Оглавление

Глава 1

Полиномы

1.1 Многочлены над $\mathbb{Z}$

Теорема 1 (рациональный корень). Пусть $F \in \mathbb{Z}[x]$, $F(x) = a_n x^n + ... + a_0$, $\frac{p}{q}$ – корень $F(x)$, $(p, q) = 1$
Тогда $a_n \vdots q$, $a_0 \vdots p$

Доказательство.

$$a_n \cdot \frac{p^n}{q^n} + a_{n-1} \cdot \frac{p^{n-1}}{q^{n-1}} + ... + a_1 \cdot \frac{p}{q} + a_0 = 0$$

Умножим на q^n:

$$a_n p^n + a_{n-1} p^{n-1} q + ... + a_1 p q^{n-1} + a_0 q^n = 0 \implies \left.\begin{matrix} \begin{cases} a_n p^n \vdots q \\ a_0 q^n \vdots p \end{cases} \\ (p, q) = 1 \end{matrix}\right\} \implies \begin{cases} a_n \vdots q \\ a_0 \vdots p \end{cases}$$

□

Следствие. Пусть $F \in \mathbb{Z}[x]$, старший коэффициент F равен 1
Тогда любой рациональный корень является целым и делит a_0

Доказательство. $q = a_n \vdots q \implies q =$ что-то □

Определение 1. Пусть $P in \mathbb{Z}[x]$, $P \neq 0$, $P(x) = a_n x^n + ... + a_0$
Содержанием $P(x)$ называется НОД$(a_n, a_{n-1}, ..., a_0)$

Обозначение. $C(P)$

Пример. $C(2x^2 + 8x + 10) = 2$

Определение 2. Многочлен $P \in \mathbb{Z}[x]$ называется примитивным, если $C(P) = 1$

Примеры.

1. $2x^2 + 8x + 10$ – **не** примитивный
2. $2x^2 + 8x + 9$ – примитивный

Свойства.

1. Пусть $F \in \mathbb{Z}[x]$, $F_1(x) = \dfrac{1}{C(F)} \cdot F(x)$

Тогда $F_1(x)$ – примитивный

Доказательство. $F(x) = a_n x^n + ... + a_0, \quad d = C(F) \implies \dfrac{a_n}{d}, ..., \dfrac{a_0}{d}$ – целые, взаимно простые в совокупности ☐

2. Пусть F, G – примитивные, $F(x) = qG(x), \quad q \in \mathbb{Q}$
   Тогда $q = 1$ или $q = -1$

   Доказательство. $F(x) = a_n x^n + ... + a_0, \quad G(x) = b_n x^n + ... + b_0, \quad q = \frac{r}{s}, \quad (r, s) = 1$
   $a_i = \frac{r}{s} \cdot b_i \quad \forall i$
   $a_i \cdot s = r \cdot b_i \quad \forall i$
   $\forall i \quad a_i \cdot s \,\vdots\, r \implies a_i \,\vdots\, r \xRightarrow[C(F)=1]{} r = \pm 1$ ☐

3. Пусть $F \in \mathbb{Q}[x]$
   Тогда $\exists! q > 0 \in \mathbb{Q} : q \cdot F(x)$ – примитивный

   Пример. $F(x) = \frac{3}{2}x + \frac{9}{4}, \quad q = \frac{2}{3},$

   Доказательство.

   - Существование
     Пусть $F(x) = \dfrac{a_n}{b_n} \cdot x^n + ... + \dfrac{a_0}{b_0}, \quad a_i, b_i \in \mathbb{Z}$
     $N := \text{НОК}(b_n, ..., b_0) \implies N \cdot F(x) \in \mathbb{Z}[x]$
     По свойству 1, $\dfrac{1}{C(N \cdot F(x))} \cdot N \cdot F(x)$ – примитивный
     $q = \dfrac{N}{C(NF(x))}$ – подходит
   - Единственность

   ☐

Лемма 1 (Гаусса). Пусть $F(x), G(x) \in \mathbb{Z}[x], \quad H = F(x) \cdot G(x)$
Тогда

