

Примерни задачи за полиноми Алгебра 2, специалност Компютърни науки

ДЕЛЕНИЕ НА ПОЛИНОМИ С ЧАСТНО И ОСТАТЪК. НАЙ-ГОЛЯМ ОБЩ ДЕЛИТЕЛ.

Задача 1. Да се намери полиномът $f_i(x) = x^3 + px + q \in \mathbb{Z}[x]$, $1 \leq i \leq 2$, ако:

- (i) $f_1(x)$ се дели на $x^2 - 3x + 2$;
- (ii) остатъкът на $f_2(x)$ при деление с $x^2 + 3x + 2$ е $2x + 3$.

Отговор: (i) $f_1(x) = x^3 - 7x + 6$; (ii) $f_2(x) = x^3 - 5x - 3$.

Задача 2. Да се намери най-големият общ делител $d_i(x)$, $1 \leq i \leq 2$ на полиномите $f_i(x), g_i(x)$ и полиноми $u_i(x), v_i(x)$, за които е изпълнено тъждеството на Безу

$$d_i(x) = f_i(x)u_i(x) + g_i(x)v_i(x),$$

ако:

- (i) $f_1(x) = x^3 + x^2 + x + 1$, $g_1(x) = x^2 - x + 2 \in \mathbb{Q}[x]$;
- (ii) $f_2(x) = x^5 + x^4 + \bar{1}$, $g_2(x) = x^4 + x^2 + \bar{1} \in \mathbb{Z}_2[x]$.

Отговор: (i) $d_1(x) = 8 = (x^2 + 4x + 5)g_1(x) - (x + 2)f_1(x)$;
(ii) $d_2(x) = x^2 + x + \bar{1} = (x + \bar{1})f_2(x) + x^2g_2(x)$.

РАЗЛАГАНЕ НА ПОЛИНОМИ С РАЦИОНАЛНИ И ЦЕЛИ КОЕФИЦИЕНТИ.

Лема 3. Нека R е комутативен пръстен с единица, I е идеал в R , а $\pi_I : R \rightarrow R/I$ е естественният епиморфизъм с ядро $\ker(\pi_I) = I$. Тогава изображението

$$\Pi_I : R[x] \longrightarrow R/I[x],$$

$$\Pi_I \left(\sum_{j=0}^n a_j x^j \right) = \sum_{j=0}^n \pi_I(a_j) x^j = \sum_{j=0}^n (a_j + I) x^j$$

е епиморфизъм на пръстени с ядро $I[x]$

Доказателство: Непосредствено се проверява, че

$$\begin{aligned}
\Pi_I \left(\sum_{j=0}^n a_j x^j \right) + \Pi_I \left(\sum_{s=0}^m b_s x^s \right) &= \left(\sum_{j=0}^n (a_j + I) x^j \right) + \left(\sum_{s=0}^m (b_s + I) x^s \right) = \\
&= \sum_{i=0}^{\max(n,m)} (a_i + b_i + I) x^i = \Pi_I \left(\sum_{j=0}^{\max(n,m)} (a_j + b_j) x^j \right) = \\
&= \Pi_I \left(\left(\sum_{j=0}^n a_j x^j \right) + \left(\sum_{s=0}^m b_s x^s \right) \right) \quad \text{и} \\
\Pi_I \left(\sum_{j=0}^n a_j x^j \right) \Pi_I \left(\sum_{s=0}^m b_s x^s \right) &= \left(\sum_{j=0}^n (a_j + I) x^j \right) \left(\sum_{s=0}^m (b_s + I) x^s \right) = \\
&= \sum_{j=0}^{n+m} \left(\sum_{s=0}^j (a_s + I)(b_{j-s} + I) \right) x^j = \sum_{j=0}^{n+m} \left(\left(\sum_{s=0}^j a_s b_{j-s} \right) + I \right) x^j = \\
&= \Pi_I \left(\sum_{j=0}^{n+m} \left(\sum_{s=0}^j a_s b_{j-s} \right) x^j \right) = \Pi_I \left(\left(\sum_{j=0}^n a_j x^j \right) \left(\sum_{s=0}^m b_s x^s \right) \right),
\end{aligned}$$

така че Π_I е хомоморфизъм на пръстени. Всеки елемент на $R/I[x]$ е от вида

$$\sum_{j=0}^n (a_j + I) x^j = \Pi_I \left(\sum_{j=0}^n a_j x^j \right) \in \text{im}(\Pi_I),$$

така че образът $\text{im}(\Pi_I) = R/I[x]$ и Π_I е епиморфизъм. Ядрото

$$\begin{aligned}
\ker(\Pi_I) &= \left\{ f(x) = \sum_{j=0}^n a_j x^j \in R[x] \mid \Pi_I(f) = \sum_{j=0}^n (a_j + I) x^j = I \right\} = \\
&= \left\{ f(x) = \sum_{j=0}^n a_j x^j \in R[x] \mid a_j \in I \quad \text{за} \quad \forall 0 \leq j \leq n \right\} = I[x],
\end{aligned}$$

Q.E.D.

