

Группоиды, кольца, поля

Александра Игоревна Кононова

НИУ МИЭТ

2 января 2017 г.

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 —
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 — группоид $((\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b}))$.

\mathbb{N} с возведением в степень — 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 — группоид $((\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b}))$.

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

Арифметика с насыщением $([-N, N], +)$ — 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 — группоид $((\vec{a} \times \vec{b}) \times \vec{b} \neq \vec{a} \times (\vec{b} \times \vec{b}))$.

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

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

$(\mathbb{N}, +)$ — циклическая полугруппа (коммутативная);

(\mathbb{N}, \cdot) —

$(\mathbb{N} \cup \{0\}, +)$ —

$(\mathbb{N} \cup \{0\}, \cdot)$ —

$(\mathbb{Z}, +)$ —

(\mathbb{Z}, \cdot) —

Примеры

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

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

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

$(\mathbb{N}, +)$ — циклическая полугруппа (коммутативная);

(\mathbb{N}, \cdot) — коммутативный моноид.

$(\mathbb{N} \cup \{0\}, +)$ —

$(\mathbb{N} \cup \{0\}, \cdot)$ —

$(\mathbb{Z}, +)$ —

(\mathbb{Z}, \cdot) —

Примеры

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

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

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

$(\mathbb{N}, +)$ — циклическая полугруппа (коммутативная);

(\mathbb{N}, \cdot) — коммутативный моноид.

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

$(\mathbb{N} \cup \{0\}, \cdot)$ —

$(\mathbb{Z}, +)$ —

(\mathbb{Z}, \cdot) —

Примеры

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

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

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

$(\mathbb{N}, +)$ — циклическая полугруппа (коммутативная);

(\mathbb{N}, \cdot) — коммутативный моноид.

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

$(\mathbb{N} \cup \{0\}, \cdot)$ — коммутативный моноид.

$(\mathbb{Z}, +)$ —

(\mathbb{Z}, \cdot) —

Примеры

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

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

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

$(\mathbb{N}, +)$ — циклическая полугруппа (коммутативная);

(\mathbb{N}, \cdot) — коммутативный моноид.

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

$(\mathbb{N} \cup \{0\}, \cdot)$ — коммутативный моноид.

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

(\mathbb{Z}, \cdot) —

Примеры

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

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

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

$(\mathbb{N}, +)$ — циклическая полугруппа (коммутативная);

(\mathbb{N}, \cdot) — коммутативный моноид.

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

$(\mathbb{N} \cup \{0\}, \cdot)$ — коммутативный моноид.

$(\mathbb{Z}, +)$ — 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 $a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$.

Аксиомы поля

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

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

Некоммутативное поле — **тело**.

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

Многочлены над полем

Многочлен степени $n \in \mathbb{N} \cup \{0\}$ над полем \mathcal{F}

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$a_n, a_{n-1}, \dots, a_1, a_0 \in \mathbb{F}$$

$p(x) = q(x)$, если равны их коэффициенты при одинаковых степенях x .

$$x^k \cdot x^m = x^{k+m} (k, m \in \mathbb{N} \cup \{0\}), \quad x^0 \equiv 1.$$

Множество всех многочленов $\mathcal{F}[x]$ — ассоциативно-коммутативное кольцо с единицей.

Делимость многочленов

$$\forall p(x), q(x) \in \mathcal{F}[x] \quad \exists s(x), r(x) \in \mathcal{F}[x] : \\ p(x) = s(x) \cdot q(x) + r(x)$$

причём $\deg r(x) < \deg q(x)$ или $r(x) = 0$.

Многочлен $s(x)$ называется **частным** (неполным частным), а многочлен $r(x)$ — **остатком** от деления $p(x)$ на $q(x)$.

Частное и остаток определяются однозначно.

Справедлива теорема Безу (и её следствия):
остаток от деления $f(x)$ на $(x - a)$ равен $f(a)$.

Неприводимые многочлены

Если для любого разложения

$$p(x) = s(x) \cdot q(x), \quad p(x), s(x), q(x) \in \mathcal{F}[x]$$

либо $\deg s(x) = 0$, либо $\deg q(x) = 0$,

многочлен $p(x)$ называется **неприводимым** (простым) в кольце $\mathcal{F}[x]$ (или над полем \mathcal{F}).

Примеры

	$x^2 + 1$	$x^2 + x + 1$
Над \mathbb{Z}_2	$(x + 1)(x + 1)$	неприводим
Над \mathbb{Z}_3	неприводим	$(x + 2)(x + 2)$
Над \mathbb{R}	неприводим	неприводим
Над \mathbb{C}	$(x + i)(x - i)$	$(x + \frac{1+i\sqrt{3}}{2})(x + \frac{1-i\sqrt{3}}{2})$

Классы вычетов многочленов

Класс вычетов по модулю многочлена $g(x)$ содержит все многочлены $\mathcal{F}[x]$, которые имеют один и тот же остаток при делении на $g(x)$.

Если $g(x)$ неприводим в $\mathcal{F}[x]$, множество классов вычетов (фактор-кольцо $\mathcal{F}[x]/g(x)$) — **поле**.

Поле $\mathcal{F}[x]/g(x)$ — расширение \mathcal{F} , полученное добавлением корня $g(x)$ (примитивное расширение) — фиктивного $c \notin \mathcal{F}$, что $g(c) = 0$.

Примитивные расширения \mathbb{R}

Многочлен $g(x) = x^2 + 1$ неприводим над \mathbb{R} .

