Группоиды, кольца, поля

Александра Игоревна Кононова

МИЭТ

8 июля 2024 г. — актуальную версию можно найти на
https://gitlab.com/illinc/otik

Алгебра, группоид

Алгебра — множество G (носитель) с заданным на нём набором операций, удовлетворяющим некоторой системе аксиом.

Группоид — алгебра $\mathcal{G} = (G, \cdot)$, сигнатура которой состоит из одной бинарной операции $\cdot \colon G \times G \to G$.

Полугруппа, моноид

Полугруппа — группоид, операция ассоциативна — $\forall a, b, c \in G$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Моноид — полугруппа с единицей: $\exists \mathbf{1} : \forall a \in G \quad a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$, $\mathbf{1}$ — нейтральный элемент (единица) моноида

Группа — моноид, в котором для каждого элемента существует обратный.

Группа

Множество G с операцией $\cdot$ — **группа**, если:

1. операция $\cdot$ в G ассоциативна: $a \cdot (b \cdot c) = (a \cdot b) \cdot c \ \ \forall a,b,c \in G$;
2. в G существует единица (нейтральный элемент) $\mathbf{1}\colon\ a \cdot \mathbf{1} = \mathbf{1} \cdot a = a \ \forall a \in G$;
3. для каждого $a \in G$ существует обратный: $a^{-1} \in G\colon\ a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1}$.

Свойства

Если $\cdot$ коммутативна, то полугруппа (группа, группоид) называется **коммутативной**, или **абелевой**.

$\exists \mathbf{0} : \forall a \;\; a \cdot \mathbf{0} = \mathbf{0} \cdot a = \mathbf{0}$ — полугруппа называется полугруппой **с нулём** (и не может быть группой).

Если все элементы полугруппы (группы, группоида) являются некоторыми целыми степенями $a \in G$ — полугруппа называется **моногенной (циклической)**, a — **примитивным (порождающим, образующим)**.

Примеры

Трёхмерные вектора с векторным умножением —

$\mathbb{N}$ с возведением в степень —

Арифметика с насыщением $([-N, N], +)$ —

$(\mathbb{N}, +)$ —

$(\mathbb{N}, \cdot)$ —

$(\mathbb{N} \cup \{0\}, +)$ —

$(\mathbb{N} \cup \{0\}, \cdot)$ —

$(\mathbb{Z},+)$ —

$(\mathbb{Z},\cdot)$ —

Примеры

Трёхмерные вектора с векторным умножением — неассоциативный группоид ($(\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b})$).

$\mathbb{N}$ с возведением в степень —

Арифметика с насыщением $([-N, N], +)$ —

$(\mathbb{N}, +)$ —

$(\mathbb{N}, \cdot)$ —

$(\mathbb{N} \cup \{0\}, +)$ —

$(\mathbb{N} \cup \{0\}, \cdot)$ —

$(\mathbb{Z}, +)$ —

$(\mathbb{Z}, \cdot)$ —

Примеры

Трёхмерные вектора с векторным умножением — неассоциативный группоид ($(\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b})$).

$\mathbb{N}$ с возведением в степень — н/а группоид ($(2^2)^3 \neq 2^{(2^3)}$).

Арифметика с насыщением $([-N, N], +)$ —

$(\mathbb{N}, +)$ —
$(\mathbb{N}, \cdot)$ —

$(\mathbb{N} \cup \{0\}, +)$ —
$(\mathbb{N} \cup \{0\}, \cdot)$ —

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

Примеры

Трёхмерные вектора с векторным умножением — неассоциативный группоид $((\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b}))$.

$\mathbb{N}$ с возведением в степень — н/а группоид $((2^2)^3 \neq 2^{(2^3)})$.

Арифметика с насыщением $([-N, N], +)$ — н/а группоид.

$(\mathbb{N}, +)$ —
$(\mathbb{N}, \cdot)$ —

$(\mathbb{N} \cup \{0\}, +)$ —
$(\mathbb{N} \cup \{0\}, \cdot)$ —

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

Примеры

Трёхмерные вектора с векторным умножением — неассоциативный группоид $((\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b}))$.

$\mathbb{N}$ с возведением в степень — н/а группоид $((2^2)^3 \neq 2^{(2^3)})$.

Арифметика с насыщением $([-N, N], +)$ — н/а группоид.

$(\mathbb{N}, +)$ — полугруппа (ассоц. группоид), коммутативная циклическая;
$(\mathbb{N}, \cdot)$ —

$(\mathbb{N} \cup \{0\}, +)$ —
$(\mathbb{N} \cup \{0\}, \cdot)$ —

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

Примеры

Трёхмерные вектора с векторным умножением — неассоциативный группоид $((\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b}))$.

$\mathbb{N}$ с возведением в степень — н/а группоид $((2^2)^3 \neq 2^{(2^3)})$.

Арифметика с насыщением $([-N, N], +)$ — н/а группоид.

$(\mathbb{N}, +)$ — полугруппа (ассоц. группоид), коммутативная циклическая;
$(\mathbb{N}, \cdot)$ — моноид (полугруппа с единицей), коммутативный.