Твърдение 4. (Редукционен критерий за неразложимост на целочислени полиноми)

Нека $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$, p е просто число, $\pi_p : \mathbb{Z} \rightarrow \mathbb{Z}_p$, $\pi_p(a) = a + p\mathbb{Z}$ е естественят епиморфизъм с ядро $\ker(\pi_p) = p\mathbb{Z}$, а

$$\Pi_p : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x],$$

$$\Pi_p \left(\sum_{i=0}^n a_j x^i \right) = \sum_{i=0}^n (a_i + p\mathbb{Z}) x^i$$

е естественият епиморфизъм с ядро $\ker(\Pi_p) = (p\mathbb{Z})[x]$.

Ако редукцията $\pi_p(a_n) = a_n + p\mathbb{Z} \neq p\mathbb{Z}$ на старшия коефициент a_n на $f(x)$ е ненулева и редукцията $\Pi_p(f) \in \mathbb{Z}_p[x]$ на полинома $f(x)$ е неразложима над полето $\mathbb{Z}_p$, то полиномът $f(x)$ е неразложим над $\mathbb{Z}$.

Доказателство: Да допуснем противното и да представим $f(x) = f_1(x)f_2(x)$ като произведение на полиноми $f_i(x) \in \mathbb{Z}[x]$ от степен $0 < \deg(f_i) = n_i < \deg(f) = n$, $n_1 + n_2 = n$. По Лемата за старшия едночлен на полиноми на една променлива с коефициенти от комутативната област с единица $\mathbb{Z}$ имаме

$$a_n x^n = LT(f) = LT(f_1)LT(f_2).$$

Оттук, старшият коефициент

$$a_n = LC(f) = LC(f_1)LC(f_2)$$

има редукция

$$p\mathbb{Z} \neq a_n + p\mathbb{Z} = (LC(f_1) + p\mathbb{Z})(LC(f_2) + p\mathbb{Z}),$$

така че $LC(f_i) + p\mathbb{Z} \neq p\mathbb{Z}$ и $\deg(\Pi_p(f_i)) = \deg(f_i) = n_i < n$ за $1 \leq i \leq 2$. В резултат получаваме разлагане

$$\Pi_p(f) = \Pi_p(f_1)\Pi_p(f_2)$$

на редукцията $\Pi_p(f)$ на f над $\mathbb{Z}_p$, което противоречи на предположението и доказва неразложимостта на $f(x) \in \mathbb{Z}[x]$ над $\mathbb{Z}$, Q.E.D.

Задача 5. Да се разложат полиномите

$$f(x) = x^4 + 6x - 7 \in \mathbb{Z}[x] \quad \text{и} \quad g(x) = x^4 + 2x^3 + 3x^2 - 2x + 5 \in \mathbb{Z}[x]$$

в произведение от неразложими над $\mathbb{Q}$ множители.

$$\text{Отговор: } f(x) = (x-1)(x^3 + x^2 + x + 7), \quad g(x) = (x^2 - x + 1)(x^2 + 3x + 5).$$

Задача 6. Да се докаже, че полиномите

$$(i) \quad f_1(x) = x^4 + 6x^3 - 3x^2 + 4x - 1 \in \mathbb{Z}[x]$$

$$(ii) \quad f_2(x) = x^4 + 2x^3 + 3x^2 + 4x + 5 \in \mathbb{Z}[x],$$

$$(iii) \quad f_3(x) = x^5 + 5x^4 + 10x^3 + 7x^2 + 2x - 2 \in \mathbb{Z}[x]$$

са неразложими над $\mathbb{Q}$.

Решение: (iii) Ако допуснем, че $f_3(x) \in \mathbb{Z}[x]$ от степен 5 със старши коефициент 1 е разложим над $\mathbb{Z}$, то $f_3(x)$ има цял корен $\alpha \in \{\pm 1, \pm 2\}$, делящ свободния член -2 или $f_3(x) = (x^3 + ax^2 + bx + c)(x^2 + px + q)$ се разлага в произведение на неразложими над $\mathbb{Z}$ множители $x^3 + ax^2 + bx + c, x^2 + px + q \in \mathbb{Z}[x]$. Непосредствено се проверява,

че $f_3(1) = 23 \neq 0$, $f_3(-1) = -3 \neq 0$, $f_3(2) = 222 \neq 0$, $f_3(-2) = -10 \neq 0$. Сравнявайки коефициентите в

$$f_3(x) = x^5 + 5x^4 + 10x^3 + 7x^2 + 2x - 2 = (x^3 + ax^2 + bx + c)(x^2 + px + q),$$

получаваме

$$x^4 : p + a = 5, \quad (1)$$

$$x^3 : b + ap + q = 10, \quad (2)$$

$$x^2 : c + bp + aq = 7, \quad (3)$$

$$x : cp + bq = 2, \quad (4)$$

$$1 : cq = -2. \quad (5)$$

От (5) следва, че $c = 2\varepsilon$, $q = -\varepsilon$ или $c = -\varepsilon$, $q = 2\varepsilon$ за $\varepsilon \in \{\pm 1\}$.