1. Если $F(x), G(x)$ – примитивные, то $H(x)$ – примитивный

   Доказательство. Пусть $F(x) = \sum a_i x^i, \quad G(x) = \sum b_i x^i, \quad H = \sum d_i x^i$
   Пусть H не примитивный $\implies$ НОД$(d_i) \neq 1 \implies \exists p \in \mathbb{P} : \forall i \quad d_i \,\vdots\, p$
   Не все a_i делятся на p, не все b_i делятся на p. Пусть $k := \min\{\, i \mid a_i \not\vdots\, p \,\}, \quad l = \min\{\, i \mid b_i \not\vdots\, p \,\}$

   $$(... + a_k x^k + ... + a_1 x + a_0) \cdot (... + b_l x^l + ... + b_1 x + b_0)$$

   $$d_{k+l} = \underset{\vdots p}{a_0 b_{k+1}} + ... + \underset{\not\vdots p}{a_k b_l} + ... + \underset{\vdots p}{a_{k+l} b_0} \quad \not\vdots\, p \quad \lightning$$

   ☐

2. $C(H) = C(F) \cdot C(G)$

   Доказательство. $F_1(x) = \dfrac{1}{C(F)} \cdot F(x), \quad G_1(x) = \dfrac{1}{C(G)} \cdot G(x)$
   $F_1(x), G_1(x)$ – примтивные (по свойству 1)

   $$\frac{1}{C(F) \cdot C(G)} \cdot H(x) = F_1(x) \cdot G_1(x) \text{ – примитивный} \xRightarrow[\text{по свойству 3}]{}$$

   $$\implies \frac{1}{C(f)C(G)} = \frac{1}{C(H)} \implies C(F) \cdot C(G) = C(H)$$

   ☐

Определение 3. Многочлен $F(x) \in \mathbb{Z}[x]$ называется неприводимым над $\mathbb{Z}$, если его нельзя разложить в произведение сногочленов из $\mathbb{Z}[x]$, отличных от *чего-то*

Теорема 2 (редукционный критерий неприводимости)**.**

1. Пусть $F \in \mathbb{Z}[x]$, F неприводимый над $\mathbb{Z}$
   Тогда F неприводимый над $\mathbb{Q}$
2. Пусть $F \in \mathbb{Z}[x]$, $\quad G, H \in \mathbb{Q}[x]$, $\quad F(x) = G(x)H(x)$
   Тогда $\exists G_1, H_1 \in \mathbb{Z}[x]$, ассоцированные с G, H над $\mathbb{Q}$, такие, что $F(x) = G_1(x)H_1(x)$

Доказательство.

(a) F примитивный

$$\underset{\in\mathbb{Z}[x],\ \text{примитивный}}{F(x)} = \underset{\in\mathbb{Q}[x]}{G(x)} \cdot \underset{\in\mathbb{Q}[x]}{H(x)}$$

По свойству 3:

$$\exists q_G, q_H > 0 \in \mathbb{Q} : q_G G(x), q_H H(x) \text{ -- примитивные}$$

$$(q_G q_H) \cdot \underset{\text{примтивный}}{F(x)} = \underset{\text{примтивный}}{(q_G G(x))} \cdot \underset{\text{примитивный}}{(q_H H(x))} \text{ -- примитивный}$$

$F(x)$ – примитивный $\implies q_G q_H = 1$

$$F(x) = q_G G(x) \cdot q_H H(x) \implies \begin{cases} G_1(x) = q_G G(x) \\ H_1(x) = q_H H(x) \end{cases}$$

Они подходят

(b) Общий случай

$$\underset{\in\mathbb{Z}[x]}{F(x)} = \underset{\in\mathbb{Q}[x]}{G(x)} \cdot \underset{\in\mathbb{Q}[x]}{H(x)}$$

Сделаем его примитивным:

$$\frac{1}{C(F)} F(x) = \frac{1}{C(F)} G(x) \cdot H(x)$$

$\dfrac{1}{C(f)} F(x)$ – примитивный

По (a) $\exists G_0(x), H_0(x)$, ассоцированные с $G(x), H(x)$, такие, что $\dfrac{1}{C(F)} F(x) = \underset{\in\mathbb{Z}[x}{G_0(x)} \cdot \underset{\in\mathbb{Z}[x]}{H_0(x)}$

$$F(x) = \underbrace{C(F) G_0(x)}_{\in\mathbb{Z}[x]} \cdot H_0(x)$$

$$\begin{cases} G_1 := C(F) G_0(x) \\ H_1(x) := H_0(x) \end{cases}$$

Они подходят

$\square$

Примечание. Первое – просто другая формулировка второго

Теорема 3 (факториальность $\mathbb{Z}[x]$)**.** Любой многочлен из $\mathbb{Z}[x]$ можно представить в виде произведения простых чисел и примитивных многочленов, неприводимых над $\mathbb{Q}$
Такое представление единственно с точностью до перестановки сомножителей и умножения сомножиетелей на (-1)

Пример. $5x^2 - 5 = 5(x-1)(x+1) = 5(-x+1)(-x-1)$

Доказательство.

