Оглавление

Глава 1

Полиномы

1.1 Факториальное кольцо (продолжение)

Примеры.

1. K – поле $\implies$ $K[x]$ факториально (доказательство потом) Примеры разложений:
   - $x^2 - 1 = 1 \cdot (x-1)(x+1) = \frac{1}{6}(2x-3)(3x+3)$
2. Кольцо тригонометриеских многочленов не факториально:

$$\sum_{i,j \geq 0} a_{ij} (\sin x)^i (\cos x)^j$$

1.2 §5. Евклидовы кольца

Определение 1. A – область целостности с 1. Кольцо A называется евклидовым, если существует отображение

$$\delta : A \setminus \{0\} \to \mathbb{N} \setminus \{0\} : \begin{cases} \delta(ab) \geq \delta(a) \quad \forall a, b \in A \setminus \{0\} \\ \forall a, b \in A,\ b \neq 0\ \exists q, r : \begin{cases} a = bq + r \\ \delta(r) < \delta(b) \end{cases} \end{cases}$$

Отображение δ называется евклидовой нормой

Пример. 1. $\mathbb{Z}$, $\quad \delta(a) = |a|$

$$a = -17,\ b = -5$$

$$-17 = (-5) \cdot \underset{q}{3} + \underset{r}{(-2)} \quad |-2| < |-5|$$

2. $K[x]$, где K – поле $\quad \delta(P) = \deg P$
3. $\mathbb{Z}[i] = \{\, a + bi \mid a, b \in \mathbb{Z} \,\}$ – кольцо Гауссовых чисел

$$\delta(a + bi) = a^2 + b^2$$

Свойства. A – евклидово кольцо, δ – евклидова норма, $a \neq 0$, $b \neq 0$

1. $a \,\vdots\, b \implies \delta(a) \geq \delta(b)$
2. a и b ассоц. $\implies \delta(a) = \delta(b)$

3. $a = bc$, c не обр. $\implies \delta(a) > \delta(b)$

Доказательство.

1. $a = bc,\ \delta(a) = \delta(bc) \geq \delta(b)$
2. Из 1): $\delta(a) \geq \delta(b),\ \delta(b) \geq \delta(a) \implies \delta(a) = \delta(b)$
3. Докажем, что $b \not\vdots\, a$. Пусть $b = ad \implies a = bc = adc \implies dc = 1 \implies c$ обратимо

$$\exists q, r : b = aq + r,\ \delta(r) < \delta(a) \text{ или } r = 0$$

$$r \neq 0, \text{ т. к. } b \not\vdots\, a$$

$$r = b - ad \implies r \vdots\, b \underset{1)}{\implies} \delta(r) \geq \delta(b)$$

$$\delta(a) > \delta(r) \geq \delta(b)$$

□

Теорема 1 (НОД в евклидовом кольце)**.** Пусть A – евклидово, $a, b \in A$, $a \neq 0$ или $b \neq 0$ (не оба нули). Тогда:

1. Существует НОД(a, b)
2. Пусть d явл. НОД (a, b). Тогда $\exists x, y \in A : d = ax + by$

Доказательство. Положим $M = \{\, au + bv \mid u, v \in A\,\}$. Пусть $M = \min\left\{\delta(c)\middle|c \in M\right\}$, пусть $d_0 : d_0 \in M,\ \delta(d_0) = m$. Докажем, что d_0 – общий делитель a, b. Пусть $a \not\vdots\, d$

$$\exists q, r : a = dq + r,\ r \neq 0,\ \delta(r) < \delta(d_0)$$

$$r = a - d_0 q = a - (ax + by)q = a(1 - qx) + b(-qy) \in M$$

$$\delta(r) < \delta(d_0) = m \quad \lightning$$

Докажем, что если k – общий делитель a и b, то $d_0 \vdots\, k$

$$\left.\begin{matrix} a \vdots k \\ b \vdots k \end{matrix}\right\} \implies \begin{Bmatrix} ax \vdots k \\ by \vdots k \end{Bmatrix} \implies d_0 = ax + by \vdots k$$

Докажем, что d_0 явл. НОД $(a, b) \implies$ НОД (a, b) существует:

$$d, d_0 - \text{НОД}(a, b) \implies d = t \cdot d_0,\ t - \text{обр.} \implies d = a(tx) + b(ty)$$

□

Свойство (Взаимная простота с произведением)**.** A – евклидово кольцо. $a_1, a_2, ..., a_k, b \in A$ $(a_i, b) = 1\ \forall i$. Тогда $(a_1 a_2 ... a_k, b) = 1$

Свойство (Взаимная простота и делимость)**.** A – евклидово кольцо.

