Тема 1-4: Алгебраические операции

А. Я. Овсянников

Уральский федеральный университет
Институт естественных наук и математики
Департамент математики, механики и компьютерных наук
Алгебра и геометрия для направлений
Механика и математическое моделирование и
Прикладная математика
(1 семестр)

Понятие алгебраической операции

Пусть X — непустое множество.

Определение

Бинарной алгебраической операцией на множестве X называется отображение из декартова квадрата $X \times X$ в X.

Отображение $f : X \times X \longrightarrow X$ является алгебраической операцией. Вместо $z = f(x, y)$ принято писать $z = x\, f\, y$, а вместо f используются символы $\circ$, $*$ и т.п.

Примеры

1. Операция сложения на множестве чисел $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R})$.
2. Операция умножения на множестве чисел $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R})$.
3. Операция сложения на множестве всех геометрических векторов.
4. Операция умножения на множестве всех отображений из множества X в множество X.
5. Операция умножения на множестве всех бинарных отношений на множестве X.
6. Операция сложения по модулю n на множестве целых чисел $\{0, 1, \ldots, n-1\}$: $x +_n y = z$, где z — остаток от деления на n числа $x + y$.
7. Операция умножения по модулю n на множестве целых чисел $\{0, 1, \ldots, n-1\}$: $x \cdot_n y = z$, где z — остаток от деления на n числа $x \cdot y$.
8. Операция $\bullet$ на множестве $\{a, b, c, d\}$, заданная таблицей Кэли

$\bullet$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Здесь первый аргумент берется в левом столбце, а второй - в первой строке, и на пересечении строки и столбца указан результат. Например, $b \bullet c = d$.

Свойства операций

Пусть $\circ$ — бинарная алгебраическая операция на множестве X.

Определения

1. Операция $\circ$ называется *коммутативной*, если $\forall x, y \in X \;\; x \circ y = y \circ x$.
2. Операция $\circ$ называется *ассоциативной*, если $\forall x, y, z \in X \;\; (x \circ y) \circ z = x \circ (y \circ z)$.
3. Элемент $e \in X$ называется *нейтральным* относительно операции $\circ$, если $\forall x \in X \;\; x \circ e = e \circ x = x$.
4. Пусть e — нейтральный элемент относительно операции $\circ$. Элемент $y \in X$ называется *симметричным* к элементу $x \in X$, если $x \circ y = y \circ x = e$.

Проверка ассоциативности для бинарных операций на конечных множествах, заданных таблицами

Пусть на конечном множестве $X = \{x_1, \ldots, x_n\}$ бинарная операция $\circ$ задана с помощью таблицы Кэли. Чтобы проверить, будет ли эта операция ассоциативной, для каждого элемента x множества X строятся таблицы Кэли двух вспомогательных операций: $y *_x z = (y \circ x) \circ z$ и $y \star_x z = y \circ (x \circ z)$. Если таблицы Кэли этих операций совпадают при любом x из X, то операция $\circ$ будет ассоциативной.
Для построения таблицы Кэли операции $*_x$ нужно записать по порядку строки из исходной таблицы Кэли, соответствующие элементам $x_1 \circ x, \ldots, x_n \circ x$. Для построения таблицы Кэли операции $\star_x$ нужно записать по порядку столбцы из исходной таблицы Кэли, соответствующие элементам $x \circ x_1, \ldots, x \circ x_n$. Для проверки ассоциативности достаточно построить таблицы Кэли операций $*_x$ и проверить, является ли каждая из них таблицей Кэли для соответствующей операции $\star_x$.

Пример

Проверим, что операция 8 на сл.3 ассоциативна. Для этого построим таблицы Кэли для операций $*_x$ и $\star_x$ для $x \in \{a, b, c, d\}$.