В случая $c = 2\varepsilon$, $q = -\varepsilon$ изразяваме $b = 2(p - \varepsilon)$ от (4). Заедно с $a = 5 - p$ от (1), заместваем в (2) и получаваме квадратното уравнение $p^2 - 7p + 3\varepsilon + 10 = 0$ за p . Дискриминантата $D(p^2 - 7p + 3\varepsilon + 10) = 3(3 - 4\varepsilon) \in \{-3, 21\}$ не е точен квадрат на рационално число, така че не съществува $p \in \mathbb{Z} \subset \mathbb{Q}$ с $p^2 - 7p + 3\varepsilon + 10 = 0$, $\varepsilon \in \{\pm 1\}$.

Ако $c = -\varepsilon$, $q = 2\varepsilon$, то от (4) получаваме, че $b = \varepsilon + \frac{p}{2}$. Заедно с $a = 5 - p$, заместваем в (2) и извеждаме, че $2p^2 - 11p - 6\varepsilon + 20 = 0$. Дискриминантата $D(2p^2 - 11p - 6\varepsilon + 20) = 48\varepsilon - 39$ е квадрат на рационално число за $\varepsilon = 1$ и уравнението $2p^2 - 11p + 14 = (2p - 7)(p - 2) = 0$ има цял корен $p = 2$. В резултат, $a = 3$, $b = 2$, $c = -1$ и $q = 2$. Но тези стойности не удовлетворяват равенството (3), така че полиномът $f_3(x) \in \mathbb{Z}[x]$ е неразложим над $\mathbb{Z}$ и над $\mathbb{Q}$.

Задача 7. За произволни цели числа $a_1, \dots, a_4 \in \mathbb{Z}$ да се докаже, че полиномите

$$f_1(x) = x^4 + 2a_1x^3 + 2a_2x^2 + (2a_3 + 1)x + (2a_4 + 1) \in \mathbb{Z}[x],$$

$$f_2(x) = x^4 + (2a_1 + 1)x^3 + 2a_2x^2 + 2a_3x + (2a_4 + 1) \in \mathbb{Z}[x],$$

$$f_3(x) = x^4 + (2a_1 + 1)x^3 + (2a_2 + 1)x^2 + (2a_3 + 1)x + (2a_4 + 1) \in \mathbb{Z}[x]$$

са неразложими над $\mathbb{Q}$.

Упътване: Използвайте редукция на коефициентите по модул 2.

Задача 8. С редукция на коефициентите по модул 3 да се докаже, че полиномът

$$g(x) = 2011x^4 + 6004x^3 + 2995x^2 + 6007x + 1549 \in \mathbb{Z}[x]$$

е неразложим над $\mathbb{Q}$.

Задача 9. (а) За произволен полином $f(x) \in \mathbb{Z}[x]$ и произволно цяло число a да се докаже, че полиномите $g(x) = f(x + a)$ и $f(x)$ са едновременно неразложими над $\mathbb{Z}$.

(б) С помощта на критерия на Айзенщайн, приложен към $f(x + a)$ за подходящо $a \in \mathbb{Z}$ да се докаже неразложимостта на полиномите

$$f_1(x) = x^4 - 8x^3 + 24x^2 - 35x + 28 \in \mathbb{Z}[x],$$

$$f_2(x) = x^5 + 5x^4 + 6x^3 - 9x - 5 \in \mathbb{Z}[x],$$

$$f_3(x) = x^{p-1} + x^{p-2} + \dots + x + 1 \in \mathbb{Z}[x] \quad \text{за просто } p,$$

$$f_4(x) = x^p - px^2 + p^2x - 1 \in \mathbb{Z}[x] \quad \text{за просто } p$$

над полето $\mathbb{Q}$ на рационалните числа.

Решение: (б)(i) Ако в полинома

$$f_1(x+a) = x^4 + 4(a-2)x^3 + 6(a-2)^2x^2 + [4(a-2)^3 - 3]x + (a-2)^4 - 3(a-4)$$

положим $a = 2$, получаваме полинома $f_1(x+2) = x^4 - 3x + 6 \in \mathbb{Z}[x]$, който е неразложим над $\mathbb{Q}$ по критерия на Айзенщайн за простото число $p = 3$.

(ii) В

$$f_2(x+a) = x^5 + 5(a+1)x^4 + [10(a+1)^2 - 4]x^3 + [10(a+1)^3 - 12(a+1) + 2]x^2 +$$

$$+ [5(a+1)^4 - 12(a+1)^2 + 4(a+1) - 6]x + (a+1)^5 - 4(a+1)^3 + 2(a+1)^2 - 6(a+1) + 2$$

избираме $a = -1$ и прилагаме критерия на Айзенщайн за простото число $p = 2$ към $f_2(x-1) = x^5 - 4x^3 + 2x^2 - 6x + 2 \in \mathbb{Z}[x]$.

