

Московский физико-технический институт  
Физтех-школа прикладной математики и информатики

БОЛЬШОЕ НАЗВАНИЕ КУРСА  
V СЕМЕСТР

Лектор: *Иван Иванович Иванов*

**$h/\nu$**

Автор: *Павел Дуров*  
*Репозиторий на Github*

осень 2022

## Содержание

<b>1</b>	<b>Неприводимые многочлены</b>	<b>2</b>
1.1	Корни многочленов . . . . .	2
1.2	Основная Теорема Алгебры . . . . .	3
1.3	Следствия из основной теоремы алгебры . . . . .	4
1.4	Формальная производная . . . . .	4

# 1 Неприводимые многочлены

**Определение 1.1.** Пусть  $F$  — поле,  $F[x]$  — кольцо многочленов над  $F$ . Многочлен  $P \in F[x]$ ,  $\deg P > 0$  называется неприводимым, если  $AB = P \Rightarrow \deg A = 0 \vee \deg B = 0$ . Иначе говоря, многочлен неприводим над полем  $F$ , если он не раскладывается в произведение многочленов более низких степеней.

**Пример.**  $x^2 + 1 \in \mathbb{R}[x]$  — неприводим. Очев, т.к. не имеет корней.

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

**Утверждение 1.1.**  $P$  — неприводимый, тогда  $\forall A : (A, P) = \begin{bmatrix} \sim 1 \\ \sim P \end{bmatrix}$

*Доказательство.* По-другому быть не может, т.к. у  $P$  нет делителей, кроме 1 и самого себя.  $\square$

**Лемма 1.1** (Евклида). Пусть  $P$  — неприводимый многочлен,  $AB : P \Rightarrow A : P \vee B : P$ .

*Доказательство.* От противного, тогда  $A \not:P, B \not:P$ . Тогда по теореме о представлении НОДа в виде линейной комбинации:

$$(A, P) = u_1 A + u_2 P = 1$$

$$u_1 AB + u_2 PB = B : P$$

Противоречие  $\square$

**Теорема 1.1** (Основная Теорема Арифметики). Пусть  $A$  — ненулевой многочлен из  $F[x]$ ,  $F$  — поле. Тогда  $\exists ! P_1, P_2 \dots P_n$  с точностью до перестановки множителей и домножения на константу, где  $P_i$  — неприводим и  $A = \prod_{i=1}^n P_i$ .

*Доказательство.*

**Существование.** По индукции: либо он неприводим и очев, либо нет, тогда разложим и для каждого множителя разложим его.

**Единственность.** Пусть не единственно, будем тогда сокращать на  $P_1, P_2, \dots$ . Получим, что в разложении должны содержаться многочлены, пропорциональные  $P_1, \dots P_n$  соответственно  $\square$

**Следствие.** Если  $A : P$ , то разложение  $A$  является подмножеством разложения  $P$

## 1.1 Корни многочленов

**Определение 1.2.** Многочлен  $P$  имеет корень  $c$  кратности  $k$ , если  $P : (x - c)^k, P \not:(x - c)^{k+1}$

**Определение 1.3.** Если многочлен раскладывается в произведение линейных множителей над полем  $F$ , то он называется линейно факторизуемым над ним.

**Замечание.** Основная Теорема Арифметики неверна (разложение может быть не единственным) для случаев, когда  $F$  — коммутативное кольцо.

## 1.2 Основная Теорема Алгебры

На лекции было миллион лемм и вспомогательных утверждений, но я просто вставлю доказательство из лекции по матану, потому что я так могу (и потому что доказательство идейно не отличается от него).

**Теорема 1.2** (Больцано-вейерштрасса). Пусть  $\{z_n\}$  ограничена, то есть  $\exists C > 0 : \forall n (|z_n| \leq C)$ . Тогда у нее существует сходящаяся подпоследовательность

*Доказательство.* По обычной теореме Больцано-Вейерштрасса, ищем подпоследовательность, действительная часть которой имеет предел. В ней выбираем последовательность, мнимая часть которой имеет предел. Получили.  $\square$

**Определение 1.4.** Функция  $f : E \subset \mathbb{C} \rightarrow \mathbb{C}$  непрерывна в точке  $z_0$ , если  $\forall \{z_n\} \subset E (z_n \rightarrow z_0 \Rightarrow f(z_n) \rightarrow f(z_0))$ .

**Утверждение 1.2.** Пусть  $f : \{|z| \leq R\} \rightarrow \mathbb{R}$  непрерывна на  $\mathbb{C}$ . Тогда  $\exists z_0, |z_0| \leq R, \inf_{|z| \leq R} f(z) = f(z_0)$ .