$(\mathbb{N} \cup \{0\}, +)$ —
$(\mathbb{N} \cup \{0\}, \cdot)$ —

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

Примеры

Трёхмерные вектора с векторным умножением — неассоциативный группоид ($(\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b})$).

$\mathbb{N}$ с возведением в степень — н/а группоид ($(2^2)^3 \neq 2^{(2^3)}$).

Арифметика с насыщением $([-N, N], +)$ — н/а группоид.

$(\mathbb{N}, +)$ — полугруппа (ассоц. группоид), коммутативная циклическая;
$(\mathbb{N}, \cdot)$ — моноид (полугруппа с единицей), коммутативный.

$(\mathbb{N} \cup \{0\}, +)$ — циклический коммутативный моноид;
$(\mathbb{N} \cup \{0\}, \cdot)$ —

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

Примеры

Трёхмерные вектора с векторным умножением — неассоциативный группоид $((\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b}))$.

$\mathbb{N}$ с возведением в степень — н/а группоид $((2^2)^3 \neq 2^{(2^3)})$.

Арифметика с насыщением $([-N, N], +)$ — н/а группоид.

$(\mathbb{N}, +)$ — полугруппа (ассоц. группоид), коммутативная циклическая;
$(\mathbb{N}, \cdot)$ — моноид (полугруппа с единицей), коммутативный.

$(\mathbb{N} \cup \{0\}, +)$ — циклический коммутативный моноид;
$(\mathbb{N} \cup \{0\}, \cdot)$ — коммутативный моноид с нулём.

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

Примеры

Трёхмерные вектора с векторным умножением — неассоциативный группоид ($(\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b})$).

$\mathbb{N}$ с возведением в степень — н/а группоид ($(2^2)^3 \neq 2^{(2^3)}$).

Арифметика с насыщением $([-N, N], +)$ — н/а группоид.

$(\mathbb{N}, +)$ — полугруппа (ассоц. группоид), коммутативная циклическая;
$(\mathbb{N}, \cdot)$ — моноид (полугруппа с единицей), коммутативный.

$(\mathbb{N} \cup \{0\}, +)$ — циклический коммутативный моноид;
$(\mathbb{N} \cup \{0\}, \cdot)$ — коммутативный моноид с нулём.

$(\mathbb{Z}, +)$ — циклическая коммутативная группа;
$(\mathbb{Z}, \cdot)$ —

Примеры

Трёхмерные вектора с векторным умножением — неассоциативный группоид ($(\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b})$).

$\mathbb{N}$ с возведением в степень — н/а группоид ($(2^2)^3 \neq 2^{(2^3)}$).

Арифметика с насыщением $([-N, N], +)$ — н/а группоид.

$(\mathbb{N}, +)$ — полугруппа (ассоц. группоид), коммутативная циклическая;
$(\mathbb{N}, \cdot)$ — моноид (полугруппа с единицей), коммутативный.

$(\mathbb{N} \cup \{0\}, +)$ — циклический коммутативный моноид;
$(\mathbb{N} \cup \{0\}, \cdot)$ — коммутативный моноид с нулём.

$(\mathbb{Z}, +)$ — циклическая коммутативная группа;
$(\mathbb{Z}, \cdot)$ — коммутативный моноид.

Аксиомы кольца

$\mathcal{K} = (\mathbb{K}, +, \cdot, \mathbf{0}, \mathbf{1})$, причём для любых $a, b, c \in \mathbb{K}$:

1. $a + (b + c) = (a + b) + c$;
2. $a + b = b + a$;
3. $a + \mathbf{0} = a$;
4. для каждого $a \in \mathbb{K}$ существует элемент $(-a)$, такой, что $a + (-a) = \mathbf{0}$;
5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
6. $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$;
7. $a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$.

По Б. Л. ван дер Вардену, кольцо — $\mathcal{K} = (\mathbb{K}, +, \cdot)$: 1, 2, 5, 7 и разрешимость $a + x = b$ — может не иметь единицы (3 и 4 доказываются). Множество чётных чисел — не кольцо по 1-7, но кольцо без единицы по ван дер Вардену.

Аксиомы поля

Поле есть алгебра $\mathcal{F} = (\mathbb{F}, +, \cdot, \mathbf{0}, \mathbf{1}), \mathbf{0} \neq \mathbf{1}$, причём:

1. $a + (b + c) = (a + b) + c$;
2. $a + b = b + a$;
3. $a + \mathbf{0} = a$;
4. для каждого $a \in \mathbb{F}$ существует элемент $(-a)$, такой, что $a + (-a) = \mathbf{0}$;
5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
6. $a \cdot b = b \cdot a$;
7. $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$;
8. для каждого $a \in \mathbb{F}$, отличного от $\mathbf{0}$, существует элемент a^{-1}, такой, что $a \cdot a^{-1} = \mathbf{1}$;
9. $a \cdot (b + c) = a \cdot b + a \cdot c$.

Поле $=$ кольцо $+ (\mathbf{0} \neq \mathbf{1}) +$ 6 $+$ 8

Некоммутативное поле (без 6) — **тело**.

