Конспект 03 — Многочлены от одной переменной

Содержание

1. Основные понятия
    1. Определение многочлена
    2. Операции с многочленами
    3. Кольцо многочленов
2. Корни многочлена
    1. Определение корня
    2. Теорема Безу
    3. Кратность корня
    4. Число корней многочлена
    5. Свойства корней

Основные понятия

Определение многочлена

Info

Многочленом $f(x)$ над полем F называется выражение вида

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = \sum_{k=0}^{\infty} a_kx^k, \tag{1}$$

где:

- $\forall k : a_k \in F$
- $\forall k > n : a_k = 0$
- $a_n \neq 0$ или $f \equiv 0$

a_k называется *коэффициентом* многочлена. Коэффициент a_n называется старшим. Коэффициент a_0 называется *свободным членом*.

Операции над многочленами

Сложение

Info

Суммой двух многочленов $f(x) = \sum_{i=0}^{+\infty} a_i x^i$ и $g(x) = \sum_{j=0}^{+\infty} = b_j x^j$ называется такой многочлен $s(x)$, что:

$$s(x) = \sum_{k=0}^{+\infty} (a_k + b_k) x^k$$

Свойства сложения

Коммутативность

Пусть заданы два многочлена f и g. Тогда:

$$f + g = g + f$$

Ассоциативность

Пусть заданы три многочлена f, g и h. Тогда:

$$(f + g) + h = f + (g + h)$$

Нейтральный элемент

Для любого многочлена f верно, что

$$f + 0 = f$$

Вычитание

Info

Разностью двух многочленов $f(x) = \sum_{i=0}^{+\infty} a_i x^i$ и $g(x) = \sum_{j=0}^{+\infty} = b_j x^j$ называется такой многочлен $d(x)$, что:

$$d(x) = \sum_{k=0}^{+\infty} (a_k - b_k) x^k$$

Свойства вычитания

Антикоммутативность

Пусть заданы два многочлена f и g. Тогда:

$$f - g = -(g - f)$$

Неассоциативность

Существуют такие три многочлена f, g и h, что

$$(f - g) - h \neq f - (g - h)$$

Нейтральный элемент

Для любого многочлена f верно, что

$$f - 0 = f$$

Умножение

Info

Произведением двух многочленов $f(x) = \sum\limits_{i=0}^{+\infty} a_i x^i$ и $g(x) = \sum\limits_{j=0}^{+\infty} = b_j x^j$ называется такой многочлен $p(x)$, что:

$$p(x) = \sum_{k=0}^{+\infty} (x^k \sum_{i+j=k} a_i b_j)$$

Свойства умножения

Коммутативность

Пусть заданы два многочлена f и g. Тогда:

$$f \times g = g \times f$$

Доказательство

Легко заметить, что

$$\sum_{k=0}^{+\infty} (x^k \sum_{i+j=k} a_i b_j) = \sum_{k=0}^{+\infty} (x^k \sum_{i+j=k} b_i a_j),$$

что и требовалось доказать.

Ассоциативность

Пусть заданы три многочлена f, g и h. Тогда:

$$(f \times g) \times h = f \times (g \times h)$$

Доказательство

По определению,

$$(f \times g) \times h = \sum_{k=0}^{\infty} \left(x^k \sum_{i+j=k} a_i b_j \right) \times h =$$

$$= \sum_{k=0}^{\infty} \left(x^k \sum_{i+j=k} \sum_{l+w=i} a_l b_w c_j \right) =$$

$$= \sum_{k=0}^{\infty} \left(x^k \sum_{l+w+j=k} a_l b_w c_j \right)$$

Легко заметить, что, поскольку умножение элементов поля ассоциативно, то и множители под знаком суммы можно переставлять в произвольном порядке.

Дистрибутивность

Пусть заданы три многочлена f, g и h. Тогда:

$$(f + g) \times h = f \times h + g \times h$$

Доказательство

По определению,

$$(f + g) \times h = \sum_{k=0}^{\infty} \left(x^k (a_k + b_k) \right) \times h =$$

$$= \sum_{k=0}^{\infty} \left(x^k \sum_{i+j=k} (a_i + b_i) c_j \right) =$$

$$= \sum_{k=0}^{\infty} \left(x^k \sum_{i+j=k} a_i c_j + b_i c_j \right) =$$

$$= f \times h + g \times h,$$

что и требовалось доказать.

Степень

Info

Степень $\deg f(x)$ многочлена $f(x)$ определяется следующим образом:

$$\deg f(x) = \begin{cases} \max n : a_n \neq 0, & \text{если } f \not\equiv 0 \\ -\infty, & \text{если } f \equiv 0 \end{cases}$$

Свойства степени

> **Замечание 1**
>
> Степень произведения равна сумме степеней множителей:
>
> $$\deg(f \times g) = \deg f + \deg g$$
>
> Этот факт напрямую следует из определения произведения многочленов.

> **Замечение 2**
>
> Степень суммы не превосходит максимума из степеней слагаемых:
>
> $$\deg(f + g) \leq \max\{\deg f, \deg g\}$$
>
> Очевидно, что она не можешь превосходить этого значения (это также следует из определения). При этом она может быть и меньше, если старшие степени исключают друг друга.

