Лекция 17.

Гайфуллин Сергей Александрович

МГУ

19 ноября, 2021

Пусть R – коммутативное ассоциативное кольцо с единицей, $a \in R$ и $f(x) \in R[x]$. Положим $y = x - a$, тогда $x = y + a$. Если подставить это в $f(x)$ и раскрыть скобки, то получится многочлен $\widetilde{f}(y) = f(y + a)$. Подставим обратно $y = x - a$. Получим разложение $f(x)$ по степеням $x - a$, то есть выражение вида

$$f(x) = b_n(x - a)^n + b_{n-1}(x - a)^{n-1} + \ldots + b_0.$$

При этом $f(a) = b_0$.

Пример

Пусть $F = \mathbb{R}$, $a = 2$, $f(x) = 3x^2 + 2x + 4$. Тогда

$$\widetilde{f}(y) = f(y + 2) = 3(y + 2)^2 + 2(y + 2) + 4 = 3y^2 + 14y + 20.$$

То есть $f(x) = 3(x - 2)^2 + 14(x - 2) + 20$.

Теорема Безу

Пусть R – коммутативное ассоциативное кольцо с единицей, $a \in R$ и $f(x) \in R[x]$. Тогда $f(a) = 0$ тогда и только тогда, когда существует представление $f(x) = (x-a)q(x)$.

Доказательство. Пусть $f(x) = (x-a)q(x)$, тогда $f(a) = 0q(a) = 0$.
Обратно, $f(x) = b_n(x-a)^n + b_{n-1}(x-a)^{n-1} + \ldots + b_0$, где $b_0 = f(a)$. Значит, если $f(a) = 0$, то

$$\begin{aligned} f(x) &= b_n(x-a)^n + b_{n-1}(x-a)^{n-1} + \ldots + b_1(x-a) = \\ &= (x-a)(b_n(x-a)^{n-1} + b_{n-1}(x-a)^{n-2} + \ldots + b_1) \end{aligned}$$

Замечание

Если R – область целостности, то $\deg q(x) = \deg f(x) - 1$.

Лемма

Пусть R – область целостности, $a \in R$, $f(x) \in R[x]$ и $f(x) = (x - a)q(x)$. Если $c \neq a$ – корень $f(x)$, то c – корень $q(x)$.

Доказательство. Имеем $0 = f(c) = (c - a)q(c)$. Так как делителей нуля нет, $q(c) = 0$.

Следствие

У многочлена степени n над областью целостности не более n различных корней.

Определение

Будем говорить, что многочлен $f(x)$ имеет корень a кратности k, если $f(x)$ может быть представлен в виде $f(x) = (x - a)^k s(x)$ и не может быть представлен в виде $(x - a)^{k+1} r(x)$.

Лемма

У многочлена степени n над областью целостности не более n корней с учетом кратностей.

Доказательство. Пусть a – корень кратности k многочлена $f(x)$ и b – корень кратности l. Тогда $f(x) = (x-a)^k q(x) = (x-b)^l s(x)$. Допустим, что кратность корня b в многочлене $q(x)$ равна $m \neq l$. Тогда $f(x) = (x-a)^k (x-b)^m r(x) = (x-b)^l s(x)$. Исходя из определения кратности, может быть лишь случай $l > m$. Имеем

$$0 = (x-a)^k (x-b)^m r(x) - (x-b)^l s(x) = \\ = (x-b)^m ((x-a)^k r(x) - (x-b)^{l-m} s(x))$$

Так как в кольце $R[x]$ нет делителей нуля, $(x-a)^k r(x) - (x-b)^{l-m} s(x) = 0$. Подствим $x = b$, получим, $(b-a)^k r(b) = 0$. Тогда $r(b) = 0$, а значит, $r(x) = (x-b)h(x)$. Это противоречит выбору $r(x)$.

Продолжение доказательства.

Итак, кратность корня b у многочленов $f(x)$ и $q(x)$ одинакова. Докажем утверждение леммы по индукции по $n = \deg f$.
База $n = 1$. У линейного многочлена $px + q$ только один корень. Это следует из предыдущего утверждения и того, что кратного корня не может быть.
Шаг. Рассмотрим один из корней многочлена $f(x)$. Пусть это a и он кратности k. Тогда $f(x) = (x - a)^k q(x)$. При этом $\deg q(x) = \deg f - k$ и кратности остальных корней f у многочлена q такие же. По предположению индукции, сумма кратностей всех корней q не больше $\deg q$. Но тогда сумма кратностей корней f не больше $\deg q + k = \deg f$.

Было в прошлый раз

Теорема

Непрерывная функция $h\colon \mathbb{C} \to \mathbb{R}$ достигает на компакте K минимального значения.

Лемма о возрастании модуля

Пусть $f(z) \in \mathbb{C}[z]$ – многочлен положительной степени. Тогда $\lim\limits_{|z|\to\infty} |f(z)| = \infty$. То есть для каждого $C \in \mathbb{R}$ существует $D \in \mathbb{R}$ такое, что при $|z| > D$ выполнено $|f(z)| > C$.

Лемма Даламбера

Пусть $z_0 \in \mathbb{C}$, $f(z) \in \mathbb{C}$, $\deg f(z) > 0$ и пусть $f(z_0) \neq 0$. Тогда для любого $\varepsilon > 0 \in \mathbb{R}$ существует $z \in U_\varepsilon(z_0)$ такое, что $|f(z)| < |f(z_0)|$.

