Лектор: Толкачева Алёна Алексеевна

06.02.2020

1 Основные алгебраические структуры

1.1 Функции, отображения множеств

Пусть A, B - множества. $A \times B = \{(a,b) | a \in A, b \in B\}$

Определение 1.1 (Функция).
Подмножество f декартова произведения называется ***функцией****, если $\forall a \in A, b_1, b_2 \in B$:*

$$\left.\begin{matrix}(a, b_1) \in f \\ (a, b_2) \in f\end{matrix}\right\} \Rightarrow b_1 = b_2$$

Эквивалентная запись:

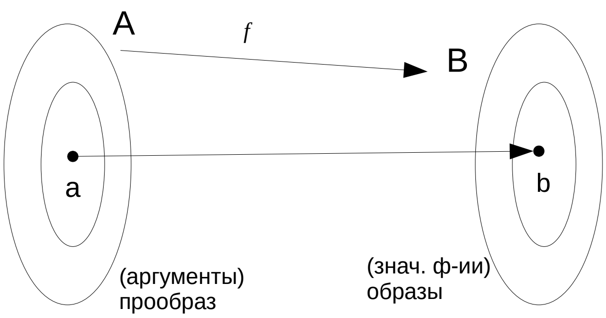
$$f \subseteq A \times B \text{ и } f : A \to B,$$
$$(a,b) \in f \text{ и } f(a) = b$$

Функция - это НЕ соответствие (!), это подмножество декартового произведения, где каждому элемента из 1-ого множества ставится не более одного элемента из 2-ого.

Определение 1.2 (Область определения).
Областью определения функции $f \subseteq A \times B$ называется множество $D_f = \{a \in A | \exists b \in B : (a, b) \in f\}$

Определение 1.3 (Область значений).
Областью значений функции $f \subseteq A \times B$ называется множеством $E_f = \{b \in B | \exists a \in A : (a, b) \in f\}$

Определение 1.4.
Нечёткое множество: лысый человек, куча сена - с какого кол-ва волос / колосков можно считать лысым / стогом. С какой долей (весом) попадает в это множество.



Определение 1.5 (Отображения).
Функция $f : A \to B$ называется отображением, если $\forall a \in A \exists! b \in B : f(a) = b$.

Теорема 1.6 (Критерий отображения).
Функция $f : A \to B$ явл-ся отображением ТТТ, когда $D_f = A$.

Доказательство. Доказываем необходимость и достаточность.

Дано: $f : A \to B$ - отображение.

Необходимость:

$$\forall a \in A \exists! \underbrace{b \in B : f(a) = b}_{\text{по усл.}}$$

$$\begin{cases} D_f \subseteq A (\text{по усл.}) \\ A \subseteq \underbrace{D_f}_{a \in D_f} \end{cases} \Rightarrow D_f = A$$

Достаточность:

Если $D_f = A$:

$$\forall a \in A = D_f$$

$$\exists b \in B : f(a) = b$$

(!) по def функции. ☐

Определение 1.7.

Отображение $f : A \to A$ наз-ся преобразованием множества A.

Свойства функций:

- Функция $f : A \to B$ наз-ся **инъективной (инъекций)**, если $\forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$.
- Отображение $f : A \to B$ называется **сюръективным (сюръекцией)**, если $\forall b \in B \exists a \in A : f(a) = b$ - для любого образа надётся прообраз.
- Отображене $f : A \to B$ называется **биективным (биекцией)**, если оно инъективно и сюръективно одновременно.