$*_d$	a	b	c	d
$(a \bullet d)a$	d	a	b	c
$(b \bullet d)b$	a	b	c	d
$(c \bullet d)c$	b	c	d	a
$(d \bullet d)d$	c	d	a	b

$\star_d$	$(d \bullet a)a$	$(d \bullet b)b$	$(d \bullet c)c$	$(d \bullet d)d$
a	d	a	b	c
b	a	b	c	d
c	b	c	d	a
d	c	d	a	b

$*_a$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$*_b$	a	b	c	d
a	b	c	d	a
b	c	d	a	b
c	d	a	b	c
d	a	b	c	d

$*_c$	a	b	c	d
a	c	d	a	b
b	d	a	b	c
c	a	b	c	d
d	b	c	d	a

$\star_a$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$\star_b$	a	b	c	d
a	b	c	d	a
b	c	d	a	b
c	d	a	b	c
d	a	b	c	d

$\star_c$	a	b	c	d
a	c	d	a	b
b	d	a	b	c
c	a	b	c	d
d	b	c	d	a

Мы видим, что во всех случаях таблицы Кэли операций $*_x$ и $\star_x$ совпадают. Следовательно, операция $\bullet$ ассоциативна.

Примеры

Операции 1–3 и 6–8 со слайда 3 являются коммутативными.

Все операции 1–8 являются ассоциативными.

Операция сложения на множестве $\mathbb{N}$ не имеет нейтрального элемента, на остальных множествах чисел нейтральный элемент — 0.
Для умножения на всех множествах чисел нейтральный элемент — 1.
Для сложения векторов нейтральный элемент $\vec{0}$,
для умножения отображений и бинарных отношений на множестве X — отношение равенства $\triangle_X$ (определение см на слайде 9 лекции 3).
Для операции 8 нейтральным элементом будет a.

Для операции сложения на множествах $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$. каждый элемент обладает симметричным.
Для операции умножения на множестве $\mathbb{N}$ симметричным обладает только 1, на множестве $\mathbb{Z}$ — только $-1, 1$, на множествах $\mathbb{Q}$, $\mathbb{R}$ — каждое ненулевое число.
Каждый вектор обладает симметричным относительно операции сложения векторов.
Биекции и только они обладают симметричными относительно операций умножения отображений и бинарных отношений.
Для операции 8 элементы a и c являются симметричными к самим себе, d является симметричным к b.

Предложение

Если операция обладает нейтральным элементом, то он единствен. Если ассоциативная операция обладает нейтральным элементом, то симметричный элемент определяется однозначно в случае, когда он существует.

$\Downarrow$ Пусть e_1, e_2 — два нейтральных элемента относительно операции $\circ$. Тогда $e_1 = e_1 \circ e_2 = e_2$ по определению нейтрального элемента.
Пусть ассоциативная операция $\circ$ обладает нейтральным элементом e и y_1, y_2 — два симметричных элемента к элементу x. Тогда $x \circ y_1 = y_1 \circ x = e$ и $x \circ y_2 = y_2 \circ x = e$. Имеем $y_1 = e \circ y_1 = (y_2 \circ x) \circ y_1 = y_2 \circ (x \circ y_1) = y_2 \circ e = y_2$, т.е. $y_1 = y_2$, что и требуется доказать.$\Uparrow$

Теорема

Если операция $\circ$ на множестве X ассоциативная, то для любых $x_1, x_2, \ldots, x_n \in X$ значение выражения $x_1 \circ x_2 \circ \ldots \circ x_n$ не зависит от способа расстановки скобок.

