1 Основные понятия

Определение 1.1:
Сигнатура - множество имён операций с указанием их местности.

$$(f^{(2)}, g^{(3)}, h^{(0)}), (+^{(2)}, \cdot^{(3)})$$

$h^{(0)}$ - символ константы, V - имена переменных

Определение 1.2:
Терм - выражение, составленное из символов сигнатуры и переменных

1. $x \in V$, x - терм
2. c - символ константы, c - терм
3. если $t_1, ..., t_n$ - термы и f - символ n-местной операции, то $f(t_1, ..., t_n)$ - терм

Пример 1.1:
Примеры термов: $-(x), -(0), +(x, y), 2 + 3 + a$

Определение 1.3:
Замкнутый терм - терм, не содержащий переменных

Определение 1.4:
Универсальная алгебра - пусть Σ - сигнатура, тогда *универсальная алгебра* сигнатуры Σ - это пара вида (A, I), где A - произвольное непустое множество, а I - некоторое отображение, которое для всякого $p^{(m)} \in \Sigma$, $I(p^{(m)})$ - n-местной операции на множестве

Пример 1.2:
Пример универсальной алгебры: пусть $\Sigma = (+^{(2)}, \cdot^{(2)}, -^{(1)}, 0^{(0)}, 1^{(0)})$, тогда

$$\begin{aligned} R = (\mathbb{R}, I) : & I(+) - \text{сложение} \\ & I(\cdot) - \text{умножение} \\ & I(-) - \text{вычитание} \\ & I(0) - 0 \\ & I(1) - 1 \end{aligned}$$

Определение 1.5:
$\mathbb{R}$ называется **основным множеством** или носителем алгебры, а I - интерпретацией или интерпретирующей функцией

Определение 1.6:
Состояние - функция, приписывающая переменной некоторый элемент носителя $\sigma : V \to A$

Пример 1.3:
Пример состояний: $\sigma = \{(x, 3), (y, -8)\}, \sigma(x) = 3$

Определение 1.7:
Значение терма на состоянии - значение того выражения, в котором переменные заменены их значениями

1. t - переменная, $\sigma(t)$ - по определению состояния
2. t - символ константы, $I(t) = \sigma(t_1) = v_1$
3. если $t_1, ..., t_n$ - термы и $\sigma(t_1) = v_1, ..., \sigma(t_n) = v_n$, то $\sigma(t) = I(f)(v_1, ..., v_n)$

2 Изоморфизм

Определение 2.1:
Изоморфизм - Пусть Σ - сигнатура, $\mathbf{A} = (A, I)$, $\mathbf{B} = (B, J)$ - универсальные алгебры сигнатуры Σ, тогда изоморфизм между $\mathbf{A}$ и $\mathbf{B}$ - это $h : \mathbf{A} \to \mathbf{B}$ - биективная функция, которая удовлетворяет следующему условию:

$$h(I(f_i)(a_1, ..., a_n)) = J(f_i)(h(a_1), ..., h(a_n))$$

для любых $a_1, ..., a_n$ и $f_i \in \Sigma$

Пример 2.1:
Пример изоморфизма: пусть $\Sigma = (f^{(2)})$, $\mathbf{A} = (\mathbb{R}, +)$, $\mathbf{B} = (\mathbb{R}, \cdot)$

Надо доказать:

$$h(a_1 + a_2) = h(a_1) \cdot h(a_2)$$

$a_1, a_2 \in \mathbb{R}$

Пусть $h(x) = e^x$, тогда

$$h(a_1 + a_2) = e^{a_1+a_2} = e^{a_1} \cdot e^{a_2} = h(a_1) \cdot h(a_2) \blacksquare$$

Теорема 2.1. *h - изоморфизм между A и B, то h^{-1} - изоморфизм между B и A*

Доказательство. пусть $b_1, ..., b_{n_i} \in B$, тогда надо доказать

$$h^{-1}(J(f_i)(b_1, ..., b_{n_i})) = I(f_i)(h^{-1}(b_1), ..., h^{-1}(b_{n_i}))$$