Деление

> **Замечание 3**
>
> Многочлен f обратим тогда и только тогда, когда $\deg f = 0$.
>
> **Доказательство**
>
> Рассмотрим произвольный многочлен f такой, что $\deg f > 0$ и предположим, что существует такой многочлен f^{-1}, что
>
> $$f \times f^{-1} = 1$$
>
> Отсюда $\deg(f \times f^{-1}) = 0$, что немедленно приводит к противоречию с условием $\deg f > 0$, а значит, что f^{-1} не может существовать, что и требовалось доказать.

Из замечания (3) следует, что частное от деления на неконстантный многочлен может не быть определено, поэтому мы прибегаем к *делению с остатком*.

> **Теорема о делении с остатком**

Пусть заданы два многочлена f и g, причём $g \neq 0$. Тогда:

$$\exists!\ q, r \in F[x] : f = gq + r, \quad \deg(r) < \deg(g)$$

Доказательство

Существование.
Если $\deg f < \deg g$, то $q = 0, r = f$. Очевидно, что это единственная подходящая пара.

Пусть теперь $\deg f \geq \deg g$. Обозначим $\deg f = n, \deg g = m$ и построим многочлен f_1 такой, что

$$f_1 = f - \frac{a_n}{b_m} \times x^{n-m} g$$

Легко заметить, что $\deg f_1 < \deg f$, поскольку это вычитание исключило из f старший член.
Будем продолжать этот процесс, пока $\deg f \geq \deg g$. Когда он остановится, получим, что

$$f - qg = r,$$

где q — собранные воедино множители $\frac{a_n}{b_m} \times x^{n-m}$, r — соответствующий f_i; отсюда легко видеть, что $\deg f < \deg g$. Тогда имеем

$$f = gq + r,$$

что и требовалось доказать.

Единственность.
Пусть $f = q_1 g + r_1 = q_2 g + r_2$. Тогда

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

Здесь $\deg(r_2 - r_1) < \deg g$. При этом $\deg(r_2 - r_1) = \deg g(q_1 - q_2) = \deg g + \deg(q_1 - q_2)$.
Если при этом $\deg(q_1 - q_2) = -\infty$, то $q_1 = q_2$, то есть искомое представление единственно; в противном случае приходим к противоречию.

Кольцо многочленов

Теорема 1

Множество $F[x]$ всех многочленов на поле F с операциями сложения и умножения является *коммутативным кольцом с единицей*.

Доказательство

> Выше были продемонстрированы все свойства, необходимые для удовлетворения всех аксиом коммутативного кольца с единицей.

Корни многочлена

> **Info**
>
> Элемент $x_0 \in F$ называется **корнем** (*la racine*) многочлена $f(x) \in F[x]$, если $f(x_0) = 0$.

> **Теорема Безу**
>
> $$\forall \alpha \in F, f(x) \in F[x] : f(x) = (x - \alpha)q(x) + f(\alpha)$$
>
> для некоторого неполного частного $q(x)$.
>
> **Доказательство**
>
> По теореме о делении с остатком, $f(x) = (x - \alpha)q(x) + r(x), \deg r(x) < \deg(x - \alpha) = 1$; отсюда $\deg r(x) \leq 0$, т.е. r — константа.
> Подставим $x = \alpha$. Тогда $f(\alpha) = (\alpha - \alpha)q(\alpha) + r = r$, что и требовалось доказать.
>
> *Следствие*. Элемент $\alpha \in F$ является корнем $f(x)$ тогда и только тогда, когда $(x - \alpha) \mid f(x)$.

Кратность корня

> **Info**
>
> **Кратность** корня $\alpha \in F$ многочлена $f(x) \in F[x]$ — целое неотрицательное число k такое, что $(x - \alpha)^k \mid f(x)$ и $(x - \alpha)^{k-1} \nmid f(x)$.
> Корень кратности 1 называется *простым* корнем.

> **Теорема 2**
>
> Число корней многочлена $f(x) \in F[x]$ с учётом их кратности не превосходит его степени.
>
> **Доказательство**
>
> Рассмотрим $\alpha_1, \alpha_2, \ldots, \alpha_n;\ \alpha_i \in F, (i \neq j) \implies (\alpha_i \neq \alpha_j)$ — все корни многочлена $f(x) \in F[x]$ и их кратности $k_1, k_2, \ldots, k_n;\ k_i \geq 1$.

