Алгебра и геометрия

Григорян Сергей

12 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

2 Лекция 2 **12**
2.1 Неприводимые многочлены 12
2.2 Корни многочленов 15
2.3 Основная теорема алгебры 16
2.3.1 Доказательство ОТА 16
2.3.2 Следствия из ОТА 18
2.4 Формальная производная 20
2.5 Поле частных области целостности 23

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* $= 2$.

2 Лекция 2

2.1 Неприводимые многочлены

$\mathbb{F}$ — поле, $\mathbb{F}[x]$ — кольцо многочленов над $\mathbb{F}$.

Определение 2.1. Ненулевой многочлен P с $\deg P > 0$ называется **неприводимым над полем** $\mathbb{F}$, если:

$$P = A \cdot B \Rightarrow \begin{bmatrix} \deg A = 0 \\ \deg B = 0 \end{bmatrix}$$

Т. е. его нельзя разложить в произведение многочленов более низких степеней $\in \mathbb{F}[x]$

Пример.

$$x^2 + 1 \in \mathbb{R}[x]$$
$$x^2 + 1 = (x - \alpha)(x - \beta), \alpha, \beta \in \mathbb{R}$$
$$x^2 - (\alpha + \beta)x + \alpha\beta$$
$$D = (\alpha + \beta)^2 - 4\alpha\beta = (\alpha - \beta)^2 \geq 0$$

Однако дискриминант $x^2 + 1 \in \mathbb{R}[x]$ отрицательный $\Rightarrow$ противоречие!.

$$x^2 + 1 \in \mathbb{C}[x]$$
$$\Rightarrow x^2 + 1 = (x - i)(x + i)$$

Замечание. *Понятие неприводимости многочлена бесмысленно, если мы не говорим о поле, над которым он построен.*

Замечание. *Пусть P — неприводим, и $P \vdots A \Rightarrow \begin{bmatrix} A = const \sim 1 \\ A \sim P \end{bmatrix}$*

$$\forall B \in \mathbb{F}, НОД(B, P) = \begin{bmatrix} 1 \\ p, p \neq 1 \end{bmatrix}$$

Похожим свойством обладают простые числа в $\mathbb{Z}$.

Утверждение 2.1. *Пусть P — неприводим над $\mathbb{F}$:*

$$(A \cdot B) \vdots P \Rightarrow \begin{bmatrix} A \vdots P \\ B \vdots P \end{bmatrix}$$

Доказательство. От противного, пусть $A \not\vdots P \wedge B \not\vdots P$, тогда:

$$\begin{cases} gcd(A, P) = 1 \\ gcd(B, P) = 1 \end{cases}$$

По лемме из прошлой лекции:

$$\exists u_1, v_1, u_2, v_2 \in \mathbb{F}[x] \colon \begin{cases} u_1 A + v_1 P = 1 \\ u_2 B + v_2 P = 1 \end{cases}$$

$\Rightarrow u_1 u_2 AB + (u_1 v_2 A + u_2 v_1 B + v_1 v_2 P)P = 1 \Rightarrow 1 \vdots P \Rightarrow$ противоречие!

□

Следствие. *Если P — неприводим, $A_1 \cdot A_2 \cdot \ldots \cdot A_n \vdots P$, то $\exists j \colon A_j \vdots P$*

Теорема 2.1 (Основная теорема арифметики для многочленов)**.** *а) Пусть A — ненулевой многочлен из $\mathbb{F}[x], F$ — поле. Тогда $\exists \alpha \in \mathbb{F}^*$ и неприво. многочлены над $\mathbb{F}$:*

$$P_1, P_2, \ldots, P_n$$

Такие, что:

$$A = \alpha P_1 P_2 \ldots P_n, n \geq 0$$

б) Если $A = \alpha P_1 \dots P_n = \beta Q_1 \dots Q_m$, *где* P_i *и* Q_i — *неприводимые многочлены, то:*

$$\begin{cases} n = m \\ \exists \sigma \in S_n \colon P_i \sim Q_{\sigma(i)} \end{cases}$$

Доказательство. а) Если $\deg A = 0, A = \alpha, \alpha \in \mathbb{F}^*$

Если $\deg A = 1$, то $A = P$ — неприводим.

ММИ по $\deg A$:

Если A — неприводим, то утверждение доказано. Иначе, $A = P \cdot Q$, т. ч. $\deg P, \deg Q < \deg A$, которые раскладываются в произведение неприводимых (по предположению индукции).

