Алгебра и геометрия

Sergio

5 февраля 2025 г.

Содержание

1 Лекция 1 **3**

1.1 Алгебра многочленов 3

1.1.1 Многочлены нескольких переменных 7

1.1.2 Деление с остатком 7

1.1.3 Теорема Безу и схема Горнера 9

1.1.4 НОД двух мн-ов. Алгоритм Евклида. 10

1 Лекция 1

1.1 Алгебра многочленов

$f : \mathbb{R} \to \mathbb{R}$

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n, n \in \mathbb{N} \cup \{ 0 \}$$

Количество a_i — конечно.

$$\mathbb{R}[x], +, \cdot, \cdot\lambda, \lambda \in \mathbb{R}$$

$$1, x, x^2, \ldots$$

$$x^m \cdot x^l = x^{m+l}$$

Определение 1.1. Алгеброй над полем $\mathbb{F}$ называется множество A с определёнными на нём операциями: $+; \cdot; \cdot\lambda, \lambda \in \mathbb{R}$. Причём выполняются следующие свойства:

1) $(A, +, \cdot\lambda)$ — ЛП над $\mathbb{F}$

2) $(A, +, \cdot)$ — кольцо (не обязательно коммутативное)

$$\lambda(x \cdot y) = x \cdot (\lambda y) = (\lambda x) \cdot y, \forall \lambda \in \mathbb{F}, x, y \in A$$

Пример. *1.* $\mathbb{R}[x]$ *— алгебра многочленов (алгебра с единицей, т. к. это кольцо с единицей)*

2. $M_n(\mathbb{F})$

Вопрос: что собой представляет $\mathbb{Z}_p[x]$? (p - простое)
По МТФ, $\forall x \neq 0, \overline{x}^{p-1} = 1 \Rightarrow \overline{x}^p = \overline{x}$.
Следовательно, $\overline{x}^p - \overline{x} \equiv 0$ (что очень плохо)
Выход из ситуации: рассм. многочлен как набор коэффициентов.
Положим $\tilde{R}$ — коммутативное кольцо с 1

Определение 1.2. Многочленом над кольцом $\tilde{R}$ **с 1** называется последовательность:

$$(a_0, a_1, \ldots, a_n, \ldots)$$

где лишь конечное число коэффициентов (из $\tilde{R}$) отличны от 0 (такие п-ти называют **финитными**).

Операции:

- Сложение: $A = (a_i), B = (b_i)$:

$$A + B = (a_i + b_i)$$

- Умножение: $A = (a_i), B = (b_i) \mapsto C = (c_i)$:

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

Пример.

$$(a_0 + a_1 x)(b_0 + b_1 x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + a_1 b_1 x^2$$

- Умножение на $\lambda \in \tilde{R}$:

$$(\lambda A) = (\lambda a_i)$$

Утверждение 1.1. *Множество $\tilde{R}[x]$ всех многочленов над $\tilde{R}$ является коммутативным кольцом относительно "$+, \cdot$"*

Доказательство. $(\tilde{R}[x], +)$ — абелева группа с нейтральным эл-ом $0 = (0, 0, 0, \ldots)$

$(\tilde{R}[x], \cdot)$ - коммутативная полугруппа.

$$BA \to c'_k = \sum_{j+i=k} b_i \cdot a_j = c_k$$

$$(A \cdot B) \cdot C \stackrel{?}{=} A \cdot (B \cdot C)$$

$$((A \cdot B) \cdot C)_k = \sum_{i=0}^{k} (A \cdot B)_i \cdot c_{k-i} = \sum_{i=0}^{k} \sum_{j=0}^{i} a_j b_{i-j} c_{k-i} \tag{1}$$

$$(A \cdot (B \cdot C))_k = \sum_{s=0}^{k} a_s (BC)_{k-s} = \sum_{s=0}^{k} \sum_{t=0}^{k-s} a_s b_t c_{k-s-t} \tag{2}$$

$$i = s + t \iff t = i - s, 0 \le t \le k - s \Rightarrow 0 \le i - s \le k - s$$

$$\Rightarrow s \le i \le k$$

$$(2) = \sum_{s=0}^{k} \sum_{i=s}^{k} a_s b_{i-s} c_{k-i} = \big[s \mapsto j\big] = \sum_{j=0}^{k} \sum_{i=j}^{k} a_j b_{i-j} c_{k-i}$$

