$\{\overline{H} \subseteq \Gamma\} \overset{\varphi}{\leftrightarrow} \{H \subseteq G : \operatorname{Ker} f \subseteq H\}$

$f = \bar{f} \circ \pi$, f отождествляется с π.

$\overline{H} \subseteq \Gamma \mapsto \pi^{-1}(\overline{H}) = f^{-1}(\overline{H})$ — Проверку биективности можно и провести на языке гом-ма f.

$H \subseteq G \mapsto \pi(H) = f(H)$ ■

Теорема об изоморфизме

(Т) [Пусть $H \triangleleft G \overset{\text{пред. теор}}{\Longleftrightarrow} H/N \triangleleft G/N$. Тогда $G/H \cong (G/N)/(H/N)$. (Формально можно „сократить" на N)]

$G \xrightarrow[\text{сюр}]{\pi} G/N \xrightarrow[\text{сюр}]{\bar{\pi}} (G/N)/(H/N) \Longrightarrow \bar{\pi}\circ\pi$ – сюръективна

По т. о гомоморфизме $(G/N)/(H/N) \cong G/\mathrm{Ker}(\bar{\pi}\circ\pi)$.

$\mathrm{Ker}(\bar{\pi}\circ\pi)$ – ?

$\mathrm{Ker}(\pi) = N$, $\mathrm{Ker}(\bar{\pi}) = H/N$ $\Big\} \Rightarrow \mathrm{Ker}(\bar{\pi}\circ\pi) =$

$= \pi^{-1}(\underbrace{\mathrm{Ker}\,\bar{\pi}}_{H/N}) = H$. (полный прообраз при определении π) ■

Произведение подгрупп

G – группа, $A, B \subseteq G$ – подгруппы

Уже определяли $AB = \{ab \mid a \in A, b \in B\}$ для множеств

(Т) [Произв. двух подгрупп является подгруппой (AB – подгруппа) $\Longleftrightarrow AB = BA$]

Обозначим $H = AB$.

H подгруппа $\Longleftrightarrow$ 1) $H \neq \varnothing$
2) $HH = H$
3) $H^{-1} = H$

($\Leftarrow$) Пусть дано $AB = BA$.

$H = AB = BA$

$HH = \underbrace{(AB)}_{AB}\underbrace{(AB)}_{AB} \overset{\text{ассоц}}{=} A(BA)B = \underbrace{(AA)}_{A}\underbrace{(BB)}_{B} = AB = H$ (т.к. A – подгруппа; H – подгр.)

$H^{-1} = (AB)^{-1} = B^{-1}A^{-1} = BA = AB = H$

($\Rightarrow$) Пусть дано $H = AB$ – подгруппа.

$\underbrace{H}_{AB} = H^{-1} = (AB)^{-1} = \underbrace{B^{-1}}_{B}\underbrace{A^{-1}}_{A} = BA$ (т.к. подгр.; т.к. A, B – подгр.) $\Rightarrow AB = BA$ ■

Следствие [Если одна из подгрупп A или B нормальна, то AB – подгруппа. Если обе нормальны, то AB – норм. подгруппа]

Пусть $A \triangleleft G$.

$AB = \bigcup_{b \in B} Ab \overset{\text{по определению нормальности}}{=} \bigcup_{b \in B} bA = BA$. + пред. теорема $\Rightarrow$ подгр.

$A \triangleleft G \Rightarrow gag^{-1} \in A\ \forall g \in G$; $B \triangleleft G \Rightarrow gbg^{-1} \in B\ \forall g \in G \Longrightarrow$
$\Longrightarrow (gag^{-1})(gbg^{-1}) \in AB \Rightarrow gabg^{-1} \in AB \Rightarrow AB$ – нормальная ■

Теорема об изоморфизме для произведения подгрупп

(Т) [Пусть G – группа, A, B – подгруппы в G, $A \triangleleft G$. Тогда $AB/A \cong B/B\cap A$]

Рассмотрим гом-м $f: B \longrightarrow AB/A$ по правилу (нормален в силу нормальности A):

$f(b) = bA$ (очевидно, что гом-м в силу умножения; опр. операции смежных классов)

$abA = b\underbrace{(b^{-1}ab)}_{\in A,\ \text{т.к. } A\text{-нормальна}}A = bA \Rightarrow$ сюръективный гомоморфизм

По т. о гомоморфизме $AB/A \cong B/\mathrm{Ker}\,f$

$\mathrm{Ker}\,f$ – ? $f(b) = A \Leftrightarrow b \in A$, т.е. $\mathrm{Ker}\,f = B \cap A$

$AB/A \cong B/\mathrm{Ker}\,f = B/B\cap A$ ■

ПРИМЕР К ТЕОРЕМЕ

① $V_4 \triangleleft S_4$

$S_4/V_4 \overset{?}{\cong} S_3 \subset S_4$ если $S_3 \equiv \{\begin{pmatrix} i_1 & i_2 & i_3 & 4 \\ j_1 & j_2 & j_3 & 4 \end{pmatrix}\}$ — подгр. в S_4

Тогда $S_3 \cap V_4 = \{e\}$. $\Rightarrow V_4 S_3 = S_4$.

$A \equiv V_4$, $B \equiv S_3$. $\underset{\text{теор.}}{\Rightarrow} \underset{S_4}{V_4 S_3}/V_4 \cong S_3/\underset{\{e\}}{S_3 \cap V_4} \cong S_3$

Прямое произведение подгрупп

PS: Прямая сумма — если операция в группе $(G;+)$

PS: Очевидным образом определяем $A_1 \cdots A_s$

Внутреннее прямое произведение подгрупп

G - группа; $G_1, \dots, G_s \subset G$.

G является прямым произв. подгрупп $G_1, \dots, G_s$ и обозначается $G = G_1 \times \dots \times G_s$, если выполнено:

1) $\forall i: G_i \triangleleft G$

2) $G = G_1 \cdots G_s$, т.е. $\forall g\ \exists g_1 \in G_1, \dots, g_s \in G_s$, т.ч. $g = g_1 \cdots g_s$ и такое представление единственно, т.е. если $g_1 \cdots g_s = g_1' \cdots g_s'$ $\forall i: g_i, g_i' \in G_i \Rightarrow g_i = g_i'$

Ⓣ Следующие условия эквивалентны:

1) $G = G_1 \times \dots \times G_s$

2) $G_i \triangleleft G$; $G = G_1 \cdots G_s$ и $\forall i: G_i \cap (G_1 \cdots \widehat{G_i} \cdots G_s) = \{e\}$

3) $G_i \triangleleft G$, $G = G_1 \cdots G_s$ и $\forall i: G_i \cap (G_1 \cdots G_{i-1}) = \{e\}$

4) $G = G_1 \cdots G_s$ $\forall g_i \in G_i, g_j \in G_j$ $(i \neq j)$: $g_i g_j = g_j g_i$

$g_1 \cdots g_s = e$, $g_i \in G_i \Rightarrow \forall i\ g_i = e$. (т.е. проверяем только (!) для единицы)

(1⇒2) Пусть $\exists a \neq e \in G_i \cap (G_1 \cdots \widehat{G_i} \cdots G_s) \Rightarrow$

$\Rightarrow a = ee \cdots e a e \cdots e = g_1 \cdots \underset{e}{\widehat{g_i}} \cdots g_s$ (в i нет одного представления) $\Rightarrow a = e$.

(2⇒3) Очевидно, т.к. если пересечение с большей $= e$, то и с меньшей — также единица.

Лемма [Пусть G - группа, $A \triangleleft G$, $B \triangleleft G$, причем $A \cap B = \{e\}$, тогда $ab = ba$ $\forall a \in A\ b \in B$]

$\underbrace{aba^{-1}b^{-1}}_{\in B} \in B$, $\underbrace{aba^{-1}b^{-1}}_{\in A} \in A$ $\Rightarrow aba^{-1}b^{-1} = e \Rightarrow$

$\Rightarrow ab = ba$ ▨

(3⇒4) Без огр. общности $i < j$. $G_i \cap G_j \overset{\text{подгр.}}{\subseteq} \{e\}$

$\Rightarrow \forall g_i \in G_i, g_j \in G_j$ $i \neq j$: $g_i g_j = g_j g_i$

Пусть $g_j \neq e$, но $g_1 \cdots g_{j-1} g_j = e \Rightarrow$

$\Rightarrow g_j = (g_1 \cdots g_{j-1})^{-1} = g_{j-1}^{-1} \cdots g_1^{-1}$ лемма

$= g_1^{-1} \cdots g_{j-1}^{-1} \in G_j \cap (G_1 \cdots G_{j-1}) \Rightarrow g_j = e$, проти.

(4⇒1) Проверим, что $\forall i\ G_i \triangleleft G$. Возьмем $\forall b_j \in G_j$ и $\forall g \in G: g = g_1 \cdots g_s$.

последовательно переставляем $g_1 \cdots g_s$ с b_j до тех пор, пока $i < j$ (иначе поправим)

$g^{-1} b_j g = g_s^{-1} \cdots g_1^{-1} b_j g_1 \cdots g_s =$

$g_j \in G_j$ можем выполнить переставлять

$= g_s^{-1} \cdots g_{j+1}^{-1} g_j^{-1} b_j g_j g_{j+1} \cdots g_s = g_j^{-1} b_j g_j \in G_j$

Проверим однозначность представления

$g_1 \cdots g_s = g_1' \cdots g_s'$

$(g_1 \cdots g_s)^{-1} g_1 \cdots g_s = (g_1 \cdots g_s)^{-1} g_1' \cdots g_s' \Longrightarrow$

$e \Rightarrow g_s^{-1} \cdots g_1^{-1} \cdot g_1' \cdots g_s' = e.$ берем g_i' и переставляем до g_i

$(g_1^{-1} g_1')(g_2^{-1} g_2') \cdots (g_s^{-1} g_s') = e \overset{\text{по условию 4}}{\Longrightarrow} g_i = g_i'$ ■

Внешнее прямое произведение

$G_1, \dots, G_s$ — s-группа (возможны повторения)

$G = \underbrace{G_1 \times \dots \times G_s}_{\text{декартово произведение}} = \{(g_1 g_2 \dots g_s) \mid \forall 1 \le i \le s : g_i \in G_i\}$

Введем на этом мн-ве операцию умножения покомпонентно:

$(g_1, \dots, g_s)(g_1', \dots, g_s') = (g_1 g_1', \dots, g_s g_s')$.

Очевидно, так задается группа, которую назовем внешним прямым произведением

(Т) 1. Если $G = G_1 \underset{\text{внутреннее}}{\times} \dots \times G_s$, то $G \cong G_1 \underset{\text{внешнее}}{\times} \dots \times G_s$.

2. Если $G = G_1 \underset{\text{внешнее}}{\times} \dots \times G_s$, то G является внутр произв. подгрупп, которые естественным образом изоморфны группам $G_1, \dots, G_s$

Д. $G = G_1 \times \dots \times G_s$ — внутреннее

$G' = G_1 \times \dots \times G_s$ — внешнее

Строим изоморфизм $f: G' \xrightarrow{f} G$, а именно:

$f[(g_1, \dots, g_s)] = g_1 \cdots g_s \in G$, $\Rightarrow$ очевидно биекция в силу однозначности представления $g = g_1 \cdots g_s$.

Покажем, что f — гомоморфизм:

$f[(g_1, \dots, g_s)(g_1', \dots, g_s')] \underset{\text{по опред. операции}}{=} f[(g_1 g_1', \dots, g_s g_s')] \underset{\text{по определению } f}{=} (g_1 g_1') \cdots (g_s g_s')$

$f[(g_1, \dots, g_s)] \cdot f[(g_1', \dots, g_s')] = (g_1 \cdots g_s) \cdot (g_1' \cdots g_s') \underset{\text{т.к. элементы из разных подгрупп коммутируют}}{=}$

② Дано $G = G_1 \underset{\text{внешнее}}{\times} \dots \times G_s$ 18.09.2015

$G_i' = \{(e, \dots, e, \underset{\text{на место } g_i \in G_i}{g_i}, e, \dots, e)\}$ — очевидно подгруппа, причем $G_i' \cong G_i$.

Покажем, что $G = \underbrace{G_1' \times \dots \times G_s'}_{\text{внутреннее}}$, проверив 4-е условие:

1) элементы из разных $G_i \neq G_j$ коммутируют

2) G — произведение этих подгрупп: действительно, т.к. $(g_1, \dots, g_s) = (g_1, e, \dots, e) \cdots (e, \dots, g_s)$

3) $(e, \dots, e) \underset{\text{проверим единственность только для единицы}}{=} (g_1, e, \dots, e) \cdots (e, \dots, e, g_s) \Longrightarrow g_i = e$. ■

В дальнейшем будем говорить просто о прямом пр-ии групп, отождествив внутреннее и внешнее.

Далее, пусть $|G| = n < \infty$ ($\Leftrightarrow |G_i| < \infty$)

Тогда $|G_1 \times \dots \times G_s| = |G_1| \cdots |G_s|$

Замечание: если группа конечна, то в условиях

проверки, что группа есть прямое произв. подгрупп, можно из двух условий 1) $G = G_1 \times \ldots \times G_s$ 2) единственность можно проверять только одно. (задача)

ПРИМЕРЫ РАЗЛОЖЕНИЙ В ПРЯМОЕ ПРОИЗВЕДЕНИЕ

① $\forall G: G = G \times \{e\}$ — тривиальное разложение

② $G = (\mathbb{R}^*, \cdot)$

$G_1 = \{\pm 1\}$; $G_2 = \mathbb{R}_+$

Тогда $\forall \overset{\neq 0}{z} \in \mathbb{R}: z = (\pm 1)|z| \Rightarrow \mathbb{R}^* = G_1 \times G_2$

③ $G = (\mathbb{C}^*, \cdot)$

$G_1 = U = \{z : |z| = 1\}$; $G_2 = \mathbb{R}_+$

Тогда $\forall z \in \mathbb{C}: z = \underbrace{|z|}_{\in \mathbb{R}_+}(\cos\alpha + \underbrace{i\sin\alpha}_{\in U}) \Rightarrow \mathbb{C}^* = \mathbb{R}_+ \times U$

④ $G = \underbrace{\sqrt[n]{1}}_{\text{корни } n\text{-й степени из единицы}} \subset \mathbb{C}^*$

Если $n = kl$; $(k,l) = 1$

Тогда $\zeta \in \sqrt[n]{1}: \zeta = \zeta_1 \cdot \zeta_2$, где $\zeta_1 \in \sqrt[k]{1}$; $\zeta_2 \in \sqrt[l]{1}$

$\Rightarrow \sqrt[n]{1} = \sqrt[k]{1} \times \sqrt[l]{1}$

Кроме того, $\sqrt[n]{1} = \langle a \rangle_n$, a — первообр. корень из 1

$n = kl$; $(k,l) = 1$

Тогда $\langle a \rangle_n = \langle b \rangle_k \times \langle c \rangle_l$

Воспользовавшись индукцией для $n = n_1 \cdot \ldots \cdot n_s$: $(n_i, n_j) = 1$ $i \neq j$

$\langle a \rangle_n = \langle a_1 \rangle_{n_1} \times \ldots \times \langle a_s \rangle_{n_s}$

$\langle a \rangle_n = \langle a^{\frac{n}{n_1}} \rangle_{n_1} \times \ldots \times \langle a^{\frac{n}{n_s}} \rangle_{n_s}$

Наименьшее разложение: $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ p_i — различные простые

$\langle a \rangle_n = \langle a_1 \rangle_{p_1^{k_1}} \times \ldots \times \langle a_n \rangle_{p_s^{k_s}}$

Примарная циклическая группа — это группа, порядок которой равен степени простого числа.

Любая цикл. группа разлагается в прямое произведение примарных цикл. групп.

Ⓣ [Примарная циклическая группа неразложима в нетривиальные прямые произведения]

Делители p^k: $0 \le i \le k$. p^i

$\langle a \rangle_{p^k} \supset \langle a^p \rangle_{p^{k-1}} \supset \ldots \supset \langle a^{p^{k-1}} \rangle_p \supset \{e\}$

Любые 2 неедини. подгр. имеют неединичное пересечение $\Rightarrow$ они не могут иметь нетривиального разложения. ■

Ⓣ [Бесконечная циклическая группа не разложима в прямое произведение.]

