Теоритично контролно №3, I, Информатика

Иван Йочев Кристиян Симов

25 май 2019 г.

1 Полиноми на една променливва

1.1 Теорема за деление с частно и остатък за полиноми

Нека F - поле
Нека $f, g \in F[x], g \neq 0$
$\Rightarrow \exists! q, r \in F[x] \; : \; f = g.q + r, \; deg(r) < deg(g)$

1.2 Схема на Хорнер

Нека F - поле
Нека $f = \sum\limits_{i=0}^{n} a_i x^{n-i}, \; g = \alpha - x \in F[x]$
$q, r \in F[x] \; : f = g.q + r, \; deg(r) < deg(g)$
$q = b_0 x^{n-1} + ... + b_n$

Схема на Хорнер:
$b_0 = a_0$
$b_1 = a_1 + \alpha b_0$
$b_2 = a_2 + \alpha b_1$
$\vdots$
$b_{n-1} = a_{n-1} + \alpha b_{n-2}$
$r = a_n + \alpha b_{n-1}$

1.3 Идеали в пръстена от полиномите с коефиценти от дадено поле

Нека F - поле
Нека $I \triangleleft F[x]$
$\Rightarrow I$ - главен идеал

1.4 Максимален брой различни корени на ненулев полином с коефиценти от дадена област и от степен n

Нека A - област
Нека $f \in A[x] \; : \; f \neq 0, \; deg(f) = n$
$\Rightarrow$ f има най-много n различни корена

1.5 Принцип за сравняване на коефицентите на полиноми

Нека А - област
Нека $g_1, g_2 \in A[x] : \ deg(g_1), deg(g_2) \leq n$
Ако $\exists \alpha_1 ... \alpha_{n+1} \ \ \forall i \in \{1, ..., n+1\} \ : \ g_1(\alpha_i) = g_2(\alpha_i)$
Тогава $g_1 = g_2$

2 Аритметика в пръстена на полиномите

2.1 Определение за деление на полиноми

Нека F - поле. Нека $g, f \in F[x], g \neq 0$
g дели f $(g \mid f)$ ако:
$\exists h \in F[x] \ : \ f = g.h$

2.2 Полином дели произведението на два полинома и е взаимно прост с един от тях

Нека F - поле Нека $g, f_1, f_2 \in F[x]$
Ако $g \mid f_1 f_2 \ \wedge \ (g, f_1) = 1 \ \Rightarrow \ g \mid f_2$

2.3 Най-голям общ делител на два полинома

Нека F - поле
Нека $f, g \in F[x]$, БОО $g \neq 0$
$\Rightarrow d \in F[x]$ е НОД на f и g $((f, g) = d)$, ако:
1) $d \mid f \ \wedge d \mid g$
2) $(\exists d_1 \in F[x] \ : \ d_1 \mid f \ \wedge d_1 \mid g \ ) \rightarrow d_1 \mid d$

2.4 Тъждество на Безу за два полинома

Нека F - поле
Нека $f, g \in F[x]$
Нека $d \in F[x] \ : \ (f, g) = d$
$\Rightarrow \exists u, v \in F[x] \ : \ uf + vg = d$

2.5 Най-малко общо кратно на два полинома

Нека F - поле
Нека $f, g \in F[x]$
$k \in F[x]$е НОК на f и g $([f, g] = k)$, ако:
1) $f \mid k \wedge g \mid k$
2) $(\exists k_1 \in F[x] : f \mid k_1 \wedge g \mid k_1) \rightarrow k_1 \mid k$

2.6 Пораждащ елемент на идеала $(f) + (g)$

Нека F - поле
Нека $f, g \in F[x]$

Тогава идеалът $(f) + (g)$ се поражда от елемента $(f, g) \in F[x]$
т.е $(f) + (g) = ((f, g))$

2.7 Пораждащ елемент на идеала $(f) \cap (g)$

Нека F - поле
Нека $f, g \in F[x]$
Тогава идеалът $(f) \cap (g)$ се поражда от елемента $[f, g] \in F[x]$
т.е $(f) + (g) = ([f, g])$

