Полугруппы

Михайлова Инна Анатольевна

Институт математики и естественных наук.
Кафедра алгебры и фундаментальной информатики.

18 ноября 2018 г.

Операции на множестве

Определение

n-арной операцией на множестве A называется отображение $f : A^n \to A$. При $n = 1$ операция называется унарной, при $n = 2$ бинарной, при $n = 3$ тернарной.

Операции на множестве

Определение

n-арной операцией на множестве A называется отображение $f : A^n \to A$. При $n = 1$ операция называется унарной, при $n = 2$ бинарной, при $n = 3$ тернарной.

- Отображение $a \mapsto -a$ на множестве действительных чисел называется унарный минус;

Операции на множестве

Определение

n-арной операцией на множестве A называется отображение $f : A^n \to A$. При $n = 1$ операция называется унарной, при $n = 2$ бинарной, при $n = 3$ тернарной.

- Отображение $a \mapsto -a$ на множестве действительных чисел называется унарный минус;
- Сложение и умножение на множестве натуральных чисел являются бинарными операциями;

Операции на множестве

Определение

n-арной операцией на множестве A называется отображение $f : A^n \to A$. При $n = 1$ операция называется унарной, при $n = 2$ бинарной, при $n = 3$ тернарной.

- Отображение $a \mapsto -a$ на множестве действительных чисел называется унарный минус;
- Сложение и умножение на множестве натуральных чисел являются бинарными операциями;
- "Вычитание" не является операцией на множестве натуральных чисел.

Операции на множестве

Определение

n-арной операцией на множестве A называется отображение $f : A^n \to A$. При $n = 1$ операция называется унарной, при $n = 2$ бинарной, при $n = 3$ тернарной.

- Отображение $a \mapsto -a$ на множестве действительных чисел называется унарный минус;
- Сложение и умножение на множестве натуральных чисел являются бинарными операциями;
- "Вычитание" не является операцией на множестве натуральных чисел.

Произвольную бинарную операцию будем обозначать $\cdot$ (эта операция не обязательно будет совпадать с умножением). Также вместо $\cdot(a, b)$ будем писать ab, опуская знак операции.

Полугруппы и свободная полугруппа

Определение

Множество $(A, \cdot)$ с бинарной операцией на ней называется полугруппой, если выполняется тождество ассоциативности:

$$\forall a, b, c \in A \quad (ab)c = a(bc)$$

Полугруппы и свободная полугруппа

Определение

Множество $(A, \cdot)$ с бинарной операцией на ней называется полугруппой, если выполняется тождество ассоциативности:

$$\forall a, b, c \in A \quad (ab)c = a(bc)$$

Пусть A — непустое множество (алфавит), элементами которого являются буквы.

Полугруппы и свободная полугруппа

Определение

Множество $(A, \cdot)$ с бинарной операцией на ней называется полугруппой, если выполняется тождество ассоциативности:

$$\forall a, b, c \in A \quad (ab)c = a(bc)$$

Пусть A — непустое множество (алфавит), элементами которого являются буквы. Словом называется последовательность букв. Тогда A^+ — это множество всех слов над алфавитом A.

Полугруппы и свободная полугруппа

Определение

Множество $(A, \cdot)$ с бинарной операцией на ней называется полугруппой, если выполняется тождество ассоциативности:

$$\forall a, b, c \in A \quad (ab)c = a(bc)$$

Пусть A — непустое множество (алфавит), элементами которого являются буквы. Словом называется последовательность букв. Тогда A^+ — это множество всех слов над алфавитом A. Зададим на A^+ операцию приписывания одного слова к другому (конкатенацию). Иными словами, для $w_1 = x_1 \cdots x_n, w_2 = y_1 \cdots y_m \in A^+$ имеем $w_1 w_2 = x_1 \cdots x_n y_1 \cdots y_m$.

Полугруппы и свободная полугруппа

Определение

Множество $(A, \cdot)$ с бинарной операцией на ней называется полугруппой, если выполняется тождество ассоциативности:

$$\forall a, b, c \in A \quad (ab)c = a(bc)$$

Пусть A — непустое множество (алфавит), элементами которого являются буквы. Словом называется последовательность букв. Тогда A^+ — это множество всех слов над алфавитом A. Зададим на A^+ операцию приписывания одного слова к другому (конкатенацию). Иными словами, для $w_1 = x_1 \cdots x_n, w_2 = y_1 \cdots y_m \in A^+$ имеем $w_1 w_2 = x_1 \cdots x_n y_1 \cdots y_m$. Тогда относительно новой операции множество A^+ образует полугруппу (проверьте, что ассоциативность выполняется), которая называется свободной полугруппой над алфавитом A.