Диаграмма, показывающая, что суммы пробегают одинаковые пары (i, j)

$$A(B + C) \stackrel{?}{=} AB + AC$$

$$(A(B + C))_k = \sum_{i=0}^{k} a_i (b + c)_{k-i} = \sum_{i=0}^{k} a_i b_{k-i} + \sum_{i=0}^{k} a_i c_{k-i}.$$

Ч. Т. Д. □

Следствие. $\mathbb{F}[x]$ — *бесконечномерная алгебра с базисом:* $1, x, x^2, \ldots$

$$1 = (1, 0, 0, 0, \ldots)$$

$$1 \cdot a \stackrel{?}{=} a$$

$$(1 \cdot a)_k = \sum_{i=0}^{k} 1_i \cdot a_{k-i} = \big[i = 0\big] = a_k$$

Вывод: когда $\tilde{R}$ - кольцо с единицей, то и $\tilde{R}[x]$ — кольцо с единицей.

Определение 1.3.

$$x \colon = (0, 1, 0, 0, \ldots)$$

$$x^2 = x \cdot x = (0, 1, 0, 0, \ldots) \cdot (0, 1, 0, 0, \ldots)$$

$$(x^2)_k = \sum_{i=0}^{k} x_i x_{k-i} = \begin{cases} 1, k = 2 \\ 0, k \neq 2 \end{cases}$$

$$x^n = (0, 0, \ldots, \underbrace{1}_{n+1}, 0, \ldots)$$

$$(a_0, a_1, \ldots, a_n + 1, 0, 0, \ldots) = a_0 \cdot 1 + a_1 \cdot x + \ldots + a_n \cdot x^n$$

Определение 1.4. Последний ненулевой коэффициент многочлена $A = (a_1, \ldots, a_n, 0, \ldots)$ называется **старшим коэффициентом многочлена** A, а его **индекс — степень многочлена**.

$$\deg A = \max \{\, i \mid a_i \neq 0 \,\}$$

Замечание. *Степень нулевого многочлена обычна неопределена, либо равна* $-\infty$

Определение 1.5. Коммутативное кольцо R с единицей $1 \neq 0$ называется **областью целостности** (или целостностным кольцом), если:

$$\forall a, b \in R \Rightarrow a \cdot b \neq 0, a \neq 0, b \neq 0$$

(Т. е. в R нет делителей нуля)

Утверждение 1.2. *Пусть* R *— область целостности. Тогда в* R *справедливо правило сокращения:*

$$\begin{cases} ab = ac \\ a \neq 0 \end{cases} \Rightarrow b = c$$

Доказательство.

$$a(b-c) = 0 \overset{\text{Область целостности}}{\Rightarrow} b - c = 0 \Rightarrow b = c$$

□

Вопрос: пусть R — коммутативное кольцо с 1, с правилом сокращения. Является ли тогда R — областью целостности.

Утверждение 1.3. *Пусть* R *— коммутативное кольцо с* 1.

$$A, B \in R[x]$$

a) $\deg(A + B) \leq \max(\deg A, \deg B)$

b) $\deg(A \cdot B) \leq \deg A + \deg B$

c) Если вдобавок к условию, R *— область целостности, то:*

$$\deg(A \cdot B) = \deg A + \deg B$$

Доказательство. a) Пусть $a = \deg A, b = \deg B$. Покажем, что если $n > \max(a, b)$, то $(A + B)_n = 0$

$$(A + B)_n = a_n + b_n = 0 + 0 = 0$$

b) Пусть $n > a + b$. Покажем, что $(A \cdot B)_n = 0$

$$(A \cdot B)_n = \sum_{i=0}^{n} a_i b_{n-i} = \underbrace{\sum_{i=0}^{a} a_i b_{n-i}}_{\text{0,т. к. } n-i>b} + \underbrace{\sum_{i=a+1}^{n} a_i b_{n-i}}_{\text{0,т. к. } i>a}$$

$$i \le a \iff -i \ge -a \Rightarrow n - i \ge n - a > b$$

c) R — область целостности:

$$(A \cdot B)_n = (A \cdot B)_{a+b} = \underbrace{\sum_{i=0}^{a-1} a_i \cdot b_{n-i}}_{0} + \underbrace{(A)_a (B)_b}_{\neq 0} + \underbrace{\sum_{i=a+1}^{n} a_i b_{n-i}}_{0} \neq 0$$

