1 Полугруппы и моноиды

Определение 1.1:
Полугруппа - многообразие заданное множеством

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

Теорема 1.1. *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 1.2:
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 1.1:
Примеры нейтрального элемента:

Теорема 1.2. *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 1.3:
Моноид - подгруппа с нейтральным элементом

Пример 1.2:
Примеры моноидов:

Определение 1.4:
Свободный моноид - моноид, элементами которого являются конечные последовательности (строки) элементов носителя моноида. Свободный моноид на множестве $A \neq \emptyset$ это $\mathcal{A} = (A^*; \&)$

Теорема 1.3. *Любой моноид, порождённый элементами множества, на котором есть свободный моноид, является гомоморфным образом этого моноида*

Доказательство. Пусть $A \neq \emptyset$, $\mathcal{A} = (A^*; \&)$,
$\mathcal{B} = (\{t^{\mathcal{B}}(a_1, ..., a_n) : a_1, ..., a_n \in A\}; *)$ 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 $h(u\&v) = h(u) * h(v)$ □

Пример 1.3:
Примеры свободных моноидов и их гомоморфных образов:

Определение 1.5:
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

$$a^k = a^i \underbrace{a^{j-i}...a^{j-i}}_{y} a^r =$$

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

$$a^i a^r = a^{i+r} (r < j - i; i + r < j)$$

Пример 1.4:
Пример циклическококококого моноида: $< a >= (\{e, a, ...\}; *)$

Таблица умножения $(*)$ -

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

Теорема 1.4. *Если j - наименьшее число такое что $a^i = a^j$ для какого-то $i < j$, то $< a >$ содержит ровно j элементов*

Доказательство.

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

если j - номер наименьшего повтора, тогда

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

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

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

□

Определение 1.6:
Идемпотент - элемент моноида a, такой что $a^2 = a$

Пример 1.5:
Примеры идемпотентов:

Определение 1.7:
Моноид типа $(i, j-i)$ - моноид с элементами

???

Теорема 1.5. *В моноиде типа $(i, j-i)$, где $i > 0$ существует идемпотент $b \neq e$*

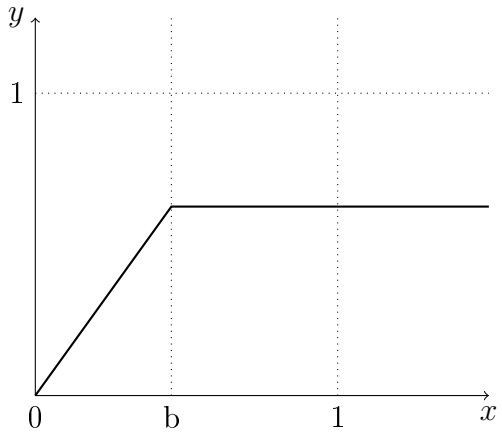
Доказательство. □

Пример 1.6:
Пример чего-то:

Определение 1.8:
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. □

Пример 1.7:
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 1.8:
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 1.9:
Построить все моноиды из двух элементов $\{e,x\}$

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

Таблица умножения $(*_1)$

	e	x
e	e	x
x	x	e

Таблица умножения $(*_2)$

	e	x
e	e	x
x	x	x

Все остальные или изоморфны или тривиальны

Теорема 1.6. *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 $\square$