Гомоморфизмы полугрупп

Определение

Пусть $(A, \cdot), (B, *)$ — полугруппы. Отображение $f : A \to B$ называется гомоморфизмом, если

$$\forall a_1, a_2 \in A \quad f(a_1 \cdot a_2) = f(a_1) * f(a_2)$$

Гомоморфизмы полугрупп

Определение

Пусть $(A, \cdot), (B, *)$ — полугруппы. Отображение $f\colon A \to B$ называется гомоморфизмом, если

$$\forall a_1, a_2 \in A \quad f(a_1 \cdot a_2) = f(a_1) * f(a_2)$$

Рассмотрим полугруппы $(\mathbb{R}, +), (\mathbb{R}^+, \cdot)$ относительно обычных операций сложения и умножения действительных чисел. Рассмотрим отображение $f\colon x \mapsto e^x$. Тогда

$$f(a_1 + a_2) = e^{a_1 + a_2} = e^{a_1} \cdot e^{a_2} = f(a_1) \cdot f(a_2),$$

следовательно, f — гомоморфизм.

Гомоморфизмы полугрупп

Определение

Пусть $(A, \cdot), (B, *)$ — полугруппы. Отображение $f\colon A \to B$ называется гомоморфизмом, если

$$\forall a_1, a_2 \in A \quad f(a_1 \cdot a_2) = f(a_1) * f(a_2)$$

Рассмотрим полугруппы $(\mathbb{R}, +), (\mathbb{R}^+, \cdot)$ относительно обычных операций сложения и умножения действительных чисел. Рассмотрим отображение $f\colon x \mapsto e^x$. Тогда

$$f(a_1 + a_2) = e^{a_1 + a_2} = e^{a_1} \cdot e^{a_2} = f(a_1) \cdot f(a_2),$$

следовательно, f — гомоморфизм.

Определение

Пусть $(A, \cdot), (B, *)$ — полугруппы. Гомоморфизм $f\colon A \to B$ называется изоморфизмом полугрупп, если f — биекция. В этом случае полугруппы $A \cong B$ называются изоморфными.

Гомоморфизмы полугрупп

Определение

Пусть $(A, \cdot), (B, *)$ — полугруппы. Отображение $f\colon A \to B$ называется гомоморфизмом, если

$$\forall a_1, a_2 \in A \quad f(a_1 \cdot a_2) = f(a_1) * f(a_2)$$

Рассмотрим полугруппы $(\mathbb{R}, +), (\mathbb{R}^+, \cdot)$ относительно обычных операций сложения и умножения действительных чисел. Рассмотрим отображение $f\colon x \mapsto e^x$. Тогда

$$f(a_1 + a_2) = e^{a_1 + a_2} = e^{a_1} \cdot e^{a_2} = f(a_1) \cdot f(a_2),$$

следовательно, f — гомоморфизм.

Отображение из примера является изоморфизмом полугрупп

Гомоморфный образ полугруппы

Определение

Полугруппа S_2 является гомоморфным образом полугруппы S_1, если существует сюръективный гомоморфизм $f : S_1 \to S_2$. В этом случае пишут $S_2 = f(S_1)$.

Гомоморфный образ полугруппы

Определение

Полугруппа S_2 является гомоморфным образом полугруппы S_1, если существует сюръективный гомоморфизм $f\colon S_1 \to S_2$. В этом случае пишут $S_2 = f(S_1)$.

Упражнение. Докажите, что полугруппа $(\mathbb{R}, \cdot)$ не может быть гомоморфным образом $(\mathbb{N}, +)$.

Гомоморфный образ полугруппы

Определение

Полугруппа S_2 является гомоморфным образом полугруппы S_1, если существует сюръективный гомоморфизм $f\colon S_1 \to S_2$. В этом случае пишут $S_2 = f(S_1)$.

Упражнение. Докажите, что полугруппа $(\mathbb{R}, \cdot)$ не может быть гомоморфным образом $(\mathbb{N}, +)$.

Теорема

Любая полугруппа является гомоморфным образом свободной полугруппы.

Доказательство теоремы

Лемма

Пусть A — непустое множество, S — полугруппа, $\varphi\colon A \to S$. Тогда существует гомоморфизм $f\colon A^+ \to S$, который продолжает φ, т.е. $\forall a \in A \quad f(a) = \varphi(a)$.