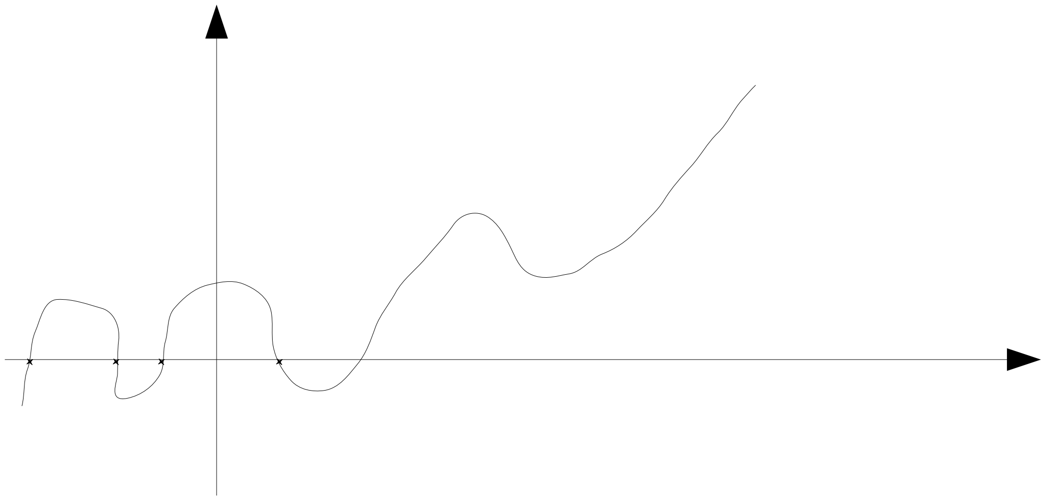
Теорема 1.8 (Критерий сюръективности)**.**

$$f : A \to B - \textit{сюр.} \Leftrightarrow E_f = B$$

Пример 1.

$$A = B = \mathbb{R}$$

$$A \times B = \mathbb{R}^2 - \text{плоскость}$$



Комплексные корни ходят сопряжёнными парами.

Любая волна (см. 1-ую четверть) отвечает за пары корней.

Отображение - область определения - всё 1-ое множество. Здесь ф-ия уходит в бесконечность в обе стороны $\Rightarrow$ является отображением (мн-н определён везде).

Функция не инъективна, т.к. для разных значений есть одинаковые значения.

Т.к. не инъективна, значит не биективна.

Сюръективна, т.к. для любого образа найдётся свой прообраз.

Пример 2. (Гардероб)

Есть номерки - 1-ая группа людей, 2-ая группа - крючки. Функция: выбираем только те элементы, которые составляют пары куртка, повешанная на крючок. Что «обрезать», чтобы получить нормальную ф-ию? Запретить вешать одну одежду на несколько крючков, а не на несколько $\Rightarrow$ возникает функциональная зависимость.

Наша функция станет отображением, когда не будет не повешенной одежды.

Станет сюръекцией, когда все крючки будут заняты.

$\Rightarrow$ устанавливает биективное отношение $\Leftrightarrow$ взаимное соответствие.

Если на крючках написать ещё номера (конечное $\{1,2,\ldots,n\}$), то установим взаимооднозначное соответствие.

1.2 Операции на множествах

Пусть A - множество.

$$A^n = \{(a_1, a_2, \ldots, a_n) | a_i \in A, \forall i = \overline{1, n}\}$$

Определение 1.9.

Произвольное отображение $f : A^n \in A$ наз-ся n-арной алгебраической операцией (операцией, замкнутой на A).

При $n = 2$ говорят о бинарных операциях.

$$f(\underbrace{a_1, a_2,\ldots,a_n}_{\in A^n}) = \underbrace{b}_{\in A}$$

$$f : \underbrace{\mathbb{R}}_{>0} \to \underbrace{\mathbb{R}}_{>0}$$

$$x \to e^{(x-1)}$$

Определение 1.10.
*Бинарная операция f **замкнута** на множестве A (алгебраическое действие), если*

$$\forall a_1, a_2 \in A : f(a_1, a_2) \in A.$$

Дано: $f(a_1, a_2) = b \sim$ ... если используем значок $+$ - используем **аддитивную запись**, если используем $\times$ или $\cdot$ - используем **мультипликативную запись**.