□

Следствие. *Если R — область целостности, то $R[x]$ — тоже область целостности.*

1.1.1 Многочлены нескольких переменных

Пусть мы строим многочлен над кольцом $R[x_1]$ (область целостности), тогда можно определить:

$$R[x_1, x_2] = (R[x_1])[x_2]$$

$$R[x_1, \ldots, x_n] := \underbrace{(R[x_1, \ldots, x_{n-1}])}_{R'}[x_n]$$

Если $(a_0, \ldots, a_n, \ldots)$ содержит бесконечно много ненулевых элементов, то оно принадлежит

$R[[x]]$ — кольцу формальных степенный рядов (ФСР)

1.1.2 Деление с остатком

Пусть $\mathbb{F}$ - поле. $\mathbb{F}[x]$ — кольцо многочленов.

Теорема 1.1. *Пусть $A, B \in \mathbb{F}[x], B \neq 0$, тогда:*

a) $\exists$ *представление.*

$$A = Q \cdot B + R, \text{ где } Q, R \in \mathbb{F}[x], R = 0, \text{либо } \deg R < \deg B$$

b) Неполное частное Q *и остаток* R *определяются по* A *и* B *однозначно.*

Доказательство. a) Пусть $A = 0$ или $\deg A < \deg B$

$$A = 0 \cdot B + A \text{ — наше разложение}$$

Пусть теперь $\deg A \geq \deg B$ (докажем с помощью ММИ по $\deg A$)

$$HT(A) = \alpha x^a \text{ — старший член многочлена } A$$

$$HT(B) = \beta x^b$$

$$HT(A) = M \cdot HT(B), M = \frac{\alpha}{\beta} x^{a-b}$$

$$A' = A - MB$$

$$A' = Q'B + R', \text{ разложение существует по индукции}$$

$$A = MB + A' = MB + Q'B + R' = (M + Q')B + R'$$

b) Единственность:

$$A = Q_1 B + R_1 = Q_2 B + R_2$$

$$(Q_1 - Q_2)B = R_2 - R_1$$

$$R_2 - R_1 \leq \max(\deg R_1, \deg R_2) < \deg B$$

$$\deg((Q_1 - Q_2)B) = \deg(Q_1 - Q_2) + \deg B$$

Пусть $Q_1 \neq Q_2 \Rightarrow \deg((Q_1 - Q_2)B) \geq B$ — противоречие.

□

Замечание. *В кольце, кот.* ***не является областью целостности****, есть необратимые элементы* $\Rightarrow$ ***доказательство в этом случае нарушается****.*

1.1.3 Теорема Безу и схема Горнера

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

Определение 1.6. Значением многочлена $f \in \mathbb{F}[x]$ на элементе $c \in \mathbb{F}$ называется:

$$f(c) = a_0c^n + a_1c^{n-1} + \ldots + a_{n-1}c + a_n$$

Элемент c называется корнем f, если:

$$f(c) = 0$$

Утверждение 1.4. *Значение f на элементе $c \in F$ равно остатку от деления f на линейный двучлен $x - c$.*

Доказательство.

$$f(x) = q(x)(x - c) + r(x)$$
$$r(x) = 0 \text{ или } \deg r < 1$$
$$f(c) = 0 + r(c) = r(c)$$

□

Теорема 1.2 (Безу)**.** *Элемент $c \in \mathbb{F}$ является корнем многочлена $f(x) \in \mathbb{F}[x] \iff (x - c)|f$*

Доказательство. c — корень $f \iff f(c) = 0 \iff r = 0 \iff (x - c)|f$ □

Схема горнера:

Требуется разделить $f(x) = a_0x^n + \ldots + a_{n-1}x + a_n$ на $(x - c)$. (Лектор демонстрирует алгоритм)

Обоснование схемы Горнера:

$$f(x) = q(x)(x - c) + r = (b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1})(x - c) + r =$$
$$= b_0x^n + (b_1 - c \cdot b_0)x^{n-1} + \ldots + (b_{n-1} - c \cdot b_{n-2})x + r - b_{n-1} \cdot c$$

$$\begin{cases} a_0 = b_0 \\ a_1 = b_1 - c \cdot b_0 \\ a_2 = b_2 - c \cdot b_1 \\ \vdots \\ a_{n-1} = b_{n-1} - c \cdot b_{n-2} \\ a_n = r - b_{n-1} \cdot c \end{cases}$$

1.1.4 НОД двух мн-ов. Алгоритм Евклида.