$\langle a \rangle_\infty$. $\underset{k,l \neq 0}{\langle a^k \rangle \cap \langle a^l \rangle} \supset \langle a^{kl} \rangle$ — содержит неединичную $\Rightarrow$ прямое пр-ние получиться не может. ■

Замечание: Прямое пр-ние обладает ассоциативностью, т.е. из большего всегда можем получить меньшее:

$$G = \underbrace{(G_1 \times \dots \times G_{i_1})}_{G'} \times \underbrace{(G_{i_2} \cdots G_{i_3})}_{G''} \times \underbrace{(G_{i_4} \times \dots \times G_{i_5})}_{G'''}$$

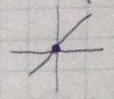
Рассмотрим V над K – лин. пр-во

$\forall L \subset V$ – подпр-во $\exists L' \subset V \Rightarrow V = L \oplus L'$.

Векторное пр-во неразложимо в прямую сумму подпр-в $\Leftrightarrow$ когда оно одномерно.

$G = G_1 \times \dots \times G_s$

Недостаточно выполнения условия $G_i \cap G_j = \{e\}$.
$i \neq j$.



Порядки элементов в прямом произведении групп.

$g \in G_1 \times \dots \times G_s$

$g = (g_1, \dots, g_s)$

(T) [g имеет конечный порядок $\Leftrightarrow$ все g_i имеют конечный порядок, причем $O(g) = НОК\{O(g_1), \dots, O(g_s)\}$]

Если $O(g_i) = \infty$, тогда $g^k = (g_1^k, \dots, g_s^k) \overset{k \neq 0}{\neq} e$.

Пусть далее $\forall i$: $O(g_i) = n_i < \infty$

$g^k = e \Leftrightarrow n_i | k \ \forall i \Rightarrow$ наим. такой порядок – это и есть НОК$\{O(g_1), \dots, O(g_s)\}$

? Когда произведение цикл. групп является цикл. группой?

$G = \langle a_1 \rangle_{n_1} \times \dots \times \langle a_s \rangle_{n_s}$ (все множители нединичные)

(T) [Это разложение является циклической группой $\Leftrightarrow$ либо $s = 1$, либо все множители конечны, а порядки — попарно взаимно просты.]

Если хотя бы один мн-ль $O(a_i) = \infty$ и G – циклич $\Rightarrow G$ – беск. циклическая $\Rightarrow$ но она не имеет нетривиального прямого разложения. $\Rightarrow s = 1$.

Если все порядки n_i конечны.

Порядок прямого пр-ния — есть пр-ние порядков:

$|G| = n_1 \cdots n_s$.

G – цикл $\Leftrightarrow \exists g = g_1 \cdots g_s \in G$, т.ч. $O(g) = n_1 \cdots n_s$.

Но $O(g) = \underset{O(g_i) | n_i}{НОК}\{O(g_i)\} = n_1 \cdots n_s$
$\Updownarrow$
когда $(n_i, n_j) = 1$ при $i \neq j$.

В качестве порождающего в G можно взять $g = (a_1, \dots, a_s)$ ■

Теорема об изоморфизме для некоторых фактор. групп прямого произведения групп.

(Т) [Если $G=G_1\times\dots\times G_s$, $H=H_1\times\dots\times H_s$ $\forall H_i\subseteq G_i$. (Тогда $H_i=G_i\cap H$). Тогда $H\triangleleft G \Leftrightarrow$ $\Leftrightarrow H_i\triangleleft G_i\ \forall i$ и $G/H\cong G_1/H_1\times\dots\times G_s/H_s$]

(⇒) Очевидно. $H\triangleleft G$, $\forall K\subseteq G \Rightarrow H\cap K\triangleleft G$

(⇐) Получим при построении изоморфизма

$g=g_1\cdots g_s$
$\overline{g_i}=g_iH_i\ \forall i$

Дано: $\forall H_i\triangleleft G_i$.

Можем построить $G_1/H_1\times\dots\times G_s/H_s$

Построим гомоморфизм $\varphi: G\to G_1/H_1\times\dots\times G_s/H_s$ по правилу $\varphi(g)=(\overline{g_1},\dots,\overline{g_s})$. — очевидно кон-ен в силу определения операции умножения, тоже он сюръективен ($\forall\ \overline{g_i}$ можно представить...)

$g\in\operatorname{Ker}\varphi \Leftrightarrow \overline{g_i}=\overline{e}$ в G_i/H_i
$\Updownarrow$
$g_i\in H_i\ \forall i \Longrightarrow$

$\Rightarrow \operatorname{Ker}\varphi=\underbrace{H_1\times\dots\times H_s}_{=H}$

По т.о гомоморфизме $G_1/H_1\times\dots\times G_s/H_s=\operatorname{Im}\varphi\cong$
$\cong G/\operatorname{Ker}\varphi=G/H$. □

Т.к. ядро нормальная подгр. $\Rightarrow H$ — нормальна ■

Абелевы группы.

Система порождающих в абелевых группах.

G — группа (PS: может быть и не абелева)

$S\subseteq G$ — подмножество

Будем н-ть подгруппу, порожденную S наименьшую подгруппу, содержащую S и обозначать $\langle S\rangle$.

$\langle S\rangle=\bigcap$ всех подгрупп, содерж. S.

Далее, пусть G — абелева, операция сложение

$S=\{x_i\}\ i\in I$

$x_{i_1},\dots,x_{i_m}\in S \Rightarrow (n_1x_{i_1}+\dots+n_mx_{i_m})\in\langle S\rangle$, где $n_i\in\mathbb{Z}$

$\{n_1x_{i_1}+\dots+n_mx_{i_m}\mid \forall x_{i_k}\in S\ n_i\in\mathbb{Z}\}$ — наименьшая подгруппа $\Rightarrow$

$\Rightarrow \langle S\rangle$

PS: В случае $(G,\circ)$ тоже самое в других обозначениях.
$\langle S\rangle=\{n_1^{x_{i_1}}\cdots n_m^{x_{i_m}}\mid \forall x_{i_k}\in S, n_i\in\mathbb{Z}\}$

Если $S=\{a\}$, то $\langle S\rangle=\langle a\rangle$

Подм-во S в группе наз-ся системой порождающих, если подгруппа, порожденная S совпадает со всей группой.

$G=\langle S\rangle$, т.е. $\forall g\in G: g=n_1x_{i_1}+\dots+n_mx_{i_m}$ (без однозначности!)
$x_{i_k}\in S$

Группа, имеющая систему порождающих из одного элемента — циклическая группа.

Абелева группа наз-ся конечнопорожденной, если она имеет конечную систему порождающих элементов.

$G=\langle a_1,..,a_m\rangle \overset{\text{базис подобно}}{\Longleftrightarrow} \forall g=n_1a_1+..+n_ma_m \quad n_i\in\mathbb{Z}$

Тривиальная система порождающих совпадает со всей группой.

$(\mathbb{Q};+)$ не имеет конечной системы порождающих
нет не только конечной, нет минимальной системы

$(\mathbb{Q}_+;\cdot)$ также не имеет конечной системы порожд.
не можем выбрать минимальную

Далее будем рассматривать только конечнопорожденные абелевы группы.

? + (T) [Пусть G - абелева, $H\triangleleft G$. G - конечнопорожд. $\Leftrightarrow$ $H, G/H$ - конечнопорожденные.]

($\Leftarrow$) $H=\langle b_1,..,b_s\rangle$, $G/H=\langle \overline{a_1},..,\overline{a_t}\rangle$ $(\overline{a_i}=a_i+H)$

$G\overset{?}{=}\langle a_1,..,a_t,b_1,..,b_s\rangle$

Возьмем $\forall g\in G$. $\overline{g}=g+H$.

$\overline{g}=p_1\overline{a_1}+..+p_t\overline{a_t}$ $\quad p_t\in\mathbb{Z}$

$g-(p_1a_1+..+p_ta_t)$ — смежный класс этого элемента равен нулю $\Rightarrow$

$g-(p_1a_1+..+p_ta_t)\in H \Rightarrow$

$g-(p_1a_1+..+p_ta_t)=q_1b_1+..+q_sb_s \Rightarrow$

$\Rightarrow g=p_1a_1+..+p_ta_t+q_1b_1+..+q_sb_s \Rightarrow g\in\langle a_1,..,a_t,b_1,..,b_s\rangle$

($\Rightarrow$) $G=\langle a_1,..,a_t\rangle \Rightarrow$

$\Rightarrow \forall g\in G: g=p_1a_1+..+p_ta_t \quad p_i\in\mathbb{Z}$

Тогда $g+H=\overline{g}=p_1\overline{a_1}+..+p_t\overline{a_t}$ $\quad(\overline{a_i}=a_i+H)$

$\forall \overline{g}\in G/H \Rightarrow G/H=\langle\overline{a_1},..,\overline{a_t}\rangle$.

Покажем, что H - конечнопорождена, причем можно выбрать порождающих не более t штук.

Индукция по t.

$t=1 \Rightarrow G$ - цикл $\Rightarrow$ любая подгр. циклическая

$t>1$. Рассмотрим $\underset{\langle p\rangle}{H_1}=\{n\in\mathbb{Z} \mid \exists g\in H, \text{т.ч. } g=na_1+\beta_2a_2+..+\beta_ta_t\}$

Очевидно $H_1\subseteq\mathbb{Z}$ - подгруппа

Но всякая подгр. в $\mathbb{Z}$ - циклическая $\Rightarrow$

$\Rightarrow H_1=\langle pa_1\rangle p\in\mathbb{Z}$.

Обозначим $H_2=H\cap\langle a_2,..,a_t\rangle$

Возьмем $g\in H$

$g=p_1a_1+p_2a_2+..+p_ta_t$

$p_1=kp$; $g'=pa_1+p_2'a_2+..+p_t'a_t\in H$

$g - kg' = (p_2 - kp_2')a_2 + \ldots + (p_t - kp_t')a_t \in H_2$

По инд. предположению H_2 имеет $t-1$ порождающий

$g = kg' + q_2 b_2 + \ldots + q_t b_t$ — верно $\forall g \in H$. $\Rightarrow$

$\Rightarrow H = \langle g', b_2, \ldots, b_t \rangle$. ■

25092015г. **Теорема о каноническом виде целочисленной матрицы**

Пусть A — матрица $m \times n$, $A = (a_{ij})$, $a_{ij} \in \mathbb{Z}$.

Будем проводить целочисленные эл. преобразования

① $i \neq j$ $A^{(j)} \mapsto A^{(j)} + \lambda A^{(i)}$, $\lambda \in \mathbb{Z}$

② $i \neq j$ $A^{(i)} \leftrightarrow A^{(j)}$ умож. на обратные элементы нельзя

③ i $A^{(i)} \mapsto \pm A^{(i)}$

(T) С помощью послед-ти целочисл. эл. преобразований над строками или столбцами целочисленной матрицы, её можно привести к диагональному виду $A' = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_m \end{pmatrix} \bigcirc_{n \geq m}$, $A' = \begin{pmatrix} d_1 & 0 \\ 0 & d_m \end{pmatrix} \bigcirc_{n \geq m}$, $d_i > 0$, $d_i \in \mathbb{Z}$ и $\forall i$ $d_i | d_{i+1}$ (также считаем, что 0 делится на 0).

И такой вид для A определен однозначно и не зависит от выбора посл-ти эл. преобр.

Индукция по числу строк

$m = 1$ $(a_{11}\ a_{12} \ldots a_{1n})$

Индукция по $\min |a_{1j}|$, где $a_{1j} \neq 0$.

Основание: $\min |a_{1j}| = 1$, $\exists a_{1j} = 1$. $\Rightarrow$ без о.о. $a_{11} = 0$

Применяя эл. преобр-ния со столбцами приводим $(a_{11} \ldots a_{1n}) \mapsto (1, 0, \ldots, 0)$

Если $\min |a_{1j}| = d < k$ $a_{1j} \neq 0$ $k > 1$, то доказано.

$\exists a_{1j} = d$. Если все остальные делятся на d, то приводим к нужному виду. Если какой-то не делится, то взяв остаток при делении — эл. преобр-ние $\Rightarrow$ для эл-т с остатком на d получаем, что $\exists$ элемент, меньший по модулю и по инд. предположению для него доказано.

Пусть для числа строк $< m$ — доказано.

$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$

$\min |a_{ij}| = d < k$. $\exists a_{ij} = d > 0$.

Переставляя строки и столбцы можем считать, что $a_{11} = d$ и так же как в случае с одной строкой, если в 1-й строке и 1-м столбце все эл-ты делятся на d,

то можем сразу в них получить нули.

Осн. инд. $d=1$ — всегда можем сделать.

Если не все делятся — делим с остатком, и применяем индукцию по $\min|a_{ij}|$.

Т.е. можем считать, что все эл-ты в 1-й строке и 1-м столбце делятся на d

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \longrightarrow \begin{pmatrix} d & 0 & \dots & 0 \\ 0 & a'_{22} & \dots & a'_{2n} \\ \vdots & & & \\ 0 & a'_{m2} & \dots & a'_{mn} \end{pmatrix}$$

Допустим, что какой-то a'_{ij}, $i>1, j>1$ не делится на d. То тогда добавляя к 1-й строке i-ю строку, получаем в 1-й строке эл-т не делящийся на d и переходим к 1-му случаю. (применяем деление с остатком и уменьш. модуля $\Rightarrow$ по инд. предп. будет все доказано).

Значит, можем считать, что $d \mid a_{ij}\ \forall i,j>1$

Применяем индукцию по числу строк для матрицы $\begin{pmatrix} a''_{22} & \dots & a''_{2n} \\ a''_{m2} & \dots & a''_{mn} \end{pmatrix}$. При эл. преобр-ниях делимость на d сохраняется $\Rightarrow$ полученный диагональный вид сохраняет делимость:

$$\begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_m \end{pmatrix} \quad d_1 \mid d_2 \mid \dots \mid d_m$$

индукция ■

Свободная абелева группа.

$G = \langle a_1, \dots, a_n \rangle$

$\forall g \in G: \ g = k_1 a_1 + \dots + k_n a_n \quad k_i \in \mathbb{Z} \ \ 1 \le i \le n.$

Похоже на разложение по базису в векторном пр-ве: $V^{\text{над } K} = \langle e_1, \dots, e_n \rangle$; $\forall v \in V \ v = r_1 e_1 + \dots + r_n e_n \ r_i \in K$, но в нем также имеется единственность $\Leftrightarrow$ $e_1, \dots, e_n$ — ЛНЗ.

$b_1, \dots, b_s \in G$ — линейно независимы, если $k_1 b_1 + \dots + k_s b_s = 0 \Longrightarrow \forall k_1, \dots, k_s = 0 \ \ k_i \in \mathbb{Z}$

$\Leftrightarrow g = k_1 b_1 + \dots + k_s b_s$ — однозначно.

В абелевой группе не всегда можно выбрать базис (ЛНЗ систему порождающих)

ПРИМЕР:

$G = \langle a \rangle_n \Rightarrow \forall g \in G \ \ ng = 0 \ \ n \ne 0 \Rightarrow$ любая система из одного эл-та ЛЗ $\Rightarrow$ базис выбрать нельзя

Конечно-порожденная абелева группа наз-ся свободной, если она обладает базисом, т.е. ЛНЗ системой порождающих. ($\Leftrightarrow$ такой системой пор-щих, через которую $\forall g \in G$ выражается единств. образом)

ПРИМЕР СВОБОДНОЙ АБЕЛЕВОЙ ГРУППЫ

① $G = \underbrace{\overset{\langle x_1\rangle}{\mathbb{Z}} \oplus \mathbb{Z} \oplus \dots \oplus \overset{\langle x_n\rangle}{\mathbb{Z}}}_{n\text{-слагаемых}}$

$x_i = (0, \dots, 0, \underset{i\text{-е место}}{1}, 0, \dots, 0)$

$g = (k_1, \dots, k_n) = k_1 x_1 + \dots + k_n x_n$, k_i – однозначно

Т [Всякая свободная абелева группа является прямой суммой бесконечных циклических групп]

$G = \langle x_1, \dots, x_n \rangle$ (базис, сооб.) ← все x_i имеют беск. порядок, т.к. если бы хоть один имел конечный порядок, то система линейно зависима.

$\forall g \in G \quad g = k_1 x_1 + \dots + k_n x_n$, $k_i \in \mathbb{Z}$ (единственно)

$G_i = \langle x_i \rangle \cong \mathbb{Z}$ $\Rightarrow \forall g = g_1 + \dots + g_n$, $g_i \in G_i = \langle x_i \rangle$ ■

Произвольная абелева группа наз-ся свободной, если в ней каждая конечная подсистема ЛНЗ.