(iii) В биномната формула $(x-1)f_3(x) = x^p - 1$ заменяме променливата x с $t = x-1$ и прилагаме критерия на Айзенщайн за простото число p към

$$f_3(t+1) = \frac{(t+1)^p - 1}{t} = t^{p-1} + \sum_{i=2}^{p-1} \binom{p}{i} t^{i-1} + p \in \mathbb{Z}[t].$$

(iv) Полиномът

$$f_4(x+a) = x^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} x^i - px^2 + p(p-2a)x + (a^p - pa^2 + p^2a - 1) \in \mathbb{Z}[x]$$

изпълнява критерия на Айзенщайн за простото число p тогава и само тогава, когато p дели $a^p - 1$, но p^2 не дели $a^p - 1 - pa^2$. Например, $a = 1$ изпълнява тези условия.

СЪЩЕСТВУВАНЕ НА КОРЕН НА ПОЛИНОМ В ПОДХОДЯЩО РАЗШИРЕНИЕ
НА ПОЛЕТО ОТ КОЕФИЦИЕНТИ.

Задача 10. Нека F е поле, $f(x) = \sum_{i=0}^n a_i x^i \in F[x] \setminus F$ е неразложим над F полином от степен $n \in \mathbb{N}$, а $E = F[x]/\langle f \rangle$ е полето, получено от $F[x]$ чрез факторизиране по идеала $\langle f \rangle \triangleleft F[x]$, породен от f . Да се докаже, че:

(i) полето $E = (F + \langle f \rangle / \langle f \rangle)[x + \langle f \rangle] \simeq F[x + \langle f \rangle]$ е изоморфно на пръстена на полиномите на $x + \langle f \rangle$ с коефициенти от F ;

(ii) полето $E = \left\{ \sum_{j=0}^{n-1} b_j x^j + \langle f \rangle \mid b_j \in F \right\} \simeq F^n$ е n -мерно линейно пространство над своето подполе F .

Решение: (i) Съгласно Задача 21 от примерните задачи за пръстени, сумата $F + \langle f \rangle$ на подпръстена F на $F[x]$ и идеала $\langle f \rangle$ на $F[x]$ е подпръстен на $F[x]$ с идеал $\langle f \rangle \triangleleft F + \langle f \rangle$. Следователно $F + \langle f \rangle / \langle f \rangle$ е подпръстен на полето $E = F[x]/\langle f \rangle$. Сега от $x + \langle f \rangle \in E$ следва $(F + \langle f \rangle / \langle f \rangle)[x + \langle f \rangle] \subseteq E$, защото E е затворено относно събиране, изваждане и умножение. За обратното включване $E \subseteq (F + \langle f \rangle / \langle f \rangle)[x + \langle f \rangle]$ е достатъчно да отбележим, че всеки елемент на E е от вида

$$\sum_{j=0}^m b_j x^j + \langle f \rangle = \sum_{j=0}^m (b_j + \langle f \rangle)(x + \langle f \rangle)^j \in (F + \langle f \rangle / \langle f \rangle)[x + \langle f \rangle],$$

съгласно пръвилата за събиране и умножение във фактор-пръстена $F[x]/\langle f \rangle$. Следователно $E = (F + \langle f \rangle / \langle f \rangle)[x + \langle f \rangle]$.

Задача 21 от примерните задачи за пръстени твърди, че

$$F/(F \cap \langle f \rangle) \simeq F + \langle f \rangle / \langle f \rangle.$$

Съгласно Задача 3 (ii) от примерните задачи за пръстени, единствените идеали в полето F са $\{0_F\}$ и F . Ако $F \cap \langle f \rangle = F$, то $1_F \in \langle f \rangle \triangleleft F[x]$ и съществува $g(x) \in F[x]$ с $1_F = f(x)g(x)$. В комутативната област с единица $F[x]$, оттук следва $\deg(f) + \deg(g) = 0$ с $\deg(f) \geq 0$, $\deg(g) \geq 0$. Следователно $n = \deg(f) = 0$, противно на предположението $n \in \mathbb{N}$. Това доказва $F \cap \langle f \rangle = \{0_F\}$ и

$$F + \langle f \rangle / \langle f \rangle \simeq F/(F \cap \langle f \rangle) = F.$$

Съгласно Лема 3, изоморфизмът на пръстени

$$\pi : F + \langle f \rangle / \langle f \rangle \longrightarrow F$$

индуцира епиморфизъм на пръстени

$$\Pi : (F + \langle f \rangle / \langle f \rangle)[x + \langle f \rangle] \longrightarrow F[x + \langle f \rangle]$$

с ядро $\ker(\Pi) = \ker(\pi)[x + \langle f \rangle] = 0_F$. Следователно Π е изоморфизъм на пръстени.

