

Лекции по алгебре, 3 сем

(преподаватель Демченко О. В.)
Записали Костин П.А., Щукин И.В.

Данный документ неидеальный, прошу сообщать о найденных недочетах в [ВКонтакте](#)

Содержание

1 Теория групп

1.1 3.09.2019

Опр

G - *множество*, $*$: $G * G \Rightarrow G$, $(g_1, g_2) \Rightarrow (g_1 * g_2) (g_1 g_2)$

1. $(g_1 g_2) g_3 = g_1 (g_2 g_3) \quad \forall g_1, g_2, g_3 \in G$
2. $\exists e \in G : eg = ge = g \quad \forall g \in G$
3. $\forall g \in G \quad \exists \tilde{g} \in G : g\tilde{g} = g\tilde{g} = e$
4. $g_1 g_2 = g_2 g_1 \quad \forall g_1, g_2 \in G$ - тогда это абелева группа

Пример

1. $(\mathbb{Z}, +)$ - группа
2. (\mathbb{Z}, \bullet) - не группа
3. $(R, +)$ - группа кольца
4. (R^*, \bullet)
5. Группа самосовмещения D_n , например D_4 - квадрат, композиция - группа, $|D_n| = 2n$
6. $GL_n(K) = \{A \in M_n(K) : |A| \neq 0\}$, умножение - группа
7. $\mathbb{Z}n\mathbb{Z}$ - частный случай п.3,4

Свойства (групп)

1. e - единственный, e, e' - нейтральные: $e = ee' = e'$

2. \tilde{g} - единственный

Пусть \tilde{g}, \hat{g} - обратные, тогда $\tilde{g}g = g\tilde{g} = e = \hat{g}g = g\hat{g}$

$$\hat{g} = e\hat{g} = (\tilde{g}g)\hat{g} = \tilde{g}(g\hat{g}) = \tilde{g}e = \tilde{g}$$

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

Это верно, если $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$, докажем первое:

$$(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$$

4. $(g^{-1})^{-1} = g$

Опр

$$g \in G \quad n \in \mathbb{Z}, \text{ тогда } g = \begin{cases} \overbrace{g \dots g}^n, & n > 0 \\ e, & n = 0 \\ \underbrace{g^{-1} \dots g^{-1}}_n, & n < 0 \end{cases}$$

Свойства (степени)

1. $g^{n+m} = g^n g^m$
2. $(g^n)^m = g^{nm}$

Опр

$g \in G, n \in \mathbb{N}$ - порядок g ($\text{ord } g = n$), если:

1. $g^n = e$
2. $g^m = e \Rightarrow m \geq n$

Пример

1. $D_4 \quad \text{ord}(\text{поворот } 90^\circ) = 4$
 $D_4 \quad \text{ord}(\text{поворот } 180^\circ) = 2$
2. $(\mathbb{Z}/6\mathbb{Z}, +) \quad \text{ord}(\bar{1}) = 6$
 $\text{ord}(\bar{2}) = 3$

Утв

$$g^m = e \quad \text{ord}(g) = n \Rightarrow m : n \quad (n > 0)$$

Док-во

$$m = nq + r, \quad 0 \leq r < n$$

$$e = g^m = g^{nq+r} = (g^n)^q g^r = g^r \Rightarrow r = 0$$

Опр

$H \subset G$ называется подгруппой G ($H < G$) (и сама является группой), если:

1. $g_1, g_2 \in H \Rightarrow g_1 g_2 \in H$
2. $e \in H$
3. $g \in H \Rightarrow g^{-1} \in H$

Пример

1. $n\mathbb{Z} < \mathbb{Z}$

2. D_4

3. $SL_n(K) = \{A \in M_n(K) : |A| = 1\}, SL_n(K) < GL_n(K)$

Мультипликативная запись	Аддитивная запись
$g_1 g_2$	$g_1 + g_2$
e	0
g^{-1}	$-g$
g^n	ng