ПРИМЕР

① $(\mathbb{Q}, +)$ не свободная (

② $(\mathbb{Q}_+, \cdot)$ свободная, с беск. базисом в виде степеней простых чисел

Рангом конечно порожденной свободной абелевой группы называется число элементов в базисе. Для проверки корректности, покажем, что ранг не зависит от выбора базиса. (теорема об инвариантности ранга)

$G = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n}$, G – абелева

$G \xrightarrow{\varphi_q} G$ $\quad \varphi_q(a) = qa$ – гомоморфизм в случае абелевых групп

$\underset{\text{подгруппа}}{\operatorname{Im}\varphi_q} \subseteq G$

Возьмем фикс. число $q > 1$.

Обозначение: $\operatorname{Im}\varphi_q = qG$.

Теперь, если G – свободная абелева

$qG = \underbrace{q\mathbb{Z} \oplus \dots \oplus q\mathbb{Z}}_{n}$ (не зависит от базиса)

Рассмотрим $G/qG \cong \underbrace{\mathbb{Z}/q\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/q\mathbb{Z}}_{n}$

Каждое слагаемое имеет порядок q, то

то $|G/qG| = q^n$ – не зависит от выбора базиса.

$\Rightarrow n$ определено однозначно $n = \log_q |G/qG|$ ■

Теорема о согласованных базисах в конечно порожденной свободной абелевой группе и ее подгруппе.

Т [Всякая подгр. H конечно порожденной свободной абелевой группы F свободна и можно выбрать базисы в $F = \langle x_1, \dots, x_m \rangle$ и в $H = \langle y_1, \dots, y_n \rangle$ так, что $y_1 = d_1 x_1, \dots, y_k = d_k x_k$, где $k \le m$, $d_i > 0$; $d_i \in \mathbb{N}$ (условие согласованности)]

Покажем, что H – свободная.

$H = \langle y_1, .., y_n \rangle$ – конечная система порождающих

$y_j = \sum_{i=1}^{m} a_{ij} x_i$, где $a_{ij} \in \mathbb{Z}$

$\Downarrow$

$A = (a_{ij})$ – целочисленная матрица (зависит от выбора базисов)

Будем рассматривать элементарные изменения базисов.

$x_1, .., x_m$. Выберем i $(1 \le i \le m)$; $\lambda \in \mathbb{Z}$

$x'_k := x_k \ \forall k \ne i$.
$x'_i := x_i - \lambda x_j$ } $\Rightarrow$ очевидно, что базисность сохранится

$y_k = a_{1k} x_1 + .. + a_{mk} x_m = a_{1k} x_1 + .. + a_{ik}(\overbrace{x_i - \lambda x_j}^{x'_i}) +$
$+ .. + (a_{jk} + \lambda a_{ik}) x_j + ..$ ← к j-й строке добавилась i-я умноженная на λ. $\Rightarrow$

$\Rightarrow$ элем. пр-ния 1-го вида соответствуют элем. преобраз. базиса

$\Rightarrow$ эл. преоб. 2-го типа — перестановка базисных векторов

$\Rightarrow$ эл. преоб. 3-го типа — умножение элем. базиса на ± 1

Преобразования базиса в H — это преобразования над столбцами м-цы A.

Т.о., применяя преобр. к матрице A и пос-ти выбора базисов в F и в H, мы можем найти такие базисы $F = \langle x'_1, .., x'_m \rangle$ и $H = \langle y_1, .., y_k \rangle$, $k \le m$, что

$y'_1 = d_1 x'_1, .., y'_k = d_k x'_k$.

← базис → H – свободная

$$A \to A' = \begin{pmatrix} d_1 & & 0 \\ & d_k & \\ 0 & & 0 \end{pmatrix}$$

$d_i \ge 0$ ■

Т Всякая конечно порожденная абелева группа изоморфна фактор-группе конечно порожд. свободной абелевой группы по некоторой её подгруппе.

Дано: $G = \langle b_1, .., b_m \rangle$ – порожд. – с

Рассмотрим $F = \langle x_1, .., x_m \rangle$ – свободная

$\varphi: F \to G$ – сюръект. будем строить по правилу:

$\varphi(c_1 x_1 + .. + c_m x_m) = c_1 b_1 + .. + c_m b_m$

← F ← из свойств своб. $\Rightarrow$ φ определено корректно.

Очевидно, что φ – гомоморфизм.

Сюръект., т.к. в виде $c_1 b_1 + .. + c_m b_m$ записывается всякий элемент $g \in G$.

Обозначим $H = \operatorname{Ker} \varphi$. По т.о гомоморфизме $G \cong F/H$ ■

H – подгруппа состоящий из всех порождающих в G

Основная теорема о конечнопорожденных абелевых группах.

(Т) Всякая конечно порожденная абелева группа разлагается в прямую сумму некоторого конечного числа беск. циклических групп и примарных циклических групп, причем в таком разложении слагаемые определены однозначно, с точностью до изоморфизма

однозначно определены порядки циклических слагаемых

т.е. разложение слагаемых а слагаемые — нет

Если же сами подгруппы опред. однозначно ⇒ сама группа циклическая.

(∃) G – абелева

$G \cong F/H$ (свб.) (подгр). Выбираем в F и H согласованные базисы $F=\langle x_1,\dots,x_n\rangle$, $H=\langle y_1,\dots,y_k\rangle$, т.е. $y_j = d_j x_j$.

$$F = \underbrace{\mathbb{Z}}_{=\langle x_1\rangle}\oplus\underbrace{\mathbb{Z}}_{=\langle x_2\rangle}\oplus\dots\oplus\underbrace{\mathbb{Z}}_{=\langle x_n\rangle}$$

$$H = \underbrace{d_1\mathbb{Z}}_{=\langle d_1x_1\rangle}\oplus\dots\oplus\underbrace{d_k\mathbb{Z}}_{=\langle d_kx_k\rangle}\oplus\underbrace{0\oplus\dots\oplus 0}_{n-k}$$

По т.о изоморфизме $G \cong F/H \cong \mathbb{Z}/d_1\mathbb{Z}\oplus\dots\oplus\mathbb{Z}/d_k\mathbb{Z}\oplus\mathbb{Z}/0\oplus\dots\oplus\mathbb{Z}/0$.

Если $d_i=1$ ⇒ нулевые слагаемые
$d_i>1$ – конечн. цикл. группы
$d_i=0$ ⇒ беск. цикл. группы

$d_i>1$ – раскладываем в примарные цикл. группы. ▨

(!) $G=\bigoplus_{i=1}^{s}\langle a_i\rangle_\infty\oplus\left(\bigoplus_j\langle b_j\rangle_{p_j^{k_j}}\right)$

s, $\{p_j^{k_j}\}$ (?) определены однозначно

G – (любая) абелева группа

$T(G)$ – мн-во всех эл-тов из группы конечного порядка

$T(G)=\{g\in G : O(g)<\infty\}$ — подгруппа в случае абелевой G (подгруппа кручения)

элемент кручения

$O(g_1)=n_1$, $O(g_2)=n_2$

$n_1n_2(g_1+g_2)=0$

Пусть p – простое

$T_p(G)=\{g\in G : O(g)$ ~~есть~~ степень $p\}$ — — подгруппа в случае абелевой G (p-кручения)

элементы p-примарного порядка

$T(G)$, $T_p(G)$ не зависят от разложения по опред.

Если $G=\bigoplus_{i=1}^{s}\langle a_i\rangle_\infty\oplus\underbrace{\left(\bigoplus_j\langle b_j\rangle_{p_j^{k_j}}\right)}_{T(G)}$

$T(G)=\bigoplus_j\langle b_j\rangle_{p_j^{k_j}}$

$T_p(G)=\bigoplus_{j:\,p_j=p}\langle b_j\rangle_{p_j^{k_j}}$

не зависят от разложения

Поэтому ~~осталось~~ показать, что s – однозначно:

$G/T(G)\cong\bigoplus_{i=1}^{s}\langle a_i\rangle_\infty$ — своб. аб. группа с рангом, равным числу беск. цикл. слаг.

не зависит от разложения и ее ранг

⟹ s не зависит от разложения

Каждое $T_p(G)$ однозначно раскладывается в прямую сумму примарных циклических:

$T_p(G)=\bigoplus_{j=1}^{t}\langle b_j\rangle_{p^{k_j}}$, $k_1\geq k_2\geq\dots\geq k_t$ безотр. аб.

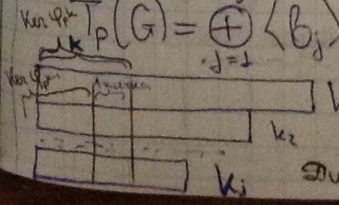


Диаграмма Юнга

$|T_p(G)|=p^{\sum k_j}$ — число клеток в диаграмме

Знаем, что $\forall$ абелевой G $\exists$ гомоморфизм

$\varphi_m : G \to G \quad \varphi_m(g) = mg$

Здесь, $\forall k$ рассмотрим гомоморфизм φ_{p^k}:

$\varphi_{p^k} : G \to G \quad \varphi_{p^k}(g) = p^k g$; и рассмотрим его ядро: $\mathrm{Ker}(\varphi_{p^k}) = \{g : p^k g = 0\}$

Элемент лежит в ядре $\Leftrightarrow$ все эл-ты лежат в ядре.

Порядок ядра $= p^{\text{число клеток левее черты}}$.

$\mathrm{Ker}\,\varphi_{p^k} = \bigoplus_{j,\, k \le k_j} \langle b_j^{k_j - k} \rangle$

Обозначим N_k – число слог. в разложении порядка $\geq p^k$, а n_k – число слог. в разложении порядка $= p^k$.

Рассмотрим $\mathrm{Ker}\,\varphi_{p^k} / \mathrm{Ker}\,\varphi_{p^{k-1}}$. Порядок (фактор-группы) равен числу клеток „между двумя чертами" $= N_k$.

$|\mathrm{Ker}\,\varphi_{p^k} / \mathrm{Ker}\,\varphi_{p^{k-1}}| = p^{N_k}$

не зависит от разложения $\Rightarrow p^{N_k}$ не зависит $\Rightarrow N_k$ не зависит от разложения

$n_k = N_k - N_{k+1} \Rightarrow n_k$ не зависит от разложения ■

Классификация с точностью до изоморфизма абелевых групп данного порядка n.

G – абелева; $|G| = n$

$G = \bigoplus_j \langle a_j \rangle_{p_j^{k_j}} \longrightarrow n = \prod_j p_j^{k_j}$ (не обязательно разложение p)

$n = \prod_j p_j^{k_j}$

$G = \bigoplus_j \langle a_j \rangle_{p_j^{k_j}}$ (внутреннее) $\Rightarrow$ получим $|G| = n$.

Вывод: имеется биективное соответствие между классами относит. изоморфизма абелевых групп порядка n и разложениями числа n в произведение степеней простых чисел.

Когда G – циклическая?

$\boxed{G\text{-циклическая} \Leftrightarrow \text{все } p_j \text{ различны}}$

ПРИМЕР: Найти с точностью до изоморфизма все абелевы группы порядка 100.

$100 = 2^2 5^2 = 2 \cdot 2 \cdot 5^2 = 2^2 \cdot 5 \cdot 5 = 2 \cdot 2 \cdot 5 \cdot 5$

$G_1 = \langle a_1 \rangle_{2^2} \oplus \langle a_2 \rangle_{5^2} \longleftarrow$ циклическая

$G_2 = \langle b_1 \rangle_2 \oplus \langle b_2 \rangle_2 \oplus \langle b_3 \rangle_{5^2}$

$G_3 = \langle c_1 \rangle_{2^2} \oplus \langle c_2 \rangle_5 \oplus \langle c_3 \rangle_5$

$G_4 = \langle d_1 \rangle_2 \oplus \langle d_2 \rangle_2 \oplus \langle d_3 \rangle_5 \oplus \langle d_4 \rangle_5$

Любая абелева G порядка 100 изоморфна одной из $G_1 - G_4$, которые в свою очередь между собой не изоморфны.

Конечные подгруппы в мультипликативной группе поля.

группа по умножению между ненул. элем. поля

(Т) [Всякая конечная подгруппа в мультипликативной группе поля — циклическая]

Пусть $|G| = n < \infty$;

$d(G)$ — показатель группы G;

$d(G) \overset{опр}{=} \min\{k>0 : g^k = e \mid \forall g \in G\} \Leftrightarrow O(g) \underset{\forall g}{\mid} k$

$\Leftrightarrow d(G) = НОК\{O(g) \mid g \in G\}$

n — общее кратное $\Rightarrow d(G) \mid n \Rightarrow d(G) \leq n$

Лемма [Абелева (конечная) группа циклическая $\Leftrightarrow d(G) = n$]

Для неабелевых групп неверно

Если G — циклическая, $G = \langle a \rangle_n \Rightarrow \exists$ элемент a порядка $n \Rightarrow d(G) = n$.

Если $d(G) = n$; $G = \bigoplus_j \langle a_j \rangle_{n_j}$; $\prod_j n_j = n$

$d(G) = НОК\{n_j\}$ $\quad d(G) = n \Leftrightarrow \prod_j n_j = НОК\{n_j\} \Leftrightarrow$

$\Leftrightarrow n_j$ попарно взаимно просты $\Leftrightarrow$ G — циклическая. ∎

утверждение на пред. странице

Доказательство теоремы:

$G \subset K^*$, $|G| = n < \infty$

$d = d(G)$. Покажем, что $d = n$.

Пусть $d < n$, тогда ($g^d = e \ \forall g \in G$)

все $g \in G$ — корни многочлена $x^d - 1$, но число корней, которое не больше его степени

Следствие [Мультипликативная группа конечного поля является циклической]

пример: $\mathbb{Z}_p$

Кольца и алгебры.

Определение кольца $(R; +, \cdot)$:

1) $(R, +)$ — абелева группа
2) $a(b+c) = ab + ac$, $(a+b)c = ac + bc$ $\quad \forall a, b, c \in R$
3) R — ассоциативное (дополнительно)
4) R — коммутативное
5) R с единицей
6) R без делителей 0

обратные по умножению элементы $U(R)$

$ab = 0$, $a, b \neq 0$.

Понятие алгебры над полем K $(R; +, \cdot, \cdot)$

умножение на скаляры из K

1) $R(+, \cdot)$ — кольцо (внутр. умн.)
2) $R(+, \cdot)$ — векторное пр-во над K (внешнее)
3) $\lambda(ab) = (\lambda a)b = a(\lambda b) \quad \forall a, b \in R, \lambda \in K$

ПРИМЕРЫ АЛГЕБР

K — поле

① $K[x_1, \ldots, x_n]$ — кольцо мн-нов с коэф-тами из поля K

② $M_n(K)$ — матрицы над полем K

③ $T_n(K)$ — верхнетреугольные матрицы над K

ПРИМЕР КОЛЕЦ, НЕ ЯВЛЯЮЩИХСЯ АЛГЕБРОЙ

$\mathbb{Z}$; $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$

не простое

$M_n(K)$: $U(M_n(K))$ — невыр. матрицы

Делители нуля — выр. матр.

$\mathbb{Z}/n\mathbb{Z}$: $U(\mathbb{Z}/n\mathbb{Z}) = \{k+n\mathbb{Z} \mid (k,n) = 1\}$ (вз. просто)

Делители нуля $= \{k+n\mathbb{Z} \mid (k,n) > 1\}$ (не вз. просто)

Подкольцо:

$S \subseteq R(+,\cdot) \Leftrightarrow S$ — кольцо, относит. этих же $(+,\cdot)$.

Подалгебра — подмн-во в алгебре, сохраняющее операции.

$M_n(\mathbb{Z}) \subset M_n(\mathbb{R})$

подкольцо, но не подалгебра (не явл. подпространством)

Центр кольца и алгебры.

R — кольцо или алгебра.

$Z(R) = \{a \in R : ar = ra \ \forall r \in R\}$

Центр — всегда подкольцо (R-кольцо) или подалгебра (R-алгебра)

Замечание: Если R-алгебра с 1 над K, то $\forall \lambda \in K$: $\lambda \mapsto \lambda \cdot 1^{\in R}$ можем определить вложение, которое является изоморфизмом K на подполе в R.

$\lambda \cdot 1 \in Z(R)$, по условию 3 в опред. алгебры.