Свойства алгебраических бинарных операций:

- Ассоциативность: $\forall a_1, a_2, a_3 \in A : (a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)$
- Коммутативность: $\forall a_1, a_2 \in A : a_1 * a_2 = a_2 * a_1$
- Обратимость справа: $\forall a_1, a_2 \in A \exists x \in A : a_1 = a_2 * x$
- Обратимость слева: $\forall a_1, a_2 \in A \exists x \in A : a_1 = x * a_2$
- Сократимость справа: $\forall a_1, a_2, x \in A : a_1 * x = a_2 * x \Rightarrow a_1 = a_2$
- Сократимость слева: $\forall a_1, a_2, x \in A : x * a_1 = x * a_2 \Rightarrow a_1 = a_2$

Пусть на множестве A введена бинарная операция $*$.

Определение 1.11.
*Элемент e множества A называется **правой (левой) единицей**, если $\forall a \in A : a * e = a (e * a = a)$.*

Определение 1.12.
*Элемент называется **нейтральным (единицей)**, если он является и левой, и правой единицами.*

Определение 1.13.
*Элемент $a \in A$ **обратим справа (слева)**, если $\exists a' \in A : a * a' = e (a' * a = e)$.*

Определение 1.14 (Обратимость элемента)**.**
Элемент обратим, если он обратим и справа, и слева.

Пример 1.1.

$$A = \{a, b, c\}, * : x * \underbrace{y}_{\text{правая единица}} = x, \forall x, y \in A$$

Таблица Кэли (таблица действий):

$*$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

$\Rightarrow$ операция замкнута и ассоциативна.

- $x * (y * z) = x * y = x; (x * y) * z = x * z = x \Rightarrow$ не коммунитативна (иначе таблица Кэли должна быть симметрична)
- Каждый элемент является левым нулём и правой единицей: $\forall x \in A : x * a = x$ - все элементы правые единицы. Нулевой элемент всё вбирает в себя.

Определение 1.15.
Элемент Θ множества A называется правым (левым) нулём, если $\forall a \in A : a * \Theta = \Theta (\Theta a = \Theta)$.

Определение 1.16.
Элемент является ***нулевым (нулём)****, если он является и левым, и правым нулём.*
Каждый элемент иденпотентен (произведение на себя - даёт сам себя).

Определение 1.17.
Элемент $a \in A$ - иденпотентен, если $a * a = a$.

Определение 1.18.
Элемент $a \in A$ наз-ся нильпотентным, если $a * a = \Theta$.

Пример 1.2.
$M_{m\times n}$
$E_{m\times m}$ - левая ед.
$E_{n\times n}$ - правая ед.

1.3 Алгебраические структуры

Определение 1.19 (Алгебраическая структура)**.**
Множество A, с введёнными на нём операциями m алгебраическими (замкнутыми) операциями. наз-ся алгебраической структурой.

$$(A, *_1, *_2, \dots, *_m)$$

Определение 1.20 (Подструктура)**.**
Подструктурой называется непустое подмножество A, являющееся алгебраической структурой относительно наследуемых операций.

Пример 1.3.
L - линейное пространство. Операции: $+$ - бинарная операция - сложение, $\lambda\cdot$ - унарная операция - умножение на число: $P \cdot \bar{a} \in L, P$ - числа. Получаем *линейное пространство*. Операция должна сохраняться и на подпространстве.

$$(A, *)$$

Определение 1.21.
Полугруппа - мн-во с одной замкнутой ассоциативной операцией. Полугруппа наз-ся ***коммутативной****, если операция на ней коммунитативна. Полугруппа с единицей -* ***моноид****.*

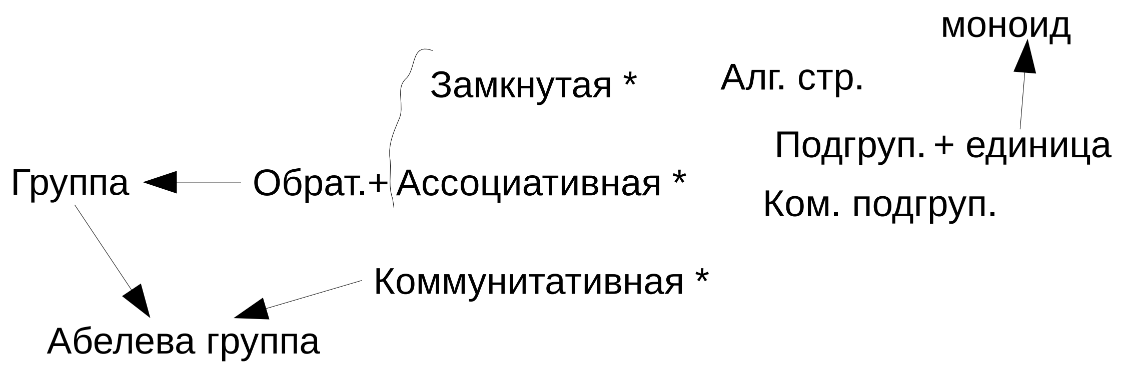
Определение 1.22.
Группа - мн-во с одной замкнутой, ассоциативной, обратимой операцией. Группа наз-ся ***коммутативной (абелевой) группой****, если операция на ней коммутативна.*