Доказательство теоремы

Лемма

Пусть A — непустое множество, S — полугруппа, $\varphi\colon A \to S$. Тогда существует гомоморфизм $f\colon A^+ \to S$, который продолжает φ, т.е. $\forall a \in A \quad f(a) = \varphi(a)$.

Зададим отображение $f\colon A^+ \to S$ по правилу:

$$\forall a \in A \quad f(a) = \varphi(a),$$

$$\forall w = a_1 a_2 \ldots a_n \in A^+ \quad f(w) = \varphi(a_1)\varphi(a_2)\ldots\varphi(a_n)$$

Доказательство теоремы

Лемма

Пусть A — непустое множество, S — полугруппа, $\varphi\colon A \to S$. Тогда существует гомоморфизм $f\colon A^+ \to S$, который продолжает φ, т.е. $\forall a \in A \quad f(a) = \varphi(a)$.

Зададим отображение $f\colon A^+ \to S$ по правилу:

$$\forall a \in A \quad f(a) = \varphi(a),$$

$$\forall w = a_1 a_2 \dots a_n \in A^+ \quad f(w) = \varphi(a_1)\varphi(a_2)\dots\varphi(a_n)$$

Тогда $\forall w = a_1 a_2 \dots a_n, v = b_1 b_2 \dots b_m \in A^+$ имеем

$$f(wv) = \varphi(a_1)\varphi(a_2)\dots\varphi(a_n)\varphi(b_1)\varphi(b_2)\dots\varphi(b_m) = f(w)f(v)$$

Следовательно, f — гомоморфизм.

Доказательство теоремы

Рассмотрим в качестве множества A любое множество, мощность которого больше или равно мощности множества S. Тогда существует биекция $g\colon S \to A' \subseteq A$.

Доказательство теоремы

Рассмотрим в качестве множества A любое множество, мощность которого больше или равно мощности множества S. Тогда существует биекция $g\colon S \to A' \subseteq A$. Пусть $s \in S$ — произвольный элемент. Построим отображение $\varphi\colon A \to S$ по правилу:

$$\varphi(x) = \begin{cases} g^{-1}(x), & x \in A' \\ s, & \text{иначе.} \end{cases}$$

Доказательство теоремы

Рассмотрим в качестве множества A любое множество, мощность которого больше или равно мощности множества S. Тогда существует биекция $g\colon S \to A' \subseteq A$. Пусть $s \in S$ — произвольный элемент. Построим отображение $\varphi\colon A \to S$ по правилу:

$$\varphi(x) = \begin{cases} g^{-1}(x), & x \in A' \\ s, & \text{иначе.} \end{cases}$$

Тогда φ — сюръективное отображение.

Доказательство теоремы

Рассмотрим в качестве множества A любое множество, мощность которого больше или равно мощности множества S. Тогда существует биекция $g\colon S \to A' \subseteq A$. Пусть $s \in S$ — произвольный элемент. Построим отображение $\varphi\colon A \to S$ по правилу:

$$\varphi(x) = \begin{cases} g^{-1}(x), & x \in A' \\ s, & \text{иначе.} \end{cases}$$

Тогда φ — сюръективное отображение. Тогда по лемме его можно продлить до сюръективного гомоморфизма $f\colon A^+ \to S$.

Полугруппа преобразований

Определение

Пусть X — непустое множество. Преобразованием множества X будем называть произвольное отображение $\tau\colon X \to X$. Множество всех преобразований обозначим через $\mathrm{T}(X)$

Полугруппа преобразований

Определение

Пусть X — непустое множество. Преобразованием множества X будем называть произвольное отображение $\tau\colon X \to X$. Множество всех преобразований обозначим через $\mathrm{T}(X)$

В качестве операции рассмотрим композицию отображений:
$\tau_1 \circ \tau_2(x) = \tau_2(\tau_1(x))$

Полугруппа преобразований

Определение

Пусть X — непустое множество. Преобразованием множества X будем называть произвольное отображение $\tau\colon X \to X$. Множество всех преобразований обозначим через $\mathrm{T}(X)$

Лемма

Композиция отображений ассоциативна.

Полугруппа преобразований

Определение

Пусть X — непустое множество. Преобразованием множества X будем называть произвольное отображение $\tau\colon X \to X$. Множество всех преобразований обозначим через $\mathrm{T}(X)$

Лемма

Композиция отображений ассоциативна.

Пусть $(x, y) \in (\tau_1 \circ \tau_2) \circ \tau_3$. Тогда
$\exists z_2 \in X \quad (x, z_2) \in \tau_1 \circ \tau_2, (z_2, y) \in \tau_3$.