Матрицы. Отождествляем скаляры со скалярными матрицами. $(\lambda 1)a = 1(\lambda a) = (\lambda a)1 = a(\lambda 1)$

В центре алгебре с 1 над K содержится само поле K.

При этом $1_R = 1_K$.

Обратно, если R — кольцо с 1, $K \subseteq Z(R)$ и $1_K = 1_R \Rightarrow R$ — алгебра над K (т.к. $K \subseteq Z(R) \Rightarrow$ ум. 3)

подполе

проверяем, т.к. опер. на эл. из поля должно оставлять элемент на месте

ПРИМЕРЫ ЦЕНТРОВ КОЛЕЦ

① $Z(M_n(K)) = \{\lambda E\} = K$

② $Z(T_n(K)) = \{\lambda E\} = K$

③ Коммут. кольцо

$\exists 1 \in R(+,\cdot,\cdot)$ 20.2015

1) $K \subseteq Z(G)$

2) $1_K = 1_R \Leftrightarrow 1_R \in K$

ПРИМЕР: $K \subset L$ — расширение полей.

Идеалы в кольцах и алгебрах.

R — кольцо.

I — идеал в R, если $I \subset R$:

1) I — подгруппа по $+$

2) $\forall r \in R, a \in I$, $ra \in I$, $ar \in I$

R-алгебра

I-идеал в R, если $I \subset R$:

1) I – подпространство в R

2) $\forall r \in R, a \in I, ra \in I, ar \in I$ (выдерживает умн. с двух сторон)

Идеал = двусторонний идеал

Можно рассм. левые и правые идеалы.

ЛЕВЫЙ: — // — 2) $\forall r \in R, a \in I, ra \in I$

ПРАВЫЙ: — // — 2) $\forall r \in R, a \in I, ar \in I$.

ПРИМЕРЫ ИДЕАЛОВ

В случае комм. кольца: левый = правый = двусторонний

R-кольцо или алгебра

$\forall a \in R$ $Ra = \{ra \mid r \in R\}$ – в силу ассоц. левый идеал

$aR = \{ar \mid r \in R\}$ – правый идеал

Каждый эл-т кольца или алгебры задает главный идеал. (левый, правый).

В случае комм. кольца $Ra = aR$ – (двусторонний) главный идеал.

① $\mathbb{Z}$, $n\mathbb{Z}$ – гл. идеал, порожденный n

② $f \in K[x]$, $fK[x]$ – мн-во мн-нов, делящихся на f

$= (f)$ – главный идеал.

$\{0\}, \{R\}$ – тривиальные двуст. идеалы, которые есть в любом кольце.

Замечание: R-алгебра с 1, I-идеал в R как в ~~некотором~~ кольце $\Rightarrow$ I-идеал в алгебре $K \subset R$

Если R-алгебра без 1. Введем умн. в поле K: $ab = 0$ $\forall a, b \in K$. Идеал в этом кольце – любая подгруппа по сложению. $(K; \cdot, \cdot)$ – одномерно и неприв. подгр. в здесь нет, в то время как в кольце их сколько угодно.

③ $M_n(K)$ кольцо/алгебра

$$\begin{pmatrix} * & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ * & * & * & * \\ * & 0 & 0 & 0 \end{pmatrix} \Rightarrow \text{левый идеал в } M_n(K)$$

$j^1 \quad j^2 \quad j^3$ – фикс. номера столбцов

$$\begin{array}{c} i_1 \\ i_2 \end{array}\begin{pmatrix} 0 & 0 & * & \cdots & 0 \\ 0 & 0 & * & \cdots & 0 \\ & & * & & \end{pmatrix} \Rightarrow \text{правый идеал в } M_n(K)$$

④ $T_n(K) = \left\{ \begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix} \right\}$ кольцо

$I = \left\{ \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix} \right\}$ – двусторонний идеал в $T_n(K)$

Гомоморфизмы колец и алгебр

$R \xrightarrow{f} S$

$R(+,\cdot)$ $S(+,\cdot)$ — кольца

f - гомоморфизм колец, если:

1) $f(a+b) = f(a)+f(b)$
2) $f(ab) = f(a)f(b)$

$R(+,\cdot,\cdot)$ $S(+,\cdot,\cdot)$, то f - гом-м алгебр, если:

1) $f(a+b) = f(a)+f(b)$
2) $f(ab) = f(a)f(b)$
3) $f(\lambda a) = \lambda f(a)$ — мн. отобр. вект. пространств

Если R, S — алгебры с 1 над одним полем K (имеет смысл говорить о гомоморфизмах)

$K \subseteq R$, $K \subseteq S$.

$f: R \to S$ - гомоморфизм колец, т.ч.

$f(1_R) = 1_S$.

Он будет гомоморфизмом алгебр $\Leftrightarrow$ когда $f(\lambda 1_R) = \lambda f(1_R) = \lambda 1_S$, $f(\lambda) = \lambda$

$\forall \lambda \in K$ (т.е. отображает поле тождественно)

$$f: (R,+) \to (S,+)$$

$$\operatorname{Ker} f \underset{\text{опр}}{=} \{r \in R : f(r) = 0\} = f^{-1}(\{0\})$$

Утверждение [Ядро любого гомоморфизма колец и алгебр является двусторонним идеалом]

$f(ra) = f(r)\underbrace{f(a)}_{0} = 0$

$f(ar) = 0$ $\Rightarrow$ $ra \in \operatorname{Ker} f$, $ar \in \operatorname{Ker} f$ ■

Строение гомоморфизма.

Гомоморфизм колец и алгебр разбивает группы по сложению на смежные классы по ядру

$b \in \operatorname{Im} f$, $f^{-1}(b)$

$b = f(a)$.

$f^{-1}(b) = a + \operatorname{Ker} f$

[Любой двуст. идеал в кольце или алгебре является ядром некоторого гом-ма колец или алгебр.]

$\underline{R\text{-кольцо}}$, $I \subset R$, I - двуст. идеал

$I \subseteq (R,+)$

$R/_{\text{по сложн.}} I = \{a+I\}$.

Вводим операцию умножения: $(a+I)(b+I) = ab + I$

Проверим корректность:

$a'+I = a+I$ $\quad a' = a+x$, $x \in I$

$b'+I = b+I$ $\quad b' = b+y$, $y \in I$

$(a'+I)(b'+I) = (ab+xb+ay+xy)+I = ab+I$

$ab+I$ Т.к. I – двуст. идеал $\Rightarrow ay, xb, xy \in I \Rightarrow$

(Все аксиомы кольца выполняются).

R-алгебра

Умножение на ф-группе вводим также.

Умножение на скаляры: аналогично, в этом случае I подпр-во.

Теорема о гомоморфизме для колец и алгебр.

(Т) [Пусть $R \xrightarrow{f} S$ – гомоморфизм колец (алгебр)

$\pi: R \to R/\mathrm{Ker} f$ (канон. гом-м) $\pi(a) = a + \mathrm{Ker} f$ (мно проверить!)

Тогда $\exists!\ \bar{f}$ – гомоморф. групп по $+$: $\bar{f}(a+\mathrm{Ker} f) = f(a)$ гом-м относ. всех двух операций: $+, \cdot$

Из теор. о гом-ме групп: $\bar{f}: R/\mathrm{Ker} f \to \mathrm{Im} f$ биективное отображение.]

(Все аналогично теореме с группами, $+$ дополнительно говорим, что все операции $+, \cdot$ сохраняются при таких отобр. $f, \pi, \bar{f}$.)

$I \subset R$ идеал. Имеется биективное соответствие между $(R/I; +)$ подгруппами в R/I и подгруппами в R, содержащими I.

Утв [При этом соотв. подкольца, идеалы, левые и правые идеалы соответствуют друг другу]

(Аналогично группам)

Простые кольца и алгебры.

Кольцо или алгебра наз-ся простым, если оно не содержит нетривиальных двуст. идеалов.

Это значит, что $\mathrm{Ker} f$ $\forall f$ – либо $\{0\}$ (инъективный); либо все кольцо (нулевой гом-м).

Т.е. всякий гом-м либо инъективный, либо 0.

ПРИМЕР

(1) [$M_n(K)$ – алгебра кв. матриц над полем является простой]

Пусть $I \triangleleft M_n(K)$ (I – двуст. идеал), K – поле.

Докажем, что если $I \neq 0$, то $I = M_n(K)$.

Пусть $A \in I$, $A \neq \begin{pmatrix} 0 & & 0 \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$, т.е. $A = (a_{ij})$ и $\exists$ k, l, т.ч. $a_{kl} \neq 0$.

$E_{ij} \cdot E_{kl} = \begin{cases} E_{il}, & j = k \\ 0, & j \neq k \end{cases}$

$A = \sum a_{ij} E_{ij}$ (матр. единицы)

$E_{ik} A E_{lj} = a_{kl} E_{ij} \in I$ — Т.к. K – поле, то $a_{kl}^{-1} a_{kl} E_{ij} \in I \Rightarrow E_{ij} \in I \Rightarrow$ $\Rightarrow$ все матрицы лежат в $I \Rightarrow I = M_n(K)$.

$E_{ik} E_{i'j'} E_{lj} = E_{ij}$, если $i' = k$, $j' = l$

Тело.

Кольцо (алгебру, но не коли) с $1 \neq 0$, в котором всякий ненулевой элемент обратим = поле без усл. коммутативности

Т [Если левый или правый идеал содержит обратимый элемент, то он (идеал) равен всему кольцу]

I - левый идеал в R, $a \in I$, a - обр.

$\exists a^{-1}: a^{-1}a = 1 \in I \Rightarrow \forall b \in R: b \cdot 1 = b \in I$

$\Rightarrow I = R$ ■

Следств [Если R - тело, то оно не содержит нетривиальных односторонних идеалов.]

[Пусть R - кольцо с 1, которое не содержит нетрив. (левых) идеалов $\overset{?}{\Longrightarrow}$ R - тело.]

$a \in R$, $a \neq 0$.

Ra - левый идеал $\neq 0 \Rightarrow Ra = R \Rightarrow$

$\Rightarrow \exists b: ba = 1$ (Всякий ненулевой эл-т имеет левый обратный) $\Rightarrow$

$\Rightarrow \exists c: cb = 1 \Rightarrow b$ имеет и левый, и правый обратный

$cba = \begin{cases} a \\ c \end{cases} \Rightarrow a = c \Rightarrow b$ имеет обратный, равный a. $\Rightarrow$

$\Rightarrow R$ - тело. ■

Если R - алгебра над K, то вместо термина тело, то R - алгебра с делением над K

[Центр тела является полем.]

R - тело, $a \in Z(R)$

$a \neq 0$, $\exists a^{-1}$ в $R \Rightarrow a^{-1} \in Z(R)$

$\forall z \in R$ $az = za$. Умн-ем на a^{-1} с обеих сторон

$\Rightarrow za^{-1} = a^{-1}z \Rightarrow a^{-1} \in Z(R) \Rightarrow Z(R)$ - поле. ■

R - кольцо с 1_R

$K \subset R$ - подполе $1_R \in K$.

Превратим R в вект. пр-во над K:

$\lambda \in K$. Определим

2 мя способами ввели умноже. на скаляры

$\lambda \cdot_1 a = \lambda a$

$\lambda \cdot_2 a = a\lambda$

вект. пр-во над K

Т.к. $a \notin Z(R)$, то это могут быть разные способы

$K \subset L \subset R$ (алг. над K; самое подполе), K, L - поля.

$1_R \in K \subset L$.

Одним из двух способов делаем R - векторным пр-вом.

Имеет смысл говорить о $\dim$.

УТВ [$\dim_K R = \dim_L R \cdot \dim_K L$]

Если одна из $\dim = \infty$, то все $\dim = \infty$ и р-во верно.

$\dim_K R = \underset{m}{\dim_L R} \cdot \underset{n}{\dim_K L}$

Выбираем базисы:

$R = \langle \underset{\text{базис}}{x_1, \dots, x_m} \rangle_L$

$L = \langle \underset{\text{базис}}{y_1, \dots, y_n} \rangle_K$.

Рассм. всевозм. произведения

$\{y_i x_j\}$! базис из $m \cdot n$ эл-тов R над K $\quad i = 1, \dots, n$, $j = 1, \dots, m$.

① $\forall r$ выражается?

$r = \sum_{j=1}^{m} b_j x_j$, $b_j \in L$ $\quad b_j = \sum_{i=1}^{n} a_{ji} y_i$

Подставляем b_j в r:

$\forall r: r \in \langle y_i x_j \rangle$.

② Эл-ты из $\{y_i x_j\}$ - ЛНЗ над K?

$\sum a_{ij} y_i x_j = 0$

$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} y_i \right) x_j = 0 \Rightarrow \sum_{i=1}^{n} a_{ij} y_i = 0 \quad \forall j \Rightarrow$

$\Rightarrow \forall a_{ij} = 0 \Rightarrow$ ЛНЗ. ■

0.2015 Есть вект. пр-во. Хотим превр. его в алгебру.

Достаточно задать умн. на базисных эл-тах.

R, K - поле.

$\dim_K R < \infty$

$R = \langle \underset{\text{базис}}{e_1 \dots e_n} \rangle$

$e_i e_j = \sum_{k=1}^{n} c_{ij}^k e_k$

$a = \sum_{i=1}^{n} a_i e_i$

$b = \sum_{j=1}^{n} b_j e_j$

$ab = \sum_{i,j} (a_i e_i)(b_j e_j) \overset{\text{чтобы получить алгебру}}{=} \sum_{i,j} a_i b_j e_i e_j \overset{\text{подставл. } e_i e_j}{=}$

Это умн будет дистриб. и удовл. З-ну ассоц алгебры умножению на скаляр.

Если хотим, чтобы R - была алг. с 1, то e_1 - единица.

Нетривиальна ассоциативность умножения

c_{ij}^k — структурные константы.

Ассоц. достаточно проверять только для базисных в-ров (т.е. $\Rightarrow$ для структ. констант)

2 важных примера

① Групповая алгебра конечной группы.

$|G| = n$ - группа. $\quad K$ - поле.

Рассм. мн-во формальных записей $\{\sum_{i=1}^{n} a_i g_i\}$, $a_i \in K$

$G = \{g_1, \dots, g_n\}$ — получим вект. пр-во над K.

Базисные эл-ты умн. так, как они умножаются в группе G.

Ассоц. выполнено т.к. G - группа $\Rightarrow$ имеем ассоц. R - алгебру называемую.

$KG = \{\sum_{i=1}^{n} a_i g_i\} \quad a_i \in K$

② Алгебра кватернионов

Введем над $\mathbb{R}^4$, и потом посмотрим, что будет для других полей.

базис

$H = \{1, i, j, k\}$ $\quad ij = k$, $jk = i$

Умн. по тому же правилу, что в Q_8.

Ассоц. проверяется автоматически.

$x \in H = a + bi + cj + dk$. $\quad a, b, c, d \in \mathbb{R}$.

кватернион

Также как в случае компл. чисел рассмотрим операцию сопряжения:

$\bar{x} = a - bi - cj - dk$

$\overline{xy} = \bar{y}\bar{x}$ (алгебра не коммут.)

Дост. проверить для базисных элементов (перебор)

$\bar{x}x = x\bar{x} = a^2 + b^2 + c^2 + d^2$

Т.к. R^{4} - алг. с 1, то $a \cdot 1 = a$

Значит всякий $x \in H \neq 0$: $\frac{\bar{x}}{a^2+b^2+c^2+d^2} = \frac{\bar{x}}{x\bar{x}}$ является обратным для x. $\frac{\bar{x}}{x\bar{x}} = x^{-1}$

Т.о. алгебра кватернионов — некоммутативная алгебра с делением.

В качестве K также можно брать такие поля, в которых $\forall\, a^2 + \ldots + d^2 \neq 0 \in K$.

Над $\mathbb{C}$ такой конструкции не получится (будут делители нуля)

Т [Всякая конечномерная ассоциативная алгебра без делителей нуля является алгеброй с делением]

R, K

$\dim_K R < \infty$.

Возьмем $a \neq 0, a \in R$ и рассм. $\varphi: R \to R$, т.ч.

$\varphi(x) = a \cdot x$. — линейный оператор на R (из св-в алгебры это видно)

Т.к. R - без делителей 0 (т.е. a - не делитель 0) $\Rightarrow$

$\Rightarrow \operatorname{Ker}\varphi = \{0\}$. $\Rightarrow \varphi$ - инъективное

А т.к. R - конечномерно, A - невыр $\Rightarrow \varphi$ - сюръект.

