1 Группы

Определение 1.1:
Группа - моноид, в котором все элементы обратимы

Определение 1.2:
Тривиальная группа - группа, состоящая из одного элемента

Теорема 1.1. *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.

$\square$

Теорема 1.2 (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 $a, b \in M$, $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$, (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:

$$(a_1, b_1) \equiv (a_2, b_2), (c_1, d_1) \equiv (c_2, d_2) \Rightarrow (a_1 c_1, b_1 d_1) \equiv (a_2 c_2, b_2 d_2)$$

$$(a_1,b_1)\equiv(a_2,b_2),(c_1,d_1)\equiv(c_2,d_2)\Rightarrow$$
$$a_1b_2=b_1a_2, c_1d_2=d_1c_2\Rightarrow a_1b_2c_1d_2=b_1a_2d_1c_2\Rightarrow$$
$$(a_1c_1)(b_2d_2)=(b_1d_1)(a_2c_2)\Rightarrow$$
$$(a_1c_1,b_1d_1)\equiv(a_2c_2,b_2d_2)$$

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

□

Пример 1.1:
Пример на теорему Гротендика:

Теорема 1.3. *G - группа тогда и только тогда, когда*

1. $(xy)z=x(yz)$
2. $xe=x$
3. $xx^{-1}=e$

Доказательство. 1. $\Rightarrow$ по определению группы

2. $\Leftarrow$

   $(xy)z = x(yz) \Rightarrow G$ ассоциативна

   $xx^{-1} = e \Rightarrow x^{-1}x = e$

   Надо доказать: $ex = x$ для любого x

$$x^{-1}x = x^{-1}xe = x^{-1}x(x^{-1}x)(x^{-1}x)^{-1} = x^{-1}(xx^{-1})x(x^{-1}x)^{-1} = x^{-1}ex(x^{-1}x)^{-1} = (x^{-1}x)(x^{-1}x)^{-1} = e \quad (1)$$

$$ex = (xx^{-1})x = x(x^{-1}x) = xe = x$$

   G - группа

$\square$

Следствие. *Группы образуют многообразие в сигнатуре* $(*, e, ^{-1})$

Определение 1.3:
Аддитивная группа - группа со сложением

Пример 1.2:
Примеры аддитивных групп: $(\mathbb{Z}; +)$

Определение 1.4:
Мультипликативная группа - группа с умножением

Пример 1.3:
Примеры мультипликативных групп: $(\mathbb{Q}; \cdot)$

Определение 1.5:
Множество вычетов -

Пример 1.4:

Определение 1.6:
Матричные группы: носитель группы - $M_n^*(R)$ и $det \neq 0$

Пример 1.5:
Примеры матричных групп:

1. $(M_n^*, \cdot, E, ^{-1})$ - группа, не коммутативная
2. $det = \pm 1$ - группа

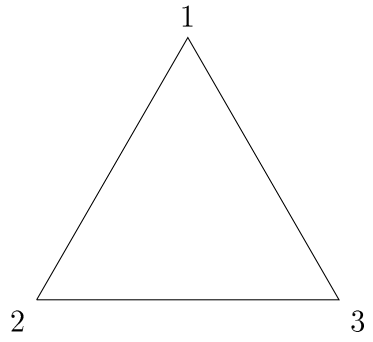
3. O_n - ортогональные, $(O_n, \cdot, E, ^{-1})$ - группа

Определение 1.7:
Группа перестановок - группа перестановок множества S называется группа всех биекций $f : S \to S$. $(F, \circ, e, ^{-1})$

Пример 1.6:

Определение 1.8:
Симметрическая группа порядка n: S - конечно и состоит из n элементов. $(A, \circ, e, ^{-1})$, A - множество автоморфизмов $h : S \to S$

Пример 1.7:
Пример симметрической группы:



$A = \{e, r_1, r_2, s_1, s_2, s_3\}$

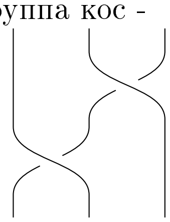
- e - тождественное преобразование
- r_1, r_2 - поворот на $120°$ и $240°$ соответственно
- s_1, s_2, s_3 - оборот вокруг высоты, идущей из первой, второй и третьей вершины соответственно

$$\mathbf{D}_3 = (A, \circ)$$

Таблица умножения $\circ$

	e	r_1	r_2	s_1	s_2	s_3
e	e	x	e	x	e	x
r_1	e	x	e	x	e	x
r_2	e	x	e	x	e	x
s_1	e	x	e	x	e	x
s_2	e	x	e	x	e	x
s_3	x	x	e	x	e	x

Определение 1.9:
Группа кос -



ещё:

потом соображу как длиннее сделать

Теорема 1.4. *Если G - полугруппа, то G является группой тогда и только тогда, когда любое уравнение вида $ax = b$ или $xa = b$, $(a, b \in G)$ имеет в G решение*

Доказательство. 1. $\Rightarrow$

$$\begin{aligned} ax &= b & xa &= b \\ a^{-1}ax &= a^{-1}b & xaa^{-1} &= ba^{-1} \\ x &= a^{-1}b & x &= ba^{-1} \end{aligned}$$

любое уравнение вида $ax = b$ или $xa = b$, $(a, b \in G)$ имеет в G решение

2. $\Leftarrow$ по теореме 1.3

   (a) по определению полугруппы

   (b) $ax = a \Rightarrow x = e$ $ya = b$, имеет решение $y = d$, $da = b$

$$be = dae = da = b \Rightarrow be = b$$

(c) для любых $ax = e$ существует решение $x = a^{-1}$ - обратное к a

$\square$

Теорема 1.5. *1.* $(ab)^{-1} = b^{-1}a^{-1}$

2. $(a^{-1})^{-1} = a$

Определение 1.10:
Абелева группа - группа, в которой $xy = yx$