2.8 Неразложим полином над дадено поле

Нека F - поле
Нека $f \in F[x],\ deg(f) > 0$
f - неразложим, ако:
$\nexists g, h \in F[x] : f = gh\ \wedge\ (0 < deg(g), deg(h) < deg(f))$

2.9 Неразложим полином дели произведението на два други

Нека F - поле
Нека $p, f_1, f_2 \in F[x]$, p - неразложим
Тогава $(p \mid f_1 f_2) \leftrightarrow p \mid f_1 \vee p \mid f_2$

2.10 Теорема за разлагане на полином на неразложими множители

Нека F - поле
Нека $f \in F[x]\ :\ deg(f) > 0$
$\Rightarrow \exists$*!$p_1, ..., p_k \in F[x]$ (p_i - неразложим, $i = 1, ..., k) : f = p_1 p_2 ... p_k$

*Разлагането е единствено с точност до реда на полиномите и мултипликативни ненулеви константи, т.е:
Ако $f = p_1, ..., p_k = q_1, ..., q_s$
$\Rightarrow k = s\ \wedge\ q_i = a_i p_i,$
$a_i \in F (a_i \neq 0),\ i = 1, ..., k$

3 Корени на полиномите

3.1 Какъв е полином е f, ако факторпръстенът F[x]/(f) е поле

Нека F - поле
Нека $f \in F[x] : deg(f) > 0$
Тогава ако $F[x]/(f)$ е поле $\Rightarrow$ f - неразложим

3.2 Какъв е факторпръстенът F[x]/(f), ако f е неразложим

Нека F - поле
Нека $f \in F[x] : deg(f) > 0$
Тогава ако f - неразложим $\Rightarrow F[x]/(f)$ е поле

3.3 Определение за поле на разлагане

Нека F - поле
Нека $f \in F[x] : deg(f) > 0$
$\alpha_1, ..., \alpha_n$ са всички корени на f
Нека $L > F : \alpha_1, ..., \alpha_n \in L$
$\Rightarrow \; K = \bigcap\limits_{\substack{F \leq P < L \\ \alpha_1, ..., \alpha_n \in P}} P$, - поле на разлагане на f над F
Ако $K_1,\; K_2$ - полета на разлагане на f над F $\Rightarrow \; K_1 \cong K_2$
т.е полето на разлагане е единствено с точност до изоморфизъм

3.4 Формули на Виет за полином от четвърта степен

Нека F - поле
Нека $f = \sum\limits_{i=0}^{4} a_i x^{4-i}$
Нека $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ - са корени на f
т.е $f = a_0(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$

Формули на Виет
1) $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = -\frac{a_1}{a_0}$
2) $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 = \frac{a_2}{a_0}$
3) $\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 = -\frac{a_3}{a_0}$
4) $\alpha_1\alpha_2\alpha_3\alpha_4 = \frac{a_4}{a_0}$

3.5 Определение за k-кратен корен на полином

Нека F - поле, K $>$ F
Нека $f \in F[x],\; \alpha \in F$
α е k-кратен корен на f, ако:
$f = (x-\alpha)^k.g,\; g \in K[x] : g(\alpha) \neq 0$

3.6 НДУ полином над поле с характеристика 0 да има k-кратен корен

Нека F - поле и char F = 0, K $>$ F
Нека $f \in F[x],\; \alpha \in K$
α е k-кратен корен $\leftrightarrow$
1) $f(\alpha) = f'(\alpha) = ... = f^{(k-1)}(\alpha) = 0$
2) $f^{(k)}(\alpha) \neq 0$

4 Симетрични полиноми

4.1 Лема за старшия едночлен за полиноми на много променливи

Нека A - област
Нека $0 \neq f, g \in A[x_1, ...x_n]$
Нека $u = a \prod\limits_{k=1}^{n} x_k^{i_k} (0 \neq a \in A)$ - старши едночлен на f
Нека $v = b \prod\limits_{k=1}^{n} x_k^{j_k} (0 \neq b \in A)$ - старши едночлен на g
$\Rightarrow u.v = ab \prod\limits_{k=0}^{n} x_k^{i_k + j_k}$ - старши едночлен на f.g