Полугруппа преобразований

Определение

Пусть X — непустое множество. Преобразованием множества X будем называть произвольное отображение $\tau\colon X \to X$. Множество всех преобразований обозначим через $\mathrm{T}(X)$

Лемма

Композиция отображений ассоциативна.

Пусть $(x, y) \in (\tau_1 \circ \tau_2) \circ \tau_3$. Тогда
$\exists z_2 \in X \quad (x, z_2) \in \tau_1 \circ \tau_2, (z_2, y) \in \tau_3.$
$\exists z_1 \in X \quad (x, z_1) \in \tau_1, (z_1, z_2) \in \tau_2, (z_2, y) \in \tau_3.$

Полугруппа преобразований

Определение

Пусть X — непустое множество. Преобразованием множества X будем называть произвольное отображение $\tau\colon X \to X$. Множество всех преобразований обозначим через $\mathrm{T}(X)$

Лемма

Композиция отображений ассоциативна.

Пусть $(x, y) \in (\tau_1 \circ \tau_2) \circ \tau_3$. Тогда
$\exists z_2 \in X \quad (x, z_2) \in \tau_1 \circ \tau_2, (z_2, y) \in \tau_3$.
$\exists z_1 \in X \quad (x, z_1) \in \tau_1, (z_1, z_2) \in \tau_2, (z_2, y) \in \tau_3$.
$(x, z_1) \in \tau_1, (z_1, y) \in \tau_2 \circ \tau_3 \Rightarrow (x, y) \in \tau_1 \circ (\tau_2 \circ \tau_3)$

Полугруппа преобразований

Определение

Пусть X — непустое множество. Преобразованием множества X будем называть произвольное отображение $\tau\colon X \to X$. Множество всех преобразований обозначим через $\mathrm{T}(X)$

Определение

Полугруппа $(\mathrm{T}(X), \circ)$ называется полугруппой преобразований множества X. Если $|X| = n$, то $\mathrm{T}(X)$ обозначается через T_n.

Полугруппа преобразований

Определение

Пусть X — непустое множество. Преобразованием множества X будем называть произвольное отображение $\tau\colon X \to X$. Множество всех преобразований обозначим через $\mathrm{T}(X)$

Определение

Полугруппа $(\mathrm{T}(X), \circ)$ называется полугруппой преобразований множества X. Если $|X| = n$, то $\mathrm{T}(X)$ обозначается через T_n.

Отображение n- элементного множества можно также записывать в виде матрицы $\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}$

Полугруппа преобразований

Определение

Пусть X — непустое множество. Преобразованием множества X будем называть произвольное отображение $\tau\colon X \to X$. Множество всех преобразований обозначим через $\mathrm{T}(X)$

Определение

Полугруппа $(\mathrm{T}(X), \circ)$ называется полугруппой преобразований множества X. Если $|X| = n$, то $\mathrm{T}(X)$ обозначается через T_n.

Отображение n- элементного множества можно также записывать в виде матрицы $\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 4 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 5 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 5 & 4 & 4 & 2 \end{pmatrix}$$

Теорема Кэли

Определение

Полугруппа S_1 называется вложимой в полугруппу S_2, если существует инъективный гомоморфизм $g\colon S_1 \to S_2$.

Теорема Кэли

Определение

Полугруппа S_1 называется вложимой в полугруппу S_2, если существует инъективный гомоморфизм $g\colon S_1 \to S_2$.

Теорема (Кэли)

Любую полугруппу можно вложить в полугруппу преобразований на подходящем множестве.

Теорема Кэли

Определение

Полугруппа S_1 называется вложимой в полугруппу S_2, если существует инъективный гомоморфизм $g\colon S_1 \to S_2$.

Теорема (Кэли)

Любую полугруппу можно вложить в полугруппу преобразований на подходящем множестве.

"Единицей" в полугруппе S называется такой элемент $a \in S$, что для любого $s \in S \quad as = sa = s$. Если в полугруппе S нет единицы, то добавим специальный элемент $1 \notin S, S^1 = S \cup \{1\}$ и положим $\forall s \in S \quad 1 \cdot s = s \cdot 1 = s, 1 \cdot 1 = 1$. Иначе $S^1 = S$

Доказательство теоремы Кэли

Для каждого $b \in S$ определим преобразование ρ_b на множестве S^1 по правилу: $\rho_b(x) = x \cdot b$

Доказательство теоремы Кэли

Для каждого $b \in S$ определим преобразование ρ_b на множестве S^1 по правилу: $\rho_b(x) = x \cdot b$
Покажем, что $\rho_{ab} = \rho_a \circ \rho_b$:

$$\forall \quad x \in S \rho_{ab}(x) = x \cdot ab = (x \cdot a)b = \rho_b(\rho_a(x)) = (\rho_a \circ \rho_b)(x)$$