(ii) Нека $E_o = \left\{ \sum_{j=0}^{n-1} b_j x^j + \langle f \rangle \mid b_j \in F \right\}$. Включването $E_o \subseteq E$ следва от определението за фактор-пръстен $E = F[x]/\langle f \rangle$. За обратното включване $E \subseteq E_o$ да отбележим, че за $\forall g(x) \in F[x]$ делението $g(x) = f(x)q(x) + r(x)$ с частно $q(x) \in F[x]$ и остътък $r(x) \in F[x]$, $\deg(r) < \deg(f) = n$ дава

$$g(x) + \langle f \rangle = f(x)q(x) + r(x) + \langle f \rangle = r(x) + \langle f \rangle = \sum_{j=0}^{n-1} b_j x^j + \langle f \rangle.$$

Това доказва, че полето E съвпада с множеството E_o .

От изоморфизма на пръстени $E \simeq F[x + \langle f \rangle]$, установен в (i) следва, че F е подполе на полето E . Следователно $E = E_o$ е линейно пространство над F . Остава да проверим, че изображението

$$\begin{aligned} \psi : F^n &\longrightarrow E_o, \\ \psi(b_0, b_1, \dots, b_{n-1}) &= \sum_{j=0}^{n-1} b_j x^j + \langle f \rangle \end{aligned}$$

е изоморфизъм на линейни пространства над F . Линейността на ψ над F следва от равенствата

$$\begin{aligned} \psi((b_0, \dots, b_{n-1}) + (c_0, \dots, c_{n-1})) &= \psi(b_0 + c_0, \dots, b_{n-1} + c_{n-1}) = \sum_{j=0}^{n-1} (b_j + c_j)x^j + \langle f \rangle = \\ &= \left(\sum_{j=0}^{n-1} b_j x^j + \langle f \rangle \right) + \left(\sum_{j=0}^{n-1} c_j x^j + \langle f \rangle \right) = \psi(b_0, \dots, b_{n-1}) + \psi(c_0, \dots, c_{n-1}) \end{aligned}$$

и

$$\begin{aligned} \psi(\lambda(b_0, \dots, b_{n-1})) &= \psi(\lambda b_0, \dots, \lambda b_{n-1}) = \sum_{j=0}^{n-1} \lambda b_j x^j + \langle f \rangle = \\ &= \lambda \left(\sum_{j=0}^{n-1} b_j x^j + \langle f \rangle \right) = \lambda \psi(b_0, \dots, b_{n-1}). \end{aligned}$$

Всеки елемент на E_o е от вида $\sum_{j=0}^{n-1} b_j x^j + \langle f \rangle = \psi(b_0, \dots, b_{n-1})$, така че $\text{im}(\psi) = E_o$.

Ако $\psi(b_0, \dots, b_{n-1}) = \psi(c_0, \dots, c_{n-1})$, то $\sum_{j=0}^{n-1} b_j x^j + \langle f \rangle = \sum_{j=0}^{n-1} c_j x^j + \langle f \rangle$. Следователно

полиномът $h(x) := \sum_{j=0}^{n-1} (b_j - c_j)x^j \in \langle f \rangle$ се дели на $f(x)$, т.е. съществува $q(x) \in F[x]$

с $h(x) = f(x)q(x)$. Допускането $h(x) \not\equiv 0_F$ води до $q(x) \not\equiv 0_F$, откъдето $\deg(q) \geq 0$. Следователно $\deg(h) = \deg(f) + \deg(q) \geq \deg(f) = n$. Но от определението на полинома $h(x)$ се вижда, че $\deg(h) \leq n - 1$. Противоречието доказва, че $h(x) \equiv 0_F$, така че $b_j = c_j$ за $\forall 0 \leq j \leq n - 1$. Следователно различни $b, c \in F^n$ се изобразяват в различни $\psi(b), \psi(c) \in E_o$ и изображението ψ е взаимно еднозначно. Линейното над F взаимно еднозначно изображение ψ е F -линеен изоморфизъм.

Задача 11. Да се определи дали фактор-пръстенът $F_i[x]/(f_i)$, $1 \leq i \leq 4$ е поле, ако:

(i) $F_1 = \mathbb{Z}_5$ е полето на остатъците при деление с 5, а $f_1(x) = x^3 + 3x^2 - \bar{1} \in \mathbb{Z}_5[x]$;
(ii) $F_2 = \mathbb{Z}_7$ е полето на остатъците при деление с 7, а $f_2(x) = x^3 - 2x^2 + 3x + \bar{3} \in \mathbb{Z}_7[x]$;

(iii) $F_3 = \mathbb{Z}_3$ е полето на остатъците при деление с 3, а $f_3(x) = x^4 + x - \bar{1} \in \mathbb{Z}_3[x]$;

(iv) $F_4 = \mathbb{Z}_2$ е полето на остатъците при деление с 2, а $f_4(x) = x^5 + x^4 + \bar{1} \in \mathbb{Z}_2[x]$.

Упътване: Фактор-пръстенът $F_i[x]/(f_i)$ е поле тогава и само тогава, когато полиномът $f_i(x) \in F_i[x]$ е неразложим над F_i .