4.2 Лексикографска наредба на едночлени на n променливи

Нека A - област
Нека $u = a \prod\limits_{k=1}^{n} x_k^{i_k} (0 \neq a \in A)$
Нека $v = b \prod\limits_{k=1}^{n} x_k^{j_k} (0 \neq a \in A)$
u и v са неподобни едночлени
$u > v$, ако $\exists k \in \mathbb{N}$:
$(\forall t \in \{1, 2, ..., k-1\}\ i_t = j_t) \wedge (i_k > j_k)$

4.3 Симетричен полином

Нека A - област
Нека $f = f(x_1, f_2, ..., f_n) \in A[x_1, x_2, ..., x_n]$
f е симетричен $\leftrightarrow \forall \sigma \in S_n$:
$f(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$

4.4 Елементарни симетрични полиноми

$\sigma_1 = \sigma_1(x_1, x_2, ..., x_n) = x_1 + x_2 + ... + x_n$
$\sigma_2 = \sigma_2(x_1, x_2, ..., x_n) = x_1x_2 + x_1x_3 + ... + x_{n-1}x_n$
$\sigma_3 = \sigma_3(x_1, x_2, ..., x_n) = x_1x_2x_3 + x_1x_2x_4 + ... + x_{n-2}x_{n-1}x_n$
$\vdots$
$\sigma_n = \sigma_n(x_1, x_2, ..., x_n) = x_1x_2x_3...x_n$

За n = 4
$\sigma_2 = \sigma_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$

4.5 Основна теорема за симетричните полиноми

Нека A - област
Нека $f = f(x_1, x_2, ..., x_n) \in A[x_1, x_2, ..., x_n]$
$\Rightarrow \exists! g \in A[x_1, x_2, ..., x_n] : f(x_1, ..., x_n) = g(\sigma_1, ..., \sigma_n)$

4.6 Формули на Нютон

Нека A - област
Нека $f = f(x_1, ...x_n) \in A[x_1, ..., x_n]$
Нека $S_k = x_1^k + x_2^k + ... + x_n^k \ 1 < k \leq n$

Формули на Нютон
$S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} - ... + (-1)^{k-1}\sigma_{k-1}S_1 + (-1)^k \sigma_k k = 0$

5 Дискриминанта и резултанта

6 Полиноми с рационални коефиценти

6.1 Определение за примитивен полином

Нека $f = a_0x^n + ... + a_n \in \mathbb{Z}[x]$
f - примитивен $\leftrightarrow (a_0, a_1, ..., a_n) = 1$

6.2 Лема на Гаус за полиноми с цели коефиценти

Нека $g = a_0x^n + ... + a_n \in \mathbb{Z}[x]$
Нека $h = b_0x^n + ... + b_n \in \mathbb{Z}[x]$
f и g са примитивни полиноми
Тогава $f = g.h$ също е примитивен полином

6.3 Редукционен критерий за неразложимост на полиноми с цели коефиценти

Нека $f \in \mathbb{Z}[x]$
Нека $p \in \mathbb{N}$ - произволно просто число
Нека $\bar{f} \in \mathbb{Z}_p[x]$ е полиномът f, редуциран по модул p
$\bar{f}$ е неразложим над $[Z]_p \Rightarrow f$ е неразложим над $\mathbb{Z}$

6.4 Критерий на Айзенщайн за неразложимост на полиноми с цели коефиценти

Нека $f = \sum_{i=0}^{n} a_i x^{n-i} \in \mathbb{Z}[x]$
f е неразложим над $\mathbb{Q}$, ако $\exists p \in \mathbb{P}$:
1) $p \nmid a_0$
2) $p \mid a_1, ..., a_n$
3) $p^2 \nmid a_n$