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

Б О Л Ь Ш О Е Н А З В А Н И Е К У Р С А

V СЕМЕСТР

Лектор: *Иван Иванович Иванов*

$h\nu$

Автор: *Павел Дуров*
Проект на Github

осень 2022

Содержание

1 Алгебра многочленов

Определение 1.1. Многочленом называется функция $f : \mathbb{R} \to \mathbb{R}, f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

Определение 1.2. $\mathbb{F}[x]$ — множество всех многочленов над $\mathbb{F}$ (с коэффициентами в $\mathbb{F}$)

1.1 Операции над многочленами

1. $+$ — сложение
2. $\cdot$ — умножение
3. $\cdot\lambda$ — домножение на константу

Замечание. Многочлены над $\mathbb{R}$ образуют коммутативное кольцо

Определение 1.3. Алгебра над полем $\mathbb{F}$ называется называется множество A, с определенными на нем операциями $+, \cdot, \cdot\lambda$, которое удовлетворяет следующим условиям:

1. $(A, +, \cdot\lambda)$ — линейное пространство над $\mathbb{F}$
2. $(A, +, \cdot)$ — кольцо (необязательно коммутативное)
3. $\lambda(xy) = x(\lambda y) = (\lambda x)y, \lambda \in \mathbb{F}, x, y \in A$

Пример.

1. $\mathbb{R}[x]$
2. $M_n(\mathbb{F})$
3. $\mathbb{Z}_p[x]$

Замечание. Возникает проблема: в $\mathbb{Z}_p[x]$ сущесвтует многочлен $x^p - x \equiv 0 \forall x \in \mathbb{Z}_p$. Но тогда у нас будет конечный базис в $\mathbb{Z}_p[x]$, чего не хотелось бы. Определим многочлен по-другому:

Определение 1.4. Многочленом над коммутативным кольцом с 1 R называется бесконечная поопоследовательность $a_0, a_1 \ldots$, в которой лишь конечное число коэффициентов отличны от 0. Такие поопоследовательности называются финитными.

1.2 Операции над новыми многочленами

Пусть $A = (a_i), B = (b_i)$

1. $A + B = C \Leftrightarrow c_i = a_i + b_i$
2. $A \cdot B = C \Leftrightarrow c_k = \sum_{i=0}^{k} a_i b_{k-i}$
3. $A \cdot \lambda = C \Leftrightarrow c_k = \lambda \cdot a_i$

Утверждение 1.1. *$R[x]$ — коммутативное кольцо относительно "+", "·"*

Доказательство.

1. $(R[x], +)$ — абелева группа (очев)
2. $A \cdot B = B \cdot A$ — тут мы пользуемся тем, что R — коммутативное кольцо. Поэтому в сумме $\sum_{i=0}^{k} a_i b_{k-i}$ если переставить множители местами, ничего не поменяется
3. $A(BC) = (AB)C$

$$\sum_{i=0}^{n} a_i \left(\sum_{j=0}^{n-i} b_j c_{n-i-j} \right) = \sum_{i=0}^{k} \sum_{j=0}^{n-i} a_i b_j c_{n-i-j} = \sum_{i+j+k=n} a_i b_j c_k = \sum_{k=0}^{n} c_k \left(\sum_{i=0}^{n-k} a_i b_{n-k-i} \right)$$

4. $A(B + C) = AB + AC$ — Достаточно раскрыть скобки, чтобы проверить, мне лень техать.

□

Следствие. $R[x]$ — бесконечномерное линейное пространство с базисом $1, x, x^2 \ldots$.

Следствие. Нетрудно проверить, что в $R[x]$, $1 = (1, 0, 0, \ldots)$. Аналогично, $x^n = (\underbrace{0, 0, \ldots 0}_{n}, 1, 0, 0, \ldots)$

Определение 1.5. Старший коэффициент — последний ненулевой элемент последовательности.

Определение 1.6. Индекс старшего коэффициента называется степенью многочлена $\deg P$. У многочлена $(0, 0, \ldots)$ степень зависит от контекста. Мы будем считать, что его степень $-\infty$.