Полиномите $f_i(x) \in F_i[x]$, $1 \leq i \leq 2$ от степен 3 са неразложими над F_i точно когато нямат корен в F_i .

Полиномът $f_3(x) \in F_3[x]$ от степен 4 със старши коефициент 1 е неразложим над F_3 точно когато $f_3(x)$ няма корен в F_3 и не се разлага в произведение

$$f_3(x) = (x^2 + ax + b)(x^2 + cx + d)$$

на неразложими над F_3 квадратни тричлени $x^2 + ax + b, x^2 + cx + d \in F_3[x]$.

Полиномът $f_4(x) \in F_4[x]$ от степен 5 със старши коефициент 1 е неразложим над F_4 точно когато $f_4(x)$ няма корен в F_4 и не се разлага в произведение

$$f_4(x) = (x^2 + ax + b)(x^3 + cx^2 + dx + e)$$

на неразложим над F_4 квадратен тричлен $x^2 + ax + b \in F_4[x]$ и неразложим над F_4 кубичен полином $x^3 + cx^2 + dx + e \in F_4[x]$.

Отговор: (i) да; (ii) не; (iii) да; (iv) не.

Задача 12. Нека $f(x) = x^2 + ax + b \in \mathbb{R}[x]$ е квадратен тричлен с реални коефициенти и отрицателна дискриминанта $D = a^2 - 4b < 0$. Да се докаже, че фактор-пръстенът $\mathbb{R}[x]/(f)$ на $\mathbb{R}[x]$ по главния идеал, породен от $f(x)$ е полето на комплексните числа $\mathbb{C}$.

Упътване: Приложете теоремата за епиморфизмите на пръстени към изображението

$$\varphi : \mathbb{R}[x] \longrightarrow \mathbb{R}[x_1] = \mathbb{C},$$

$$\varphi(g(x)) = g(x_1) \quad \text{за} \quad \forall g(x) \in \mathbb{R}[x]$$

и за някой от корените $x_1 = \frac{-a+i\sqrt{-D}}{2}$ или $x_1 = \frac{-a-i\sqrt{-D}}{2}$ на $f(x) = 0$. Използвайте, че ако $g(x_1) = 0$, то $0 = \overline{g(x_1)} = g(\overline{x_1})$ за $\forall g(x) \in \mathbb{R}[x]$, така че $\ker \varphi$ е главният идеал, породен от полинома $(x - x_1)(x - \overline{x_1}) = f(x)$.

Задача 13. Нека $\mathbb{Z}_5$ е полето с 5 елемента. Да се докаже, че:

(i) фактор-пръстенът $\mathbb{Z}_5[x]/(x^2 - 2)$ на $\mathbb{Z}_5[x]$ по главния идеал, породен от $x^2 - 2$ е поле;

(ii) множеството $F = \left\{ \begin{pmatrix} \alpha & 2\beta \\ \beta & \alpha \end{pmatrix} \mid \alpha, \beta \in \mathbb{Z}_5 \right\}$ е поле относно обичайните операции събиране и умножение на матрици;

(iii) полето $\mathbb{Z}_5/(x^2 - 2)$ е изоморфно на полето F .

Упътване: Полиномът $x^2 - 2$ е неразложим над $\mathbb{Z}_5$, така че фактор-пръстенът $\mathbb{Z}_5[x]/(x^2 - 2)$ е поле. Всеки елемент $g(x) + (x^2 - 2) \in \mathbb{Z}_5[x]/(x^2 - 2)$, $g(x) \in \mathbb{Z}_5[x]$ има единствено представяне във вида $g(x) + (x^2 - 2) = \alpha + \beta x + (x^2 - 2)$ с $\alpha, \beta \in \mathbb{Z}_5$. Това определя взаимно-однозначното изображение

$$\varphi : \mathbb{Z}_5[x]/(x^2 - 2) \longrightarrow F,$$

$$\varphi(\alpha + \beta x + (x^2 - 2)) = \begin{pmatrix} \alpha & 2\beta \\ \beta & \alpha \end{pmatrix}$$

Достатъчно е да докажем, че φ е изоморфизъм на пръстени, за да твърдим, че F е поле, изоморфно на $\mathbb{Z}_5[x]/(x^2 - 2)$.

Изобщо, ако F_1 е поле и $\psi : F_1 \rightarrow F$ е изоморфизъм на пръстени, то F е поле. По-точно, комутативността на умножението в $F = \text{im} \psi$ следва от равенствата $\psi(a)\psi(b) = \psi(ab) = \psi(ba) = \psi(b)\psi(a)$ за $\forall \psi(a), \psi(b) \in F$. Пръстенът F има единица $1_F = \psi(1_{F_1})$, съгласно $\psi(1_{F_1})\psi(a) = \psi(a)\psi(1_{F_1}) = \psi(a \cdot 1_{F_1}) = \psi(a)$ за $\forall \psi(a) \in F$. Всеки ненулев елемент $\psi(a) \in F \setminus \{0_F = \psi(0_{F_1})\}$ е образ на ненулев елемент $a \in F_1 \setminus \{0_{F_1}\}$ и има обратен $\psi(a)^{-1} = \psi(a^{-1}) \in F$. Следователно F е поле.