Следовательно, отображение $a \mapsto \rho_a$ является гомоморфизмом

Доказательство теоремы Кэли

Для каждого $b \in S$ определим преобразование ρ_b на множестве S^1 по правилу: $\rho_b(x) = x \cdot b$
Покажем, что $\rho_{ab} = \rho_a \circ \rho_b$:

$$\forall \quad x \in S \rho_{ab}(x) = x \cdot ab = (x \cdot a)b = \rho_b(\rho_a(x)) = (\rho_a \circ \rho_b)(x)$$

Следовательно, отображение $a \mapsto \rho_a$ является гомоморфизмом
Покажем, что это отображение инъективно: Пусть $\rho_{a_1} = \rho_{a_2}$.
Возьмем $x = 1$, тогда $\rho_{a_1}(1) = \rho_{a_2}(1)$. Откуда $a_1 = a_2$.

Подполугруппы

Определение

Подмножество S_1 называется подполугруппой полугруппы S, если $\forall x, y \in S_1 \quad xy \in S_1$.

Договариваются считать пустое множество подполугруппой любой полугруппы.

Подполугруппы

Определение

Подмножество S_1 называется подполугруппой полугруппы S, если $\forall x, y \in S_1 \quad xy \in S_1$.

Договариваются считать пустое множество подполугруппой любой полугруппы.

- Множество четных натуральных чисел является подполугруппой полугруппы всех натуральных чисел по сложению;

Подполугруппы

Определение

Подмножество S_1 называется подполугруппой полугруппы S, если $\forall x, y \in S_1 \quad xy \in S_1$.

Договариваются считать пустое множество подполугруппой любой полугруппы.

- Множество четных натуральных чисел является подполугруппой полугруппы всех натуральных чисел по сложению;
- Множество всех слов над алфавитом $\{0, 1\}$, в которые 0 входит четное число раз является подполугруппой соответствующей свободной полугруппы;

Подполугруппы

Определение

Подмножество S_1 называется подполугруппой полугруппы S, если $\forall x, y \in S_1 \quad xy \in S_1$.

Договариваются считать пустое множество подполугруппой любой полугруппы.

- Множество четных натуральных чисел является подполугруппой полугруппы всех натуральных чисел по сложению;
- Множество всех слов над алфавитом $\{0, 1\}$, в которые 0 входит четное число раз является подполугруппой соответствующей свободной полугруппы;
- Множество всех преобразований множества $\{1, \ldots, n\}$, которые являются перестановками, образуют подполугруппу полугруппы преобразований этого множества.

Подполугруппы

Определение

Подмножество S_1 называется подполугруппой полугруппы S, если $\forall x, y \in S_1 \quad xy \in S_1$.

Договариваются считать пустое множество подполугруппой любой полугруппы.

Лемма

Пусть $f : S_1 \to S_2$ — гомоморфизм полугрупп. Тогда $f(S_1)$ — подполугруппа полугруппы S_2.

Подполугруппы

Определение

Подмножество S_1 называется подполугруппой полугруппы S, если $\forall x, y \in S_1 \quad xy \in S_1$.

Договариваются считать пустое множество подполугруппой любой полугруппы.

Лемма

Пусть $f : S_1 \to S_2$ — гомоморфизм полугрупп. Тогда $f(S_1)$ — подполугруппа полугруппы S_2.

Пусть $y_1, y_2 \in f(S_1)$, тогда $\exists x_1, x_2 \in S_1 \quad y_1 = f(x_1), y_2 = f(x_2)$. Откуда $y_1 y_2 = f(x_1) f(x_2) = f(x_1 x_2) \in f(S_1)$.

Подполугруппы

Определение

Подмножество S_1 называется подполугруппой полугруппы S, если $\forall x, y \in S_1 \quad xy \in S_1$.

Договариваются считать пустое множество подполугруппой любой полугруппы.

Лемма

Пусть $f : S_1 \to S_2$ — гомоморфизм полугрупп. Тогда $f(S_1)$ — подполугруппа полугруппы S_2.

Пусть $y_1, y_2 \in f(S_1)$, тогда $\exists x_1, x_2 \in S_1 \quad y_1 = f(x_1), y_2 = f(x_2)$. Откуда $y_1 y_2 = f(x_1)f(x_2) = f(x_1 x_2) \in f(S_1)$.