Определение 1.7. Кольцо с $1 \neq 0$ называется областью целостности, если в нем нет делителей нуля.

Утверждение 1.2. *Пусть R — область целостности. Тогда $ab = ac, a \neq 0 \Rightarrow b = c$*

Доказательство.

$$a(b - c) = 0$$
$$b - c = 0$$
$$b = c$$

□

Утверждение 1.3. *$A, B \in R[x], 1 \in R$. Тогда:*

1. $\deg A + \deg B \leqslant \max(\deg A, \deg B)$
2. $\deg AB \leqslant \deg A + \deg B$

Причем, если R — область целотности, то во втором пункте будет равенство.

Доказательство. Все понятно □

Следствие. Если R — область целостности, то $R[x]$ — тоже.

Определение 1.8. Многочлен от n переменных определяется рекурсивно: многочлен от одной переменной — как мы определяли выше, далее $R[x_1, x_2, \ldots x_n] = R[x_1, x_2, \ldots x_{n-1}][x_n]$.

1.3 Деление многочленов с остатком

Теорема 1.1. *Пусть F — поле, $A, B \in F[x], B \neq 0$. тогда*

1. $\exists! Q, R : A = BQ + R, \deg R < \deg B$

Доказательство. Существование доказывается алгоритмом деления в столбик. Проверим единственность:

$$BQ + R = BS + T$$

$$BQ - BS = T - R$$

$$\deg(B(Q - S)) > \deg(T - R)$$

Противоречие □

Теорема 1.2 (Безу)**.** *Пусть $P \in F[x]$. Тогда $P(x) - P(c) \vdots (x - c)$*

Доказательство. Разделим многочлен P на $x-c$ с остатком. Получится $P = Q(x-c)+R$, причем R — константа. Тогда подставим $x = c$, получим, что $R = P(c)$. □

1.3.1 Схема Горнера

Задан многочлен:

$$P(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_n x^n, \quad a_i \in \mathbb{R}$$

Пусть требуется вычислить значение данного многочлена при фиксированном значении $x = x_0$. Представим многочлен $P(x)$ в следующем виде:

$$P(x) = a_0 + x(a_1 + x(a_2 + \cdots x(a_{n-1} + a_n x) \ldots))$$

Определим следующую последовательность:

$$b_n = a_n,$$

$$b_{n-1} = a_{n-1} + b_n x_0,$$

$$\vdots$$

$$b_i = a_i + b_{i+1} x_0,$$

$$\vdots$$

$$b_0 = a_0 + b_1 x_0.$$

Искомое значение $P(x_0)$ есть b_0. Покажем, что это так.

В полученную форму записи $P(x)$ подставим $x = x_0$ и будем вычислять значение выражения, начиная с внутренних скобок. Для этого будем заменять подвыражения через b_i

$$\begin{aligned} P(x_0) &= a_0 + x_0(a_1 + x_0(a_2 + \cdots x_0(a_{n-1} + a_n x_0) \ldots)) = \\ &= a_0 + x_0(a_1 + x_0(a_2 + \cdots x_0 b_{n-1} \ldots)) = \\ &\vdots \\ &= a_0 + x_0 b_1 = \\ &= b_0. \end{aligned}$$

1.4 НОД двух многочленов. Алгоритм Евклида

Определение 1.9. Многочлен f делится на g, если $f = gh$ для некототорого h

Определение 1.10. Многочлены f, g называются ассоциированными, если $f \vdots g, g \vdots f$.

Определение 1.11. Многочлен d называется Наибольшим общим делителем двух многочленов f, g, если:

1. $f \vdots d, g \vdots d$
2. $f \vdots d', g \vdots d' \Rightarrow d \vdots d', d \vdots d'$

Теорема 1.3 (О представлении НОДа)**.**

1. *НОД любых двух многочленов существует*
2. *НОД любых двух многочленов представим в виде их линейной комбинации*