Так как $b_1 = h(a_1), ..., b_{n_i} = h(a_{n_i})$,

$$I(f_i)(h^{-1}(b_1), ..., h^{-1}(b_{n_i})) = I(f_i)(h^{-1}(h(a_1)), ..., h^{-1}(h(a_{n_i}))) = I(f_i)(a_1, ..., a_{n_i})$$

По определению изоморфизма

$$h^{-1}(J(f_i)(b_1, ..., b_{n_i})) = h^{-1}(h(I(f_i)(a_1, ..., a_{n_1}))) = I(f_i)(a_1, ..., a_{n_1})$$

Из этих двух равенств следует то, что надо доказать $\square$

Определение 2.2:
Системы, между которыми существует изоморфизм называют **изоморфными**

$$\mathbf{A} \simeq \mathbf{B}$$

операции в изоморфных системах обладают одними и теми же свойствами

Определение 2.3:
$t(x_1, ..., x_n)$ - терм t не содержит других переменных кроме $x_1, ..., x_n$

Определение 2.4:
Пусть $\mathbf{A}$ - алгебра, $a_1, ..., a_n$ - элементы алгебры $\mathbf{A}$, тогда

$$t(a_1, ..., a_n) = \sigma(t), \sigma(x_1) = a_1, ..., \sigma(x_n) = a_n$$

Теорема 2.2. *h - изоморфизм между $\mathbf{A} = (A, I)$ и $\mathbf{B} = (B, J)$, то для любого терма $t(x_1, ..., x_n)$ и любых $a_1, ..., a_n$ выполняется*

$$h(t^{\mathbf{A}}(a_1, ..., a_n)) = t^{\mathbf{B}}(h(a_1), ..., h(a_n))$$

Доказательство. Индукция по построению терма t

1. $t = x$
$$t^{\mathbf{A}}(a) = a \Leftrightarrow h(t^{\mathbf{A}}(a)) = h(a) \Leftrightarrow t^{\mathbf{B}}(h(a)) = h(a)$$

2. $t = c$
$$\sigma(c) = I(c) = J(c) \Rightarrow t^{\mathbf{A}} = I(c), t^{\mathbf{B}} = J(c) \Rightarrow h(I(c)) = J(c)$$
по определению гомоморфизма

3. $t = f(t_1, ..., t_k)$
$$\begin{aligned} &h(t^{\mathbf{A}}(a_1, ..., a_n)) = \\ &\quad h(I(f)(t_1^{\mathbf{A}}(a_1, ..., a_n), ..., t_k^{\mathbf{A}}(a_1, ..., a_n))) = \\ &\quad J(f)(h(t_1^{\mathbf{A}}(a_1, ..., a_n)), ..., h(t_k^{\mathbf{A}}(a_1, ..., a_n))) = \\ &\quad J(f)(t_1^{\mathbf{B}}(h(a_1), ..., h(a_n)), ..., t_k^{\mathbf{B}}(h(a_1), ..., h(a_n)) = \\ &\quad t^{\mathbf{B}}(h(a_1), ..., h(a_n)) \end{aligned}$$

□

Пример 2.2:
Доказать что $\mathcal{A} = (\mathbb{R}; \cdot) \ncong \mathcal{B} = (\mathbb{R}^+; \cdot)$

Доказательство. Предположим что существует изоморфизм $h : \mathcal{A} \to \mathcal{B}$, тогда

$h(0) = x, x \in \mathbb{R}^+$
$$x = h(0) = h(0 \cdot 0) = h(0) \cdot h(0) = x^2$$
$$x = x^2 \Rightarrow x = 1$$

$h(1) = y, y \in \mathbb{R}^+$
$$y = h(1) = h(1 \cdot 1) = h(1) \cdot h(1) = y^2$$
$$y = y^2 \Rightarrow y = 1$$

$h(0) = 1 = h(1)$ - противоречие (h не биективна). Утверждение не верно. □

Пример 2.3:
Доказать что $\mathcal{A} = (\mathbb{R}; +) \ncong \mathcal{B} = (\mathbb{R}; \cdot)$