Упражнение. Докажите, что пересечение двух подполугрупп полугруппы S является подполугруппой S. Что можно сказать про объединение?

Порождающие множества для полугрупп

Определение

Пусть S — полугруппа, $M \subseteq S$. Тогда полугруппой, порожденной множеством M называется пересечение всех подполугрупп, содержащих M. Обозначение $< M >$.

Порождающие множества для полугрупп

Определение

Пусть S — полугруппа, $M \subseteq S$. Тогда полугруппой, порожденной множеством M называется пересечение всех подполугрупп, содержащих M. Обозначение $< M >$.

Теорема

$< M >= \{m_1 \dots m_k \mid m_i \in M, k \in \mathbb{N}\}$

Порождающие множества для полугрупп

Определение

Пусть S — полугруппа, $M \subseteq S$. Тогда полугруппой, порожденной множеством M называется пересечение всех подполугрупп, содержащих M. Обозначение $< M >$.

Теорема

$< M >= \{m_1 \dots m_k \mid m_i \in M, k \in \mathbb{N}\}$

Обозначим множество справа через S_1. Тогда S_1 — подполугруппа S и $M \subseteq S_1$. Так как $< M >$ пересечение всех таких полугрупп, то $< M > \subseteq S_1$.

Порождающие множества для полугрупп

Определение

Пусть S — полугруппа, $M \subseteq S$. Тогда полугруппой, порожденной множеством M называется пересечение всех подполугрупп, содержащих M. Обозначение $< M >$.

Теорема

$< M >= \{m_1 \dots m_k \mid m_i \in M, k \in \mathbb{N}\}$

Обозначим множество справа через S_1. Тогда S_1 — подполугруппа S и $M \subseteq S_1$. Так как $< M >$ пересечение всех таких полугрупп, то $< M > \subseteq S_1$.

Рассмотрим произвольную подполугруппу, которая содержит в себе множество M, тогда она должна содержать всевозможные произведения элементов из M, то есть S_1 является подмножеством любой такой подполугруппы, в том числе и $< M >$.

Порождающие множества для полугрупп

Определение

Пусть S — полугруппа, $M \subseteq S$. Тогда полугруппой, порожденной множеством M называется пересечение всех подполугрупп, содержащих M. Обозначение $< M >$.

Теорема

$< M >= \{m_1 \dots m_k \mid m_i \in M, k \in \mathbb{N}\}$

Обозначим множество справа через S_1. Тогда S_1 — подполугруппа S и $M \subseteq S_1$. Так как $< M >$ пересечение всех таких полугрупп, то $< M > \subseteq S_1$.
Рассмотрим произвольную подполугруппу, которая содержит в себе множество M, тогда она должна содержать всевозможные произведения элементов из M, то есть S_1 является подмножеством любой такой подполугруппы, в том числе и $< M >$.

Полугруппа $(\mathbb{N}, \cdot)$ порождается множеством всех простых чисел и 1.

Полугрупповые коды

Определение

Множество слов X над алфавитом A называется полугрупповым кодом, если каждое слово из полугруппы $< X >$ можно единственным образом представить в виде конкатенации слов из X.

Полугрупповые коды

Определение

Множество слов X над алфавитом A называется полугрупповым кодом, если каждое слово из полугруппы $< X >$ можно единственным образом представить в виде конкатенации слов из X.

1. Множество слов $\{a, ba, ab\}$ не является полугрупповым кодом, так как $aba = aba$;

Полугрупповые коды

Определение

Множество слов X над алфавитом A называется полугрупповым кодом, если каждое слово из полугруппы $< X >$ можно единственным образом представить в виде конкатенации слов из X.

1. Множество слов $\{a, ba, ab\}$ не является полугрупповым кодом, так как $aba = aba$;
2. Множество слов $\{ab, ba\}$ является полугрупповым кодом.

Полугрупповые коды

Определение

Множество слов X над алфавитом A называется полугрупповым кодом, если каждое слово из полугруппы $< X >$ можно единственным образом представить в виде конкатенации слов из X.

Лемма

Множество слов $X = \{ba^i b \mid i \in \mathbb{N}\}$ является полугрупповым кодом.

Полугрупповые коды

Определение

Множество слов X над алфавитом A называется полугрупповым кодом, если каждое слово из полугруппы $< X >$ можно единственным образом представить в виде конкатенации слов из X.

Лемма

Множество слов $X = \{ba^i b \mid i \in \mathbb{N}\}$ является полугрупповым кодом.

Очевидно, что каждое слово из X^+ имеет вид $ba^{j_1} b^2 a^{j_2} b^2 \cdots b^2 a^{j_k} b$, откуда получаем требуемое.