КРАТНИ КОРЕНИ.

Определение 14. Формалната производна на полинома $f(x) = \sum_{i=0}^n a_i x^i \in F[x]$ с коефициенти от поле F е полиномът

$$f'(x) = \sum_{i=1}^n i a_i x^{i-1} \in F[x].$$

Лема 15. За произволни полиноми $f(x), g(x) \in F[x]$ с коефициенти от поле F е в сила

$$(f + g)' = f' + g', \quad (fg)' = f'g + fg'.$$

Доказателство: Ако $f(x) = \sum_{i=0}^n a_i x^i$ и $g(x) = \sum_{j=0}^m b_j x^j$, то

$$\begin{aligned} f' + g' &= \sum_{i=1}^n i a_i x^{i-1} + \sum_{j=1}^m j b_j x^{j-1} = \sum_{i=1}^{\max(n,m)} i(a_i + b_i) x^{i-1} = \\ &= \left(\sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i \right)' = (f + g)'. \end{aligned}$$

В израза

$$f'g + fg' = \left(\sum_{i=1}^n i a_i x^{i-1} \right) \left(\sum_{j=0}^m b_j x^j \right) + \left(\sum_{i=0}^n a_i x^i \right) \left(\sum_{j=1}^m j b_j x^{j-1} \right)$$

транслираме индексите на сумиране така, че да започват от 0 и извършваме означените умножения. Получаваме

$$\begin{aligned}
f'g + fg' &= \left(\sum_{i=0}^{n-1} (i+1)a_{i+1}x^i \right) \left(\sum_{j=0}^m b_jx^j \right) + \left(\sum_{i=0}^n a_ix^i \right) \left(\sum_{j=0}^{m-1} (j+1)b_{j+1}x^j \right) = \\
&= \sum_{i=0}^{n-1+m} \left(\sum_{p=0}^i (p+1)a_{p+1}b_{i-p} \right) x^i + \sum_{i=0}^{n+m-1} \left(\sum_{q=0}^i (i-q+1)a_qb_{i-q+1} \right) x^i = \\
&= \sum_{i=0}^{n+m-1} \left(\sum_{p=0}^i (p+1)a_{p+1}b_{i-p} + \sum_{q=0}^i (i-q+1)a_qb_{i-q+1} \right) x^i.
\end{aligned}$$

За да извършим сумирането в скобите заменяме индекса на сумиране p с $s = p + 1$. Това дава

$$\begin{aligned}
f'g + fg' &= \sum_{i=0}^{n+m-1} \left(\sum_{s=1}^{i+1} sa_sb_{i+1-s} + \sum_{q=0}^i (i-q+1)a_qb_{i-q+1} \right) x^i = \\
&= \sum_{i=0}^{n+m-1} \left((i+1)a_0b_{i+1} + \sum_{s=1}^i (i+1)a_sb_{i+1-s} + (i+1)a_{i+1}b_0 \right) x^i = \\
&= \sum_{i=0}^{n+m-1} (i+1) \left(\sum_{s=0}^{i+1} a_sb_{i+1-s} \right) x^i.
\end{aligned}$$

След замяна на индекса на сумиране i с $j = i + 1$ пресмятаме, че

$$f'g + fg' = \sum_{j=1}^{n+m} j \left(\sum_{s=0}^j a_sb_{j-s} \right) x^{j-1} = \left(\sum_{j=0}^{n+m} \left(\sum_{s=0}^j a_sb_{j-s} \right) x^j \right)' = (fg)',$$

Q.E.D.

Задача 16. Нека F е поле с произволна характеристика, а $f(x) = x^3 + px + q \in F[x]$. Да се намерят стойностите на $p, q \in F$, за които $f(x)$ се дели на $(x - 1_F)^2$.

Отговор: $f(x) = x^3 - 3x + 2$

Задача 17. Да се намери полиномът $f(x) = x^4 + ax^2 + bx + c \in \mathbb{R}[x]$, ако $f(x)$ има остатък $r(x) = x^2 - x + 1 \in \mathbb{R}[x]$ при деление с $(x - 1)^3 \in \mathbb{R}[x]$.

Отговор: $f(x) = x^4 - 5x^2 + 7x - 2$

Задача 18. Да се намери остатъкът $r(x) \in \mathbb{Z}[x]$ при деление на полинома $f(x) = x^n - 3^{n-1}x + 1 \in \mathbb{Z}[x]$, $n \geq 3$ с полинома $g(x) = x^3 - 3x^2 \in \mathbb{Z}[x]$.

