Раздел 2

Алгебраические структуры

ITMO University

Лекция 4-5
Группы

- 1. Алгебраические операции. Понятие алгебры.
- 2. Полугруппа. Моноид. Группа.
- 3. Теоремы о свойствах группы.

ITMO University

Литература

1. Белоусов А.И. Дискретная математика. М., 2002.
2. Бухштаб А.А. Теория чисел: учебное пособие. СПб., 2015.
3. Нестеренко Ю.В. Теория чисел. М., 2008.

В широком смысле алгебра – раздел математики, изучающий операции над элементами множеств произвольной природы.

Алгебраические структуры определяются множеством элементов и конечным набором заданных на этом множестве алгебраических операций.

1. Алгебраические операции. Понятие алгебры

$X \neq \emptyset, \ n \in \boldsymbol{N}.$

Определение 1

Любое *отображение*

$$f: \ X^n \to X$$

называется n-арной (n-местной) алгебраической операцией на X.

Операция f называется:

- при $n=0$ – нульарной (это произвольный фиксированный элемент множества X);
- при $n=1$ – унарной;
- при $n=2$ – бинарной.

Обозначение: $y = f(x_1, x_2, \ldots, x_n)$

$x_1, x_2, \ldots, x_n$ – аргументы операции f,

$y \in X$ – результат применения операции f к аргументам.

Определение 2

Пусть на множестве X заданы несколько операций:

$$f_k : \; X^{n_k} \to X,$$

где $\kappa = 1,2,\ldots,m$,

n_k – натуральное число, зависящее от κ.

Множество X с такой структурой называется алгеброй.

Обозначение: $A = < X, f_1, f_2, \ldots f_m >$.

Множество X называется носителем алгебры;

множество операций $f_1, f_2, \ldots, f_m$ – сигнатурой алгебры.

Алгебра называется конечной, если X – конечное множество.

Определение 3

Множество $M \subseteq X$ называется системой образующих (порождающих) или базисом алгебры A, если любой элемент X можно получить из элементов M при помощи операций алгебры A.

Пусть $A = < X, * >$, $*$ – бинарная операция.

Определение 4

Операция $*$ называется:

- ассоциативной, если

$$\forall x, y, z \in X \quad (x * y) * z = x * (y * z);$$

- коммутативной, если

$$\forall x, y \in X \;\; x * y = y * x;$$

- идемпотентной, если

$$\forall x \in X \;\; x * x = x.$$

Ассоциативность операции $*$ позволяет для любых элементов $x_1, x_2, \ldots, x_n \in X$ однозначно понимать результат выражения $x_1 * x_2 * \ldots * x_n$:

$$x_1 * x_2 * \ldots * x_n = x_1 * (x_2 * \ldots * x_n) =$$
$$= (x_1 * x_2) * (x_3 * \ldots * x_n) = \ldots =$$
$$= (x_1 * x_2 * \ldots * x_{n-1}) * x_n$$

Определение 5

Элемент $e \in X$ называется нейтральным по операции $*$, если

$$\forall x \in X \quad x * e = e * x = x.$$

Теорема 1

Если нейтральный элемент по операции $*$ существует, то он *единственный.*

Если нейтральный элемент существует, то его можно задать как нульарную операцию и включить в сигнатуру.

$X=\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ где $a,b \in \boldsymbol{R}$

$A = < X, \cdot >$

Любая матрица $\begin{pmatrix} 1 & 0 \\ d & 0 \end{pmatrix}$ где $d \in \boldsymbol{R}$ –

правый нейтральный элемент:

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix};$$

левый нейтральный элемент ?

$< X, *, e >$ – алгебра, причем существует нейтральный элемент относительно $*$;

$x \in X.$

Определение 6

Элемент $y \in X$ называется обратным к элементу x по операции $*$, если

$$x * y = y * x = e.$$

Элемент x, для которого существует обратный элемент, называется обратимым.

Для *ассоциативной бинарной операции* $*$ существует две формы записи:

1) аддитивная запись:

$$x * x * \ldots * x = x + x + \ldots + x = nx,$$

здесь нейтральный элемент называют *нулем* и обозначают символом **0**, т.е.

$$x + \mathbf{0} = \mathbf{0} + x = x;$$

обратный элемент к x называют *противоположным* и обозначают $-x$, т.е.

$$x + (-x) = (-x) + x = \mathbf{0};$$

операция + называется *сложением алгебры*;

2) мультипликативная запись:

$$x * x * \ldots * x = x \cdot x \cdot \ldots \cdot x = x^n,$$

здесь нейтральный элемент называют *единицей* и обозначают символом **1**, т.е.

$$x \cdot \mathbf{1} = \mathbf{1} \cdot x = x,$$

обратный элемент к x обозначают x^{-1}, т.е.

$$x \cdot x^{-1} = x^{-1} \cdot x = \mathbf{1},$$

операция $\cdot$ называется *умножением алгебры*.