Доказательство. Предположим что существует изоморфизм $h : \mathcal{B} \to \mathcal{A}$, тогда
$h(0) = x, h(1) = y; x, y \in \mathbb{R}$ □

3 Гомоморфизм

4 Декартовы произведения

5 Полугруппы и моноиды

Определение 5.1:
Полугруппа - многообразие заданное множеством

$$(x * y) * z = x * (y * z)$$

Теорема 5.1. *Значение терма не зависит от расстановки скобок (Ассоциативный закон)*

$$t = t_1 * t_2 = (a_1 a_2 ... a_m)(a_{m+1} ... a_n) = a_1 a_2 ... a_n$$

Доказательство. Индукция по длине t
Базис: $n = 1$, нет скобок
Шаг: для $n - 1$ верно, тогда

1. $m = n - 1$
$$t = t_1 * a_n = (a_1 a_2 ... a_m) * a_n = a_1 a_2 ... a_n$$

2. $1 \leq m \leq n - 1$

$$t = t_1 * t_2 = (a_1 a_2 ... a_m)(a_{m+1} ... a_n) = (a_1 a_2 ... a_m)(a_{m+1} ... a_{n-1}) a_n = (a_1 a_2 ... a_{n-1}) a_n = a_1 a_2 ... a_n$$

□

Определение 5.2:
e_l называется **нейтральным слева** в подгруппе, если $e_l * a = a$ для всех a, e_r называется **нейтральным справа** в подгруппе, если $a * e_r = a$ для всех a, e - нейтральный слева и справа

Пример 5.1:
Примеры нейтрального элемента:

Теорема 5.2. *Если существуют нейтральный слева и нейтральный справа то они равны*

Доказательство.
$$e_l = e_l * e_r = e_r$$
□

Следствие. *Если нейтральный элемент существует, то он единственный.*

Определение 5.3:
Моноид - подгруппа с нейтральным элементом

Пример 5.2:
Примеры моноидов:

Определение 5.4:
Свободный моноид - моноид, элементами которого являются конечные последовательности (строки) элементов носителя моноида. Свободный моноид на множестве $A \neq \emptyset$ это $\mathcal{A} = (A^*; \&)$

Теорема 5.3. *Любой моноид, порождённый элементами множества, на котором есть свободный моноид, является гомоморфным образом этого моноида*

Доказательство. Пусть $A \neq \emptyset$, $\mathcal{A} = (A^*; \&)$,
$\mathcal{B} = (\left\{t^{\mathcal{B}}(a_1, ..., a_n) : a_1, ..., a_n \in A\right\}; *)$ и $h : \mathcal{A} \to \mathcal{B}$ - Гомоморфизм

$$h(a_1 ... a_n) = (a_1, ..., a_n)^{\mathcal{B}}$$

$$h(\varepsilon) = e^{\mathcal{B}}$$

Надо доказать свойство гомоморфизма:

$$h(u\&v) = h(u) * h(v)$$

Пусть $u = a_1...a_n$, $v = a'_1...a'_n$, тогда

$$h(u\&v) = h(uv) = h(a_1...a_n a'_1...a'_n) = (a_1...a_n a'_1...a'_n)^{\mathcal{B}}$$

$$h(u) * h(v) = h(a_1...a_n) * h(a'_1...a'_n) = \\ (a_1...a_n)^{\mathcal{B}} * (a'_1...a'_n)^{\mathcal{B}} = (a_1...a_n a'_1...a'_n)^{\mathcal{B}}$$

Из этого следует что $h(u\&v) = h(u) * h(v)$ $\square$

Пример 5.3:
Примеры свободных моноидов и их гомоморфных образов:

Определение 5.5:
Циклический моноид - моноид порождённый одним элементом. $< a >$ - циклический моноид, порождённый элементом a.
$e, a, a^1, a^2, a^3, ...$ - элементы моноида $< a >$

1. $a^i \neq a^j$ при $i \neq j$
   $h :< a >\to (\{a\}^*; \&)$, $h(a^i) = i$ - изоморфизм.