Полугрупповые коды

Определение

Множество слов X над алфавитом A называется полугрупповым кодом, если каждое слово из полугруппы $< X >$ можно единственным образом представить в виде конкатенации слов из X.

Лемма

Множество слов $X = \{ba^i b \mid i \in \mathbb{N}\}$ является полугрупповым кодом.

Очевидно, что каждое слово из X^+ имеет вид $ba^{j_1}b^2a^{j_2}b^2 \cdots b^2a^{j_k}b$, откуда получаем требуемое.

Теорема

Любая свободная полугруппу со счетным числом образующих изоморфна некоторой подполугруппе свободной полугруппы над алфавитом из двух букв.

Доказательство теоремы

Теорема

Любая свободная полугруппа со счетным числом образующих изоморфна некоторой подполугруппе свободной полугруппы над алфавитом из двух букв.

Доказательство теоремы

Теорема

Любая свободная полугруппа со счетным числом образующих изоморфна некоторой подполугруппе свободной полугруппы над алфавитом из двух букв.

Пусть $S = A^+$, где A — счетно. Тогда $A = \{a_1, a_2, \ldots\}$.

Доказательство теоремы

Теорема

Любая свободная полугруппа со счетным числом образующих изоморфна некоторой подполугруппе свободной полугруппы над алфавитом из двух букв.

Пусть $S = A^+$, где A — счетно. Тогда $A = \{a_1, a_2, \ldots\}$.
Рассмотрим отображение $g\colon a_i \mapsto ba^i b$, которое является биекцией из A в множество слов X. Это отображение можно продолжить до гомоморфизма $f\colon A^+ \to X^+$.

Доказательство теоремы

Теорема

Любая свободная полугруппа со счетным числом образующих изоморфна некоторой подполугруппе свободной полугруппы над алфавитом из двух букв.

Пусть $S = A^+$, где A — счетно. Тогда $A = \{a_1, a_2, \ldots\}$.
Рассмотрим отображение $g\colon a_i \mapsto ba^i b$, которое является биекцией из A в множество слов X. Это отображение можно продолжить до гомоморфизма $f\colon A^+ \to X^+$.
f является инъекцией, так как $f(a_{j_1} \cdots a_{j_n}) = g(a_{j_1}) \cdots g(a_{j_n}) \in X^+$, а так как X — полугрупповой код, то такое разбиение на слова из X единственно. Очевидно, что f — сюръекция. Откуда f — изоморфизм, а X^+ — подполугруппа $\{a, b\}^+$.

Классификация циклических полугрупп

Определение

Полугруппа S называется циклической, если она порождается одним элементом

Классификация циклических полугрупп

Определение

Полугруппа S называется циклической, если она порождается одним элементом

Полугруппа $(\mathbb{N}, +) =< 1 >$ является циклической.

Классификация циклических полугрупп

Определение

Полугруппа S называется циклической, если она порождается одним элементом

Полугруппа $(\mathbb{N}, +) =< 1 >$ является циклической.

Найдем подполугруппу T_5, порожденную элементом
$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 3 \end{pmatrix}$
Согласно лемме это множество состоит из $\{\tau, \tau^2 = \tau \circ \tau, \tau^3, \ldots\}$

Классификация циклических полугрупп

Определение

Полугруппа S называется циклической, если она порождается одним элементом

Полугруппа $(\mathbb{N}, +) =< 1 >$ является циклической.

Найдем подполугруппу T_5, порожденную элементом

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 3 \end{pmatrix}$$

Согласно лемме это множество состоит из $\{\tau, \tau^2 = \tau \circ \tau, \tau^3, \ldots\}$

$$\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 3 & 4 \end{pmatrix}, \tau^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 4 & 5 \end{pmatrix},$$

$$\tau^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 5 & 3 \end{pmatrix}, \tau^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 3 & 4 \end{pmatrix} = \tau^2$$

Классификация циклических полугрупп

Определение

Полугруппа S называется циклической, если она порождается одним элементом

Полугруппа $(\mathbb{N}, +) =< 1 >$ является циклической.

Найдем подполугруппу T_5, порожденную элементом
$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 3 \end{pmatrix}$
Согласно лемме это множество состоит из $\{\tau, \tau^2 = \tau \circ \tau, \tau^3, \ldots\}$
$\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 3 & 4 \end{pmatrix}$, $\tau^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 4 & 5 \end{pmatrix}$,
$\tau^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 5 & 3 \end{pmatrix}$, $\tau^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 3 & 4 \end{pmatrix} = \tau^2$ Итак,
$< \tau >= \tau, \tau^2, \tau^3, \tau^4, \tau^5$.