Доказательство. Разложим $f(z)$ по степеням $z - z_0$:

$$f(z) = c_0 + c_k(z - z_0)^k + \ldots + c_n(z - z_0)^n.$$

При этом $c_0 = f(z_0) \neq 0$. Считаем, что $c_k \neq 0$. Подберем аргумент $z - z_0$ таким образом, чтобы

$$\arg\left(c_k(z - z_0)^k\right) = \pi + \arg(c_0).$$

Далее будем подбирать модуль числа $z - z_0$ (в пределах ε-окрестности). Для этого фиксируем некоторое $\widetilde{z}$ с подходящим аргументом $\widetilde{z} - z_0$ и положим $z - z_0 = t(\widetilde{z} - z_0), t \in \mathbb{R}_{>0}$.

Продолжение доказательства.

Получаем

$$f(z) = c_0 + c_k(z - z_0)^k + \ldots + c_n(z - z_0)^n =$$

$$= c_0 + c_k t^k(\widetilde{z} - z_0)^k + \ldots + c_n t^n(\widetilde{z} - z_0)^n =$$

$$= c_0 + c_k t^k(\widetilde{z} - z_0)^k + t^{k+1}(c_{k+1}(\widetilde{z} - z_0)^{k+1} + \ldots + t^{n-k-1}c_n(\widetilde{z} - z_0)^n)).$$

Оценим модуль $f(z)$:

$$|f(z)| \leq |c_0 + c_k t^k(\widetilde{z} - z_0)^k| +$$

$$+ t^{k+1}|c_{k+1}(\widetilde{z} - z_0)^{k+1} + \ldots + c_n t^{n-k-1}(\widetilde{z} - z_0)^n| \leq$$

$$\leq |c_0 + c_k t^k(\widetilde{z} - z_0)^k| + t^{k+1}(|c_{k+1}(\widetilde{z} - z_0)^{k+1}| + \ldots + |c_n t^{n-k-1}(\widetilde{z} - z_0)^n|)$$

Пусть $|\widetilde{z} - z_0| = A < 1$ и пусть $\max |c_i| = B$. Тогда $|c_0 + c_k t^k(\widetilde{z} - z_0)^k| = |c_0| - |c_k| t^k A^k$ (считаем $|c_0| > |c_k| t^k A^k$) и $|c_p t^{p-k-1}(\widetilde{z} - z_0)^p| \leq B$. В итоге

$$|f(z)| \leq |c_0| - |c_k| t^k A^k + t^{k+1} nB = |f(z_0)| - t^k(|c_k| A^k - tnB).$$

Можно подобрать $0 < t < \varepsilon$ так, чтобы $|c_k| A^k - tnB > 0$.

Теорема (основная теорема алгебры)

Любой многочлен $f \in \mathbb{C}[z]$ положительной степени имеет комплексный корень, то есть число $w \in \mathbb{C}$ такое, что $f(w) = 0$.

Доказательство. Выберем произвольное $z_0 \in \mathbb{C}$. По лемме о возрастании модуля существует $D \in \mathbb{R}$ такое, что при $|z| \geq D$ выполнено $|f(z)| > |f(z_0)|$. Рассмотрим круг $K = \{|z| \leq D\}$. Это замкнутое и ограниченное множество, то есть компакт. Значит, существует точка $w \in K$ в которой достигается минимум функции $|f(z)|$. Заметим, что w не лежит на границе K, так как на границе данная функция больше, чем в точке $z_0 \in K$. Значит, существует $\varepsilon > 0 \in \mathbb{R}$ такой, что $U_\varepsilon(w) \subset K$. Если $f(w) = 0$, то корень найден. Допустим, что $f(w) \neq 0$. Тогда по лемме Даламбера существует $w' \in U_\varepsilon(w)$ такое, что $|f(w')| < |f(w)|$. Но $w' \in K$. Получаем противоречие с выбором w.

Следствие

Любой многочлен $f \in \mathbb{C}[z]$ степени n раскладывается на линейные множители и имеет ровно n корней с учетом кратностей.

Доказательство. Индукция по $n = \deg f$. База $n = 1$. Линейный многочлен имеет 1 корень и уже разложен на линейные множители.
Шаг. Пусть z_0 – корень $f(z)$. Тогда $f(z) = (z - z_0)q(z)$. По предположению индукции $q(z)$ раскладывается на линейные множители. Тогда и $f(z)$ тоже. Значит, сумма кратностей корней не менее n. Но уже было доказано, что она не более n.

Предложение

Пусть z – комплексный корень многочлена $f(x) \in \mathbb{R}[x]$. Тогда $\overline{z}$ – также корень f.

Доказательство.

$$f(\overline{z}) = a_n\overline{z}^n + \ldots + a_0 = \overline{a_n}\,\overline{z}^n + \ldots + \overline{a_0} = \overline{f(z)} = \overline{0} = 0.$$

Следствие

Любой многочлен с вещественными коэффициентами раскладывается в произведение линейных и квадратичных с отрицательным дискриминантом множителей.

Доказательство. Индукция по степени многочлена. База $\deg f = 0$ и $\deg f = 1$ очевидна. Пусть $f(x) \in \mathbb{R}[x]$. Если $f(x)$ имеет вещественный корень c, то $f(x) = (x-c)g(x)$, при этом $\deg g < \deg f$ и к g можно применить предположение индукции.

Пусть теперь у $f(x)$ есть комплексный корень λ. Тогда $\overline{\lambda}$ – также корень $f(x)$. Значит, $f(x) = (x-\lambda)(x-\overline{\lambda})h(x)$. При этом $(x-\lambda)(x-\overline{\lambda}) = x^2 - 2\mathrm{Re}\lambda + |\lambda|^2$. При этом дискриминант равен $D = 4(\mathrm{Re}\lambda)^2 - 4|\lambda|^2 < 0$. К h можно применить предположение индукции.