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

<u>**Опр**</u>

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

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. $\forall g \in G \quad \exists \widetilde{g} \in G : g\widetilde{g} = g\widetilde{g} = e$
4. $g_1 g_2 = g_2 g_1 \quad \forall g_1, g_2 \in G$ - тогда это абелева группа

<u>**Пример**</u>

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

<u>**Свойства**</u> **(групп)**

1. e - единственный, e, e' - нейтральные: $e = ee' = e'$
2. $\widetilde{g}$ - единственный

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

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

$g \in G \quad n \in \mathbb{Z}$, тогда $g = \left[\begin{array}{l} \overbrace{g...g}^{n}, \quad n > 0 \\ e, \quad n = 0 \\ \underbrace{g^{-1}...g^{-1}}_{n}, \quad n < 0 \end{array}\right.$

Свойства (степени)

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

Опр

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

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

Пример

1. D_4 ord(поворот 90°) $= 4$
   D_4 ord(поворот 180°) $= 2$
2. $(\mathbb{Z}/6\mathbb{Z}, +)$ $\operatorname{ord}(\overline{1}) = 6$
   $\operatorname{ord}(\overline{2}) = 3$

Утв

$g^m = e \quad \operatorname{ord}(g) = n \Rightarrow m \,\vdots\, n$ (n>0)

Док-во

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

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

Мультипликативная запись	Аддитивная запись
g_1g_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. $g_1 = g_2h$, $h \in H$ (левое)

2. $g_2 = hg_1$, $h \in H$ (правое)

Док-во (эквивалентности)

1. (симметричность) $g_1 = g_2h \overset{*h^{-1}}{\Rightarrow} g_2 = g_1h^{-1}$

2. (рефлексивность) $g = ge$

3. (транзитивность) $g_1 = g_2h$, $g_2 = g_3h \Rightarrow g_1 = g_3(h_2h_1)$, где $h_2h_1 \in H$

Опр

$[a] = \{b : a\ b\}$ 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?
$gh_1 = gh_2 \overset{*g^{-1}}{\Rightarrow} h_1 = h$

Теорема (Лагранжа)

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

1.2 10.09.2019

Следствие

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

Док-во

$\{a^0 = e, a_1, ..., a^{m-1}\}$ - подмножество H
Докажем, что все остальные элементы тоже здесь есть
$n \in \mathbb{Z} \Rightarrow n = mq + r$, $0 \leqslant m - 1$
$a^n = a^{mq+r} = (a^m)^q a^r = a^r$
$a^k = a^l$, $0 \leqslant k \leqslant l \leqslant m - 1$, умножим на a^{-k}
$e = a^{l-k}$ $o \leqslant l - k \leqslant m - 1$ m - наименьшее $\mathbb{N}$ такое что $a^m = e$
$l - k = 0 \Rightarrow l = k$
Докажем, что $|H| = m$
$\Rightarrow |G| \vdots m = \operatorname{ord} a$, т.о. в группе порядок эл-та - делитель порядка группы

Напоминание

Следствие (теорема Эйлера)

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

Док-во

Рассмотрим $G = (\mathbb{Z}/n\mathbb{Z})* \ |G| = \varphi(n)$
$\overline{a} \in G$, $\operatorname{ord} \overline{a} = k$
$\varphi(n) \vdots k \Rightarrow \varphi(n) = kl$
$\overline{a} = \overline{1}$
$\overline{a}^{\varphi(n)} = \overline{1}$

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 - коммунитативна

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 $(g,h) * (g',h') \overset{def}{=} (g *_G g', h *_H h')$
Докажем, что это группа.
Доказательство ассоциативности:

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

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

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

Нейтральный элемент:

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

Утв

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

Рассмотрим $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ - циклическая
$((\overline{1},\overline{1}),(\overline{0},\overline{2}),(\overline{1},\overline{0}),(\overline{0},\overline{1}),(\overline{1},\overline{2}))$
Рассмотрим $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ - не циклическая

Опр

$\varphi : G \to H$ - 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. $D_3 \to S_3$

2. $U_n = \{z \in \mathbb{C} : z^n = 1\} \leftarrow \mathbb{Z}/n\mathbb{Z}$
   $(\frac{2\pi a}{n} + i\sin\frac{2\pi a}{n} = \varphi\overline{a}\overline{a})$
   $\overline{a} = \overline{b} \to \varphi(\overline{a}) = \varphi(\overline{b})$
   $\varphi(\overline{a}+\overline{b}) \overset{?}{=} \varphi(\overline{a})\varphi(\overline{b})$
   $\cos\frac{2\pi(a+b)}{n} + i\sin\frac{2\pi(a+b)}{n} = (\cos\frac{2\pi a}{n} + i\sin\frac{2\pi a}{n})$