$$K, +, \cdot - \text{кольцо, если}$$

- $(K, +)$ - абелева группа
- $(K, \cdot)$ - полугруппа

- $\forall a, b, c \in K$:

$$(a+b)c = ac + bc$$
$$a(b+c) = ab + ac$$



Определение 1.23 (Кольцо)**.**
Кольцо - это мн-во в двумя операциями, связанными между собой дистрибутивными законами, если по одной из них оно является абелевой группой, по другому - полугруппой.

Примечание. Операции в кольце условно наз-ся сложением и умножением, поэтому говорят об аддитивной группе и мультипликативной полугруппе кольца.

Примечание. Если операция умножения в кольце обладает нейтральным элементом, то говорят, что это **кольцо с единицей**. Если операция умножения в кольце коммунитативна, то кольцо наз-ся **коммутативным**.

Пример 1.

$$(M_n, +, \cdot)$$

Абелева группа по сложению, коммунитативна по сложения и т.д. Квадратные матрица образуют кольцо (некоммутативное, но с единицой).

Пример 2.

$$(\mathbb{Z}, +, \cdot)$$

Кольцо, коммунитативное, с единицей.

Пример 3.

$$(P[x], +, \cdot)$$

Кольцо многочленов.

Определение 1.24.
Множество $A = (K, +, \cdot)$ - поле, если на нём определены две бинарные операции: условно называемые сложение и умножение, удовлетворяющие следующим условиям:

- $(K, +)$ - *абелева группа относительно сложения (с нейтральным элементом Θ)*

- $(K, \cdot), K^* = K \setminus \{\Theta\}$ - *абелева группа относительно сложения (с нейтральным элементом e)*

- *Верен закон дистрибутивности* $\forall a, b, c \in K$:

$$(a+b)c = ac + bc$$
$$a(b+c) = ab + ac$$

Примечание. Каждое поле - кольцо, но не каждое кольцо - поле.

$\{0,1\}$ - самое маленько (двухэлементное) поле.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$$

$\mathbb{H}$ - квадранион. $\mathbb{H} = \{a + bi + cj + dR | a, b, c, c \in R\}, i^2 = j^2 = R^2 = -1$. "x" - вектор.

Алг. действие	$\mathbb{N}$	Кольцо цел. чисел $\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$
+	КП	АГ	АГ	Поля		АГ
$\cdot$	моноид (КП с ед.)	КП с ед.	КП с ед. $\mathbb{Q}^* \setminus \{0\}$ - АГ			Группоид

- КП - коммутативная полугруппа

- КП с ед. - коммутативная полугруппа с единицей

- АГ - абелева группа

13.02.2020

1.4 Группа преобразований

Пусть функции $f : A \to B$ и $g : B \to C$ таковы, что $E_f = D_g$.

Определение 1.25 (Композиция).
Композицией (суперпозицией) функций $f : A \to B$ *и* $g : B \to C$ *наз-ся новая функция* $f \circ g : A \to C$, *для которой верно условие* $\forall a \in D_f : f \circ f(a) = g(f(a))$.