Классификация циклических полугрупп

Определение

Пусть i, p — наименьшие натуральные числа такие, что $x^i = x^{i+p}$, тогда i называется индексом, а p — периодом элемента x. Тогда полугруппу $< x >$ называют (i, p)- полугруппой.

Классификация циклических полугрупп

Теорема (о классификации циклических полугрупп)

Любая конечная циклическая полугруппа изоморфна некоторой (i, p) -полугруппе. Любая бесконечная — $(\mathbb{N}, +)$.

Классификация циклических полугрупп

Теорема (о классификации циклических полугрупп)

Любая конечная циклическая полугруппа изоморфна некоторой (i, p) -полугруппе. Любая бесконечная — $(\mathbb{N}, +)$.

Пусть $S =< a >$ — циклическая полугруппа, рассмотрим отображение $f : \mathbb{N} \to S$, которое действует по правилу $f(n) = a^n$. Так как $f(n + m) = a^{n+m} = f(n)f(m)$, то f — сюръективный гомоморфизм.

Классификация циклических полугрупп

Теорема (о классификации циклических полугрупп)

Любая конечная циклическая полугруппа изоморфна некоторой (i, p) -полугруппе. Любая бесконечная — $(\mathbb{N}, +)$.

Пусть $S =< a >$ — циклическая полугруппа, рассмотрим отображение $f : \mathbb{N} \to S$, которое действует по правилу $f(n) = a^n$. Так как $f(n + m) = a^{n+m} = f(n)f(m)$, то f — сюръективный гомоморфизм.

Сл 1 Если f — инъекция, то мы получаем, что $(\mathbb{N}, +) \cong S =< a >$.

Классификация циклических полугрупп

Теорема (о классификации циклических полугрупп)

Любая конечная циклическая полугруппа изоморфна некоторой (i, p) -полугруппе. Любая бесконечная — $(\mathbb{N}, +)$.

Пусть $S =< a >$ — циклическая полугруппа, рассмотрим отображение $f : \mathbb{N} \to S$, которое действует по правилу $f(n) = a^n$. Так как $f(n + m) = a^{n+m} = f(n)f(m)$, то f — сюръективный гомоморфизм.

Сл 2 Если f не инъекция, то рассмотрим наименьшее числа i, p такие, что $a^i = f(i) = f(i + p) = a^{i+p}$.

Классификация циклических полугрупп

Теорема (о классификации циклических полугрупп)

Любая конечная циклическая полугруппа изоморфна некоторой (i, p) -полугруппе. Любая бесконечная — $(\mathbb{N}, +)$.

Пусть $S =< a >$ — циклическая полугруппа, рассмотрим отображение $f : \mathbb{N} \to S$, которое действует по правилу $f(n) = a^n$. Так как $f(n + m) = a^{n+m} = f(n)f(m)$, то f — сюръективный гомоморфизм.

Сл 2 Если f не инъекция, то рассмотрим наименьшее числа i, p такие, что $a^i = f(i) = f(i + p) = a^{i+p}$.

Покажем, что $\forall k > i + p \quad \exists i \leq s < i + p \quad a^k = a^s$. Действительно, так как $k - i > p$, то разделим $k - i$ с остатком на p и получим $k - i = sp + r$, откуда $k = (i + r) + sp$, где $i \leq i + r < i + p$.

Классификация циклических полугрупп

Теорема (о классификации циклических полугрупп)

Любая конечная циклическая полугруппа изоморфна некоторой (i, p) -полугруппе. Любая бесконечная — $(\mathbb{N}, +)$.

Пусть $S =< a >$ — циклическая полугруппа, рассмотрим отображение $f : \mathbb{N} \to S$, которое действует по правилу $f(n) = a^n$. Так как $f(n + m) = a^{n+m} = f(n)f(m)$, то f — сюръективный гомоморфизм.

Сл 2 Если f не инъекция, то рассмотрим наименьшее числа i, p такие, что $a^i = f(i) = f(i + p) = a^{i+p}$.

Покажем, что $\forall k > i + p \quad \exists i \leq s < i + p \quad a^k = a^s$. Действительно, так как $k - i > p$, то разделим $k - i$ с остатком на p и получим $k - i = sp + r$, откуда $k = (i + r) + sp$, где $i \leq i + r < i + p$. Тогда $a^k = a^{i+r+sp} = a^r a^{i+sp} = a^r a^i = a^{r+i}$.