1 Теория групп

2019-09-17

Опр

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

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. $g_1 g_2 = g_2 g_1 \quad \forall g_1, g_2 \in G$

Примеры

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

Теорема (простейшие св-ва 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 $g = \left[\begin{array}{l} \overbrace{g...g}^{n}, \quad n > 0 \\ e, \quad n = 0 \\ \underbrace{g^{-1}...g^{-1}}_{n}, \quad n < 0 \end{array}\right.$

Теорема (св-ва степени)

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

Опр

$g \in G$, $n \in N$ - порядок g $(ordg = n)$, если:

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

Примеры

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

Утв

$g^m = e \quad ord(g) = n \to m \,\vdots\, n$ (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. $g_1, g_2 \in H \to g_1 g_2 \in H$
2. $e \in H$
3. $g \in H \to g^{-1} \in H$

Примеры

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
$g_1 g_2$	$g_1 + g_2$
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 (эквивалентность)

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

2. (рефлексивность) $g = ge$

3. (транзитивнось) $g_1 = g_2 h$, $g_2 = g_3 h \to g_1 = g_3(h_2 h_1)$, где $h_2 h_1 \in H$

Опр

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

Опр

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

Утв

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

Теорема (Лагранжа)

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