б) Докажем ММИ по числу неприводимых множителей (n):

Если $n = 0 \Rightarrow A = \alpha \in \mathbb{F}^*$ — единственно.

Иначе:

$$A = \alpha P_1 \dots P_n = \beta Q_1 \dots Q_m$$

$$\beta Q_1 \dots Q_m \vdots P_n$$

По утверждению (2.1) $\exists j \colon Q_j \vdots P_n \Rightarrow Q_j = \gamma P_n$

$$\Rightarrow \alpha P_1 \dots P_n = \beta\gamma Q_1 \dots Q_{j-1} Q_{j+1} \dots Q_m P_n$$

Так как $\mathbb{F}[x]$ — область целостности, мы можем сократить обе части на P_n:

$$\alpha P_1 \dots P_{n-1} = \beta\gamma Q_1 \dots Q_{j-1} Q_{j+1} Q_m$$

По предположению индукции:

$$\begin{cases} n - 1 = m - 1 \\ \exists \sigma \colon \{1, 2, \dots, n-1\} \to \{1, 2, \dots, j-1, j+1, \dots, n\} \end{cases}$$

Доопределим: $\sigma(n) = j$, тогда $\forall i = 1, \dots, n \colon P_i \sim Q_{\sigma(i)}$. Переход индукции доказан!

□

Следствие. *Пусть* $A = \alpha P_1^{n_1} \dots P_s^{n_s}$, *причём* $P_i \not\sim P_j$, *при* $i \neq j$. *Тогда произвольный делитель многочлена* A *имеет вид:*

$$D = \gamma P_1^{m_1} \dots P_s^{m_s}$$

где $\forall i, 0 \leq m_i \leq n_i$

Доказательство.

$$A \vdots D \Rightarrow A = QD$$

D, Q не имеют непр. множителей, которых нет в A:

$$\Rightarrow Q = \beta P_1^{l_1} \dots P_s^{l_s}$$

$$D = \gamma P_1^{m_1} \dots P_s^{m_s}$$

$$P_i^{n_i} = P_i^{m_i} \cdot P_i^{l_i} \Rightarrow n_i = m_i + l_i \Rightarrow 0 \leq m_i \leq n_i$$

□

2.2 Корни многочленов

Определение 2.2. Пусть $f \in \mathbb{F}[x]$, $\mathbb{F}$ — поле, тогда:

$$c \in F, f(c) = 0 \Rightarrow f \vdots (x - c)$$

Пусть:

$$f \vdots (x-c), f \vdots (x-c)^2, \dots, f \vdots (x-c)^k, f \vdots (x-c)^{k+1}$$

Тогда c называется **корнем кратности** k.

Замечание. *c — корень кратности k* $\iff$ $f = (x-c)^k q(x), q(c) \neq 0$. *Если допустить $q(c) = 0$, то:*

$$q(x) = (x-c)p(x) \Rightarrow f(x) = (x-c)^{k+1}p(x), \text{ противречие}$$

Теорема 2.2. *Пусть $f \in \mathbb{F}[x], c_1, \dots, c_m$ — корни f, а $k_1, \dots, k_m$ — их кратности, и пусть* $\deg f = n$, *тогда:*

$$n \geq \sum_{i=1}^{m} k_i \tag{3}$$

Доказательство.

$$f \vdots (x-c_1)^{k_1}, f \vdots (x-c_2)^{k_2}, \dots, f \vdots (x-c_m)^{k_m}$$

Т. к. $c_i \neq c_j$ при $i \neq j$, то $(x-c_i) \not\sim (x-c_j)$:

$$f \vdots (x-c_1)^{k_1} \dots (x-c_m)^{k_m}$$

$$f = (x - c_1)^{k_1} \dots (x - c_m)^{k_m} g$$
$$\sum_{i=1}^{m} k_i = \deg f - \deg g \leq n$$

□

Замечание. *В неравенстве* (3) *равенство достигается* $\iff$ f *разлагается в произведение линейным множителей над* $\mathbb{F}$

Определение 2.3. Если f **разлагается в произведение линейный множителей** над полем $\mathbb{F}$, то говорят, что он **линейно факторизуем** над $\mathbb{F}$

Вопрос: что будет, если поле $\mathbb{F}$ заменить на R — коммутативное кольцо с 1?