$\Rightarrow \exists\, e_1 \in R$, т.ч. $a \cdot e_1 = a$.

Умножим справа на $\forall b$ (польз. ассоциат.):

$a(e_1 b) = ab \Rightarrow$ т.к. a - не делитель 0 можем на a сократить $\Rightarrow$

$e_1 b = b \Rightarrow e_1$ - левая единица.

Аналогично: $\exists\, e_2$ - правая единица

Если в кольце $\exists\, e_1, e_2$, то $e_1 = e_1 e_2 = e_2 \Rightarrow$

$\Rightarrow e_1 = e_2 = e$ - единица $\Rightarrow R$ - алгебра с 1 $\Rightarrow$

из-за сюръект φ: $\exists\, c$, т.ч. $ac = e \Rightarrow c$ - правый обр. для a.

Аналогично, a имеет левый обратный.

$ac=e$; $ba=e$

$b=bac=c \Rightarrow b=c=a^{-1} \Rightarrow$ каждый ненул. эл-т имеет обратный $\Rightarrow R$ - алгебра с делением. ■

Главные идеалы в комм. кольце.

R - коммут. кольцо.

$I = \underbrace{Ra}_{\text{главный идеал}} - aR$ - идеал (двуст)

Когда $Ra = Rb$?

Это $\Leftrightarrow a|b$ и $b|a$.

Если R - обл. целостности $\Rightarrow a$ и b ассоциированы (отличаются обратимым множителем).

Кольцо главных идеалов - это комм. кольцо с 1 в котором всякий идеал главный.

ПРИМЕРЫ

① $\mathbb{Z}$

Все подгруппы в $\mathbb{Z}$ имеют вид $n\mathbb{Z}$ $n \in \mathbb{N} \cup \{0\}$

Все они являются глав. идеалами.

② $K[x]$ K-поле

Покажем, что всякий идеал главный. $I \subseteq K[x]$

$I \neq 0$ (иначе очевидно),

Выбираем в I: $f \neq 0$, т.ч. $\min \deg f$, $f \in I$.

Утверждаем, что $I = fK[x]$

Т.к. $f \in I \Rightarrow fK[x] \subseteq I$.

Возьмем $\forall g \in I$ и поделим с остатком g на f.

$g = fq + r$ $\deg r < \deg f$

$r = g - fq \in I$.

Т.к. выбрали f мин. степени $\Rightarrow r = 0 \Rightarrow$

$\Rightarrow I \subseteq fK[x]$ $\Rightarrow I = fK[x]$

$fK[x] = (f)$ - гл. идеал, порожденный элементом f.

$(f) = (g) \Rightarrow f$ и g отличаются постоянным мн-лем.

Рассмотрим фактор кольца $\mathbb{Z}$ и $K[x]$ по какому-либо идеалу I.

$\mathbb{Z}/n\mathbb{Z}$ — фактор-кольцо здесь — кольцо классов вычетов по модулю n

$K[x]/fK[x]$ — кольцо классов многочленов f по идеалу $fK[x]$

мн-во элем.

$K[x]/fK[x] = \{g + fK[x]\} = [g]$

Пусть $f \neq 0$ и $\deg f = n$

В каждом кл. классе ! образом в качестве представителя можем выбрать остаток от деления g на f.

Можем с самого начала считать, что

$\deg g < n$.

$[g] = a_0 + a_1[x] + \ldots + a_{n-1}[x]^{n-1}$ $[x^{n-1}]$

$g = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$

Это фактор-кольцо вычетов явл. алгеброй над K

Каждый эл-т из $K[x]/fK[x]$ единств образом представляется в виде, то

$1 = [1], [x], \ldots, [x]^{n-1}$ — базис в $K[x]/(f)$

Причем отсюда: $\dim_K K[x]/(f) = \deg f$.

Если $f \neq 0$, то $K[x]/(f)$ — конечномерная алгебра.

Когда оно является полем?

$\mathbb{Z}/n\mathbb{Z}$ - поле $\Leftrightarrow$ n-простое

$K[x]/(f)$ - поле $\Leftrightarrow$ f-неприводимый

Если f-приводим, $f = gh$, то $\underset{\neq 0}{[g]}\underset{\neq 0}{[h]} = [f] = 0$

[Заметим, обратное, т.е. если f-неприводим, то в $K[x]/(f)$ нет делителей нуля.]

Пусть $[g][h] = 0 \Rightarrow f \mid gh$. Т.к. f-неприводим, то $f \mid g$ или $f \mid h \Rightarrow [g] = 0$, или $[h] = 0$.

(С1) [в конечномерной алгебре без делителей нуля $\forall$ обратимый элемент обратим (т.е. это поле)]

Прямая сумма колец.

(Для алгебр то же самое)

R - кольцо

$R_1, \ldots, R_s \subset R$ — подкольца

Внутренняя прямая сумма:

R — (внутр) прямая сумма $R_1, \ldots, R_s$, если:

1) $R = R_1 \oplus \ldots \oplus R_s$ как групп по сложению

2) R_i — идеалы (двуст.) $\forall r \in R$ $r = r_1 + \ldots + r_s$ единственно, $r_i \in R_i$

$r_i \in R_i$, $r_j \in R_j$ $i \neq j$

$r_i r_j \in R_j \cap R_i = \{0\}$ — произв. элементов из разных слагаемых равно нулю.

$t \in R$: $t = t_1 + \ldots + t_s$ $t_s \in R_s$.

$rt = r_1 t_1 + \ldots + r_s t_s$ ← произведения любых 2-х эл-тов представляется в виде.

В частности, можем разложить 1.

$1 = e_1 + \ldots + e_s$ $e_i \in R_i$.

Умножим на e_i:

$\underset{\in R_i}{e_i} = e_i \cancel{e_1}^{0} + \ldots + e_i e_i + \ldots + e_i \cancel{e_s}^{0} \Rightarrow e_i^2 = e_i$ идемпотенты (опред)

$\Rightarrow e_i e_j = 0$ при $i \neq j$

Покажем, что $e_i \in Z(R)$.

$r \in R$.

$r = re_1 + \dots + re_i + \dots + re_s$ (слева) $\quad re_i \in R_i$ ← т.к. идеал

$r = e_1 r + \dots + e_i r + \dots + e_s r$ (справа) $\quad e_i r \in R_i$

А т.к. разложение однозначно, то имеем:

2) $re_i = e_i r \Rightarrow e_i \in Z(G)$.

e_i — центральные попарно-ортогональные идемпотенты, сумма которых равна 1.

Задача: Если в кольце задана система ..., то она задает разложение кольца R в прямую сумму идеалов

Каждое e_i — единица в соотв. слагаемом R_i.

$r \in R_i \quad r = re_1 + \dots + re_i + \dots + re_s$

Из ! разложения все слагаемые, кроме i равны нулю.

$re_i = r$. Аналогично $e_i r = r$.

Отсюда $R_i = Re_i = e_i R$

эти главные левый и правый идеалы с порождающим элементом e_i

Внешняя прямая сумма

$R_1, \dots, R_s$ — кольца, то R — внешн. пр. сумма $R_1, \dots, R_s$, если

1) внешн. пр. сумма как групп по сложению (абелев. групп)

2) умножение вводим покомпонентно → получаем кольцо

[Всякая внутр. прямая сумма изоморфна внешней прямой сумме, (и т.д. как в теореме для групп)]

ПРИМЕР

$R = K[x]/(f) \quad f \neq 0$.

$f = f_1 \cdots f_s \quad (f_i, f_j) = 1 \quad i \neq j$

(Т) $\left[K[x]/(f) \cong \bigoplus_{i=1}^{s} K[x]/(f_i) \right]$

Строим гомоморфизм φ: $\varphi(g) := (g + f_1, \dots, g + f_s)$

$K[x] \xrightarrow{\varphi} \bigoplus_{i=1}^{s} K[x]/(f_i)$

Найдем его ядро:

$\operatorname{Ker}\varphi = \{ g \mid g \in (f_i) \ \forall i \}$ все компоненты должны быть нулевые

Т.к. $(f_i, f_j) = 1$ $\quad f_i \mid g \Leftrightarrow f \mid g \Leftrightarrow g \in (f)$.

Итого, $\operatorname{Ker}\varphi = (f)$ — идеал, порожденный f $\Rightarrow$ по теор о гом-ме для колец: $\operatorname{Im}\varphi \cong K[x]/(f) \Rightarrow$

$\Rightarrow \dim_K (\operatorname{Im}\varphi) = \deg f$.

Разм. прямой суммы — сумма размерностей слагаемых

$\dim \bigoplus_{i=1}^{s} K[x]/(f_i) = \sum_{i=1}^{s} \dim K[x]/(f_i) = \sum_{i=1}^{s} \deg f_i = \deg f$.

$\Rightarrow \operatorname{Im}\varphi = \bigoplus_{i=1}^{s} K[x]/(f_i)$ ■

$f = p_1^{k_1} \cdots p_t^{k_t}$ $\quad p_i$ — различные неприводимые

$R = K[x]/(f) \cong \bigoplus_{i=1}^{t} K[x]/(p_i^{k_i})$.

(Т) [Фактор кольцо по степени неприводимого многочлена не раскладывается в прямую сумму]

Какие $\exists\ \overset{\text{идеал}}{I} \subseteq K[x]/(f)$? $\Leftrightarrow$ (мор ранее) $I \subseteq K[x]$; $I \ni f \Leftrightarrow I \ni (f)$)

Пусть $(f) \subseteq (g) \Leftrightarrow g \mid f$

Идеалы, содержащие f нах-ся в биективном соответствии с делителями f с точностью до ассоциированности. (утв. на конст.)

$\Rightarrow$ тоже самое верно для фактор-кольца $K[x]/(f)$

$f = p^k$, p-неприводимый

$g \mid f$. $g = p^l$ $0 \le l \le k$. $\Rightarrow$ такие идеалы вложены друг в друга $\Rightarrow$ $(g) \subseteq (f)$

$\Rightarrow$ верно для идеалов в фактор-кольце $\Rightarrow$ не расш. в прямую сумму. ■

Теорема об остатках

Пусть $f_1, \dots, f_s \in K[x]$; $(f_i, f_j) = 1$ $i \ne j$.

$g_1, \dots, g_s \in K[x]$. (можем считать, что это соотв. остатки, но это несущественно)

Тогда $\exists\ g \in K[x]$, т.ч. $g \equiv g_i \pmod{f_i}$ $i = 1, \dots, s$

Т.к. $(f_i, f_j) = 1$, имеем изоморф. гомоморфизм

$\varphi: K[x] \xrightarrow{\varphi} \bigoplus K[x]/(f_i)$. (как в примере)

Возьмем $(g_1 + (f_1), \dots, g_s + (f_s)) \in \bigoplus K[x]/(f_i)$ $\Rightarrow$

$\Rightarrow \exists g$, т.ч. $\varphi(g) = \Leftrightarrow g \equiv g_i \pmod{f_i}$ $\forall i$ ■

R-алгебра с 1 над K

$a \in R$ $K[x] \xrightarrow{\varphi} R$

$\varphi(1) = 1$, $\varphi(x) = a$

$\operatorname{Im}\varphi = K[a]$

$\operatorname{Im}\varphi \cong K[x]/\operatorname{Ker}\varphi$

$f(x) \in K[x]$

$f(x) = a_0 + a_1 x + \dots + a_n x^n$

$\varphi(f(x)) = a_0 + a_1 a + \dots + a_n a^n$ $a \in K$

при замене обр. алгебры является алгеброй.

1) $\operatorname{Ker}\varphi = \{0\}$

$\operatorname{Im}\varphi \cong K[x]$

$p_a(x) = 0$ — мин. мн-н равен нулю (единств. ан. мн-н нулевой)

2) $\operatorname{Ker}\varphi \ne \{0\}$

$\operatorname{Ker}\varphi$ — идеал в $K[x]$

$\operatorname{Ker}\varphi = \{f : f(a) = 0\}$ аннулирующий

$\operatorname{Ker}\varphi = (p(x))$ $p(x) \ne 0$ — минимальный

Если ст. коэф. $= 1$, то $p_a(x)$ — минимальный со ст. коэф. 1.

$\dim_K K[a] = \deg p_a(x)$

$K[a] \cong K[x]/(p_a(x))$

Терминология:

Если $\operatorname{Ker}\varphi = \{0\}$, то a — трансцендентный элемент над K

Если a имеет ненул. аннул. мн-н, то a — алгебраический над K

(Т) [В конечномерной алгебре все эл-ты алгебраические]

Если R-ал. над K, $a \in R$ — транс. $\Rightarrow R \supseteq K[a] \cong K[x] \Rightarrow \dim K[a] = \infty \Rightarrow$ и вся алгебра бесконечномерная ■

Подалгебра $K[a]$ наз-ся подалгеброй, порожденной элементом a, т.к. $K[a]$ - наим. подал., содержащая 1 и элемент a.

Подалгебра такого вида наз-ся однопорожденными (многочленами).

Пусть имеются два элемента $a, b \in R_2$ (ам. с 1. над K) $\in R_1$ $K[a]$, $K[b]$

Когда $\exists$ изоморфизм алгебр $\psi: K[a] \to K[b]$, т.ч. $\psi(1)=1 \Leftrightarrow \psi(\lambda)=\lambda \ \forall \lambda \in K$; $\psi(a)=b$?

(T) [Он существует $\Leftrightarrow$ когда a и b имеют одинаковые многочлены, т.е. $p_a(x)=p_b(x)$]

($\Rightarrow$) Подалгебры отождествимы с помощью гомоморфизма $\Rightarrow p_a(x)=p_b(x)$

($\Leftarrow$) Пусть $p_a(x)=p_b(x)=p(x)$

$$\begin{tikzcd} & K[x] \arrow[dl, "\varphi_a"'] \arrow[dr, "\varphi_b"] & \\ K[a] \arrow[d, "\overline{\varphi_a}"', "\cong"] & & K[b] \arrow[d, "\overline{\varphi_b}", "\cong"'] \\ K[x]/p_a(x) \arrow[rr, "\text{т.к. } p_a(x)=p_b(x)=p(x)"'] & & K[x]/p_b(x) \end{tikzcd}$$

см. классы

$\overline{\varphi_a}(x+p(x))=a$

$\overline{\varphi_b}(x+p(x))=b$

$\Downarrow$

Рассмотрим композицию $\Rightarrow$

$K[a]=K[b]$ ■

Когда $K[a]$ является полем?

(T) [$K[a]$ - поле $\Leftrightarrow$ если a - алгебраический над K и минимальный многочлен $p_a(x)$ неприводим]

($\Rightarrow$) Если a - транц. над K $\Rightarrow K[a] \cong K[x]$ - не поле

($\Leftarrow$) Если вып., что a - алгебраич., $p_a(x)$ - неприводим $\Rightarrow K[a] \cong K[x]/p_a(x)$ - поле (теорема ранее) ■

Применим это к частному случаю:

(T) [Если R - алгебра с делением над K, то $\forall$ алгебраического элемента a минимальный многочлен неприводим $\longrightarrow K[a]$ - поле.]

Докажем, что в случае алгебры с делением $p_a(x)$ неприводим.

Пусть $p_a(x)=g(x)h(x)$

$0=p_a(a)=g(a)h(a)$. Т.к. R - алгебра с делением $\Rightarrow$ в ней нет делителей нуля $\Rightarrow g(a)=0$, или $h(a)=0$.

$\Rightarrow$ либо g, либо h - аннулирующие $\Rightarrow p_a|g$ или $p_a|h$

$\Rightarrow$ неприводим.

Конечномерные алгебры с делением над полями $\mathbb{C}$ и $\mathbb{R}$.

D - алгебра с делением над $\mathbb{C}$

$\dim_{\mathbb{C}} D < \infty$. (T) [Всякая конечномерн. D над $\mathbb{C}$ совпадает с полем комплексных чисел $\mathbb{C}$]

$\forall a \in D$ – алгебраический над $\mathbb{C}$, т.к. $\dim < \infty$.

$p_a(x)$ – неприводим $\Rightarrow p_a(x) = x - z \quad z \in \mathbb{C}$

$0 = p_a(a) = a - z \Rightarrow a = z \in \mathbb{C}$

Т.е. $\forall a \in D \to \in \mathbb{C} \Rightarrow D = \mathbb{C}$ ■

D – конечн. алгебра с делением над $\mathbb{R}$

Знаем уже 3 алгебры: $\mathbb{R}, \mathbb{C}, \mathbb{H}$ (кватернионы)

Теорема Фробениуса [Всякая D над $\mathbb{R}$ либо совпадает с $\mathbb{R}$, либо $\cong \mathbb{C}$, либо $\cong \mathbb{H}$.]

