# 1 Группы, абелевы группы, циклические группы. Вложение моноида в группу

**Определение 1.1** (Группа)**.** Группа - моноид, в котором все элементы обратимы

**Определение 1.2** (Тривиальная группа)**.** Тривиальная группа - группа, состоящая из одного элемента

**Теорема 1.3.** *Если $M$ - моноид и $G \subseteq M$ - подмножество обратимых элементов, то $G$ - группа*

Доказательство. $G \subseteq M$ следовательно $G$ ассоциативна, $e$ - обратимый следовательно $G$ имеет нейтральный элемент. Надо доказать замкнутость: $x * y \in G$

$x', y'$ - обратные к $x$ и $y$ элементы, тогда

$$(x * y) * (y' * x') = x * (y * y') * x' = x * e * x' = x * x' = e$$

$$(y' * x') * (x * y) = y' * (x' * x) * y = y * e * y' = y * y' = e$$

$x * y$ обратим $\Rightarrow xy \in G$

если $x \in G$, то $x' * x = x * x' = e$, тогда $x'$ имеет обратный элемент, тогда $x' \in G$. Любой элемент $G$ имеет обратный.

$G$ - группа. Теорема доказана.

$\square$

**Определение 1.4** (Абелева группа)**.** Абелева группа - группа, в которой $xy = yx$

**Определение 1.5** (Циклическая группа)**.** Циклическая группа - группа, порождённая одним элементом. $< a >$ - циклическая группа порождённая $a$.

$(\omega, +, 0)$ изоморфно бесконечной циклической группе

моноид типа $(i, j)$ изоморфен конечной циклической группе

**Теорема 1.6.** *$\mathcal{G} = \langle a \rangle$, тогда $\mathcal{G} \cong (\mathbb{Z}, +)$ или $\mathcal{G} \cong (\mathbb{Z}_n, +)$ для некоторого $n$*

Доказательство. Пусть $\mathcal{M}$ - подмоноид, порождённый $a$. $\mathcal{M}$ - циклический

1. $\mathcal{M} \overset{\text{h}}{\simeq} (\omega, +, 0)$

   $x \in \mathcal{M}\ x^{-1}\ xx^{-1} = e$

   $x \in \mathcal{M}\ x \neq e\ x^{-1} \neq \mathcal{M}$

   $$h(x) + h(x^{-1}) = h(xx^{-1}) = h(e) = 0$$

   $h(x) = h(x^{-1}) = 0$

   $h(x) = h(x^{-1}) = e$

   $x \in \mathcal{M}$

   $h(x^{-1}) = -h(x)$

2. $\mathcal{M}$ - конечный $(i, j)$ моноид, если $i > 0$, то в $\mathcal{M}$ есть нееденичный идемпотент, следовательно он необратимый, следовательно в группе должно быть $i = 0$

   $$a^x a^y = \begin{cases} a^{x+y} & \text{, если } x + y < j \\ a^{(x+y) \pmod j} & \text{, если } x + y \geq j \end{cases}$$

   $\mathcal{M}$ - группа

   $$a^x = a^{j-x} = a^{j \pmod j} = e$$

   $\mathcal{M}$ - группа порождённая $a$, $\mathcal{M} = \mathcal{G}$

   $h : a^x \to x$

□

**Теорема 1.7.** *В циклической группе существуют нетривиальные группы тогда и только тогда когда она бесконечна или $n$ в $(\mathbb{Z}_n, +)$ составное*

Доказательство. 1. $\Rightarrow$ пусть имеется $(\mathbb{Z}_n, +)$, $n$ - простое, $a \neq 0$, $a < n$, $a$ и $n$ взаимно простые, следовательно $xa + yn = 1$. пусть $b \in \mathbb{Z}$, тогда

$$b = b \cdot 1 = b(ax + yn) = (bx)a + (by)n$$

$$(\underbrace{a + a + ... + a}_{bx}) \mod n = (b - (by)n) \mod n = b \mod n = b$$

Таким образом любые подгруппы, содержащие не только 0 содержат $\mathbb{Z}_n$

2. $\Leftarrow$

   (a) бесконечная циклическая группа имеет нетривиальную подгруппу

   (b) пусть $n = xy$, тогда $(\mathbb{Z}_{xy}, +) \supseteq \{0, x, 2x, ..., (y-1)x\}$

$\square$

**Теорема 1.8** (Теорема Гротендика). *Каждый коммутативный моноид, в котором все элементы сократимы можно вложить в группу*

Доказательство. Пусть $M$ - коммутативный моноид, $G' = M \times M = (a, b)$, где $a, b \in M$, $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$, $(e_1, e_2)$ - нейтральный элемент.

Пусть $(a, b) \equiv (c, d) \Leftrightarrow ad = bc$. Является ли $\equiv$ конгруэнтностью?

1. $(a, b) \equiv (a, b)$, $ab = ba$
2. $(a, b) \equiv (c, d)$, $ad = bc \Rightarrow cb = da \Rightarrow (c, d) \equiv (a, b)$
3. $(a, b) \equiv (c, d) \equiv (u, v) \Rightarrow (a, b) \equiv (u, v)$

Надо доказать:

$$(a_1, b_1) \equiv (a_2, b_2), (c_1, d_1) \equiv (c_2, d_2) \Rightarrow (a_1c_1, b_1d_1) \equiv (a_2c_2, b_2d_2)$$

$$\begin{aligned}
&(a_1, b_1) \equiv (a_2, b_2), (c_1, d_1) \equiv (c_2, d_2) \Rightarrow \\
&\qquad a_1b_2 = b_1a_2, c_1d_2 = d_1c_2 \Rightarrow a_1b_2c_1d_2 = b_1a_2d_1c_2 \Rightarrow \\
&\qquad\qquad (a_1c_1)(b_2d_2) = (b_1d_1)(a_2c_2) \Rightarrow \\
&\qquad\qquad\qquad (a_1c_1, b_1d_1) \equiv (a_2c_2, b_2d_2)
\end{aligned}$$

$(a, b) \equiv (c, d) \Leftrightarrow ad = bc$ - конгруэнтность

Пусть $G = {}^{G'}/_{\equiv}$ надо доказать что $G$ - группа и $M$ вкладывается в $G$

$$ab = ba \Rightarrow abe = ab = ba = bae \Rightarrow (ab, ba) \equiv (e, e)$$

$$\widehat{(a, b)} * \widehat{(b, a)} = \widehat{(ab, ba)} = \widehat{(e, e)}$$

$\Rightarrow$ каждый элемент $G$ имеет обратный $\Rightarrow$ $G$ - группа

Пусть $h : M \to G$ и $h(a) = \widehat{(a, e)}$, тогда

$$h(ab) = \widehat{(ab, e)} = \widehat{(a, e)}\widehat{(b, e)} = h(a)h(b)$$

$$h(e) = \widehat{(e, e)}$$

$h$ - гомоморфизм

Пусть $h(a) = h(b)$

$$\widehat{(a, e)} = \widehat{(b, e)} \Rightarrow (a, e) \equiv (b, e) \Rightarrow ae = eb \Rightarrow a = b$$

следовательно $h$ - инъекция, следовательно $h$ - вложение

$\square$

**Пример 1.9** (Пример на теорему Гротендика)**.**