Опр

$H < G, g_1, g_2 \in G$, тогда $g_1 \sim g_2$, если:

1. $g_1 = g_2 h, h \in H$ (левое)
2. $g_2 = h g_1, h \in H$ (правое)

Док-во (эквивалентности)

1. (симметричность) $g_1 = g_2 h \xrightarrow{*h^{-1}} g_2 = g_1 h^{-1}$
2. (рефлексивность) $g = g e$
3. (транзитивность) $g_1 = g_2 h, g_2 = g_3 h \Rightarrow g_1 = g_3 (h_2 h_1)$, где $h_2 h_1 \in H$

Опр

$[a] = \{b : a \sim b\}$ классы эквивалентности

Опр

$[g] = gH = \{gh, h \in H\}$ (левый класс смежности)
 $gh \sim g \Rightarrow gh \in [g]$
 $g_1 \in [g] \Rightarrow g_1 \sim g \Rightarrow g_1 = gh$

Утв

$[e] = H$
Установим биекцию:
 $[g] = gh \leftarrow H$
 $gh \leftarrow h$
Очевидно, сюръекция, почему инъекция?
 $gh_1 = gh_2 \xrightarrow{*g^{-1}} h_1 = h_2$

Теорема (Лагранжа)

$H < G, |G| < \infty$, тогда $|G| : |H|$ (уже доказали!)

1.2 10.09.2019

Следствие

G - кон. группа, $a \in G$, $\text{ord } a = m$, $H = \{a^n : n \in \mathbb{Z}\}$, тогда $|H| = m$

Док-во

$\{a^0 = e, a_1, \dots, a^{m-1}\}$ - подмножество H

Докажем, что все остальные элементы тоже здесь есть

$$n \in \mathbb{Z} \Rightarrow n = mq + r, 0 \leq m - 1$$

$$a^n = a^{mq+r} = (a^m)^q a^r = a^r$$

$$a^k = a^l, 0 \leq k \leq l \leq m - 1, \text{ умножим на } a^{-k}$$

$$e = a^{l-k} \text{ } 0 \leq l - k \leq m - 1 \text{ } m - \text{ наименьшее } \mathbb{N} \text{ такое что } a^m = e$$

$$l - k = 0 \Rightarrow l = k$$

Докажем, что $|H| = m$

$\Rightarrow |G| : m = \text{ord } a$, т.о. в группе порядок эл-та - делитель порядка группы

Напоминание

Следствие (теорема Эйлера)

$n, a \in \mathbb{N}$, $(a, n) = 1$, тогда $a^{\varphi(n)} \equiv 1 \pmod{n}$

Док-во

Рассмотрим $G = (\mathbb{Z}/n\mathbb{Z})^*$ $|G| = \varphi(n)$

$$\bar{a} \in G, \text{ord } \bar{a} = k$$

$$\varphi(n) : k \Rightarrow \varphi(n) = kl$$

$$\bar{a} = \bar{1}$$

$$\bar{a}^{\varphi(n)} = \bar{1}$$

Опр

G - циклическая группа, если $\exists g \in G : \forall g' \in G : \exists k \in \mathbb{Z} : g' = g^k$

Такой g называется образующим

Пример

\mathbb{Z} (образующий - единица и минус единица)

Замечание

Любая циклическая группа - коммутативна

Док-во

$$g'g'' = g''g' = g^k g^l = g^l g^k$$

Пусть G, H - группы, рассмотрим $G \times H = \{(g, h) : g \in G, h \in H\}$

Введем операцию $(g, h) * (g', h') \stackrel{\text{def}}{=} (g *_G g', h *_H h')$

Докажем, что это группа.

