Примеры

Операции 1–4 со слайда 2 и 8–10 со слайда 3 являются коммутативными.

Все операции 1–10 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 сложения матриц – нулевая матрица, для умножения матриц – единичная матрица.

Для умножения отображений и бинарных отношений на множестве X нейтральный элемент — отношение равенства $\triangle_X = \{(x,x) | x \in X\}$.
$\Downarrow$Для $\alpha \subseteq X \times X$ имеем $\alpha \circ \triangle_X = \{(x,y) | \exists z \in X : (x,z) \in \alpha, (z,y) \in \triangle_X\}$. Следовательно, $z = y$ по определению отношения равенства $\triangle_X$ и $\alpha \circ \triangle_X = \alpha$. Аналогично проверяется, что $\triangle_X \circ \alpha = \alpha$. Таким образом, отношение равенства $\triangle_X$ является нейтральным элементом для операции умножения бинарных отношений на множестве X.
Так как отображения являются бинарными отношениями, для операции умножения отображений нейтральным элементом будет $\triangle_X$, рассматриваемое как отображение, т.е. тождественное отображение ε множества X на себя: $\varepsilon(x) = x$ для любого $x \in X$.$\Uparrow$

Для операции 10 нейтральным элементом будет a.

Примеры-2

Для операции сложения на множествах $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 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.

Каждая матрица обладает симметричной относительно операции сложения матриц.

Симметричными элементами относительно умножения матриц обладают обратимые матрицы и только они.

Биекции множества X на X и только они имеют симметричные элементы относительно операций умножения отображений и бинарных отношений. $\Downarrow$ Пусть $\alpha, \beta \subseteq X \times X$ и $\alpha \circ \beta = \beta \circ \alpha = \triangle_X$. Тогда $D(\alpha) = X$ и $E(\alpha) = X$, т.е. α – всюду определенное сюрьективное соответствие. Если $x\alpha y$ и $x\alpha z$, то $y\beta x$ и $z\beta x$, иначе $x(\alpha \circ \beta)u$ при $x \neq u$. Отсюда $z(\beta \circ \alpha)y$ и $y = z$. Таким образом, α – функциональное соответствие. Аналогично проверяется, что α инъективно. Итак, α – биекция.$\Uparrow$

Для операции 10 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.$\Uparrow$

Если операция $\circ$ на множестве A не ассоциативная, то необходимо ставить скобки при записи выражений: $x \circ (y \circ z)$ может быть не равно $(x \circ y) \circ z$. Расставлять скобки в произведениях, содержащих более 3-х элементов, можно многими способами. Например, в произведениях 4-х элементов скобки можно расставить следующими способами:
$x_1 \circ (x_2 \circ (x_3 \circ x_4))$, $x_1 \circ ((x_2 \circ x_3) \circ x_4)$, $(x_1 \circ (x_2 \circ x_3)) \circ x_4$, $((x_1 \circ x_2) \circ x_3) \circ x_4$, $(x_1 \circ x_2) \circ (x_3 \circ x_4)$.

Свойство ассоциативных операций

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 $(x_1 \circ x_2 \ldots \circ x_m) \circ (x_{m+1} \circ \ldots \circ x_n)$.
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 $x_1 \circ (x_2 \circ (x_3 \circ \ldots \circ x_m))$.
Применяя свойство ассоциативности, получаем
$(x_1 \circ x_2 \circ \ldots \circ x_m) \circ (x_{m+1} \circ \ldots \circ x_n) = (x_1 \circ (x_2 \circ (x_3 \circ \ldots \circ x_m))) \circ (x_{m+1} \circ \ldots \circ x_n) = x_1 \circ ((x_2 \circ (x_3 \circ \ldots x_m)) \circ (x_{m+1} \circ \ldots \circ x_n))$, 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, если он существует, обозначается через a^{-1} и называется *обратным* к a элементом. Сам элемент a, для которого существует обратный элемент, называется *обратимым элементом*.