Пример.

$$f = x^2 + x, f \in \mathbb{Z}_6[x]$$

Корни: $0, 2, 3, 5$

Разложения:

1)

$$x^2 + x = x(x + 1) \Rightarrow \textit{Корни: } 0, -1 \equiv 5 \pmod 6$$

2)

$$x^2 + x = (x+3)(x+4) \Rightarrow \textit{Корни: } -3 \equiv 3 \pmod 6, -4 \equiv 2 \pmod 6$$

2.3 Основная теорема алгебры

2.3.1 Доказательство ОТА

Теорема 2.3. *Пусть* $f \in \mathbb{C}[z], \deg f > 0$*, тогда* f *имеет корень. В общем случае – комплексный.*

Определение 2.4. Будем говорить, что последовательность $\{ z_n \} \to z$ (сходится к z), если:

$$|z_n - z| \to 0, n \to +\infty$$

Или же:

$$\lim_{n \to \infty} z_n = z$$

Лемма 2.4.

$$\lim_{n\to\infty} z_n = z \iff \begin{cases} \lim_{n\to\infty} x_n = x \\ \lim_{n\to\infty} y_n = y \end{cases}$$

где $z_n = x_n + iy_n, z = x + iy$

Лемма 2.5. *Если* $\lim_{n\to\infty} z_n = z \Rightarrow \lim_{n\to\infty} |z_n| = |z|$

Лемма 2.6. *Если:*

$$\begin{cases} \lim_{n\to\infty} z_n = z \\ \lim_{n\to\infty} w_n = w \end{cases} \Rightarrow \begin{cases} \lim_{n\to\infty}(z_n \pm w_n) = z \pm w \\ \lim_{n\to\infty}(z_n \cdot w_n) = z \cdot w \end{cases}$$

Следствие. *Если* $\lim_{n\to\infty} z_n = z$, *то* $\forall f \in \mathbb{C}[z] \Rightarrow \lim_{n\to\infty} f(z_n) = f(z)$

Определение 2.5. Будем говорить, что последовательность z_n сходится к ∞, если:

$$\lim_{n\to\infty} z_n = \infty$$

Лемма 2.7. $\forall$ *последовательности* $\{ z_n \}$, $\exists$ *подпоследовательсть* $\{ z_{n_k} \}$, *т. ч.:*

$$z_{n_k} \to z_0 \text{ или } z_{n_k} \to \infty$$

Лемма 2.8. *Если* $\lim_{n\to\infty} = \infty$, *то* $\forall f \in \mathbb{C}[z]$ — *положительной степени:*

$$\lim_{n\to\infty} f(z_n) = \infty$$

Лемма 2.9 (Даламбер)**.** *Пусть* $f \in \mathbb{C}[z]$ *и* $f(z_0) \neq 0$, *тогда* $\forall \varepsilon > 0$ *в* $U_\varepsilon(z_0)$, *есть* $z \in U_\varepsilon(z_0)$, *т. ч.:*

$$|f(z)| < |f(z_0)|$$

Доказательство ОТА:.

$$A = \inf_{z\in\mathbb{C}} |f(z)| \in \mathbb{R}_{\geq 0}$$

Покажем, что inf достигается, т. е. $\exists z_0 \in \mathbb{C}$:

$$|f(z_0)| = A$$

По определению inf, $\exists z_n \in \mathbb{C}$: $\lim_{n\to\infty} |f(z_n)| = A$

По лемме (2.7), $\exists \{ z_{n_k} \}$, т. ч.:

$$z_{n_k} \to z_0 \vee z_{n_k} \to \infty$$

Покажем, что случай $\{ z_{n_k} \} \to \infty$ невозможен.

$$\lim_{k\to\infty} z_{n_k} = \infty \Rightarrow \lim_{k\to\infty} |f(z_{n_k})| = \infty \text{ — противоречие}$$

Поэтому $\{ z_{n_k} \} \to z_0 \Rightarrow f(z_{n_k}) \to f(z_0)$

$$\lim_{k\to\infty} f(z_{n_k}) = |f(z_0)| = A$$

По лемме Даламбера:

$$A \neq 0 \Rightarrow f(z_0) \Rightarrow \exists z \in U_\varepsilon(z_0) \colon\ |f(z)| < |f(z_0)| = A = \inf_{z\in\mathbb{C}} |f(z)|$$

Это противоречие $\Rightarrow A = 0, f(z_0) = 0$ □

Замечание. *На экзамене нужно будет привести леммы (все кроме леммы Даламбера - б/д, док-во леммы Даламбера из анализа), и соотв. доказать теорему*

2.3.2 Следствия из ОТА

Определение 2.6. Поле $\mathbb{F}$ называется алгебраически замкнутым, если:

$$\forall f \in \mathbb{F}[x], \deg F > 0$$

Обязательно имеет хотя бы один корень.