1. $ab \vdots c,\ (a, c) = 1 \implies b \vdots c$
2. $a \vdots b,\ a \vdots c,\ (b, c) = 1 \implies a \vdots bc$

Теорема 2. Любое евклидово кольцо факториально

Доказательство.

1. $\exists$
Докажем, что любой ненулевой элемент можно представить в виде произведения неразложимых элементов и обратимого элемента:
Пусть a не представляется, и $\delta(a)$ – наименьшее возможное. a не обратим, т. к. иначе $a = a$ – нужное представление. a не неразложимый, т. к. иначе $a = 1 \cdot a$ – нужное представление.
$$\exists b, c : a = bc,\ b, c \text{ не обратимы}$$
$$\delta(b) < \delta(a),\ \delta(c) < \delta(a)$$
b и c можно представить в виде произведения неразлодимых элементов и обратимого элемента. Пусть $\left.\begin{aligned} b &= up_1...p_k \\ c &= vq_1...q_m \end{aligned}\right\} \implies a = (uv)p_1...p_k q_1...q_m \quad \lightning$

2. !
Докажем, что представление единственно с точностью до перестановки сомножителей и замены сомножителей на ассоциированные:
Пусть не для всех элементов единственно. Пусть a – такой, что для него не единственно, и $\delta(a)$ – наименьшая возможная.
$$a = up_1...p_k, \quad a = vq_1...q_n$$
$$vq_1...q_m \vdots p_1$$
$$v \not\vdots p_1$$
$$q_i \vdots p_q \text{ или } (q_i, p_1) = 1\ \forall i$$
$$(v, p_1) = 1$$
Если $(q_i, p_1) = 1\ \forall i \implies (vq_1...q_m, p_1) = 1 \implies vq_1...q_m \not\vdots p_1 \implies a \not\vdots p_1 \quad \lightning$
$$\exists i : q_i \vdots p_q \implies q_i \text{ ассоц. с } p_1$$
Переставим сомножители и будем считать, что q_1 ассоц. с p_1. Пусть $q_1 = wp_1,\ w$ обратимо
$$\begin{cases} a = up_1...p_k \\ a = v(wp_1)q_2...q_m \end{cases}$$
Пусть $b : bp_1 = a \implies \begin{cases} b = up_2...p_k \\ b = (vw)q_2...q_m \end{cases}$
$$\delta(b) < \delta(a)$$
Произведение $up_2...p_k$ и $(vw)q_2...q_m$ совпадают с точностью до перестановки сомножителей и замены сомножителей на ассоциированные $\implies up_1p_2...p_k$ и $vq_1q_2...q_m$ совпадают с точностью до перестановки сомножителей и замены сомножителей на ассоциированные
$\square$

Следствие. Пусть K – поле. Тогда $[k]$ факториально

1.3 §6. Разложение многоленов над $\mathbb{R}$ и $\mathbb{C}$

Определение 2. Пусть K – поле, $P \in K[x],\ c$ – корень $P(x)$
Показателем кратности корня c называется такое число k, что $P(x) \vdots (x-c)^k,\ \not\vdots (x-c)^{k+1}$

- Если $P(x) \vdots x - c,\ \not\vdots (x-c)^2$, то c называется простым корнем
- Если $P(x) \vdots (x-c)^2$, то c называется кратным корнем

Теорема 3 (Основная теорема алгебры). Любой многочлен с комплексными коэффициентами, отличный от константы имеет корень в $\mathbb{C}$

Следствие. Пусть $P \in \mathbb{C}[x],\ \deg P = n$. Тогда $P(x)$ имеет n корней с учётом кратности, P можно представить в виде

$$P(x) = a(x - x_1)(x - x_2)...(x - x_n) \quad a, x_i \in \mathbb{C}$$

Доказательство. Индукция □