2. $a^i = a^j$ при $i \neq j$

$$k = i + (k - i) = i + y(j - i) + r$$

$$r = (k - i) mod (j - i)$$

$$r < j - i$$

   тогда

$$a^k = a^i \underbrace{a^{j-i}...a^{j-i}}_{y} a^r = \\ (a^i a^{j-i}) \underbrace{a^{j-i}...a^{j-i}}_{y-1} a^r \overset{(a^i a^{j-i} = a^{i+j-i} = a^j = a^i)}{=} a^i \underbrace{a^{j-i}...a^{j-i}}_{y-1} a^r = \\ a^i a^r = a^{i+r} (r < j - i; i + r < j)$$

	e	a	a^2
e	a	a	a^2
a	a	a^2	a
a^2	a^2	a	a^2

Пример 5.4:
Пример циклическокококого моноида: $< a >= (\{e, a, ...\}; *)$

Таблица умножения $(*)$ -

Теорема 5.4. *Если j - наименьшее число такое что $a^i = a^j$ для какого-то $i < j$, то $< a >$ содержит ровно j элементов*

Доказательство.

$$\underbrace{e, a^1, ..., a^{j-1}}_{\text{нет равных}}, \underbrace{a^j = a^i, a^{j+1} = a^{i+1}, ...}_{\text{повоторяющиеся}}$$

если j - номер наименьшего повтора, тогда

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

$$x + y = k, \qquad \begin{aligned} k &= i + (k - i \cdot z + r \\ r &= (k - i)mod(j - i) \\ a^k &= a^{i+z} \end{aligned}$$

$$a^{x+y} = a^k = a^{i+(x+y-i)mod(j-i)}$$

□

Определение 5.6:
Идемпотент - элемент моноида a, такой что $a^2 = a$

Пример 5.5:
Примеры идемпотентов:

Определение 5.7:
Моноид типа $(i, j-i)$ - моноид с элементами

$$???$$

Теорема 5.5. *В моноиде типа $(i, j-i)$, где $i > 0$ существует идемпотент $b \neq e$*

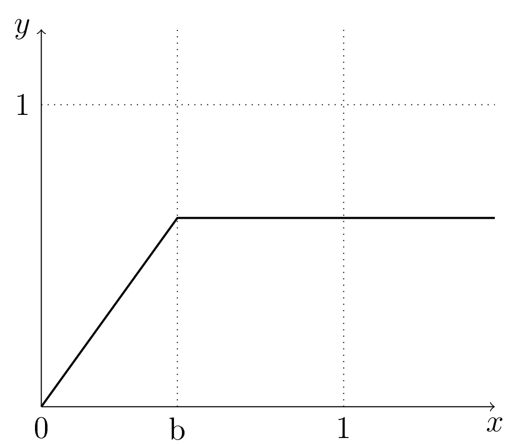
Доказательство. $\square$

Пример 5.6:
Пример чего-то:

Определение 5.8:
b_l - левый обратный для элемента a, если $b_l * a = e$, b_r - правый обратный для элемента a, если $a * b_l = e$, b - обратный для элемента a, если $b * a = a * b = e$

Доказать что множество функций этого вида замкнуты относительно композиции:

$$f(x) = \begin{cases} ax & \text{при } x < b \\ ab & \text{при } x \geq b \end{cases}$$



Доказательство. $\square$

Пример 5.7:
Пример изоморфизма: Доказать

$$(P(A \cup B); \cup, \cap) \cong (P(A); \cup, \cap) \times (P(B); \cup, \cap)$$

где $P(A)$ - множество всех подмножеств множества A

Доказательство. Надо доказать

$$h(x_1 \cup x_2) = h(x_1) \cup h(x_2)$$
$$h(x_1 \cap x_2) = h(x_1) \cap h(x_2)$$

и h - биекция

По сути функция h должна выдавать пару, первая часть которой состоит из элементов A, вторая из B □