$\Downarrow$Докажем индукцией по n, что при $n \geq 3$ и любых $x_1, x_2, \ldots, x_n \in X$ выражение $x_1 \circ x_2 \circ \ldots \circ x_n$ при любом способе расстановки скобок равно $x_1 \circ (x_2 \circ (\ldots \circ x_n) \cdots)$. База индукции ($n = 3$) следует из определения ассоциативной операции: $(x_1 \circ x_2) \circ x_3 = x_1 \circ (x_2 \circ x_3)$.
Шаг индукции. Предположим, что для всех $3 \leq k < n$ утверждение уже доказано. Рассмотрим произведение $(x_1 \circ x_2 \ldots \circ x_m) \circ (x_{m+1} \circ \ldots x_n)$. Если $m = 1$, то требуемое сразу получается из предположения индукции, примененного к второй скобке. Пусть $m > 1$. По предположению индукции выражение в первой скобке равно $x_1 \circ (x_2 \circ (\ldots \circ x_m))$.
Применяя свойство ассоциативности, получаем $(x_1 \circ x_2 \ldots x_m) \circ (x_{m+1} \circ \ldots x_n) = (x_1 \circ (x_2 \circ (\ldots x_m)) \circ (x_{m+1} \circ \ldots \circ x_n) = x_1 \circ ((x_2 \circ (\ldots x_m)) \circ (x_{m+1} \circ \ldots x_n))$, откуда в силу предположения индукции следует требуемое утверждение.$\Uparrow$

С учетом теоремы в случае ассоциативной операции выражения вида $x_1 \circ x_2 \circ \ldots \circ x_n$ принято записывать без скобок.

Аддитивный и мультипликативный способы представления алгебраической операции

1. Аддитивный способ.
Если операция на множестве коммутативна и ассоциативна, то ее часто обозначают знаком $+$ и называют *сложением*. При этом нейтральный элемент, если он существует, обозначается 0 и называется *нулем*, а (единственный) симметричный элемент к элементу a обозначается через $-a$ и называется *противоположным* к a элементом.

2. Мультипликативный способ. Если операция на множестве ассоциативна, то ее часто обозначают знаком $\cdot$ и называют *умножением*. При этом нейтральный элемент, если он существует, обозначается 1 и называется *единицей*, а (единственный) симметричный элемент к элементу a обозначается через a^{-1} и называется *обратным* к a элементом.

Пусть на множестве G определена операция умножения.

Определение

Множество G называется *группой*, если

1. Операция на множестве G ассоциативна;
2. в множестве G существует единица;
3. для любого элемента из множества G существует обратный элемент.

Если операция на группе G коммутативна, то группа G называется *абелевой*.

Обычно для абелевых групп используется аддитивный способ представления операции.

Абелевыми группами являются множества чисел $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ относительно сложения, множество векторов относительно сложения, множество из примера 8 на слайде 3.

Предложение

Пусть G — группа с операцией умножения, $x, y, z \in G$. Тогда

1. *Если $xy = xz$ или $yx = zx$, то $y = z$ (закон сокращения).*
2. *Имеет место равенство $(xy)^{-1} = y^{-1}x^{-1}$.*

$\Downarrow$Пусть $xy = xz$. Умножив обе части этого равенства слева на x^{-1}, получим $x^{-1}(xy) = x^{-1}(xz)$, откуда в силу ассоциативности и определения обратного элемента следует $(x^{-1}x)y = (x^{-1}x)z$ и $1y = 1z$, т.е. $y = z$.
Аналогично доказывается, что из $yx = zx$ следует $y = z$.
Для доказательства утверждения 2 вычислим
$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}(xy)) = y^{-1}((x^{-1}x)y) = y^{-1}(1y) = y^{-1}y = 1$.
Значит, $(y^{-1}x^{-1})(xy) = 1$. Так как $(xy)^{-1}(xy) = 1$, из утверждения 1 следует утверждение 2.

Разность в абелевой группе

Пусть $(V, +)$ – абелева группа. Тогда $\forall a, b \in V\ \exists! x \in V : a + x = b$.
Указанный элемент x обозначается через $b - a$ и называется *разностью* элементов a и b.

Положим $x = b + (-a)$, тогда ясно, что $a + x = a + b + (-a) = b$.
Единственность элемента x следует из утверждения 1 предложения.$\Uparrow$

Пусть K — множество с операциями сложения и умножения.