*Доказательство.*

$$m = \inf_{|z| \leq R} f(z)$$

Рассмотрим  $r_n \rightarrow m, r_n > m$ .  $\exists z_n, |z_n| \leq R, m \leq f(z_n) \leq r_n$ . В частности,  $f(z_n) \rightarrow m$ . При этом,  $\{z_n\}$  — ограничена,  $\Rightarrow \exists z_{n_k} \rightarrow z_0 \Rightarrow |z_0| \leq R$ . В частности  $||z| - |z_0|| \leq |z - z_0|$ . В силу непрерывности  $f$  в  $z_0$ :  $f(z_{n_k}) \rightarrow f(z_0), f(z_{n_k}) \rightarrow m \Rightarrow m = f(z_0)$ .  $\square$

**Теорема 1.3.** Пусть  $f \in \mathbb{C}[z], \deg f > 0$ . Тогда  $f$  имеет корень.

*Доказательство.* 1. Покажем, что  $\exists z_0 \in \mathbb{C} \inf_{z \in \mathbb{C}} |P(z)| = |P(z_0)|$ . Для начала возьмем  $R \geq 1$ .

$$\left| \sum_{k=0}^{n-1} a_k z^k \right| \leq \sum_{k=0}^{n-1} |a_k| |z|^k \leq |z|^n \sum_{k=0}^{n-1} |a_k| = A$$

Теперь рассмотрим  $|z| \geq \frac{2A}{|a_n|} \Rightarrow A|z|^{n-1} \leq \frac{1}{2}|a_n||z|^n$ . Тогда  $|P(z)| \geq |a_n z^n| - \left| \sum_{k=0}^{n-1} a_k z^k \right| = \frac{1}{2}|a_n|z^n$ . Возьмем радиус  $R = \max \left\{ 1, \frac{2A}{|a_n|}, \sqrt[n]{\frac{2|a_0|}{|a_n|}} \right\}$ . Тогда при  $|z| \geq R$  выполнено  $|P(z)| \geq |P(0)|$ , поэтому  $\inf_{\mathbb{C}} |P(z)| = \inf_{|z| \leq R} |P(z)|$ . Но тогда найдется такое  $|z_0| \leq R$ , что у нас  $\inf_{\mathbb{C}} |P(z)| = |P(z_0)|$

2. Докажем, что если  $P(z_0) \neq 0$ , то  $\exists z_* \in \mathbb{C} |P(z_*)| < |P(z_0)|$ . Рассмотрим многочлен  $Q(z) = \frac{P(z+z_0)}{P(z_0)}$ . Тогда  $Q(0) = 1$ . Обозначим через  $\alpha_k$  — наименьший коэффициент  $Q$ , отличный от 0 и  $k \geq 1$ .  $Q(z) = 1 + \alpha_k z^k + \dots$ . Возьмем  $z_1 \in \mathbb{C}, \alpha_k z_1^k = -1$ , пусть  $t \in (0, 1)$ .  $Q(tz_1) = 1 - t^k + t^{k+1}\varphi(t)$ ,  $\varphi(t)$  — многочлен степени  $n-k-1$ .  $C$  — наибольший из модулей коэффициентов  $\varphi(t)$ , тогда  $|\varphi(t)| \leq C(n-k)$ . Тогда

$$Q(tz_1) < 1 - t^k |\varphi(t)| \leq 1 - t^k (1 - tC(n-k))$$

Рассмотрим произвольное  $t \in \left(0, \frac{1}{C(n-k)}\right)$ . Тогда  $|Q(tz_1)| < 1$ . Но тогда при  $z_* = tz_1$  верно, что  $|P(z_*)| < |P(z_0)|$

Но тогда, точка  $z_0$  (из первого пункта) такова, что  $P(z_0) = 0$ .  $\square$

### 1.3 Следствия из основной теоремы алгебры

**Определение 1.5.** Поле  $F$  называется алгебраически замкнутым, если  $\forall f \in F[x], \deg f > 0$  он имеет хотя бы один корень.

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

**Следствие.** Любой многочлен из  $\mathbb{C}$  — линейно факторизуем.

**Следствие.** Любой многочлен из  $\mathbb{R}$  раскладывается в произведение многочленов 1 и 2 степени

*Доказательство.* Пусть  $c \notin \mathbb{R}$  — корень  $f$ . Тогда  $\bar{c}$  — тоже. Но тогда  $f: (x - c)(x - \bar{c})$   $\square$

### 1.4 Формальная производная

**Определение 1.6.**

$$(a_n x^n + \dots + a_1 x + a_0)' = n a_n x^{n-1} + \dots + 2 a_2 x + a_1$$

**Замечание.** Все свойства обычной производной верны

1.  $(fg)' = f'g + fg'$
2.  $(f \pm g)' = f' \pm g'$
- 3.