1 Полугруппы и моноиды

Определение 1.1:
Полугруппа - многообразие заданное множеством

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

Пример 1.1:
Примеры полугрупп:

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 полугруппе, если $e_l * a = a$ для всех a, e_r называется **нейтральным справа** в полугруппе, если $a * e_r = a$ для всех a, e - нейтральный слева и справа

Пример 1.2:
Примеры нейтрального элемента:

$(\omega, +)$ - 0, $(\omega, \cdot)$ - 1, (ω, max) - 0, (ω, min) - нет нейтрального

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 - полугруппа с нейтральным элементом ИЛИ

Моноид - это элементы многообразия, которые определяются равенствами

$$\begin{cases} x * (y * z) = (x * y) * z \\ x * e = x \\ e * x = x \end{cases}$$

Пример 1.3:
Примеры моноидов:

$(\omega, +, 0)$, $(\omega, \cdot, 1)$, $(\omega, max, 0)$

A^A - множество одноместных функций из A в A $h = f \circ g$, если $h(a) = g(f(a))$ для любого $a \in A$

Доказать что $(A^A, \circ)$ - моноид

Доказательство. $e(a) = a$ для всех a, тогда

$$\left.\begin{aligned} (e \circ f)(a) = f(e(a)) = f(a) \\ (f \circ e)(a) = e(f(a)) = f(a) \end{aligned}\right\} e \circ f = f \circ e = f$$

e - нейтральный элемент

$$((f \circ g)h)(a) = h(f \circ g)(a) = h(g(f(a)))$$
$$(f(g \circ h))(a) = (g \circ h)(f(a)) = h(g(f(a)))$$
$$((f \circ g)h)(a) = (f(g \circ h))(a)$$

Выполняется ассоциативность, соответственно $(A^A, \circ, e)$ - моноид

□

Определение 1.4:
Свободный моноид - моноид, элементами которого являются конечные последовательности (строки) элементов носителя моноида. Свободный моноид на множестве $A \neq \emptyset$ это $\mathcal{A} = (A^*; \&, \varepsilon)$, A^* - множество всех слов в алфавите A, $\&$ - конкатенация, ε - пустое слово.

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

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

Пример 1.4:
Примеры свободных моноидов и их гомоморфных образов:

Пусть дан алфавит $A = \{1\}$, который образует $A^* = \{\varepsilon, 1, 11, ...\}$ и моноид $\mathcal{A} = (A^*; \&, \varepsilon)$, тогда

1. $mathcalB = (1; \cdot, 1)$, порождённый элементами A является гомоморфным образом $\mathcal{A}$, $h : A \to B$, $h(1...1) = 1$

2. $mathcalC = (\omega; +, 0)$, порождённый элементами A(натуральные числа можно получить сложением единицы) является гомоморфным образом $\mathcal{A}$, $h : A \to B$, $h(\underbrace{1...1}_{n}) = n$

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 1.5:

Пример циклическокококого 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.

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

если j - номер наименьшего повтора, тогда

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

$$x + y = k, \qquad k = i + (k - i \cdot z + r$$

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

$$a^k = a^{i+z}$$

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

□

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

Пример 1.6:
Примеры идемпотентов: $(\omega; +)$ - 0

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

$$???$$

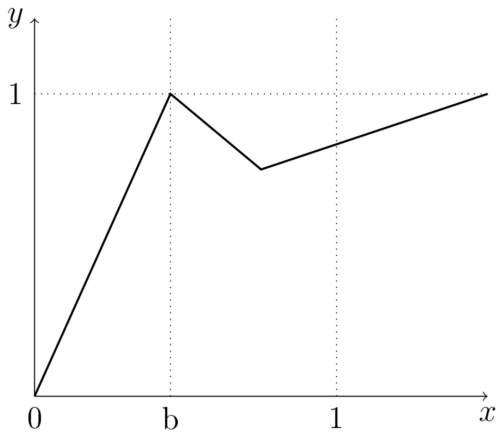
Теорема 1.5. *В моноиде типа $(i, j-i)$, где $i > 0$ существует идемпотент $b \neq e$*

Доказательство. □

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 $b * a = a * b = e$

Пример 1.7:
Пример чего-то: 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 1.8:
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 $\square$

Пример 1.9:
Пример полугруппы: является ли $(\omega, \text{НОД}())$ полугруппой

Доказательство. Предположим что является, надо доказать

$$\text{НОД}(\text{НОД}(x, y), z) = \text{НОД}(x, \text{НОД}(y, z))$$

1. $\Rightarrow$ Пусть $d : d|\text{ НОД}(x, y), d|z$

   Надо доказать $d|\text{ НОД}(y, z)$, $d|x$

$$d|\text{ НОД}(x, y) \Rightarrow d|x$$
$$d|\text{ НОД}(x, y) \Rightarrow d|y$$
$$d|x, d|y \Rightarrow d|\text{ НОД}(y, z)$$

2. $\Leftarrow$ также

$\square$

Пример 1.10:
Построить все моноиды из двух элементов $\{e, x\}$

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

Доказать их ассоциативность: $a * (b * c) = (a * b) * c$

Таблица умножения ($*_1$)

	e	x
e	e	x
x	x	e

Таблица умножения ($*_2$)

	e	x
e	e	x
x	x	x

1. $a = e$
$$e * (b * c) = b * c = (e * b) * c$$
2. $b = e$ также
3. $c = e$ также
4. $a = b = c = x$

$$x * (x * x) = x * e = e * x = (x * x) * x$$

Все остальные моноиды или изоморфны или тривиальны

Теорема 1.6. *Если в конечном моноиде каждый элемент имеет левый обратный, то существует правый обратный*

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

НЕ ДОКАЗАНО □

Определение 1.9:
Сократимый слева (справа) - такой элемент моноида, что из $ax = ay$ ($xa = ya$) следует $x = y$

Пример 1.11:
$(\mathbb{Z}, +, 0)$, $x + a = y + a \Rightarrow x = y$

Теорема 1.7. *Неединичные идемпотенты несократимы*

Доказательство. $a \cdot a = a = e \cdot a$ но $a \neq e$, соответственно a несократим справа, $a \cdot a = a = a \cdot e$ но $a \neq e$, соответственно a несократим слева

a несократим □

Теорема 1.8. *Все обратимые слева(справа) элементы сократимы слева(справа)*

Доказательство. Пусть a - обратимый слева, тогда $ax = ay \Rightarrow b_l ax = b_l ay \Rightarrow ex = ey \Rightarrow x = y$, следовательно a - сократимый слева □

Пример 1.12:
$(\mathbb{Z}^+, \cdot, 1)$, обратимый только 1, сократимы все. (Какой к половым органам это пример?)