1 Подгруппы и моноиды

Определение 1.1:
Подгруппа - 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 $A \neq \emptyset$, $\mathcal{A} = (A^*; \&)$,
$\mathcal{B} = (\left\{t^{\mathcal{B}}(a_1, ..., a_n) : a_1, ..., a_n \in A\right\}; *)$ 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 1.3:
Примеры свободных моноидов и их гомоморфных образов:

Определение 1.5:
Циклический моноид - моноид порождённый одним элементом. $< a >$ - циклический моноид, порождённый элементом a.

$e, a, a^1, a^2, a^3, \ldots$ - элементы моноида $< a >$

1. $a^i \neq a^j$ при $i \neq j$

   $h :< a > \rightarrow (\{a\}^*; \&)$, $h(a^i) = i$ - 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

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

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

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

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

Таблица умножения $(*)$ -

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