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

1 Неприводимые многочлены

Определение 1.1. Пусть F — поле, $F[x]$ — кольцо многочленов над F. Многочлен $P \in F[x], \deg P > 0$ называется наприводимым, если $AB = P \Rightarrow \deg A = 0 \vee \deg B = 0$. Иначе говоря, многочлен неприводим над полем F, если он не раскладывается в произведение многолченов 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* $\forall A : (A, P) = \left[\begin{array}{l} \sim 1 \\ \sim P \end{array} \right.$

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

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

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

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

$$u_1 AB + u_2 PB = B \vdots P$$

Противоречие □

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 $A = \Pi_{i=1}^n P_i$.*

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

□

Следствие. Если $A \vdots P$, то разложение A является подмножеством разложения P

1.1 Корни многочленов

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

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 утвеждений, 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* $\exists C > 0 : \forall n(|z_n| \leqslant C)$*. 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. □

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

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

Доказательство.

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

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

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 $R \geqslant 1$.
$$\left|\sum_{k=0}^{n-1} a_k z^k\right| \leqslant \sum_{k=0}^{n-1} |a_k||z|^k \leqslant |z|^n \sum_{k=0}^{n-1} |a_k| = A$$
Теперь рассмотрим $|z| \geqslant \frac{2A}{|a_n|} \Rightarrow A|z|^{n-1} \leqslant \frac{1}{2}|a_n||z|^n$. Тогда $|P(z)| \geqslant |a_n z^n| - \left|\sum_{k=0}^{n-1} a_k z^k\right| = \frac{1}{2}|a_n|z^n$. Возьем радиус $R = \max\left\{1, \frac{2A}{|a_n|}, \sqrt[n]{\frac{2|a_0|}{|a_n|}}\right\}$. Тогда при $|z| \geqslant R$ выполнено $|P(z)| \geqslant |P(0)|$, поэтому $\inf_{\mathbb{C}} |P(z)| = \inf_{|z|\leqslant R} |P(z)|$. Но тогда найдется такое $|z_0| \leqslant R$, 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 α_k — наименьший коэффициент Q, отличный от 0 и $k \geqslant 1$. $Q(z) = 1 + \alpha_k z^k + \dots$. 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 $|\varphi(t)| \leqslant C(n - k)$. Тогда
$$Q(tz_1) < 1 - t^k|\varphi(t)| \leqslant 1 - t^k(1 - tC(n - k))$$
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 $P(z_0) = 0$.

□

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 многолчен из $\mathbb{C}$ — линейно факторизуем.

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

Доказательство. Пусть $c \notin \mathbb{R}$ — корень f. Тогда $\overline{c}$ — тоже. Но тогда $f \vdots (x-c)(x-\overline{c})$ □

1.4 Формальная производная

Определение 1.6.

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

Замечание. Все свойства обычной производной верны

1. $(\alpha P + \beta Q)' = \alpha P' + \beta Q'$
2. $(PQ)' = P'Q + PQ'$
3. $(P_1 P_2 P_3 \dots P_{n-1} P_n)' = P_1' P_2 P_3 \dots P_{n-1} P_n + P_1 P_2' P_3 \dots P_{n-1} P_n + \dots P_1 P_2 P_3 \dots P_{n-1} P_n'$
4. $(P^n)' = nP^{n-1}$

Доказательство.

1. Доказательство по определению:
$\left(\sum_{i=1}^k \alpha_i x^i\right)' + \left(\sum_{i=1}^i \beta_k x^{i-1}\right)' = \left(\sum_{i=1}^k i\alpha_i x^{i-1}\right) + \left(\sum_{i=1}^i i\beta_i x^{i-1}\right)' =$
$= \sum_{i=0}^k (\alpha_i + \beta_i) \cdot i x^{i-1} = \left(\sum_{i=0}^k (\alpha_i + \beta_i) x^i\right)'$
2. Раскроем скобки: $\left(\sum_{i=0}^k \alpha_i x^i \cdot Q(x)\right)' = \left(\sum_{i=0}^k \sum_{j=0}^l \alpha_i \beta_j x^{i+j}\right)' =$
$= \sum_{i=0}^k \sum_{j=0}^l (i+j) \alpha_i \beta_j x^{i+j-1} = \sum_{i=0}^k \sum_{j=0}^l i\alpha_i \beta_j x^{i+j-1} + \sum_{i=0}^k \sum_{j=0}^l j\alpha_i \beta_j x^{i+j-1} =$
$= P'Q + PQ'$
3. Индукция: *База* $n = 2 \to$ см п. 2. *Переход:* Объединим $P_{n-1} P_n$ в $Q \to 2$ раза п. 2.
4. Применяем п. 4 для $P_1 = P_2 = \dots = P_{n-1} = P_n = P$

□