Теорема 1.26 (Корректность определения).
Компизиция функции $f : A \to B$ *и* $g : B \to C$ *при* $E_f = D_g$ *явл-ся функцией.*

$$h \text{ - функция} \Leftrightarrow \forall X \in D_h : \begin{cases} h(x) = c_1 \\ h(x) = c_2 \end{cases} \Rightarrow c_1 = c_2$$

$$h = f \circ g, \forall x \in D_h : \begin{cases} f \circ g(x) = c_1 \\ f \circ g(x) = c_2 \end{cases} \Rightarrow \begin{cases} g(f(x)) = c_1 \\ g(f(x)) = c_2 \end{cases} \Rightarrow f, g - \text{функция} \Rightarrow c_1 = c_2.$$

$$f = g \Leftrightarrow \forall x \in D_f = D_g : f(x) = g(x)$$

Определение 1.27 (Нейтральная функция).
id(x) = x

Свойства композиции функций:

1. $f \circ g \neq g \circ f$
2. $f \circ (g \circ h) = (f \circ g) \circ h$
3. $\forall f : id \circ f = f \circ id = f$, если $id(x) = x, \forall x$
4. Композиция сюръекций - сюръекция
5. Композиция инъекций - инъекция
6. $\exists f' : f \circ f' = f' \circ f = id \Leftrightarrow f$ - инъекция

Теорема 1.28 (О группе биективных преобразований)**.**
Биективные преобразования множества относительно действия композиции образуют группу.

Определение 1.29 (Преобразование)**.**
Биективное отображение множества A в себя называется преобразованием множества A.

$$G = \{f_i : A \to A | f_i - \text{биекция}\}$$

$$(G, \circ) - \text{группа}$$

$$GL_n(P) = \{A_n | detA_n \neq 0\}$$

Пусть A - конечное множество, то есть $|A| = n$, где n - натуральное число. $A = \{1, 2, 3, \ldots, n\}$.

Определение 1.30 (Симметрическая группа)**.**
Группа биективная преобразований конечного множества называется симметрической группой. Обозначение: $S_n, |S_n| = n!$

Определение 1.31 (Подстановка)**.**
Подстановка - элемент u из S_n, записанный в виде

$$u = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix}$$

где $u(\alpha_i) = \beta_i, i = \overline{1,n}$.

12.03.2020

1.5 Подстановки

$$(S(\chi),^\circ)$$
$$|\chi| = n \Rightarrow S(\chi) = S_n$$

По сути - это группа перестановок биективного множества и, следовательно, $|S_n| = n!$.

$$u = \begin{pmatrix} 1 & 2 & \ldots & n \\ u(1) & u(2) & \ldots & u(n) \end{pmatrix}$$

$$\forall i : \alpha_i, \beta_i, \gamma_i \in \{1, \ldots, n\}$$

Пример 1.4.
Есть две подстановки:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 1 & 2 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 4 & 3 & 5 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 7 & 2 & 3 & 5 & 6 \end{pmatrix}$$

Пример 1.5 (Транспозиция).

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 3 & 5 & 6 & 7 \end{pmatrix} = (3{,}4)$$

Определение 1.32 (Иденпотентный элемент)**.**
Элемент u называется идентпотентным, если $u^2 = id$. *Меняем 3 и 4 местами, опять меняем → они остались на своих местах → любой идентпотентный элемент является обратным самому себе.*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 1 & 2 & 5 & 6 & 7 & 8 \end{pmatrix} = (1, 4, 2, 3)$$

$$(1{,}2{,}3)^2 = (1{,}2{,}3)(1{,}2{,}3) = (1{,}3{,}2)$$

$$r^3 = (1{,}3{,}2)(1{,}2{,}3) = (1)(2)(3)$$

Цикл ^{2} - всё осталось на месте, а 2-ка перешла в себя - тождественное преобразование.

$$sign(u) = \begin{cases} 1, u - \text{чет.} \\ -1, u - \text{нечёт.} \end{cases}$$

2 Группы

Определение 2.1 (Нейтральный элемент)**.**
e_1, e_2 *- нейтральные,* $e_1 * e_2 = e_2 = e_1$

$*$ - обратима, если:

$$\forall a, b \in A \exists x, y \in A :$$

$$\begin{cases} a * x = b \\ y * a = b \end{cases}$$

Содержание