$\forall a \in D \setminus \mathbb{R}$ – алгебр над $\mathbb{R}$ (считаем, что $D \neq \mathbb{R}$ по тоже 3)

$p_a(x)$ – неприводим.

1) либо $\deg p_a(x) = 1 \Rightarrow$ аналогично $0 = p(a) = a - z$
$\Rightarrow a = z \in \mathbb{R}$.

Но мы взяли $a \notin \mathbb{R}$.

2) $\deg p_a(x) = 2$ и он имеет отриц. дискриминант

Тогда он имеет z – корень $p_a(x)$ в $\mathbb{C} (\setminus \mathbb{R})$.

$p_z(x) = p_a(x)$ (т.к. корни неприводимого $\Rightarrow$ совпадает с ним)

$a \in D,\ z \in \mathbb{C} \underset{\text{по теор.}}{\Longrightarrow} \mathbb{R}[a] \cong \mathbb{R}[z] \subseteq \mathbb{C}$ (двумерн. вект. пр-во над $\mathbb{R}$)

$\mathbb{R}[z] \to \mathbb{R}(z) = \mathbb{C}$

$\Rightarrow \mathbb{R}(a) \cong \mathbb{C}$

1) $\mathbb{R}(a) = D \to D \cong \mathbb{C}$.

2) В дальнейшем обозначаем $\mathbb{R}(a) = \mathbb{C}$.

$D \neq \mathbb{C}$.

Тогда $Z(D) = \mathbb{R}$.

Если бы $Z(D)$ был больше $\Rightarrow$ могли взять $a \in Z(D)$ и получили бы, что $\mathbb{C} \subset Z(D) \Rightarrow D$ было бы конечной алгеброй с делением над $\mathbb{C} \Rightarrow$ но в этом случае $D = \mathbb{C}$, а мы предполагаем, что $D \neq \mathbb{C}$.

$\mathbb{C} \subset D$ (по)

Превратим D в вект. пр-во над $\mathbb{C}$

$1_{\mathbb{C}} = 1_D \Rightarrow$ можно 2-мя способами ввести умн. $(\cdot)$ на скаляры $\lambda \in \mathbb{C}$:

$\lambda \in \mathbb{C},\ v \in D$: $\lambda \cdot v = v \lambda$

(умножение на скаляры; умн. в алгебре)

Рассмотрим лин. оператор φ над $\mathbb{R}$

$\varphi: D \to D$

$\varphi(v) = i \cdot v$ (в алгебре)

$\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$ в силу дистриб.

Покажем, что $\varphi(\lambda \cdot v) = \lambda \cdot \varphi(v)$:

$\varphi(\lambda \cdot v) = \varphi(v\lambda) = i(v\lambda) = (iv)\lambda = \varphi(v)\lambda =$

(ассоциат.)

$= \lambda \cdot \varphi(v)$. → линейный оператор

$\varphi^2(v) = i(iv) = i^2 v = -v$

$\varphi^2(v) + v = 0 \Leftrightarrow (\varphi^2 + id)v = 0 \Leftrightarrow$

$x^2 + 1$ – аннулирующий для φ

$x^2+1=(x-i)(x+i)$

$\lambda_1=i,\ \lambda_2=-i.$

Т.к. он не имеет кратных корней $\overset{\text{мин. алгебр}}{\Longrightarrow}$ φ — диагонализируем $\Rightarrow$ все пр-во разлагается в прямую сумму собст. подпр-в, относящихся к собственным значениям $i, -i$.

$D=D_i\oplus D_{-i}$

$D_i=\{v\in D \mid iv=vi=i\cdot v\}$

$D_{-i}=\{v\in D \mid iv=-vi\}$ антикомут. с i.

Мн-во элементов, коммутирующих с i = мн-во векторов, комм. с любым комплексным числом

$\{v: \lambda v=v\lambda\ \forall\lambda\in\mathbb{C}\}\Rightarrow D_i$ — подалгебра (состоящая для с делением)

Если элемент коммутирует, то и обратный коммутирует

$\mathbb{C}\subseteq D_i \quad \mathbb{C}\in Z(D_i)$

$\Rightarrow D_i=\mathbb{C}$ по доказанному ранее

$\Rightarrow D_{-i}\neq\{0\}$, иначе бы $D=\mathbb{C}$. (мы предпол. $D\neq\mathbb{C}$).

Возьмем $b\in D_{-i}$ $b\neq 0$.

Рассмотрим D — вект. пр-во над $\mathbb{C}$ и введем линейный оператор $\psi(v)=bv$ (аналогично φ).

Покажем, что $\psi(D_{-i})\subseteq D_i$.

Возьмем $c\in D_{-i}$, $\psi(c)=bc$

$(bc)i=b(ci)=b(-ic)=-(bi)c=-(-ib)c=ibc$

$\Rightarrow bc\in D_i$.

Но ψ — инъективный, т.к. b — не делитель нуля.

$\psi(D_{-i})\subseteq D_i \Longrightarrow$ (инъектив подпр-во)

$\dim_{\mathbb{C}}D_i=1\Rightarrow\dim_{\mathbb{C}}D_{-i}=\dim_{\mathbb{C}}(\psi(D_{-i}))=1$

Значит $\dim_{\mathbb{C}}D=2$.

Базис $D_i=\langle 1\rangle_{\mathbb{C}}$; базис $D_{-i}=\langle b\rangle_{\mathbb{C}}\Rightarrow$ по ф-ле для размерности башни:

$\dim_{\mathbb{R}}D=\dim_{\mathbb{C}}D\cdot\dim_{\mathbb{R}}\mathbb{C}=4.$

$b^2\in D_i=\mathbb{C}$.

b^2 коммут. с любым $\lambda\in\mathbb{C}$ и сам с собой. $\lambda_1,\lambda_2\in\mathbb{C}$

Но $\forall\ v\in D$ имеет вид $v=\lambda_1+\lambda_2\cdot b=\lambda_1+b\lambda_2\Rightarrow$ b^2 ком. с каждым слагаемым $\Rightarrow$ с $\forall\ v\in D\Rightarrow$ $b^2\subset Z(D)=\mathbb{R}$

Пусть $b^2=\alpha\in\mathbb{R}\Rightarrow x^2-\alpha$ — аннулирующий мн-н для b.

Покажем отрицательность α:

Если бы $\alpha\geq 0\Rightarrow x^2-\alpha$ — приводим над $\mathbb{R}\Rightarrow$ но мин. должен быть неприв. $\Rightarrow$ он бы был 1-й степени $\Rightarrow \deg p_b(x)=1\Rightarrow b\in\mathbb{R}$, но $b\notin\mathbb{R}$.

Значит $\alpha<0$.

Обозначим через $j=\frac{b}{\sqrt{-\alpha}}\Rightarrow j^2=-1$

Базис $D = \langle 1, j \rangle_{\mathbb{C}}$
Базис $\mathbb{C} = \langle 1, i \rangle_{\mathbb{R}}$ $\Big\}$ $\Rightarrow$ базис D над $\mathbb{R}$ это: $\langle 1, i, j, ij \rangle_{\mathbb{R}}$

Обозначим $k = ij$.

Проверим, что умн. базисных эл-тов в $\langle 1, i, j, k \rangle_{\mathbb{R}}$ такое же как в алгебре $\mathbb{H}$:

$ji = -ij = -k$.

$k^2 = (ij)(ij) = i(-ij)j = -(i^2)(j^2) = -1$.

Значит $D \cong \mathbb{H}$. ■

Расширение полей.

$K \subseteq L$ ← L-расширение поля K. K, L - поля. L - алгебра над K

Если однопорождённая алгебра $K[a]$ является полем (когда a - алгебр, $p_a(x)$ - неприводим), то обозначают $K(a)$.

Если a - трансцендентный, то $K(a)$ - поле частных области $K[a]$ — поле рациональных дробей над K от a.

Если L - расширение полей, то

$\dim_K L = (L:K)$ — степень L над K.

Если F - башня подполей $K \subseteq L \subseteq F$, то ф-ла для разм. башни: $(F:K) = (L:K)(F:L)$

Элемент из L - алгебраический над K, если он является корнем ненулевого многочлена над K.

В противном случае — трансцендентный.

$a \in L$ - алгебраический над K

$K[a] = K(a)$

При этом $(K(a):K) < \infty$ ($\deg p_a(x)$)

$K \subseteq K(a) = K[a] \cong K[x]/(p_a(x))$ — простое алгебраическое расширение

$K \subseteq K_1 \subseteq L$

Если $a \in L$ - алгебр над K, то он и алгебр. над K_1.

Пусть $a_1, \dots, a_s \in L$.

$K \subseteq K(a_1) \subset K(a_1)(a_2) \subset \dots \subset K(a_1)(a_2)(a_s) \subset L$

На каждом „этаже" a_i - алгебраические над $K(a_1)\dots(a_{i-1})$ добавляем алгебраический элемент.

$(K(a_1)\dots(a_s):K) < \infty$ — т.к. конечно для всех „нижних этажей".

Расширение наз-ся алгебраическим, если все элементы из L являются алгебраическими над K.

(Т) [Всякое расширение конечной степени является ~~конечномерным~~ (алгебраическим)] ← лемма

$a_0 = 1$, $a_1, \dots, a_s \in L$

$K \subseteq K(a_1) \subseteq K(a_1)(a_2) \subseteq \dots \subseteq K(a_1)\cdot(a_s) \subseteq L$

$K(a_1)\cdot(a_i) \supseteq K(a_1)(a_{i+1})$

$\forall a_i = 1, \dots, s$ — алгебраическое над пред. расширением

$\Rightarrow K(a_1)\cdot(a_s) \supseteq K$ алгебраическое конечной степени

Т [Пусть $K \subset L$ — расширение полей. Тогда мн-во всех алгебраич. элементов над K из L образует подполе в L]

$a_1, a_2 \in L$ алгебр. $\overset{Т}{\Longrightarrow}$ 1) $a_1 a_2$, $a_1 + a_2$ — алгебр над K
2) a^{-1} — алг. над K

2) $K(a) \supseteq K$ алг. $\longrightarrow$ $a^{-1} \in K(a)$ a^{-1} — алгебр.

1) $a_1 a_2 \in K(a_1)(a_2) \supseteq K$ по лемме алг. расширение $\Rightarrow$ любые элементы суммы и пр-ния алгебраические над K. ■

Т.е. образуется подполе, называемое алгебраическим замыканием K в L

Т [Пусть $K \subseteq L \subseteq F$ — башня расширений, L — алг. над K, F — алг. над L. Тогда F — алгебраическое над K]

Возьмем $\forall a \in F$ — алгебр. $\Rightarrow \exists f(x) = a_0 + a_1 x + \dots + a_n x^n$, $a_i \in L$ и $f(a) = 0$

Но по условию, $a_0, \dots, a_n$ — алгебраические над K

$\Rightarrow K \subset K(a_0) \subseteq K(a_0)(a_1) \subseteq \dots \subseteq \underbrace{K(a_0)\cdot(a_n)}(a)$.

а явл. алгебр. над этим подполем

Находимся в условиях леммы

$\Rightarrow$ Все расширение $K(a_0)\cdot(a_n)$ — алг. над K $\Rightarrow$

$\Rightarrow a$ — алгебраический над K. ■

Т [$K \subset L$ — расширение полей, $\overline{K}$ — алгебраическое замыкание K в L, т.е. имеем $K \subseteq \overline{K} \subseteq L$. $\overline{K}$ — алг. замыкание $\overline{K}$ в L. Тогда $\overline{\overline{K}} = \overline{K}$]

В силу пред. теор. $\forall$ элем. алг. над $\overline{K}$ является алгебраич. над K $\Rightarrow$ лежит в $\overline{K}$. ■

ПРИМЕР

$\mathbb{Q} \subset \mathbb{C}$. Комп. числа, алгебр. над $\mathbb{Q}$ наз-ся алгебраическими числами. Иначе — трансцендентные.

e, π — трансцендентные

$e + \pi$ — ? неизвестно

Мн-во всех алг. чисел является подполем в $\mathbb{C}$, называемое полем всех алгебраических чисел. Оно алгебраически замкнуто в $\mathbb{C}$.

ЗАДАЧА: Оно алг. замкнуто (следует из того, что ....)

Т [Пусть K - поле, $f(x) \in K[x]$, тогда $\exists K \subset L$ - расширение полей, т.ч. $f(x) = \prod (x - c_i) \in L(x)$]

$K \subseteq L_1$

$f(x)$ имеет корень в L_1

$p(x) \in K[x]$ - делитель f.

$L_1 = K[x]/(p(x))$ поле, т.к. p - неприв. ; $L_1 \supseteq K$;

$[x] = \underset{\text{см. класс}}{x + (p(x))}$ является корнем.

$p([x]) = [p(x)] = 0 \Rightarrow p(x)$ имеет корень $\Rightarrow$

f - имеет корень.

Далее индукция по $\deg f$.

Если $\deg f = 1$, то док-ть нечего.

Пусть $\deg f = n \quad n > 1$.

По пред. утв. $\exists\ c_1 \in L_1$, т.ч. $f(x) = (x - c_1) g(x)$

$g(x) \in L_1[x]$.

$\deg g = n - 1 \Rightarrow$ для g доказано $\Rightarrow \exists$ расширение

$K \subseteq L_1$, т.ч. $g(x) = (x - x_2) \cdots (x - x_n)$ над L $\Rightarrow f$ разлагается на лин. мн-ли над L.

Характеристика поля.

$(K, +, \cdot)$ поле

$(K, +) \quad 1 \in K$.

1) $\underline{O(1) = \infty}$, тогда $\ldots, -1 \cdot 1, 0, 1, 2 \cdot 1, \ldots$ $= \langle 1 \rangle$ - все различны,

Характеристика поля $K = 0$ — ПРИМЕР: числовые поля

2) $\underline{O(1) = p < \infty}$ $\quad 0, 1, \ldots, (p-1) \cdot 1$ $= \langle 1 \rangle_p$ — только p различных

Характеристика поля $K = p$. — ПРИМЕР: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ поля вычетов по модулю

Т [Характеристика поля — простое число]

(первый семестр)

Поле наз-ся простым, если оно не содержит подполей, отличных от него самого.

ПРИМЕР:

1) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \langle 1 \rangle_p$ любое подполе содержит 1.

2) $\mathbb{Q} \supseteq F \supseteq \langle 1 \rangle_\infty$ приняли $\langle 1 \rangle_\infty$ подкольцо $\cong \mathbb{Z}$ $\Rightarrow F$ содержит все рац. числа.

Т [Всякое поле содержит единственное простое подполе, изоморфное $\mathbb{Q}$, если характ. $= 0$; и изоморфное $\mathbb{F}_p$, если характеристика $= p$.
($\Rightarrow$ других простых подполей, кроме $\mathbb{Q}$, и $\mathbb{F}_p$ $\nexists$).]

F - любое поле характ. 0.

Оно содержит подкольцо, изоморфное $\mathbb{Z}$.

Рассмотрим отображение $\varphi: \mathbb{Q} \to F$, т.ч.

$\varphi\left(\frac{m}{n}\right) = (m \cdot 1)\cdot(n \cdot 1)^{-1}$. (Не зависит от выбора записи раз. чисел $\Rightarrow$ φ - корректно определено)

Это ненулевой гомом-м $\Rightarrow$ он инъективен, т.е. $\mathbb{Q} \cong \operatorname{Im}\varphi \subseteq F$ подполе ▨

Если характеристика $F = p$

Тогда гом-м $\varphi: \mathbb{F}_p \to F$

$\varphi([k]) := k \cdot 1 \in F$ (Корректно, пользуемся тем, что характеристика p - простое)

класс вычетов по мод p

Гом-м, ненулевой $\Rightarrow$ его образ $\operatorname{Im}\varphi \cong \mathbb{F}_p$ ■

Конечные поля.

Пусть F - конечное поле

Т.к. $|F| = q < \infty \Rightarrow$ хар. $F = p$ - простое число $\Rightarrow$

$\Rightarrow \mathbb{F}_p \subseteq F$

Свойства конечных полей.

① [Порядок всякого конечного поля является степенью простого числа]

Т.к. $\mathbb{F}_p \subseteq F$ и $|F| < \infty \Rightarrow (F : \mathbb{F}_p) = n < \infty$.

