Лекция 16, 17.01.24

Пример циклических групп

1) $(\mathbb{Z}, +)$ - цикл числа по сложению

2) $(\mathbb{Z}_n, +_{mod\,n})$ - группа вычетов по mod n

3) $(\sqrt[n]{1}, \cdot)$ - компл. корни n-й степени из 1 с опер. умн. к.ч.

$1 = \cos 0 + i \sin 0$

$\sqrt[n]{1} = \{ \cos \frac{0+2\pi k}{n} + i \sin \frac{0+2\pi k}{n} \mid k = \overline{0, n-1} \}$

$\varepsilon_0 = 1$ - нейтральный эл-т по умнож.

$\varepsilon_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} = e^{i\frac{2\pi}{n}}$

$\varepsilon_k = e^{i\frac{2\pi k}{n}} = \varepsilon_1^k$

$(\sqrt[n]{1}, \cdot) = \langle \varepsilon_1 \rangle$ - цикл. группа, порожд. элементом ε_1

4) $(\{-1, 1\}, \cdot)$ - цикл. группа

Опр: Порядком группы наз. число элементов в ней (мощность).

Обознач: $|G|$ - порядок группы G

В примерах: $|(\mathbb{Z}, +)| = \infty$, $|(\mathbb{Z}_n, +)| = n$, $|(\sqrt[n]{1}, \cdot)| = n$, $|\{-1, 1\}, \cdot| = 2$

Замеч.: В произвольной группе G каждый эл-т $g \in G$ порождает циклич. подгруппу $\langle g \rangle$ (т.е. все степени эл-та g).

Утв. 1: Пусть G - группа (любая) и $g \in G$. Тогда $\operatorname{ord} g = |\langle g \rangle|$ - порядок циклич. подгруппы $\langle g \rangle$, порождённой эл-том g.

□ Пусть $H = \langle g \rangle$ ← мн-во степеней эл-та g. (H - подгруппа в G)

Если найдётся $k > s$, что $g^k = g^s$, то

$\Leftrightarrow g^{k-s} = e \Rightarrow$ эл-т g имеет конечный порядок

$\Rightarrow$ если $\operatorname{ord} g = \infty$, то все степени g^n различны

$\Rightarrow H$ тоже бесконечно ($|H| = |\langle g \rangle| = \infty$).

Если $\operatorname{ord} g = m < \infty$, то по опр. m - это минимальное натур. число, для которого $g^m = e$.

Покажем, что $H = \underbrace{\{\underset{= e}{g^0}, g^1, g^2, \dots, g^{m-1}\}}_{\text{все различны}}$

Рассмотрим произв. эл-т g^n из H, и разделим n с ост. на m.

$\Rightarrow g^n = g^{m\cdot q + r} = (\underset{\substack{\shortparallel \\ e,\ \text{т.к. } m = \operatorname{ord} g}}{g^m})^q \cdot g^r = e^q \cdot g^r = g^r$, где $0 \le r < m$

Т.е. $\forall$ эл-т из H имеет вид g^r, где r меняется от 0 до $m-1$

и $\Rightarrow |H| = |\langle g \rangle| = m = \operatorname{ord} g$ ■

Замеч: Попутно доказано, что если $G = \langle a \rangle$ - цикл. группа бесконечного порядка, то все степени a^n различны.

Утв 2: Все циклич. группы одинакового порядка изоморфны.

□ Покажем, что если $|G| = |\langle a \rangle| = \infty$, то $G \cong (\mathbb{Z}, +)$ - группа целых чис. по слож.

Рассмотрим отображение $\varphi(a^n) = n$ $(= n \cdot 1)$ (оно задано корректно, все степени a^n различны).

Это биективное отображение (инъект. и сюръект.) и это гомоморфизм:

т.к. $\varphi(a^m \cdot a^n) = \varphi(a^{m+n}) = m+n = \varphi(a^m) + \varphi(a^n) \Rightarrow \varphi$ - изоморфизм.

Если порядок G конечен $(|G| = |\langle a \rangle| = n)$, то покажем

$G \cong (\mathbb{Z}_n, +)$

$G = \{e, a, a^2, \dots, a^{n-1}\}$

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

Рассм. $\varphi: G \to \mathbb{Z}_n$, $\varphi(a^k) = \bar{k}$ - биекция и гомоморфизм (т.к. сохр. операцию)

$\Rightarrow$ изоморфизм. ∎

Свойства гомоморфизма

Пусть f - гомоморфизм, $f: (G_1, *, e_1) \to (G_2, \circ, e_2)$

нейтр. эл-ты

(т.е. $\forall a, b \in G_1 \quad f(a * b) = f(a) \circ f(b)$)

① $f(e_1) = e_2$, т.е. нейтр. эл-т всегда переходит в нейтр. („единицу")

② $f(g^{-1}) = (f(g))^{-1} \quad \forall g \in G_1$, т.е. обратный переходит в обратный

□ 1) Покажем (по опр.), что эл-т $f(e_1)$ - нейтр. в G_2

$$\left.\begin{aligned} f(g) \circ f(e_1) &= f(g * e_1) = f(g) \\ f(e_1) \circ f(g) &= f(e_1 * g) = f(g) \end{aligned}\right| \Rightarrow \text{по опр.}$$

$\Rightarrow f(e_1)$ - нейтр. эл-т. в G_2, т.е. $f(e_1) = e_2$

2) $$\left.\begin{aligned} f(g^{-1}) \circ f(g) &= f(g^{-1} * g) = f(e_1) = e_2 \\ f(g) \circ f(g^{-1}) &= f(g * g^{-1}) = f(e_1) = e_2 \end{aligned}\right| \Rightarrow \begin{aligned} &f(g^{-1}) \text{ - обратный к } f(g) \text{ в } G_2, \text{ т.е.} \\ &f(g^{-1}) = (f(g))^{-1} \end{aligned}$$ ∎

Замеч.: Если f - изоморфизм, то f^{-1} тоже изоморфизм.