Определение

Множество K называется *кольцом*, если относительно сложения K является абелевой группой и
$\forall x, y, z \in K \;\; x(y+z) = xy + xz, \;\; (x+y)z = xz + yz.$

Последние условия называются *левой дистрибутивностью* и *правой дистрибутивностью*.
На операцию умножения в кольце никаких ограничений не налагается.
Кольцами относительно операций сложения и умножения являются множества чисел $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, а также множества классов вычетов по модулю n.
Кольцам даются названия по свойствам операции умножения. Если она коммутативна (ассоциативна), то кольцо называется *коммутативным* (*ассоциативным*).
Если для операции умножения существует единица, то кольцо называется *кольцом с единицей*.

Пусть K — кольцо.

Предложение

Для любого элемента $x \in K$ имеют место равенства $0x = x0 = 0$.

$\Downarrow$ Умножим равенство $0 + 0 = 0$ слева на элемент x, получим $x(0+0) = x0$. Пользуясь дистрибутивностью, имеем $x0 + x0 = x0 = x0 + 0$, откуда в силу свойства 1 групп (слайд 12) следует $x0 = 0$.
Аналогично доказывается, что $0x = 0$.$\Uparrow$

Определение

Элементы x, y кольца K называются *делителями нуля*, если $x, y \neq 0$, но $xy = 0$.

Делители нуля имеются в кольце вычетов по модулю n, когда n — составное число. Если $n = n_1 n_2$, где $n_1 < n$, $n_2 < n$, то $n_1 n_2 = 0$ в кольце вычетов по модулю n, но $n_1, n_2 \neq 0$.

Определение

Полем называется коммутативное ассоциативное кольцо с единицей, в котором каждый ненулевой элемент имеет обратный (по умножению). В поле $0 \neq 1$, т.е. поле не может состоять из одного элемента.

Полями относительно операций сложения и умножения яаляются множества чисел $\mathbb{Q}, \mathbb{R}$, а также множества классов вычетов по простому модулю n.

Предложение

Поле не имеет делителей нуля.

$\Downarrow$Предположим, что $xy = 0$ и $x \neq 0$. Тогда в поле существует элемент x^{-1}. Умножим обе части равенства $xy = 0$ слева на x^{-1}, получим $x^{-1}(xy) = x^{-1}0 = 0$, откуда $0 = (x^{-1}x)y = 1y = y$, т.е. $y = 0$. Следовательно, поле не может содержать делителей нуля.$\Uparrow$

Характеристика поля

Пусть F – поле, e – единица F, т.е. нейтральный элемент относительно умножения. Рассмотрим отображение $\varphi : \mathbb{N} \longrightarrow F$, полагая $\varphi(n) = e + e + \ldots + e$ (сумма n слагаемых).
Если это отображение инъективно, то говорят, что поле F *имеет характеристику* 0.
Если φ не инъективно, то $\varphi(m) = \varphi(n)$ при некоторых $m, n \in \mathbb{N}$ таких что $m < n$. Тогда $\varphi(n - m) = 0$ (нуль поля F).
В этом случае *характеристикой* поля F называется наименьшее натуральное число p такое что $\varphi(p) = 0$. Характеристику поля обозначим через $\mathrm{char}(F)$.

Предложение

Если характеристика поля не равна нулю, то она является простым числом.

$\Downarrow$Пусть $\mathrm{char}(F) \neq 0$. Так как в поле F справедливо $e \neq 0$, имеем $\mathrm{char}(F) \neq 1$. Легко вычислить, что $\varphi(n \cdot k) = \varphi(n)\varphi(k)$.
Если $\mathrm{char}(F) = n \cdot k$, где $n, k < \mathrm{char}(F)$, то $\varphi(n)\varphi(k) = 0$, в то время как $\varphi(n) \neq 0$ и $\varphi(k) \neq 0$. Так как поле в силу предложения сл.12 не имеет делителей нуля, такая ситуация невозможна.
Следовательно, $\mathrm{char}(F)$ – простое число.$\Uparrow$

Поля $\mathbb{Q}$, $\mathbb{R}$ имеют характеристику 0; поле вычетов по простому модулю p