Кольцо с 6 — коммутативное кольцо.

Кольцо с 8 — тело либо нулевое кольцо (единственный элемент $\mathbf{0} = \mathbf{1}$).

Примеры

$\mathbb{Z}$ —

$\mathbb{Z}_k = \big(\{0{,}1,\dots,k-1\}, \oplus_k, \odot_k, 0{,}1\big)$ с операциями сложения и умножения по модулю k —

$\mathbb{H}$ с операциями сложения и умножения кватернионов —

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ —

$\mathbb{Z}_p$ (p — простое) —

$\big(\{a + b\cdot\sqrt{2}\}, +, \cdot, 0{,}1\big)$, $a, b \in \mathbb{Q}$ —

Примеры

$\mathbb{Z}$ — коммутативное кольцо.

$\mathbb{Z}_k = (\{0,1,\ldots,k-1\}, \oplus_k, \odot_k, 0,1)$ с операциями сложения и умножения по модулю k —

$\mathbb{H}$ с операциями сложения и умножения кватернионов —

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ —

$\mathbb{Z}_p$ (p — простое) —

$(\{a + b \cdot \sqrt{2}\}, +, \cdot, 0,1)$, $a, b \in \mathbb{Q}$ —

Примеры

$\mathbb{Z}$ — коммутативное кольцо.

$\mathbb{Z}_k = \big(\{0{,}1,\ldots{,}k-1\}, \oplus_k, \odot_k, 0{,}1\big)$ с операциями сложения и умножения по модулю k — коммутативное кольцо (кольцо классов вычетов по модулю k).

$\mathbb{H}$ с операциями сложения и умножения кватернионов —

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ —

$\mathbb{Z}_p$ (p — простое) —

$\big(\{a + b \cdot \sqrt{2}\}, +, \cdot, 0{,}1\big)$, $a, b \in \mathbb{Q}$ —

Примеры

$\mathbb{Z}$ — коммутативное кольцо.

$\mathbb{Z}_k = \big(\{0,1,\ldots,k-1\}, \oplus_k, \odot_k, 0,1\big)$ с операциями сложения и умножения по модулю k — коммутативное кольцо (кольцо классов вычетов по модулю k).

$\mathbb{H}$ с операциями сложения и умножения кватернионов — тело.

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ —

$\mathbb{Z}_p$ (p — простое) —

$\big(\{a + b \cdot \sqrt{2}\}, +, \cdot, 0,1\big)$, $a, b \in \mathbb{Q}$ —

Примеры

$\mathbb{Z}$ — коммутативное кольцо.

$\mathbb{Z}_k = \big(\{0,1,\ldots,k-1\}, \oplus_k, \odot_k, 0,1\big)$ с операциями сложения и умножения по модулю k — коммутативное кольцо (кольцо классов вычетов по модулю k).

$\mathbb{H}$ с операциями сложения и умножения кватернионов — тело.

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — поля.

$\mathbb{Z}_p$ (p — простое) —

$\big(\{a + b \cdot \sqrt{2}\}, +, \cdot, 0,1\big)$, $a, b \in \mathbb{Q}$ —

Примеры

$\mathbb{Z}$ — коммутативное кольцо.

$\mathbb{Z}_k = \left(\{0,1,\ldots,k-1\}, \oplus_k, \odot_k, 0,1\right)$ с операциями сложения и умножения по модулю k — коммутативное кольцо (кольцо классов вычетов по модулю k).

$\mathbb{H}$ с операциями сложения и умножения кватернионов — тело.

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — поля.

$\mathbb{Z}_p$ (p — простое) — поле.

$\left(\{a + b \cdot \sqrt{2}\}, +, \cdot, 0,1\right)$, $a, b \in \mathbb{Q}$ —

Примеры

$\mathbb{Z}$ — коммутативное кольцо.

$\mathbb{Z}_k = \big(\{0,1,\ldots,k-1\}, \oplus_k, \odot_k, 0,1\big)$ с операциями сложения и умножения по модулю k — коммутативное кольцо (кольцо классов вычетов по модулю k).

$\mathbb{H}$ с операциями сложения и умножения кватернионов — тело.

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — поля.

$\mathbb{Z}_p$ (p — простое) — поле.

$\big(\{a + b\cdot\sqrt{2}\}, +, \cdot, 0,1\big)$, $a, b \in \mathbb{Q}$ — поле.

Конечные поля (поля Галуа)

Конечное поле или поле Галуа

Поле, состоящее из конечного числа элементов. $\mathbb{F}_q$ или $\mathrm{GF}(q)$, где q — число элементов (мощность).

$q = p^n$, где p — простое число (**характеристика** поля), $n \in \mathbb{N}$.
С точностью до изоморфизма:
для $q = p$ $\quad \mathrm{GF}(q) = \mathbb{Z}_p$
для $q = p^n$ $\quad \mathrm{GF}(q)$ — расширение поля $\mathbb{Z}_p$

Спасибо за внимание!

МИЭТ
www.miet.ru

Александра Игоревна Кононова
illinc@mail.ru
gitlab.com/illinc/raspisanie