Доказательство ассоциативности:

$$((g, h)(g', h'))(g'', h'') \stackrel{?}{=} (g, h)((g', h')(g'', h''))$$

$$(gg', hh')(g'', h'') \stackrel{?}{=} (g, h)(g'g'', h'h'')$$

$$((gg')g'', (hh')h'') \stackrel{?}{=} (g(g'g''), h(h'h'')) - \text{очевидно}$$

Нейтральный элемент:

$$\text{Рассмотрим } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$$

УТВ

Конечная группа порядка n является циклической тогда и только тогда, когда она содержит элемент порядка n ($|G| = n$, G - циклическая $\equiv \exists g \in G : \text{ord } g = n$)

Рассмотрим $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ - циклическая

$$((\bar{1}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{2}))$$

Рассмотрим $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ - не циклическая

Опр

$\varphi : G \rightarrow H$ - биекция и $\varphi(g_1, g_2) = \varphi(g_1)\varphi(g_2) \quad \forall g_1, g_2 \in G$, тогда φ - изоморфизм

$$1. D_3 \rightarrow S_3$$

$$2. U_n = \{z \in \mathbb{C} : z^n = 1\} \leftarrow \mathbb{Z}/n\mathbb{Z}$$

$$\left(\frac{2\pi a}{n} + i \sin \frac{2\pi a}{n} = \varphi(\bar{a})\right)$$

$$\bar{a} = \bar{b} \rightarrow \varphi(\bar{a}) = \varphi(\bar{b})$$

$$\varphi(\bar{a} + \bar{b}) \stackrel{?}{=} \varphi(\bar{a})\varphi(\bar{b})$$

$$\cos \frac{2\pi(a+b)}{n} + i \sin \frac{2\pi(a+b)}{n} = \left(\cos \frac{2\pi a}{n} + i \sin \frac{2\pi a}{n}\right)$$

Опр

Две группы называются изоморфными, если между ними существует изоморфизм

УТВ

Изоморфизм - отношение эквивалентности

Док-во

т.к. композиция изоморфизмов - изоморфизм $G \xrightarrow{\varphi} H \xrightarrow{\psi} H$

$$(\psi \circ \varphi)(g_1 g_2) = \psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1) \varphi(g_2)) = \psi(\varphi(g_1)) \psi(\varphi(g_2)) = (\psi \circ \varphi)(g_1) \circ (\psi \circ \varphi)(g_2)$$

Рефлексивность - тождественное отображение - изоморфизм

Транзитивность: $G \xrightarrow{\varphi} H, H \xrightarrow{\varphi^{-1}} G$

Теорема

G - циклическая группа

1) $|G| = n \Rightarrow G \cong \mathbb{Z}/n\mathbb{Z}$

2) $|G| = \infty \Rightarrow G \cong \mathbb{Z}$

Док-во

1) g - обр. G , значит $G = \{e, g, g^2, \dots, g^{n-1}\}$ (среди них нет одинаковых),

построим изоморфизм в $\mathbb{Z}/n\mathbb{Z}$: $\varphi(g^k) = \bar{k}$

Проверим, что $\varphi(g^k g^l) = \varphi(g^k) + \varphi(g^l) = \bar{k} + \bar{l}$

Левая часть: $\varphi(g^{k+l}) = (k+l) \bmod n = \bar{k} + \bar{l}$

2) $G = \{\dots, g^{-1}, e, g, g^2, \dots\}$ (тоже нет совпадающих элементов, иначе $g^k = g^l$, при $k > l$, тогда $g^{k-l} = e$, но тогда конечное число элементов, потому что оно зацикливается через каждые $k-l$ элементов), построим отображение в \mathbb{Z} .

$\varphi(g^n) = n$ -, очевидно, биекция. И нужно доказать, что $\varphi(g^n g^k) = \varphi(g^n) + \varphi(g^k) = n + k$

1.3 17.09.2019

УТВ

$$|G| = p, p - \text{простое} \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$$

Док-во

$$g \in G, g \neq e, \text{ord } g = p$$

$$\Rightarrow G = \{e = g^0, g, \dots, g^{p-1}\}$$

УТВ

$$H, G - \text{группы}, \varphi : G \rightarrow H - \text{изоморфизм} \Rightarrow n = \text{ord } g = \text{ord } \varphi(g)$$