Опр

Две группы называются изоморфными, если между ними существует изоморфизм

Утв

Изоморфизм - отношение эквивалентности

Док-во

т.к. композиция изоморфизмов - изоморфизм $G \xrightarrow{e} H \xrightarrow{\psi} H$
$(\psi \circ \varphi)(g_1 g_2) = \psi(\varphi(g_1 g_2) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\psi(\varphi(g_2)) = (\psi \circ \varphi)(g_1) \circ (\psi \circ \varphi)(g_2)$
Рефлексивность - тождественное отображение - изоморфизм
Транзитивность: $G \underset{\varphi}{\to} H$, $H \underset{\varphi^{-1}}{\to} G$

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 $G = \{e, g, g^2, ..., g^{n-1}\}$ (среди них нет одинаковых), построим изоморфизм в $\mathbb{Z}/n\mathbb{Z}$: $\varphi(g^k) = \overline{k}$
Проверим, что $\varphi(g^k g^l) \underline{= \varphi(g^k) + \varphi(g^l)} = \overline{k} + \overline{l}$
Левая часть: $\varphi(g^{k+l} = \overline{(k+l) \mod n} = \overline{k} + \overline{l}$
2) $G = \{..., g^{-1}, e, g, g^2, ...\}$ (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 - простое $\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$

Док-во

$g \in G$, $g \neq e$, $\operatorname{ord} g = p$
$\Rightarrow G = \{e = g^0, g, ..., g^{p-1}\}$

Утв

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

Док-во

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

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

Теперь докажем, что меньшего нет

$$\varphi(g)^m = e,\ m \in \mathbb{N} \overset{?}{\Rightarrow} m \geqslant n$$

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

Опр

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

Замечание

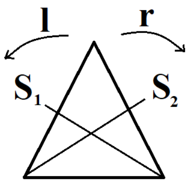
Элементы подгруппы при сопряжении переходят в элементы подгруппы

Замечание

Подгруппа любой коммунитативной группы нормальна

Пример

D_3 - 6 элементов, 3 поворота и 3 симметрии



$\{e, l, r\}$ - нормальная
$\{e, s_1\}$ - не нормальная

Утв

$H \lhd G \Leftrightarrow$ разбиение на Л и П кдассы смежности по H совпадают

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

Док-во

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

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

$$gh = \underbrace{(g^{-1})^{-1}hg^{-1}}_{\in H}g = h_1 g$$

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

$H \triangleleft G \; g_1H * g_2H \overset{\text{def}}{=} g_1g_2H$

Док-во (коррекнтности)

Хотим проверить, что

$$\widetilde{g}_1H = g_1H, \quad \widetilde{g}_2H = g_2H \overset{?}{\Rightarrow} \widetilde{g}_1\widetilde{g}_2H = g_1g_2H$$

Аналогично прошлому доказательству

$$g_2^{-1}h_1g_2 = h_3 \in H$$

$$\widetilde{g}_1\widetilde{g}_2h = g_1h_1g_2h_2h = g_1g_2(\underbrace{g_2^{-1}h_1g_2}_{=h_3})h_2h$$

$$\widetilde{g}_1H = g_1H \Rightarrow \widetilde{g}_1 = g_1h_1$$

$$\widetilde{g}_2H = g_2H \Rightarrow \widetilde{g}_2 = g_2h_2$$

Не использовали условие $g_2^{-1}h_1g_2 = h_3 \in H$

$$\widetilde{g}_1\widetilde{g}_2H = g_1h_1g_2h_2h = g_1g_2(\underbrace{g_2^{-1}h_1g_2}_{=h_3})h_2h$$

Осталось доказать, что получается группа

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

2) Ассоциативность $\quad (g_1H + g_2H) * g_3H \overset{?}{=} g_1H * (g_2H * g_3H)$

$(g_1g_2)H * g_3H = (g_1g_2)g_3H$

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

G/H

Была эквивалентность: $a \sim b \Leftrightarrow a - b \; \vdots \; h$

$G = \mathbb{Z}$

$H = h\mathbb{Z}, \quad g_1g_2^{-1} \in H$ - мульт. запись , $\quad g_1 - g_2 \in n\mathbb{Z}$ - 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 проззведений всех возможных коммунтаторов

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

Док-во (коммутант - подгруппа)

$K(G) < G$

Нейтральный элемент: $[e, e] = e$

Обратный элемент? $[g_1, h_1]...[g_n, h_n]$

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

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

Значит это подгруппа

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

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

Нужно доказать, что сопряжение коммунтатора 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 - коммунитативна

Док-во

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

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

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

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

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

Инъективность:

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

На языке сравнений:

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

На самом деле достаточно было проверить одно

Опр

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

изоморфизм = гомоморфизм + биективность

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

Примеры

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

$z \to |z|$

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

$A \to \det A$

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

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

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

$g \to a^{-1} g a$

$(a^{-1} g a)(a^{-1} g_1 a) = a^{-1} g_1 g a$