Поле \mathbb{C} — примитивное расширение \mathbb{R} , полученное добавлением фиктивного корня $x^2 + 1$ — «мнимой единицы» $i \notin \mathbb{R}$.

x , $x + 1$, $x + 2$, $x^2 + 4$, $x^2 + x + 1$ и $x^4 + 1$ также неприводимы над \mathbb{R} .

Как будут выглядеть примитивные расширения?

Примитивные расширения \mathbb{Z}_2

Многочлен $g(x) = x^2 + x + 1$ неприводим над \mathbb{Z}_2 .

Пусть $i \notin \mathbb{Z}_2$ — фиктивный корень $x^2 + x + 1$.

$$i^2 + i + 1 = 0$$

Элементы примитивного расширения $0, 1, i, i + 1$.

$$i^2 = -(i + 1) = i + 1$$

Поле $\text{GF}(4)$

Полиномиальное представление	Числовое представление	Степени		
		0	1	2
1	1	1	1	1
i	2	1	i (2)	$i + 1$ (3)
$i + 1$	3	1	$i + 1$ (3)	i (2)

Из обобщённой малой теоремы Ферма $a^3 = 1$ для всех ненулевых a .

i и $i + 1$ — примитивные элементы, наименьший i :

$$\begin{aligned} 1 &= 1 &= i^0 \\ 2 &= i &= i^1 \\ 3 &= i + 1 &= i^2 \end{aligned}$$

Сложение и умножение в $GF(4)$

Сложение — сложение многочленов
с учётом $1 + 1 = 0$
(побитовое по модулю 2)

+	0	1	2	$i+1$
0	0	1	i	$i+1$
1	1	0	$i+1$	i
i	i	$i+1$	0	1
$i+1$	$i+1$	i	1	0

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Умножение — умножение
степеней примитивного
элемента с учётом $i^3 = 1$

·	0	1	i	i^2
0	0	0	0	0
1	0	1	i	i^2
i	0	i	i^2	1
i^2	0	i^2	1	i

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Разрежённые полиномы, неприводимые по модулю 2 (порождающие табличные)

$$x^2 + x + 1$$

$$x^3 + x + 1$$

$$x^4 + x + 1$$

$$x^5 + x + 1$$

$$x^6 + x + 1$$

$$x^7 + x^3 + 1$$

$$x^8 + x^4 + x^3 + x^2 + 1 \text{ (RS)}$$

$$x^8 + x^4 + x^3 + x + 1 \text{ (AES)}$$

$$x^9 + x^4 + 1$$

$$x^{10} + x^3 + 1$$

$$x^{11} + x^2 + 1$$

$$x^{12} + x^3 + 1$$

$$x^{13} + x^4 + x^3 + x + 1$$

$$x^{14} + x^5 + 1$$

$$x^{15} + x + 1$$

$$x^{16} + x^5 + x^3 + x + 1$$

$$\dots$$

$$x^{32} + x^7 + x^3 + x^2 + 1$$

$$\dots$$

$$x^{64} + x^4 + x^3 + x + 1$$

$$\dots$$

$$x^{128} + x^7 + x^2 + x + 1$$

$$\dots$$

$$x^{256} + x^{10} + x^5 + x^2 + 1$$

$$\dots$$

$$x^{512} + x^8 + x^5 + x^2 + 1$$

Наименьший примитивный элемент расширения: i (2) (для большинства).

Для используемого в AES $x^8 + x^4 + x^3 + x + 1$ примитивный элемент $i + 1$ (3).

Таблица степеней GF(8), порождающий полином $x^3 + x + 1$

			Степени							
			0	1	2	3	4	5	6	7
Полиномиально с представление	1	1	1	1	1	1	1	1	1	1
	x	2	1	2	4	3	6	7	5	1
	x+1	3	1	3	5	4	7	2	6	1
	x ²	4	1	4	6	5	2	3	7	1
	x ² +1	5	1	5	7	6	3	4	2	1
	x ² +x	6	1	6	2	7	4	5	3	1
	x ² +x+1	7	1	7	3	2	5	6	4	1

Таблица степеней GF(16)

	Степени															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	3	6	12	11	5	10	7	14	15	13	9	1
3	1	3	5	15	2	6	10	13	4	12	7	9	8	11	14	1
4	1	4	3	12	5	7	15	9	2	8	6	11	10	14	13	1
5	1	5	2	10	4	7	8	14	3	15	6	13	12	9	11	1
6	1	6	7	1	6	7	1	6	7	1	6	7	1	6	7	1
7	1	7	6	1	7	6	1	7	6	1	7	6	1	7	6	1
8	1	8	12	10	15	1	8	12	10	15	1	8	12	10	15	1
9	1	9	13	15	14	7	10	5	11	12	6	3	8	4	2	1
10	1	10	8	15	12	1	10	8	15	12	1	10	8	15	12	1
11	1	11	9	12	13	6	15	3	14	8	7	4	10	2	5	1
12	1	12	15	8	10	1	12	15	8	10	1	12	15	8	10	1
13	1	13	14	10	11	6	8	2	9	15	7	5	12	3	4	1
14	1	14	11	8	9	7	12	4	13	10	6	2	15	5	3	1
15	1	15	10	12	8	1	15	10	12	8	1	15	10	12	8	1

Спасибо за внимание!

НИУ МИЭТ

<http://miet.ru/>

Александра Игоревна Кононова

illinc@mail.ru