Определение 1.7. f делится на g, если:

$$f = q \cdot g, q \in \mathbb{F}[x]$$

Обозначение: $f \vdots g$ или $g|f$

Определение 1.8. $f, g \in \mathbb{F}[x]$ называются **ассоциированными**, если:

$$f \vdots g \text{ и } g \vdots f$$

$$f = q_1 \cdot g, \deg f = \deg q_1 + \deg g \Rightarrow \deg f \geq \deg g$$
$$g = q_2 \cdot f \Rightarrow \deg g \geq \deg f$$
$$\Rightarrow \deg g = \deg f$$
$$\deg q_1 = \deg q_2 = 0$$

Определение 1.9 (НОД)**.** Мн-н $d \in \mathbb{F}[x]$ наз-ся наибольшим общим делителем f и g, (НОД$(f, g) = d$), если:

a) $f \vdots d$ и $g \vdots d$

b) Если d' — общий делитель f и g, то $d \vdots d'$

Замечание. *НОД(f, g) определён* ***с точностью до ассоциированности.***

$$d \text{ и } d' - \text{два НОДа}$$

$$\Rightarrow d \vdots d', d' \vdots d \Rightarrow d \sim d'$$

Определение 1.10. НОД(f, g) называется **нормализованным**, если его старший коэффициент равен 1.

Теорема 1.3 (О сущ-ии НОД)**.** *Пусть $f, g \in \mathbb{F}[x]$, причём хотя бы один из них ненулевой. Тогда:*

a) НОД(f, g) существует, НОД$(f, g) \in \mathbb{F}[x]$

b) *Если* $d = НОД(f, g)$, *то* $\exists u, v \in \mathbb{F}[x]$:

$$u \cdot f + v \cdot g = d$$

Доказательство. a) Доказательство конструктивное (изложение алгоритма Евклида).

– $f = 0, g \neq 0 \Rightarrow$ НОД$(f, g) = g$

$$0 \cdot f + 1 \cdot g = g \text{ — ЛК}$$

– $f \neq 0, g \neq 0$:

1) $f = q_1 \cdot g + r_1$, где $r_1 = 0$ или $\deg r_1 < \deg g$
2) $g = q_2 \cdot r_1 + r_2, \ldots$
3) $r_1 = q_3 \cdot r_2 + r_3, \ldots$

$\vdots$

n) $r_{n-2} = q_n \cdot r_{n-1} + r_n, r_n \neq 0$

$n+1$) $r_{n-1} = q_{n+1} r_n$

Получаем убывающую последовательность натуральных чисел:

$$\deg r_1 > \deg r_2 > \ldots$$

Где $r_i = 0$ или $\deg r_i = 0$

Покажем, что r_n - искомый НОД.

$$r_{n-1} \vdots r_n \Rightarrow r_{n-2} \vdots r_n \Rightarrow \ldots \Rightarrow f \vdots r_n, g \vdots r_n$$

Пусть $f \vdots d'$ и $g \vdots d'$. Покажем, что $r_n \vdots d'$.

Из Рав-ва (1) получаем, что и $r_1 \vdots d' \Rightarrow r_2 \vdots d' \Rightarrow \ldots \Rightarrow r_n \vdots d'$

b) Покажем, что все остатки r_i являются ЛК f и g. r_1 — очев. явл-ся ЛК f и g. Далее:

$$r_2 = g - q_2 r_1 = g - q_2(f - q_1 g) = (1 - q_1)g - q_2 f$$

$$r_{n-2} = u'' f + v'' g$$

$$r_{n-1} = u' f + v' g$$

$$r_n = r_{n-2} - q_n r_{n-1} = u''f + v''g - q_n u'f - q_n v'g =$$
$$= (u'' - q_n u')f + (v'' - q_n v')g$$

Ч. Т. Д.

□

Определение 1.11. Многочлены f и g называются **взаимнопростыми** если НОД(f, g)= 1

Замечание. *f и g взаимнопросты* $\iff \exists u, v \in \mathbb{F}[x]$:

$$u \cdot f + v \cdot g = 1$$

Замечание. *Схему горнера можно обобщить, когда степень делителя* $= 2$.