Глава III. Основные понятия

§ 4. Группы, кольца, поля

А. Я. Овсянников

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

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 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ относительно сложения, множества геометрических векторов и матриц одинаковых размеров относительно сложения, множество из примера 10 на слайде 3 §3.

Данное выше определение группы было впервые сформулировано Артуром Кэли. Абелевы группы получили название по фамилии норвежского математика начала XIX века Нильса-Хенрика Абеля (1802-1829).

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

⇓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.⇑

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 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, множество квадратных матриц размеров $n \times n$, 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*.
Например, кольцо целых чисел $\mathbb{Z}$ является коммутативным ассоциативным кольцом с единицей, а кольцо квадратных матриц размеров $n \times n$ – ассоциативным кольцом с единицей.

Свойство нуля кольца. Делители нуля

Пусть K — кольцо.

Предложение

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

$\Downarrow$ Умножим равенство $0 + 0 = 0$ слева на элемент x, получим $x \cdot (0 + 0) = x \cdot 0$. Пользуясь дистрибутивностью, имеем $x \cdot 0 + x \cdot 0 = x \cdot 0 = x \cdot 0 + 0$, откуда в силу свойства 1 групп (слайд 3) следует $x \cdot 0 = 0$.
Аналогично доказывается, что $0 \cdot x = 0$.$\Uparrow$

Определение

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

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 $\overline{n}_1 \cdot \overline{n}_2 = 0$ в кольце вычетов по модулю n, но $\overline{n}_1, \overline{n}_2 \neq 0$.
Имеются делители нуля и в кольце квадратных матриц любого порядка больше 1. Пример рекомендуется придумать в качестве упражнения.

Определения

Коммутативное ассоциативное кольцо с единицей и без делителей нуля называется *областью целостности*.
Говорят, что кольцо K является *кольцом с законом сокращения*, если для любых $x, y, z \in K$ при $x \neq 0$ из $xy = xz$ или $yx = zx$ следует $y = z$.

Пример области целостности, а также кольца с законом сокращения – кольцо целых чисел $\mathbb{Z}$.

Предложение

Коммутативное ассоциативное кольцо с единицей является областью целостности тогда и только тогда, когда оно является кольцом с законом сокращения.

$\Downarrow$Пусть K – область целостности, и $x, y, z \in K$, причем $x \neq 0$. Из $xy = xz$ следует $x(y - z) = 0$. Значит, $y - z = 0$ и $y = z$. В силу коммутативности K этого достаточно. Обратно, пусть K – коммутативное ассоциативное кольцо с единицей и законом сокращения. Предположим, что для $x, y \in K$ имеет место $x \neq 0$ и $x \cdot y = 0$. По предложению сл.5 $x \cdot 0 = 0$, значит, в силу закона сокращения из $x \cdot y = x \cdot 0$ следует $y = 0$. Следовательно, K – кольцо без делителей нуля, т.е. область целостности.$\Uparrow$

Что такое обратимый элемент кольца?

Определение

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

Полями относительно операций сложения и умножения являются множества чисел $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, а также множества классов вычетов по простому модулю n. В последнем случае для любого натурального $0 < k < n$ числа k и n взаимно просты, поэтому существуют целые u, v такие что $uk + vn = 1$. Обратным к классу вычетов $\overline{k}$ будет класс вычетов, определенный числом u.

Предложение

Поле не имеет делителей нуля.

$\Downarrow$Предположим, что $x \cdot y = 0$ и $x \neq 0$. Тогда в поле существует элемент x^{-1}. Умножим обе части равенства $x \cdot y = 0$ слева на x^{-1}, получим $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0$, откуда $0 = (x^{-1} \cdot x) \cdot y = 1 \cdot y = y$, 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.7 не имеет делителей нуля, такая ситуация невозможна. Следовательно, $\mathrm{char}(F)$ – простое число.$\Uparrow$

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