Пусть $< X, *, \ldots >$, $< Y, \circ, \ldots >$

– две алгебры с одинаковым числом соответствующих n-арных алгебраических операций.

Определение 7

Отображение $f : X \to Y$ называется изоморфизмом алгебр, если:

- f биективно:

  все операции первой алгебры поставлены в биективное соответствие всем операциям второй алгебры,
- при этом для соответствующих операций выполняется

$$f(x*y) = f(x) \circ f(y),$$

где $x, y \in X$; $f(x), f(y) \in Y$.

$f: \boldsymbol{R} \to \boldsymbol{R}^+$, где $\boldsymbol{R}^+ = \{x \in \boldsymbol{R}: x > 0\}$

$f(x) = 10^x$, $x \in \boldsymbol{R}$

$f(x+y) = 10^{x+y} = 10^x \cdot 10^y$

- f – биекция:

бинарной операции (+) поставлена в биективное соответствие бинарная операция (·)

- $f(x+y) = f(x) \cdot f(y)$

Вывод: f – изоморфизм алгебры $< \boldsymbol{R}, + >$ на алгебру $< \boldsymbol{R}^+, \cdot >$

2. Полугруппа. Моноид. Группа

$< X, * >$ – алгебра.

Определение 8

Алгебра, сигнатура которой состоит из одной *ассоциативной* бинарной операции называется полугруппой.

Определение 9

Если заданная бинарная операция коммутативна, то полугруппа называется коммутативной (абелевой).

Полугруппу, операция которой

- коммутативна,
- идемпотентна

называют полурешеткой.

Нильс Хенрик
Абель
1802 - 1829

Определение 10

Полугруппа с нейтральным элементом называется моноидом или полугруппой с единицей.

Определение 11

Алгебра называется группой, если она моноид, в котором каждый элемент обратим.

Обозначение: $G = < X, * >$

Порядком конечной группы называется число элементов этой группы.

Определение 12

Если алгебра $G_1 = < X, * >$ – группа,

$Y \subseteq X$ и алгебра $G_2 = < Y, * >$ – группа

с той же операцией, что и в G_1,

то G_2 называется подгруппой группы G_1.

3. Теоремы о свойствах группы

$G = < X, * >$ – группа.

Теорема 2

В любой группе $\forall x \in X$ элемент, обратный к x, *единственный*.

Аксиомы группы:

(1) $*$ *ассоциативная* бинарная операция

(2) $\exists!$ *нейтральный* элемент по операции $*$

(3) $\forall x \in X$ $\exists!$ *обратный* элемент по операции $*$

Теорема 3

Пусть $G = < X, \cdot , \mathbf{1} >$ – группа.

$\forall x,y \in X$ верны тождества:

$$(x.y)^{-1} = y^{-1}.x^{-1},$$

$$(x^{-1})^{-1} = x.$$

$G = < X, \cdot, \mathbf{1} >$ – группа,

$a, b \in X$ – фиксированные элементы X.

Теорема 4

В любой группе справедливы:

1) левый закон сокращения:

$$a \cdot x = a \cdot y \Rightarrow x = y$$

2) правый закон сокращения:

$$x \cdot a = y \cdot a \Rightarrow x = y$$

Рассмотрим уравнения:

$$a \cdot x = b \qquad (1)$$

$$x \cdot a = b \qquad (2)$$

- **Теорема 5**

В любой группе каждое из уравнений (1), (2) имеет решение, и притом *единственное*:

$$x = a^{-1} \cdot b$$

$$x = b \cdot a^{-1}$$

В мультипликативной форме записи *коммутативной группы* решение обоих уравнений (1), (2):

$$x = b \cdot a^{-1}.$$

Выражение вида $b \cdot a^{-1}$ называется *частным от деления* b на a и обозначается $\frac{b}{a}$; сама операция – операцией *деления*.

Решение уравнений записывают в виде:

$$x = \frac{b}{a}.$$

В аддитивной форме записи *коммутативной группы* $G = < X, +, \mathbf{0} >$ оба уравнения (1), (2) имеют вид:

$$a + x = b, \qquad (3)$$

которое имеет единственное решение

$$x = b + (-a),$$

где правая часть называется *разностью* элементов b и a и обозначается $b - a$.

Решение уравнения (3) записывают в виде:

$$x = b - a.$$