Док-во

$$\text{Пусть } g^n = e, \varphi(g^n) = \varphi(e) \stackrel{?}{=} e$$

$$\varphi(e)^2 = \varphi(e^2) = \varphi(e)$$

Теперь докажем, что меньшего нет

$$\varphi(g)^m = e, \quad m \in \mathbb{N} \stackrel{?}{\Rightarrow} m \geq n$$

$$\varphi(g^m) = \varphi(g)^m = e = \varphi(e) \Rightarrow g^m = e \Rightarrow m \geq n$$

Опр

$H < G$, тогда H - нормальная подгруппа, если $\forall h \in H, g \in G \Rightarrow g^{-1}hg \in H$
 - сопряжение элемента h с помощью элемента g , обозначается: $H \triangleleft G$

Замечание

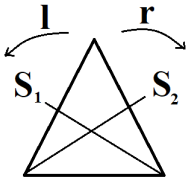
Элементы подгруппы при сопряжении переходят в элементы подгруппы

Замечание

Подгруппа любой коммутативной группы нормальна

Пример

D_3 - 6 элементов, 3 поворота и 3 симметрии



$\{e, l, r\}$ - нормальная

$\{e, s_1\}$ - не нормальная

УТВ

$H \triangleleft G \Leftrightarrow$ разбиение на L и Π классы смежности по H совпадают

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

Док-во

Берем произвольный элемент из левого и правого и докажем, что совпадают. Берем слева:

$$h \in H \quad gh \in gH$$

$$gh = \underbrace{(g^{-1})^{-1}hg^{-1}}_{\in H} g = h_1g$$

Теперь справа:

$$g \in G, \quad h \in H, \quad g^{-1}hg = h_1$$

$$hg \in Hg = gH \Rightarrow gh_1, h_1 \in H$$

Опр

$$H \triangleleft G \quad g_1 H * g_2 H \stackrel{\text{def}}{=} g_1 g_2 H$$

Док-во (корректности)

Хотим проверить, что

$$\tilde{g}_1 H = g_1 H, \quad \tilde{g}_2 H = g_2 H \stackrel{?}{\Rightarrow} \tilde{g}_1 \tilde{g}_2 H = g_1 g_2 H$$

Аналогично прошлому доказательству

$$g_2^{-1} h_1 g_2 = h_3 \in H$$

$$\tilde{g}_1 \tilde{g}_2 h = g_1 h_1 g_2 h_2 h = g_1 g_2 (g_2^{-1} h_1 g_2) h_2 h$$

$=_{h_3}$

$$\tilde{g}_1 H = g_1 H \Rightarrow \tilde{g}_1 = g_1 h_1$$

$$\tilde{g}_2 H = g_2 H \Rightarrow \tilde{g}_2 = g_2 h_2$$

Не использовали условие $g_2^{-1} h_1 g_2 = h_3 \in H$

$$\tilde{g}_1 \tilde{g}_2 H = g_1 h_1 g_2 h_2 h = g_1 g_2 (g_2^{-1} h_1 g_2) h_2 h$$

$=_{h_3}$

Осталось доказать, что получается группа

1) Нейтральный элемент $eH = H, \quad eH * gH = (eg)H = gH$

2) Ассоциативность $(g_1 H * g_2 H) * g_3 H \stackrel{?}{=} g_1 H * (g_2 H * g_3 H)$

$$(g_1 g_2) H * g_3 H = (g_1 g_2) g_3 H$$

3) $gH * g^{-1}H = (gg^{-1})H = eH$

$$G/H$$

Была эквивалентность: $a \sim b \Leftrightarrow a - b \in h$

$$G = \mathbb{Z}$$

$$H = h\mathbb{Z}, \quad g_1 g_2^{-1} \in H - \text{мульт. запись}, \quad g_1 - g_2 \in n\mathbb{Z} - \text{адд. запись}$$

$$[a] + [b] = [a + b]$$

Аддитивная группа кольца класса вычетов - это то же самое, что фактор группа группы \mathbb{Z} по подгруппе $n\mathbb{Z}$

Пример

Как в произвольной группе найти подгруппу?