Следствие. *Поле $\mathbb{C}$ — алгебраически замкнуто*

Следствие. *Всякий многочлен положительной степени n из $\mathbb{C}[x]$ линейно факторизуем. (можно разложить в произведение n линейный множителей)*

Доказательство.

$$\deg f = n$$

По ОТА $\exists$ корень в $\mathbb{C}$:

$$f = (x - c_1)q_1(x), \deg q_1 = n - 1$$

$$f = \alpha(x - c_1)(x - c_2)\dots(x - c_n)$$

□

Следствие. *Всякий многочлен из $\mathbb{C}[x]$ степени $n > 0$ имеет ровно n корней, если $\forall$ корень считать столько раз, какова его кратность.*

Следствие. *Всякий многочлен из $\mathbb{R}[x]$ степени $n > 0$ разлагается в произведение линейный многочленов, а также квадратичных многочленов с отрицательным дискриминантом.*

Доказательство.

$$f \in \mathbb{R}[x] \subset \mathbb{C}[x]$$

Пусть c — корень f, если:

а) $c \in \mathbb{R} \Rightarrow f \vdots (x - c) \Rightarrow f = (x - c)q(x), q \in \mathbb{R}[x]$

К $q(x)$ применим предположение индукции.

б) $c \in \mathbb{C}\backslash\mathbb{R}$ — корень $f(x)$

$$f \vdots (x - c)$$

Заметим, что $f(\overline{c}) = 0$, т. е. $\overline{c}$ — тоже корень:

$$f \vdots (x - \overline{c})$$

$$\Rightarrow f \vdots (x - c)(x - \overline{c}) = x^2 - 2\operatorname{Re} c \cdot x + |c|^2$$

$$f = (x^2 - 2\operatorname{Re} c \cdot x + |c|^2)q(x)$$

Для многочлена:

$$x^2 - 2\alpha x + (\alpha^2 + \beta^2), \alpha, \beta \in \mathbb{R}, \beta \neq 0$$

$$D = 4\alpha^2 - 4(\alpha^2 + \beta^2) = -4\beta^2 < 0$$

Поэтому всё ок и к q применимо предположение индукции.

□

Замечание. *Если $f \in \mathbb{R}[x]$ и c — корень f кратности k, $c \in \mathbb{C}\backslash\mathbb{R}$, то $\overline{c}$ тоже корень кратности k.*

Доказательство.

$$f(x) = (x-c)^k q(x), q(x) \neq 0$$

Применим слева и справа комплексное сопряжение:

$$f(x) = (x-\overline{c})^k \overline{q}(x)$$

Следовательно кратность корня $\overline{c}$ не меньше чем k. Пусть она больше, тогда:

$$\overline{q}(\overline{c}) = 0 \iff \overline{q(c)} = 0 \iff q(c) = 0 \text{ противоречие}$$

□

Следствие. *Если $f \in \mathbb{R}[x]$ и $\deg f$ — нечётное число, то найдётся $c \in \mathbb{R}, f(c) = 0$*

Доказательство. Каждому комплексному корню соотвествует сопряжённый ему же $\Rightarrow$ убрав все комплексные корни, останется хотя бы один "непарный"вещественный корень. □

Следствие (Описание неприводимых многочленов над полями $\mathbb{C}$ и $\mathbb{R}$)**.**

а) Над полем $\mathbb{C}$ неприводимым являются многочлены первой степени, и только они.

б) Над полем $\mathbb{R}$ неприводимыми являются многочлены первой степени, а также многочлены второй степени с отрицательным дискриминантом, и только они.

2.4 Формальная производная

$\mathbb{F}$ — поле, $\mathbb{F}[x]$ — алгебра с базисом $1, x, x^2, \ldots$

$$\frac{d}{dx} : x^n \mapsto nx^{n-1}, \forall n \geq 0$$

Распространим $\frac{d}{dx}$ на всё ЛП $\mathbb{F}[x]$ по линейности:

$$\frac{d}{dx} : \mathbb{F}[x] \to \mathbb{F}[x]$$

Это оператор назовём **формальной производной**.