- Существование
  $F(x) \in \mathbb{Q}[x], \quad \mathbb{Q}[x]$ факториально $\implies F(x)$ можно представить как $F(x) = a \cdot P_1(x) \cdot ... \cdot P_k(x), \quad a \in \mathbb{Q}, \quad a \neq 0, \quad P_i(x) \in \mathbb{Q}[x], \quad P_i$ неприводимы над $\mathbb{Q}$
  Заменим $P_1(x)$ на $aP_1(x)$
  $F(x) = P_1(x) \cdot ... \cdot P_k(x), \quad P_i(x)$ неприводимы над $\mathbb{Q}$
  $\exists H_i(x) \in \mathbb{Z}[x]$, ассоциированные с $P_i(x)$
  $F(x) = H_1(x) \cdot ... \cdot H_k(x), \quad H_i$ неприводимы над $\mathbb{Q}$
  Пусть $T_i(x) = \dfrac{1}{C(H_i)} \cdot H_i(x)$ – примитивный, неприводимый над $\mathbb{Q}$
  Пусть $C(H_1) \cdot ... \cdot C(H_k) = p_1^{\alpha_1} \cdot ... \cdot p_m^{\alpha_m}, \quad p_i \in \mathbb{P}$
  Тогда $F(x) = p_1^{\alpha_1} \cdot ... \cdot p_m^{\alpha_m} \cdot T_1(x) \cdot ... \cdot T_k(x)$ – нужное разложение

- Единственность
  $F(x) = \pm p_1 p_2 ... \underbrace{T_1(x)T_2(x)...}_{\text{примитивный}}$ и $F(x) = \pm q_1 q_2 ... \underbrace{H_1(x)H_2(x)...}_{\text{примитивный}}$
  $C(F) = p_1 p_2 ... C(F) = q_1 q_2 ...$
  Вспоминаем основную теорему арифметики (или факториальность $\mathbb{Z}$) – $\lightning$
  $$T_1(x)T_2(x)... = H_1(x)H_2(x)...$$
  $\mathbb{Q}[x]$ – факториально $\implies$ произведения совпадают с точностью до порядка и ассоциированности
  Перенумеруем: $C_i(x) \coloneqq q_i H_i(x)$
  $T_i(x) H_i(x)$ – примитивные $\implies q_i = \pm - 1$

$\square$

Теорема 4 (критерий неприводимости Эйзенштейна). Пусть $a_0, a_1, ..., a_{n-1} \in \mathbb{Z}, \quad a_n = 1, \quad p \in \mathbb{P}$
Все a_i, кроме a_n делятся на $p, \quad a_0 \not\vdots\, p^2$
Тогда $F(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ неприводим над $\mathbb{Q}$

Доказательство. Достаточно доказать неприводимость над $\mathbb{Z}$
Пусть приводим
$$x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = (... + b_1 x + b_0) \cdot (... + c_1 x + c_0), \quad b_i, c_i \in \mathbb{Z}$$
$b_0 c_0 = a_0 \quad \vdots\, p \quad \not\vdots\, p^2$
Одно из чисел b_0, c_0 делится на p, другое – нет
Пусть $b_0 \vdots\, p, \quad c_0 \not\vdots\, p$
Не все b_i делятся на p, так как $C(F) \not\vdots\, p$ (т. к. старший коэффициент 1)
Пусть $k \coloneqq \min\{\, i \mid b_i \not\vdots\, p \,\}, \quad k \leq \deg(... + b_1 x + b_0) < \deg F < n$
Тогда $a_k = \underbrace{\underset{\not\vdots p}{b_k}\underset{\not\vdots p}{c_0}} + \underbrace{\underset{\vdots p}{b_{k-1}c_1} + ... + \underset{\vdots p}{b_0 c_k}}_{\vdots p} \implies a_k \not\vdots\, p$ – $\lightning$ с $k < n$ $\square$