Возьмем базис $e_1, \dots, e_n \Rightarrow \forall a \in F$ однозначно записывается в виде $a = a_1 e_1 + \dots + a_n e_n$ $a_i \in \mathbb{F}_p$

Каждое a_i может принимать p значений $\Rightarrow$ разных наборов получается $p^n = q$ ■

(далее $q = p^n$)

② [$x^q - x \in \mathbb{F}_p[x]$ разлагается в F на линейные множители: $x^q - x = \prod_{i=1}^{q} (x - c_i)$ ← все элементы поля F]

Рассм. мульт. группу $F^* = F \setminus \{0\}$

$|F^*| = q - 1$

$(F^*, \cdot) \Rightarrow \forall a \in F^*$ $a^{q-1} = 1 \Rightarrow a^q = a$ (но уже верно и для $a = 0$)

Т.е. все элементы поля являются корнями (их q штук) $\Rightarrow$

$\Rightarrow$ разлагается на линейные мн-ли ■

③ [Конечное поле характеристики p является простым алгебраическим расширением поля $\mathbb{F}_p$]

$\exists a \in F$, т.ч. $F = \mathbb{F}_p(a)$. Докажем это:

то есть..

Всякая конечная подгруппа в мульт. группе поля явл. циклической (доказывалось ранее) $\Rightarrow$

$\Rightarrow$ в частности F^* - цикл. группа по $\cdot$.

$F^* = \langle a \rangle_{q-1}$. Простое расш. $F(a)$ содержит все степени $a \Rightarrow$ содержит все эл-ты F^* и нулевой $\Rightarrow$ все эл-ты поля F. ■

Теорема $\exists!$ конечных полей.

Ⓣ [Для всякого $q = p^n$ $\exists!$ с точностью до изоморфизма поле порядка q.]

(∃) Рассмотрим $x^q - x \subseteq \mathbb{F}_p[x]$.

∃ расширение $F_p \subset L$, в котором мн-н разлагается на линейные мн-ли. Он не имеет кратных корней в L (т.к. если f имеет кратные корни, то он имеет общий корень с f' ⇒ не взаимно прост с f'. Но $(x^q - x)' = \underbrace{qx^{q-1}}_{0} - 1 = -1$, т.к. q делится на характеристику, не имеет общих корней с $x^q - x$.)

⇒ в поле L ∃ $c_1, \dots, c_q$ — все различные корни многочлена $x^q - x$.

Докажем, что это $\{c_1, \dots, c_q\}$ — поле.

$$\left[\begin{array}{l} \forall a, b \in F \text{ - поле хар-ки } p \text{ выполнено} \\ (a+b)^{p^k} = a^{p^k} + b^{p^k} \end{array}\right]$$

Для $k=1$:

$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$ При $i \neq 0$ и $i \neq p$ коэф-т делится на p → является нулем в нашем поле

$= a^p + b^p$.

Далее по индукции

$(a+b)^{p^k} = \left((a+b)^{p^{k-1}}\right)^p = \left(a^{p^{k-1}} + b^{p^{k-1}}\right)^p = a^{p^k} + b^{p^k}$ ■

c — корень $x^q - x \iff c^q = c$. ⟹

$$\left.\begin{array}{l} (c_i + c_j)^q = c_i^q + c_j^q = c_i + c_j \\ (c_i c_j)^q = c_i^q c_j^q = c_i c_j \\ (c_i^{-1})^q = (c_i^q)^{-1} = c_i^{-1} \end{array}\right\}$$ получили поле из q элементов

∃ ■

(!) Докажем, что любые 2 поля порядка q изоморфны между собой.

$|F_1| = q$; $|F_2| = q$ $\quad q = p^n$

$F_p \subseteq F_1$; $F_p \subseteq F_2$.

F_1 — простое расширение поля F_p ⟹ ∃ $a \in F_1$, т.ч.

$F_1 = F_p(a) \cong F_p[x] / (p_a(x))$ $\quad p_a(x) \in \mathbb{F}_p[x]$

$(F_1 : F_p) = n$ ⟹ $\deg p_a(x) = n$.

Но a — корень многочлена $x^q - x \in \mathbb{F}_p[x]$

⇒ $p_a(x)$ и $x^q - x$ имеют общий корень a ⇒ не взаимно просты ⟹ но $p_a(x)$ неприводим (нельзя представить 1 в виде лин. комб. с коэфиц.-многочленами)

⇒ $p_a(x) \mid x^q - x$ $\quad 1 \neq u(x) p_a(x) + v(x)(x^q - x)$ если подставить a

Над F_2 $x^q - x$ также разлагается на лин. мн-ли

⇒ всякий его неприв. множитель над $\mathbb{F}_p$ имеет корень в F_2 ⟹ $p_a(x)$ (тоже разлож. на лин. мн-ли) имеет корень в F_2

⇒ ∃ $b \in F_2$, т.ч. $p_a(b) = 0$.

$F_p \subseteq F_p(b) \subseteq F_2$

Т.к. $\deg p_a(x) = n$, то $|F_p(b)| = p^n = q$

$(F_p(b) : F_p) = \deg p_a(x) = n$ ⟹

⇒ $F_p(b) = F_2$ (число элементов совпад.) ⟹ $F_2 \cong F_p(x) / (p_a(x)) \cong F_1$. ■

Мн. эл-ов один лин. мн-н ⇒ однопор. или изоморфны изоморфн.

Теорема о конечных полях.

[Пусть F – конечное поле, $m \in \mathbb{N}$. Тогда в F $\exists$ неприв. многочлен степени m.]

$q^m = p^{nm}$ $\quad |F_q| = q$ ← единственное поле порядка q.

F_{q^m} – рассмотрим поле.

$x^{q^m} - x$ – разлагается на линейные мн-ли над F_{q^m}

$x^{q^m} - x = (x^{q^m-1} - 1)x$ делится на $x^q - x = (x^{q-1} - 1)x$

$\Rightarrow q-1$ делит $q^m - 1 \Rightarrow x^q - x$ также разлагается на линейные мн-ли над F_{q^m}. Но корни этого мн-на образуют подполе из q элементов (по теореме о $\exists$) $\Rightarrow$ изоморфное подполю F_q.

Поэтому можем считать, что $F_q \subseteq F_{q^m}$. Но F_{q^m} – простое расширение

$F_q(a) = F_{q^m}$, где a – порожд. мультипликат. группы.

$(F_{q^m} : F_q) = m$
чтобы число элементов совпадало

Пусть $p_a(x)$ – минимал. для a над F_q, поэтому

$(F_q(a) : F_q) = \deg p_a(x)$

Отсюда $\deg p_a(x) = m$. ■
производ.

Порождающие элементы в группе.

2310.2015

G – группа $\quad X \subseteq G$
подмнож.

Подгр., порожд. X — это наименьшая подгруппа, содержащая X.

$\langle X \rangle = \begin{cases} \text{содержит элементы из } X, \\ \text{обратные к ним,} \\ \text{всевозможные произв. элементов из } X \end{cases}$

$\langle X \rangle = \left\{ x_{i_1}^{\varepsilon_1} \cdots x_{i_t}^{\varepsilon_t} \mid x_{i_k} \in X,\ \varepsilon_k = \pm 1 \right\}$ – очевидно, что образуют подгруппу.
один и тот же элемент из X может повторяться

Подгруппа, порожденная одним элементом — циклическая подгруппа

X – система порождающих G, если $G = \langle X \rangle$, т.е. всякий $g \in G$ записывается в виде $g = x_{i_1}^{\varepsilon_1} \cdots x_{i_t}^{\varepsilon_t}$, $x_{i_k} \in X$, $\varepsilon_k = \pm 1$

(Она определена неоднозначно. Все эл-ты группы G – очевидно система порожд.)

ПРИМЕРЫ СИСТЕМ ПОРОЖДАЮЩИХ

S_n

1. Все циклы
2. Все транспозиции
3. Транспозиции вида $\langle \overbrace{(1,2), (2,3), \ldots, (n,n-1)}^{n-1 \text{ штука}} \rangle$
4. $S_n = \langle (1,2), (1, \ldots, n) \rangle$

A_n

1. Все тройные циклы $\langle \{i_1, i_2, i_3\} \rangle$

$GL(n,K)$

1. Мн-во всех элементарных матриц

D_n

1. $a,b \Rightarrow \{a^k b^\varepsilon \mid \varepsilon = 0,1\} \Rightarrow a,b$ – система порождающих

Q_8

1. $\langle i,j \rangle = Q_8$

Коммутаторы в группе.

ОПЕРАЦИЯ СОПРЯЖЕНИЯ

Пусть $g,h \in G$. Тогда элемент ghg^{-1} наз-ся сопряжен с h посредством g.

Фиксируем элемент $g \in G$, и $\forall h \in G$ положим

$\varphi_g(h) = ghg^{-1}$ $\quad \varphi_g: G \to G$

[Операция сопряжения является гомоморфизмом группы G на себя.]

$\varphi_g(h_1h_2) = g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = \varphi_g(h_1)\varphi_g(h_2)$

φ_g является изоморфизмом G на себя (автоморфизм группы G)

Подгруппа нормальна, если вместе с каждым эл-том она содержит его сопряженный (перефразир. в новых терминах)

Другими словами, подгруппа нормальна, если при $\forall$ операции сопряжения она отображается в себя.

Возьмем $a,b \in G$

Рассмотрим $\underbrace{aba^{-1}}b^{-1}$ (на сколько отличается aba^{-1} от b)

$aba^{-1}b^{-1} = [a;b]$ – коммутатор a и b

СВОЙСТВА КОММУТАТОРОВ

1. $[a;b] = e \Leftrightarrow aba^{-1} = b \Leftrightarrow ab = ba$.
2. [Сопряженный к коммутатору является коммутатором]
   $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$
3. [Пусть $f: G \to K$ – гомоморфизм. Тогда коммутатор переходит в коммутатор]
   $f([a,b]) = f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} =$
   $= [f(a); f(b)]$.
4. $[a,b]^{-1} = [b,a]$

Коммутант в группе.

Коммутантом гр. группы наз-ся подгруппа, порожденная коммутаторами. (мн-во всевозм. произв. коммутаторов)

$G \supseteq \underset{\text{мн-во}}{X}$

$H = \langle X \rangle$

Будет ли H нормальна?

Достаточно показать, что $\forall x \in X$ (лишь для порождающих), $g \in G$ элемент $gxg^{-1} \in \langle X \rangle$, т.к. сопряж. к обратному — есть обратный к сопряженному и сопр. произведения — есть произв. сопряженных: $gx^{-1}g^{-1} = (gxg^{-1})^{-1} \Rightarrow$ сопр. к любому пр-нию лежит в этой подгруппе.

Коммутант — нормальная подгруппа, т.к. сопряженный к коммутатору — снова коммутатор.

Высшие коммутанты.

$G' = [G,G]$ — обозначение коммутанта
(иногда называют производной подгруппой)

$G^{(k)}$ $\forall k \geq 0$: вводим индукт. способом.

1) $G^{(0)} = G$

2) Если $G^{(k-1)}$ определена, то $G^{(k)} = (G^{(k-1)})'$

$G^{(1)} = G'$

Свойство [При $\forall$ гомоморфизме групп $f: G \to L$, то $f(G^{(k)}) \subseteq L^{(k)}$ и если f — сюръективен, то $f(G^{(k)}) = L^{(k)}$]

По индукции. Для $k=1$ имеем:
$f(G') \subseteq L'$ (уже доказывали).
Если f — сюръективен, возьмем $\forall c,d \in L$.
$c = f(a)$, $d = f(b) \Rightarrow [c,d] = f[a,b]$.
Для каждого ком-ра имеет место это равенство $\Rightarrow$ $\forall$ произведений коммутаторов
$\Rightarrow f(G') = L'$.
Пусть для $k-1$ доказано.
Применяем такое же рассуждение к коммутанту G^{k-1}, т.к. $G^k = (G^{k-1})'$. ■

<u>Следствие</u> [Все высшие коммутанты являются нормальными подгруппами]

Применяя пред. гом. сопряжения $\Rightarrow$ при гомом. сопряжения k-й коммут переходит в k-й коммутант $\Rightarrow$ является нормальной подгруппой. ■

(Т) [Фактор-группа по коммутанту явл. абелевой. Коммутант является меньшей нормальной подгруппой, фактор по которой абелев; т.е. если $H \triangleleft G$ и G/H — абелева, то $G' \subseteq H$]

A — абелева (G/G' — абелева) $\Leftrightarrow A' = \{e\}$.

Рассм. $G \xrightarrow{\pi} G/G'$ (сюръективен) $\Rightarrow \pi(G') = (G/G')'$ ($\{e\}$)

Но это $\Rightarrow$ $\{e\} = (G/G')' \Rightarrow G/G'$ — абелева.

$\pi: G \to G/H$. $\pi(G') = (G/H)' = \{e\} \Rightarrow G' \in H$ ■

(по мно-ву эл-тов из H переходят в $\{e\}$ при канон. гомом. для фактор-гр. группы)

ПРИМЕРЫ

S_3

$A_3 \triangleleft S_3$ $\qquad S_3^{(k)} = \{e\} \ \forall k \geq 2$

S_3/A_3 — абелева. $\quad A_3$ - миним. подгр., по которой S_3/A_3 - абелева (т.к. более миним. подгр. только $\{e\}$).

$\Rightarrow$ тройной цикл в S_3 явл. коммутатором.

ЗАДАЧА: Как тройной цикл выражается в S_3 в качестве коммутатора.

S_n

Знаем, что все тройн. циклы явл. коммут $\Rightarrow (i_1 i_2 i_3) \in S_n'$

$\Rightarrow S_n' \supseteq A_n$ Но S_n/A_n — абелева $\Rightarrow A_n \supseteq S_n'$
порядка 2

Значит $S_n' = A_n \ \forall n \geq 3$

A_4

$V_4 \triangleleft A_4$ $\quad A_4/V_4$ — порядка 3 $\Rightarrow$ абелева, т.к. A_4 и V_4 - абелевы

$\Rightarrow A_4' \subseteq V_4$. Но меньшей неединичной подгр. в V_4 нет $\Rightarrow V_4$ наим. норм. подгруппа, фактор по которой абелев $\Rightarrow A_4' = V_4$

$V_4' = \{e\} \Rightarrow A_4^{(k)} = \{e\}$ при $k \geq 2$.

S_4

$$S_4 \supset \underset{S_4'}{\underset{\shortparallel}{A_4}} \supset \underset{S_4''}{\underset{\shortparallel}{V_4}} \supset \underset{S_4^{(k)}}{\underset{\shortparallel}{\{e\}}} \ \forall k \geq 3$$

D_n

$\langle a \rangle_n \subset D_n \quad D_n' \subseteq \langle a \rangle_n \quad D_n' = \langle a^d \rangle_{n/d} \quad d \mid n$

$D_n = \{a^k b^\varepsilon\}$. $\bar{a}, \bar{b}$ — образы в фактор-группе

$D_n/\langle a^d \rangle_{n/d} = \{\bar{a}^k \bar{b}^\varepsilon\} \cong D_d$

Когда D_d — абелева? $\Leftrightarrow d = 1$ или $d = 2$

Если n - нечетно, то $d = 2$ быть не может $\rightarrow$

$\underset{\text{для нечетных}}{D_n'} = \langle a \rangle$. $\underset{\text{для четных}}{D_n'} = \langle a^2 \rangle_{n/2}$

$D_n'' = \{e\}$. (т.к. D_n' - абелева). То есть

$$D_n \supset \underset{\substack{\langle a \rangle_n \\ n\text{-нечетно}}}{\underset{\shortparallel}{D_n'}} \supset \underset{D_n^{(k)}}{\underset{\shortparallel}{\{e\}}} \ \forall k \geq 2.$$

$\langle a^2 \rangle_{n/2}$ n-четно

Q_8

$\{\pm 1\} \triangleleft Q_8 \Rightarrow Q_8/\{\pm 1\} \cong V_4$ - абелева $\Rightarrow$

$$Q_8 \supset \underset{\langle \pm 1 \rangle}{\underset{\shortparallel}{Q_8'}} \supset \underset{Q_8^{(k)}}{\underset{\shortparallel}{\{e\}}} \ \forall k \geq 2.$$

ЗАДАЧА: При $n \geq 5$ всякий тройной цикл в A_n является коммутатором.

$$S_n \supset \underset{A_n}{\underset{\shortparallel}{S_n'}} = S_n^{(k)} \quad k \geq 1.$$

для $n \geq 5$, т.к. $A_n' = A_n$

Разрешимые группы.

