

# Группоиды, кольца, поля

Александра Игоревна Кононова

МИЭТ

30 ноября 2022 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  $\cdot: G \times G \rightarrow G$ .

# 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:  $\exists 1 : \forall a \in G \quad a \cdot 1 = 1 \cdot a = a$ ,  
 $1$  — 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:  $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$ ;
- ② в  $G$  существует единица (нейтральный элемент)  
 $1: a \cdot 1 = 1 \cdot a = a \quad \forall a \in G$ ;
- ③ для каждого  $a \in G$  существует обратный:  
 $a^{-1} \in G: a \cdot a^{-1} = a^{-1} \cdot a = 1$ .

# Свойства

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

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

Если все элементы полугруппы (группы, группоиды) 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  $((\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c}))$ .

$\mathbb{N}$  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  $((\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c}))$ .

$\mathbb{N}$  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  $((\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c}))$ .

$\mathbb{N}$  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  $((\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c}))$ .

$\mathbb{N}$  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  $((\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c}))$ .

$\mathbb{N}$  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  $((\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c}))$ .

$\mathbb{N}$  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  $((\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c}))$ .

$\mathbb{N}$  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  $((\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c}))$ .

$\mathbb{N}$  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  $a, b, c \in \mathbb{K}$ :

- ❶  $a + (b + c) = (a + b) + c$ ;
- ❷  $a + b = b + a$ ;
- ❸  $a + \mathbf{0} = a$ ;
- ❹ для каждого  $a \in \mathbb{K}$  существует элемент  $(-a)$ , такой, что  $a + (-a) = \mathbf{0}$ ;
- ❺  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ;
- ❻  $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ ;
- ❼  $a \cdot (b + c) = a \cdot b + a \cdot c, (b + c) \cdot a = b \cdot a + c \cdot a$ .

По Б. Л. ван дер Вардену, кольцо —  $\mathcal{K} = (\mathbb{K}, +, \cdot)$ : ❶, ❷, ❺, ❻ и разрешимость  $a + x = b$  — может не иметь единицы (❸ и ❹ доказываются). Множество чётных чисел — не кольцо по ❶-❷, но кольцо без единицы по ван дер Вардену.





# Аксиомы поля

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

- ❶  $a + (b + c) = (a + b) + c$ ;
- ❷  $a + b = b + a$ ;
- ❸  $a + 0 = a$ ;
- ❹ для каждого  $a \in \mathbb{F}$  существует элемент  $(-a)$ , такой, что  $a + (-a) = 0$ ;
- ❺  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ;
- ❻  $a \cdot b = b \cdot a$ ;
- ❼  $a \cdot 1 = 1 \cdot a = a$ ;
- ❽ для каждого  $a \in \mathbb{F}$ , отличного от  $0$ , существует элемент  $a^{-1}$ , такой, что  $a \cdot a^{-1} = 1$ ;
- ❾  $a \cdot (b + c) = a \cdot b + a \cdot c$ .

Поле = кольцо + ( $0 \neq 1$ ) + ❻ + ❽

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

Кольцо с ❻ — коммутативное кольцо.

Кольцо с ❽ — тело либо нулевое кольцо (единственный элемент  $0 = 1$ ).

# Примеры

$\mathbb{Z}$  —

$\mathbb{Z}_k = (\{0, 1, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$  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.

$\mathbb{Z}_k = (\{0, 1, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$  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.

$\mathbb{Z}_k = (\{0, 1, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$  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) —

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

# Примеры

$\mathbb{Z}$  — коммутативное кольцо.

$\mathbb{Z}_k = (\{0, 1, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$  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) —

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

# Примеры

$\mathbb{Z}$  — коммутативное кольцо.

$\mathbb{Z}_k = (\{0, 1, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$  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) —

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

# Примеры

$\mathbb{Z}$  — коммутативное кольцо.

$\mathbb{Z}_k = (\{0, 1, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$  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.

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

# Примеры

$\mathbb{Z}$  — коммутативное кольцо.

$\mathbb{Z}_k = (\{0, 1, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$  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.

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



# Конечные поля (поля Галуа)

## Конечное поле или поле Галуа

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

$q = p^n$ , где  $p$  — простое число (**характеристика** поля),  $n \in \mathbb{N}$ .

С точностью до изоморфизма:

для  $q = p$       $\text{GF}(q) = \mathbb{Z}_p$

для  $q = p^n$       $\text{GF}(q)$  — расширение поля  $\mathbb{Z}_p$

# Спасибо за внимание!

МИЭТ

`www.miet.ru`

Александра Игоревна Кононова

`illinc@mail.ru`

`gitlab.com/illinc/raspisanie`