По т. Безу,

$$f(x) = (x - \alpha_1)q_1(x), \quad q_1(\alpha_1) \neq 0$$

Разделим $q_1(x)$ на $(x - \alpha_2)$ максимальное возможное число раз. Получим

$$q_1(x) = (x - \alpha_2)^{S_2} q_2(x)$$

Повторяя этот процесс для каждого нового корня, получим, что

$$f(x) = (x - \alpha_1)^{S_1 = k_1}(x - \alpha_2)^{S_2} \dots (x - \alpha_n)^{S_n} q_n(x)$$

Заметим, что $\forall x \in F : q_n(x) \neq 0$, поскольку если бы у $q_n(x)$ были корни в F, то они являлись бы и корнями $f(x)$, то есть мы бы учли их в каких-то из α_i, и после сокращения они бы перестали быть корнями $q_n(x)$.
Тогда для произвольного i выполняется, что

$$f(x) = (x - \alpha_i)^{s_i}[q_n(x) \prod_{j \neq i}(x - \alpha_j)^{S_j}] = (x - \alpha_i)^{S_i} h(x)$$

Тогда поскольку $\forall 1 \leq i \leq n : q_n(\alpha_i) \neq 0$ и $\forall 1 \leq j \leq n, j \neq i : (\alpha_i - \alpha_j) \neq 0$, то $h(\alpha_i) \neq 0$.
Отсюда $s_i = k_i$, то есть

$$f(x) = (x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \dots (x - \alpha_n)^{k_n} q_n(x),$$

а значит, что $\deg f(x) = \sum_{i=1}^{n} k_i + \deg q_n(x) \implies \sum_{i=1}^{n} k_i = \deg f(x) - \deg q_n(x) \leq \deg f(x)$, что и требовалось доказать.

Следствие. Число корней многочлена $f(x) \in F[x]$ с учётом их кратности равно его степени тогда и только тогда, когда он раскладывается на линейные множители над полем F.

Свойства корней

Основная теорема алгебры

Любой многочлен на поле комплексных чисел имеет хотя бы один корень.

Доказательство если и будет приведено, то ближе к экзамену. Это очень тяжелая для осознания теорема, требующая возведения дополнительных сложных конструктов. Её доказательство вообще не должны спрашивать на сессии.

Теорема Гаусса

Всякий многочлен $P_n(x)$ имеет в комплексной области ровно n корней с учётом кратности.

Доказательство

Докажем по индукции.

База. При $n = 1$ имеем:

$$a_1 x + a_0 = 0 \implies x = -\frac{a_0}{a_1}$$

Переход. Допустим, утверждение верно для $k < n$. Покажем, что в таком случае оно верно и для $k = n$.
Рассмотрим многочлен $p = \sum\limits_{i=0}^{n} a_i x^i$. По основной теореме алгебры, он имеет по меньшей мере один комплексный корень x_0. По теореме Безу,

$$p = (x - x_0)q, \quad \deg q = n - 1$$

По предположению индукции, q имеет $n - 1$ корень, каждый из которых также является корнем p; помимо этого, p также имеет корень x_0, т.е общее их число составляет n, что и требовалось доказать.

Теорема 3

Если $z \in \mathbb{C}$ является корнем многочлена с вещественными коэффициентами $f \in \mathbb{R}[x]$, то $\overline{z}$также является его корнем.

Доказательство

По условию теоремы,

$$\sum_{i=0}^{\infty} a_i z^i = 0$$

Подставим комплексно сопряжённое к z:

$$\sum_{i=0}^{\infty} a_i \overline{z}^i = \sum_{i=0}^{\infty} a_i \overline{z^i} = \overline{f(z)} = \overline{0} = 0,$$

что и требовалось доказать.

Следствие 1. Любой многочлен с действительными коэффициентами имеет чётное число комплексных корней.
Следствие 2. Любой многочлен с действительными коэффициентами, имеющий нечётную степень, имеет хотя бы один вещественный корень.

Теорема 4

Если $z_0 = a_0 + b_0 i$ является корнем многочлена f, то f делится без остатка на многочлен вида

$$z^2 + pz + q,$$

где $p = -2a_0, q = a_0^2 + b_0^2$.

Доказательство

По теореме о комплексно сопряжённом корне и теореме Безу, имеем $(z - z_0)(z - \overline{z_0}) \mid f$. Тогда:

$$(z - z_0)(z - \overline{z_0}) = z^2 - z(z_0 + \overline{z_0}) + (z_0\overline{z_0}) = z^2 - 2a_0^2 z + a_0^2 + b_0^2,$$

что и требовалось доказать.

Теорема о рациональном корне

Если несократимая дробь $\frac{p}{q} \in \mathbb{Q}$ является корнем многочлена $f = a_0 + a_1 x + \dots + a_n x^n,\;\; a_i \in \mathbb{Z}$, то p является делителем a_0, а q — делителем a_n.

Доказательство

По условию,

$$\sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i = 0$$

Умножим все слагаемые на q^n:

$$\sum_{i=0}^{n} a_i p^i q^{n-i} = 0$$

Перенесём все члены, кроме свободного, в правую часть:

$$a_0 q^n = -\sum_{i=1}^{n} a_i p^n q^{n-i}$$

Легко видеть, что правая часть делится на p, поскольку каждое слагаемое имеет в своём составе множитель p. Отсюда левая часть также должна делиться на p, т.е. имеем $p \mid a_0 q^n$. Поскольку при этом $\gcd\{p, q\} = 1$, то $p \mid a_0$.

Теперь оставим в левой части только старший член:

$$a_n p^n = -\sum_{i=0}^{n-1} a_i p^n q^{n-i}$$

> Снова можно заметить, что права часть делится на q. Аналогичными рассуждениями получаем $q \mid a_n$, что и требовалось доказать.