$[g, h] = ghg^{-1}h^{-1}$, $g, h \in G$ - коммутатор элементов $h, g \in G$

Коммутант - множество произведений всех возможных коммутаторов

Обозначается $K(G) = \{[g_1, h_1] \dots [g_n, h_n], g_i, h_i \in G\}$

Док-во (коммутант - подгруппа)

$K(G) < G$

Нейтральный элемент: $[e, e] = e$

Обратный элемент? $[g_1, h_1] \dots [g_n, h_n]$

Как его найти? $[g, h^{-1}]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h, g]$

$([g_1, h_1] \dots [g_n, h_n])^{-1} = [g_1, h_1] \dots [g_n, h_n]$

Значит это подгруппа

Нормальная ли? $g^{-1}[g_1, h_1] \dots [g_n, h_n]g$

$g^{-1}[g_1, h_1]g(g^{-1}[g_2, h_2]g) \dots (g^{-1}[g_n, h_n]g)$

Нужно доказать, что сопряжение коммутатора лежит в коммутанте

$$g^{-1}g_1h_1g_1^{-1}h_1^{-1}g = \underbrace{g^{-1}g_1h_1g_1^{-1}h_1^{-1}}_{=[g^{-1}g_1, h_1]} \underbrace{h_1g^{-1}h_1^{-1}g}_{=[h_1, g^{-1}]}$$

УТВ

Фактор-группа $(G/K(G))$ по коммутанту - коммутативна

Док-во

$$g_1, g_2 \in G \quad g_1K(G)g_2K(G) \stackrel{?}{=} g_2K(G)g_1K(G)$$

$$g_1g_2K(G) = g_1g_2K(G) \quad g_2K(G)g_1K(G) = g_2g_1K(G)$$

$$[g_1, g_2] = g_1g_2(g_2g_1)^{-1} \in K(G)$$

УТВ

$$\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{mn}, \text{ если } (m, n) = 1$$

Док-во

Нужно построить изоморфизм $[a]_{mn} \mapsto ([a]_n, [a]_m)$

$$[a]_{mn} = [a']_{mn} \Rightarrow [a]_n = [a']_n, [a]_m = [a']_m$$

Теперь нужно проверить биекцию

$$\text{Сюръекция: } \forall b, c \in \mathbb{Z} \exists x \in \mathbb{Z} : \begin{cases} [x]_n = [b]_n \\ [x]_m = [c]_m \end{cases}, \text{ по КТО всё хорошо}$$

Инъективность:

$$\begin{aligned} [a]_n = [b]_n \\ [a]_m = [b]_m \end{aligned} \Rightarrow [a]_{mn} = [b]_{mn}$$

На языке сравнений:

$$\begin{aligned} a \equiv b(n) \\ a \equiv b(m) \end{aligned} \Rightarrow a \equiv b(mn)$$

На самом деле достаточно было проверить одно

Опр

$\varphi : G \rightarrow H$ - гомоморфизм, если $\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$

изоморфизм = гомоморфизм + биективность

$\varphi \in \text{Hom}(G, H)$ - множество гомоморфизмов

Примеры

1) $\mathbb{C}^* \rightarrow \mathbb{R}^*$

$$z \rightarrow |z|$$

2) $GL_n(K) \rightarrow K^*$

$$A \rightarrow \det A$$

3) $S_n \rightarrow \{\pm 1\}$

$$\sigma \rightarrow \begin{cases} +1, & \text{если } \sigma - \text{четн.} \\ -1, & \text{если } \sigma - \text{неч.} \end{cases}$$

4) $a \in G \quad G \rightarrow G$

$$g \rightarrow a^{-1}ga$$

$$(a^{-1}ga)(a^{-1}g_1a) = a^{-1}g_1ga$$