Пример 5.8:
Пример полугруппы: является ли $(\omega, GCD())$ полугруппой

Доказательство. Предположим что является, надо доказать

$$GCD(GCD(x, y), z) = GCD(x, GCD(y, z))$$

1. $\Rightarrow$ Пусть $d : d|GCD(x, y), d|z$

   Надо доказать $d|GCD(y, z)$, $d|x$

$$d|GCD(x, y) \Rightarrow d|x$$
$$d|GCD(x, y) \Rightarrow d|y$$
$$d|x, d|y \Rightarrow d|GCD(y, z)$$

2. $\Leftarrow$ также

□

Пример 5.9:
Построить все моноиды из двух элементов $\{e, x\}$

$$A_1 = (\{e, x\}; *_1), A_2 = (\{e, x\}; *_2)$$

Все остальные или изоморфны или тривиальны

Теорема 5.6. *Если в конечном моноиде каждый элемент имеет первый обратимый, то существует правый обратимый*

Доказательство. Предположим обратное: Если в конечном моноиде каждый элемент имеет первый обратимый, то хотя бы для одного не существует правый обратимый: $ab_r \neq e$ для всех b_r

НЕ ДОКАЗАНО □

Таблица умножения ($*_1$)

	e	x
e	e	x
x	x	e

Таблица умножения ($*_2$)

	e	x
e	e	x
x	x	x

6 Группы

Определение 6.1:
Группа - моноид, в котором все элементы обратимы

Определение 6.2:
Тривиальная группа - группа, состоящая из одного элемента

Теорема 6.1. *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.

□

Теорема 6.2 (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 $a, b \in M$, $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$, (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 6.1:
Пример на теорему Гротендика:

Теорема 6.3. *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 6.3:
Аддитивная группа - группа со сложением

Пример 6.2:
Примеры аддитивных групп:

Определение 6.4:
Мультипликативная группа - группа с умножением

Пример 6.3:
Примеры мультипликативных групп:

Определение 6.5:
Множество вычетов -

Пример 6.4:

Определение 6.6:
Матричные группы: носитель группы - $M_n^*(R)$ и $det \neq 0$

Пример 6.5:
Примеры матричных групп:

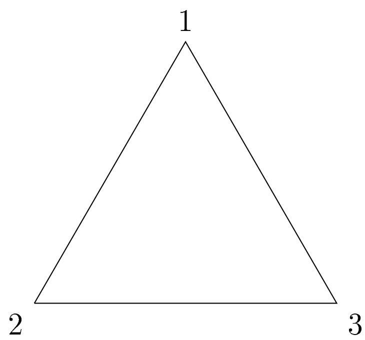
1. $(M_n^*, \cdot, E, ^{-1})$ - группа, не коммутативная
2. $det = \pm 1$ - группа
3. O_n - ортогональные, $(O_n, \cdot, E, ^{-1})$ - группа

Определение 6.7:
Группа перестановок - группа перестановок множества S называется группа всех биекций $f : S \to S$. $(F, \circ, e, ^{-1})$

Пример 6.6:

Определение 6.8:
Симметрическая группа порядка n: S - конечно и состоит из n элементов. $(A, \circ, e, ^{-1})$, A - множество автоморфизмов $h : S \to S$

Пример 6.7:
Пример симметрической группы:



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

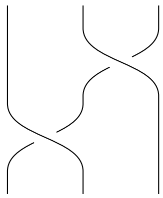
- e - тождественное преобразование
- r_1, r_2 - поворот на $120°$ и $240°$ соответственно
- s_1, s_2, s_3 - оборот вокруг высоты, идущей из первой, второй и третьей вершины соответственно

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

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 6.9:
Группа кос -



ещё:

потом соображу как длиннее сделать

Теорема 6.4. *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. $\Rightarrow$

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

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

2. $\Leftarrow$ по теореме 6.3

   (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

□

Теорема 6.5. *1.* $(ab)^{-1} = b^{-1}a^{-1}$

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

Определение 6.10:
Абелева группа - группа, в которой $xy = yx$