□ f^{-1} - это биекция (т.к. f - биекция)

$$f^{-1}(f(a) \circ f(b)) = f^{-1}(f(a * b)) = a * b = f^{-1}(f(a)) * f^{-1}(f(b))$$

$\Rightarrow$ гомоморфизм $\Rightarrow$ изоморфизм ■

Опр: Ядром гомоморфизма $f: G_1 \to G_2$ наз. мн-во

$\mathrm{Ker}\, f = \{a \in G_1 \mid f(a) = e_2\} \subseteq G_1$ (подмн-во в G_1)

- все эл-ты G_1, которые переходят в нейтральный.

Пример: $f = \det : GL_n(\mathbb{R}) \to \mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot)$

все невыр. матрицы $n \times n$

$\mathrm{Ker} \det = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\} \Rightarrow \mathrm{Ker} \det = SL_n(\mathbb{R})$ - спец. лин. группа

Утв: Пусть $f: G_1 \to G_2$ - гомоморфизм групп.

Тогда f - мономорфизм (т.е. $\forall x_1 \neq x_2 \quad f(x_1) \neq f(x_2)$, т.е. f - инъективное отображение (вложение))

$\Leftrightarrow \mathrm{Ker}\, f = e_1$ (т.е. $\mathrm{Ker}\, f$ - тривиально)

(Замеч: $\mathrm{Ker}\, f \neq 0$, т.к. $f(e_1) = e_2$, т.е. e_1 есть)

□ „$\Rightarrow$" (Необх.) Если $\forall x_1 \neq x_2 \quad f(x_1) \neq f(x_2)$,

то $\forall x \neq e_1 \quad f(x) \neq f(e_1) = e_2 \Rightarrow$ ядро тривиально.

„$\Leftarrow$" (Дост.) ОП Предположим, что $\exists x_1 \neq x_2$, что $f(x_1) = f(x_2)$.

Домножим справа на $(f(x_2))^{-1} \Rightarrow$

$f(x_1) \circ (f(x_2))^{-1} = e_2$

По св.② гом-зма $\to$ „ $f(x_1) \circ f(x_2^{-1}) \overset{\text{по опр.}}{=} f(x_1 * x_2^{-1}) = e_2$

Но ядро тривиально по усл. $\Rightarrow x_1 * x_2^{-1} = e_1 \Leftrightarrow x_1 = x_2$ ① ■

Утв: Ядро $\forall$ гомоморфизма $f: G_1 \to G_2$ явл. подгруппой в G_1

□ (Критерий подгруппы: H – подгруппа в $G \Leftrightarrow \forall a, b \in H \quad a \cdot b^{-1} \in H$)

Если a и $b \in \operatorname{Ker} f$, то $f(a \cdot b^{-1}) \overset{\text{опр.}}{=} f(a) \cdot f(b^{-1}) \overset{②}{=} \underbrace{f(a)}_{= e_2} \cdot (\underbrace{f(b)}_{= e_2})^{-1} =$

$= e_2 \cdot e_2^{-1} = e_2$

$\Rightarrow a \cdot b^{-1} \in \operatorname{Ker} f \Rightarrow$ по крит. подгруппы $\operatorname{Ker} f$ явл. подгр. в G_2 ■

Опр: Прямым произведением групп G_1 и G_2 наз. их прямое (декартово) произведение как множество (т.е. $G_1 \times G_2$), снабжённое операцией:

$$(x_1, y_1) \star (x_2, y_2) = (x_1 \circ x_2, \; y_1 * y_2)$$

$x_1 \in G_1$, $y_1 \in G_2$ $\quad$ $x_2 \in G_1$, $y_2 \in G_2$ $\quad$ $\circ$ – операция в G_1 $\quad$ $*$ – операция в G_2

В примерах: $(\sqrt[n]{1}, \cdot) \cong (\mathbb{Z}_n, +)$

$(\{-1, 1\}, \cdot) \cong (\mathbb{Z}_2, +) = (\{\bar{0}, \bar{1}\}, +)$

Обознач: $G_1 \times G_2$ – прямое произв. групп G_1 и G_2.

$\mathbb{Z}_2 = (\{\bar{0}, \bar{1}\}, +)$

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

$\mathbb{Z}_2 \times \mathbb{Z}_2$

эл-ты в $\mathbb{Z}_2 \times \mathbb{Z}_2$

★	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

Вопрос: $\mathbb{Z}_2 \times \mathbb{Z}_2 \overset{?}{\cong} \mathbb{Z}_4$ – нет

$\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(0,0) – нейтр. элемент

В $\mathbb{Z}_2 \times \mathbb{Z}_2$ все эл-ты имеют порядок не выше 2

В $\mathbb{Z}_4 = \langle \bar{1} \rangle \quad \operatorname{ord} \bar{1} = 4$