Пример.

$$f(x) = x^{2p} + x^p, \mathbb{F} = \mathbb{Z}_p$$

$$\frac{df}{dx} = f'(x) = 2px^{2p-1} + px^{p-1} = 0, (p \equiv 0 \pmod{p})$$

Утверждение 2.2. *Для формальной производной справедливы тождества:*

а) *Правило Лейбница:*

$$(fg)' = f'g + fg'$$

б)

$$(f_1 \dots f_n)' = f_1' f_2 \dots f_n + f_1 f_2' \dots f_n + \dots + f_1 f_2 f_n'$$

в)

$$(f^n)' = nf^{n-1}f'$$

Доказательство. а) Пользуясь произв.:

$$f = x^k, g = x^m$$

$$(x^{k+m})' = (k+m)x^{k+m-1}$$

$$kx^{m+k-1} + mx^{m+k-1} = (k+m)x^{m+k-1}$$

LHS = RHS, Ч. Т. Д.

б) Индукцией по n:

$$((f_1 \dots f_{n-1})f_n)' = (f_1 \dots f_n)' f_n + (f_1 \dots f_n)f_n' =$$

$$= f_1' f_2 \dots f_n + \dots + f_1 f_2 \dots f_n'$$

в) Следствие б), при $f_1 = \dots = f_n$

□

Теорема 2.10. *Пусть $f \in \mathbb{F}[x]$, f — положж. степень, $F \ni c$ — корень f, тогда:*

а) *c — кратный корень f (т. е. кратность ≥ 2) $\iff$ $f(c) = f'(c) = 0$*

б) *Если c — корень кратности k, то:*

$$f(c) = f'(c) = \dots = f^{(k-1)}(c) = 0$$

в) Если, вдобавок к б), $\operatorname{char}\mathbb{F} = 0$ *или* $\operatorname{char}\mathbb{F} > k$*, то:*

$$f^{(k)}(c) \neq 0$$

Доказательство. а)

$$f(x) = q(x)(x-c)$$
$$f'(x) = q(x) + q'(x)(x-c)$$
$$\Rightarrow f'(c) = q(c)$$

c — кратный корень $\iff q(x) \vdots (x-c) \iff q(c) = 0$, по т. Безу $\iff f'(c) = 0$

б)

$$f(x) = q(x)(x-c)^k$$

$f'(x) = k(x-c)^{k-1}q(x) + q'(x)(x-c)^k = (x-c)^{k-1}(kq(x) + q'(x)(x-c))$

Следовательно c — корень производной кратности $\geq k-1$. Применяя то же рассуждение много раз, получаем, что c — корень кратности ≥ 1 многочлена $f^{(k-1)}$:

$$\Rightarrow f^{(k-1)}(c) = 0$$

в) Рассмотрим ту скобку в п. б), подставим туда c:

$$(\ldots)|_{x=c} = kq(c)$$
$$q(c) \neq 0$$
$$k \neq 0, (\text{по ограничнию на } \operatorname{char}\mathbb{F})$$

$\Rightarrow$ Тогда, проделывая те же рассуждения, что и в б), получаем, что c — простой корень (кратность $= 1$) многочлена $f^{(k-1)}$. Пусть $f^{(k)}(c) = 0$, тогда по п. а), c — кратный корень $f^{(k-1)}$ — противоречие, следовательно $f^{(k)}(c) \neq 0$.

□

Замечание. *Из п. в) следует, что* c *— корень кратности* k *многочлена* f*.*

Замечание. *Условие на* $\operatorname{char}\mathbb{F}$ *существенно.*

Пример.

$$f(x) = x^{10} - x^5 \in \mathbb{Z}_5[x]$$
$$f'(x) = 10x^9 - 5x^4 = 0$$

$x = 0$ *— корень кратности* 5*, но п. в) не выполняется, т. к.* $\operatorname{char}\mathbb{Z}_5 = 5$

2.5 Поле частных области целостности

Пусть A — область целостности, $A^* = A \setminus \{ 0 \}$, рассмотрим:

$$A \times A^* = \{ (f, g) \mid f \in A, g \in A^* \}$$

Будем записывать элементы этого множества, как:

$$\frac{f}{g} := (f, g)$$

Определение 2.7.

$$\frac{f_1}{g_1} = \frac{f_2}{g_2} \iff f_1 g_2 - f_2 g_1 = 0$$

1) $A \times A^* \to A \times A^*$