$G \supseteq G' \supseteq G^{(2)} \supseteq \dots$

В случае $|G| = \infty$ имеется возможность может быть бесконечно убывающей.

В конечной группе G последовательность коммутантов стабилизируется.

Группа наз-ся разрешимой, если последовательность коммутантов стабилизируется на единице, т.е. $\exists k: G^{(k)} = \{e\}$

(Т) [① Всякая подгруппа разрешимой группы разрешима
② Если G имеет нормальную подгруппу $H \triangleleft G$, то G - разрешима $\Leftrightarrow$ H - разрешима и G/H - разрешима.]

① Пусть H - произвольная подгруппа.
$f: H \to G$ - гомоморфизм вложения
По св-ву коммутантов, $f(H^{(k)}) \subseteq G^{(k)}$.
Если G - разрешима $\Rightarrow$ $G^{(k)} = \{e\}$ для некоторого k
$\Rightarrow f(H^{(k)}) = \{e\} \Rightarrow H^{(k)} = \{e\} \Rightarrow H$ - разрешима.

② $\Rightarrow$ Пусть $H \triangleleft G$ и G - разрешима.
$\Rightarrow H$ - разрешима. ① Докажем, что G/H - разреш.
Рассмотрим $\pi: G \to G/H$.
$G^{(k)} = \{e\}$
Т.к. π - сюрьективно, то $\pi(G^{(k)}) = (G/H)^{(k)}$. $\Rightarrow$
$\Rightarrow (G/H)^{(k)} = \{e\} \Rightarrow G/H$ - разрешима

$\Leftarrow$ Пусть H, G/H - разрешимы $\Rightarrow \exists k\ (G/H)^{(k)} = \{e\}$
и $\exists l$, т.ч. $(H)^{(l)} = \{e\}$.
Рассм. кан. гомоморфизм $\pi: G \to G/H$
$\pi(G^{(k)}) = (G/H)^{(k)} = \{e\} \Rightarrow G^{(k)} \subseteq H$.
Поскольку H - разрешима $(G^{(k)})^{(l)} \subseteq H^{(l)} = \{e\}$.
Но $G^{(k+l)} = (G^{(k)})^{(l)} = \{e\} \Rightarrow G$ - разрешима ■

Примеры разрешимых и неразрешимых групп.
1) S_n, A_n - неразрешимы при $n \geq 5$
2) S_3, A_4, D_n, Q_8 - разрешимы
0) Любая абелева группа разрешима.
3) Рассм. произвольное поле K.
$T_n(K)$ - невыр. верхнетреугольные матрицы
(Т) [$T_n(K)$ - разрешима при любом $n \in \mathbb{N}$]
Рассм. гомоморфизм $f: T_n(K) \to D_n(K)$
(очевидно) невырожд. диагональн. матр.

$\operatorname{Ker} f = UT_n(K)$ — группа нильп. верхнетреуг. матриц

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

Остается док-ть, что $UT_n(K)$ разрешима.

Индукция по n. База $n=1$. $UT_n(K) = \{e\}$

$\varphi: UT_n(K) \to UT_{n-1}(K)$ (сопоставляем верхнедиагональный блок размера $(n-1)\times(n-1)$)

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \\ \hline 0 & 0 \cdots 0 & 1 \end{pmatrix}$$

очевидно гомоморфизм (сюръективный)

По инд. предположению $UT_{n-1}(K)$ — разрешима

Покажем, что $\operatorname{Ker}\varphi$ — разрешимо

$$\operatorname{Ker}\varphi = \left\{ \left(\begin{array}{ccc|c} 1 & & 0 & a_1 \\ & \ddots & & \vdots \\ 0 & & 1 & a_{n-1} \\ \hline 0 & \cdots & 0 & 1 \end{array}\right) \right\}.$$

Рассмотрим биекцию $\operatorname{Ker}\varphi \longleftrightarrow (K^{n-1}, +)$ (сопост. столбцу $\begin{pmatrix} a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$)

вект. прво с операцией $+$

При перемн. матриц из $\operatorname{Ker}\varphi$ элементы $a_1, \dots, a_{n-1}$ складываются $\Rightarrow$ это есть изоморфизм ядра $\operatorname{Ker}\varphi \cong K^{n-1} \xleftarrow{\text{абелева}} \Rightarrow \operatorname{Ker}\varphi$ — абелева $\Rightarrow UT_n(K)$ — разрешима. ■

26.10.2015

Действие группы на мн-ве

(Представление группы перестановками)

Дано: G — группа, X — мн-во

G действует на X, если задана операция умн. слева эл. мн-ва X на эл-ты группы G, т.е. задано отображение:

$G \times X \to X$

внешнее умн.

$(g, x) \mapsto gx \in I$

Причем должны выполняться след. условия:

1) $\forall g, h \in G,\ x \in X \quad (gh)x = g(hx)$

2) $ex = x \quad \forall x \in X$

Представлением группы G перестановками на мн-ве X назов. гомоморфизм $\rho: G \to S_X$ — группу перестановок (биек. отображений) мн-ва X. $\rho(e)(x) = ex = x$ — тождеств. гомоморф-м

Покажем эквивалентность определений:

$\Downarrow$ $\rho(g)(x) := gx$

Покажем, что $\rho(g): X \to X$

Покажем ас-ть: $\underline{\rho(gh)}(x) = (gh)x = g(hx) =$

$= \underline{(\rho(g) \circ \rho(h))}(x)$

Проверяем биективность

$\rho(g^{-1})\circ\rho(g) \overset{\text{гомом}}{=} \rho(g^{-1}g) = \rho(e) = 1_X$

$\rho(g)\circ\rho(g^{-1}) = \rho(gg^{-1}) = \rho(e) = 1_X$

Т.е. получили отобр. в группу перестановок

$\Uparrow$ Задано ρ.

Определим $gx = \rho(g)(x)$. Тогда

1) $(hg)x = \rho(hg)(x) = (\rho(h)\circ\rho(g))(x) = \rho(h)(\rho(g)(x)) = h(gx)$

2) $ex = \rho(e)(x) = 1_X(x) = x$. $\quad \rho(e) = 1_X$

Обозначение: (G, X, ρ) — задано действие G на X

ПРИМЕРЫ

1. S_n $\{1, .., n\}$ — по определению
2. V — вект. пр-во над K. $\dim V = n$

   $GL(V)$ — группа всех невыр. лин. операторов на пр-ве V

   $GL(V) \underset{\text{подгр.}}{\subset} S_V$ $\quad$ $GL(V)$ действует на V

   Если в V задан базис, то по нему строим изом-м:

   Конф. базис определяет действие на всем V $GL(V)$

   $GL(n, K) \xrightarrow{\cong} GL(V)$.
3. $\varphi: H \to G \xrightarrow{\rho} S_X$

   (G, X, ρ_G) — действие G на X

   $\rho_H := \rho_G \circ \varphi$

   $hx = \varphi(h)x$ $\forall h \in H$.

Если H — вложение как подгр. в G, то получаем индуц. действие группы

Если H — норм. и задано $(G/H, X, \rho)$, тогда

$\pi: G \to G/H$

Действие фактор-группы задает действие группы.

<u>Ядро действий</u> — это $\operatorname{Ker}\rho$, т.е. состоит из таких $g \in G$, что $gx = x$ $\forall x \in X$.

Если $\operatorname{Ker}\rho = \{1\}$, т.е. ρ инъективен, то получаем инъект. отобр. G в группу перестановок, т.е. получаем реализацию всей гр. G как группы S_n. $\Rightarrow$ можем отождествить G с некоторой подгр. в группе перестановок.

Инвариантное (под)множество $Y \subseteq X$ — такое подмн-во, если $gy \in Y$ $\forall y \in Y$, $g \in G$.

$\Downarrow$ можем говорить о действии G на инвар. подмножестве

КАКИЕ НАИМЕНЬШИЕ ИНВАРИАНТНЫЕ ПОДМН-ВА?

Орбитой эл-та $x \in X$ относит. заданного действия группы G наз-ся мн-во $Gx = \{gx \mid g \in G\} \subseteq X$ (очевидно, инвар. мн-во)

Орбита — наименьшее инвар. подмн-во (см. бо №2)

СВОЙСТВА ОРБИТ

① $x \in Gx$

⑤ $Gx = \{x\} \Leftrightarrow gx = x \ \forall g \in G$ (отсюда неподвижный элемент мн-ва X)

⑥ $Gx = X \Leftrightarrow \forall x_1, x_2 \in X \ \exists g : gx_1 = x_2$

② Любой эл-т орбиты определяет эту орбиту, т.е.

$\forall x_1 \in Gx : \ Gx_1 = Gx$

$\exists g \in G : x_1 = gx \Leftrightarrow Gx_1 = G(gx) \underset{\text{ассоц}}{=} (Gg)x = Gx$

③ Любые две орбиты либо совпадают, либо не пересекаются

Если $\exists x_3 \in Gx_1 \cap Gx_2 \Rightarrow \underset{Gx_2}{\parallel} Gx_3 = Gx_1$.

④ Орбиты задают разбиение мн-ва X на попарно непересек. мн-ва. $X = \bigcup Gx_i$ $\{x_i\}$ – мн-во представителей орбит

В частности: любое инвар. подмн-во явл. объединением орбит.

Тем самым задается отношение эквив-ти:

$x_1 \sim x_2$ – лежат в одной орбите.

Стабилизатор элемента x при действии группы G – это мн-во $St(x) = \{g \in G : gx = x\}$. (Стабилизатор – это подгруппа)

Действие транзитивно, когда мн-во X состоит из одной орбиты (св-во ΔG)

Действие группы на любой орбите явл. транзитивным

Для неподв. точек $St(x) = X$.

Т [Если $x \in X$, то эл-ты орбиты Gx находятся в биективном соотв-вии с левыми смежными классами по стабилизатору X.]

$\forall h \in G$

$(h\,St(x))(x) = hx \overset{y}{=}$ каждый левый см. класс дает одну точку

Возьмем $\forall y \in Gx$

$\{g : gx = y\} = K$, выберем $\forall h \in K$

$x = g^{-1}y$ (по усл.)

$y = hx \Rightarrow g^{-1}hx = x \Rightarrow$

$\Rightarrow g^{-1}h \in St(x) \Rightarrow h \in g\,St(x)$

Т.е. $\forall$ эл-т из K лежит в левом см. классе по стаб-ру.

Получим биекцию. ■

СЛЕДСТВИЕ [Число элементов в орбите равно индексу стабилизатора для любой точки орбиты]

Орбитальная формула

$X = \bigcup_{x_i} Gx_i$ – по представителям орбит

$|X| = \sum_{x_i} |Gx_i| = \sum_{\{x_i\}} (G : St(x))$ – мн-во представителей орбит

Т [Число эл-тов в мн-ве равно сумме индексов стабилизаторов орбит, $|X| = \sum (G : St(x))$]

ПРИМЕРЫ

① Действие группы на себе левыми сдвигами.

$X = G \quad g, x \in G$

$\underset{\text{внешнее}}{g \bullet x} = gx$

Получаем гом-м $G \xrightarrow{\rho} S_G$

Правые сдвиги не подходят (нарушается ассоциативность) $g \bullet x = xg$

$\underset{gx=x \Leftrightarrow g=e}{\operatorname{Ker} \rho} = \{e\}$ ⇒ тем самым действие явл. точным,

причем $\rho : G \subset S_G$

$|G| = n \quad G \underset{\operatorname{Im}\rho}{\cong} H \subset S_n$

Орбита будет только одна

② Ограничение действия группы на себе левыми сдвигами на подгруппе $H \leq G$

$X = G, \ \underset{\text{подгр}}{H \leq G}$

$x \in G$ Орбита здесь: Hx — правый смежный класс

Действие явл. точным, т.к. $hx = x \Leftrightarrow h = e$, т.е. $\operatorname{Ker} \rho = \{e\}$.

Более того, $St(x) = \{e\}$. Число эл-тов в каждой орбите равно порядку H.

По орбит. ф-ле: $|G| = \sum_{x_i} (\underbrace{H : \underbrace{St(x_i)}_{\{e\}}}_{H})$, т.е. орбитальная ф-ла превращается в теорему Лагранжа.

Если рассм. действие H посредством правых сдвигов то орбиты — левые смежные классы ⇒ также получается т. Лагранжа

③ $S_n, \ X = \{1, \dots, n\}$

$\pi \in S_n. \quad G = \langle \pi \rangle_k$ — цикл. группа, порожд. перестановкой

Возьмем $i_1 \in X$, тогда орбитой будет:

$G i_1 = \{ i_1, \underset{i_2}{\pi i_1}, \underset{i_3}{\pi^2 i_1}, \dots \}$ — элементы цикла $(i_1 i_2 \dots i_k)$ перестановки π

Цикл — это не просто орбита, а орбита с указанием, как действует π на этой орбите.

Цикл — это перестановка, сост. из эл-тов одной орбиты,

Получим теор. об однозн. представлении перестановки в в виде произведения независимых циклов

④ Действие группы на себе посредством сопряжения.

$X = G$.

$\underset{\text{внешнее}}{g \bullet x} = \underset{\text{в группе}}{gxg^{-1}}$ Проверим аксиомы:

1) $gh \bullet x = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g \bullet (h \bullet x)$

2) $e \bullet x = x$.

Орбита этого действия — класс сопряженного эл-та

Т.е. задается разбиение на классы сопряженных элементов.

$St(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = Z(x)$ — мн-во элементов, перестановочных с данным эл-том x.

Неподвижные точки действия:

$g \cdot x = x \quad \forall g \in G \Leftrightarrow St(x) = Z(x) = G$, т.е. x перестановочен со всеми эл-тами группы.

Мн-во неподвижных эл-тов относительно действия сопряжения — это центр группы.

Мно элементов в классе сопряженных с x равно индексу стабилизатора x

$Cl(x) = \{gxg^{-1} \mid g \in X\}$

$|Cl(x)| = (G : Z(x))$

Орбитальная формула:

$$|G| = \underbrace{|Z(G)|}_{\text{из орбит по одному элементу}} + \sum_{x_i} \underbrace{(G : Z(x_i))}_{\text{из орбит длины больше 1, т.е. } \neq Z(G)}$$

ПРИМЕРЫ КЛАССОВ СОПРЯЖЕННЫХ ЭЛЕМЕНТОВ

① $G = GL(n, \mathbb{C})$

Сопряж. элементы — сопряженные матрицы. $\overset{\text{итак}}{\Longleftrightarrow}$ когда у них одинаковые жордановы формы

Т.е. класс сопряженных задается собств. значением и размерами жордановых клеток

В абелевой группе все классы одноэлементны

② $G = Q_8$

Ответ: $\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}$ — разбиение Q_8 на классы сопряженности

③ $G = D_n$

$\{e\}, \{a^k, a^{-k}\}_{k=1,\dots,(n-1)/2}, \{b, ab, \dots, a^{k-1}b\}$ — если n - нечетно

$\{e\}, \{a^{n/2}\}, \{a^k, a^{-k}\}_{k=1,\dots,\frac{n}{2}-1}, \{b, a^2b, \dots, a^{n-2}b\}, \{ab, a^3b, \dots, a^{n-1}b\}$ — n-четно.

④ $G = S_n$

Т [π_1 и π_2 сопряжены $\Leftrightarrow$ совпадают длины их независимых циклов.]

($\Rightarrow$) $\pi_1 = (i_1 \dots i_k) \dots (i_{l+1} \dots i_n)$ ← также и циклы длины 1

$$\sigma = \begin{pmatrix} i_1 \dots i_k & \dots & i_{l+1} \dots i_n \\ j_1 \dots j_k & \dots & j_{l+1} \dots j_n \end{pmatrix}$$

$$\sigma \pi_1 \sigma^{-1} = (j_1, j_2, \dots, j_k) \dots (j_{l+1} \dots j_n)$$

($\Leftarrow$) π_1 и π_2 - одинаковые длины

$\pi_2 = (j_1 \dots j_k) \dots (j_{l+1} \dots j_n)$

$\pi_1 = (i_1 \dots i_k) \dots (i_{l+1} \dots i_n)$

$\sigma = \begin{pmatrix} \quad \end{pmatrix} \Rightarrow \pi_2 = \sigma \pi_1 \sigma^{-1}$ ■