Отговор: $r(x) = 3^{n-2}x^2 - 3^{n-1}x + 1$

ФОРМУЛИ НА ВИЕТ

Задача 19. За кои стойности на параметъра p корените $x_1, \dots, x_4$ на полинома

$$f(x) = x^4 - 8x^3 + 22x^2 + px + 16 \in \mathbb{R}[x]$$

изпълняват равенството $x_1 + x_2 + x_3 = x_4$.

Решение: При наличие на равенството $x_1 + x_2 + x_3 = x_4$, формулите на Виет за $f(x)$ приемат вида

$$8 = (x_1 + x_2 + x_3) + x_4 = 2x_4,$$

$$22 = (x_1 + x_2 + x_3)x_4 + (x_1x_2 + x_2x_3 + x_3x_1) = 16 + (x_1x_2 + x_2x_3 + x_3x_1),$$

$$16 = (x_1x_2x_3)x_4 = 4x_1x_2x_3,$$

$$-p = (x_1x_2 + x_2x_3 + x_3x_1)x_4 + x_1x_2x_3 = 6 \cdot 4 + 4 = 28,$$

откъдето $p = -28$. Следователно $p = -28$ е необходимо условие за $x_1 + x_2 + x_3 = x_4$.

Условието $p = -28$ е достатъчно за $x_1 + x_2 + x_3 = x_4$, защото $x_4 = 4$ е корен на полинома $f(x) = x^4 - 8x^3 + 22x^2 - 28x + 16 \in \mathbb{R}[x]$. Частното при деление на $f(x)$ с $x - 4$ е $g(x) = x^3 - 4x^2 + 6x - 4 \in \mathbb{R}[x]$. По първата формула на Виет за корените x_1, x_2, x_3 на полинома $g(x)$ имаме $x_1 + x_2 + x_3 = 4 = x_4$.

Задача 20. За кои стойности на параметрите p, q полиномът

$$f(x) = x^4 - 8x^3 + px^2 + qx + 8$$

има четири корена $x_1, \dots, x_4$, изпълняващи равенствата

$$5x_1 + 5x_2 = 3x_3 + 3x_4 \quad \text{и} \quad x_1^2x_2^2 = x_3x_4,$$

ако тези корени са :

(а) реални;

(б) комплексни;

Решение: Замествайки с $x_3 + x_4 = \frac{5}{3}(x_1 + x_2)$ и $x_3x_4 = (x_1x_2)^2$ във формулите на Виет получаваме, че

$$\frac{8}{3}(x_1 + x_2) = 8,$$

$$p = (x_1 + x_2)(x_3 + x_4) + x_1x_2 + x_3x_4 = 15 + x_1x_2 + (x_1x_2)^2,$$

$$-q = x_1x_2(x_3 + x_4) + (x_1 + x_2)x_3x_4 = 5x_1x_2 + 3(x_1x_2)^2,$$

$$8 = (x_1 x_2)^3.$$

(а) Ако $x_1, \dots, x_4 \in \mathbb{R}$, то $y = x_1 x_2 \in \mathbb{R}$ и $y = 2$, $p = 21$, $q = -22$.

Непосредствено се проверява, че корените на полинома

$$f(x) = x^4 - 8x^3 + 21x^2 - 22x + 8 = (x^2 - 3x + 2)(x^2 - 5x + 4)$$

изпълняват равенствата $5(x_1 + x_2) = 5.3 = 3(x_3 + x_4)$ и $(x_1 x_2)^2 = 2^2 = 4 = x_3 x_4$.

(б) Ако $x_1, \dots, x_4 \in \mathbb{C}$, то $y = x_1 x_2$ е комплексен корен на полинома $y^3 - 8 = 0$ или $y \in \{2, 2\omega_3, 2\omega_3^2\}$ за $\omega_3 = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Вече видяхме, че ако $y = 2 \in \mathbb{R}$, то $p = 21$, $q = -22$. Оттук нататък ще предполагаме, че комплексното число $y \in \{2\omega_3^i \mid 1 \leq i \leq 2\} = \{-1 + i\sqrt{3}, -1 - i\sqrt{3}\}$. Третите корени ω_3^i , $1 \leq i \leq 2$ на 1, различни от 1 са корените на полинома $\frac{z^3-1}{z-1} = z^2 + z + 1 = 0$. Следователно $y^2 = (2\omega_3^i)^2 = -2(2\omega_3^i) - 4 = -2y - 4$ и

$$p = y^2 + y + 15 = -y + 11, \quad q = -3y^2 - 5y = y + 12.$$

За $y = -1 + i\sqrt{3}$ получаваме $p = 12 - \sqrt{3}i$, $q = 11 + i\sqrt{3}$, а за $y = -1 - i\sqrt{3}$ пресмятаме, че $p = 12 + i\sqrt{3}$, $q = 11 - i\sqrt{3}$.

Непосредствено се проверява, че корените $x_1, \dots, x_4$ на полинома

$$\begin{aligned} f(x) &= x^4 - 8x^3 + (12 - \sqrt{3}i)x^2 + (11 + \sqrt{3}i)x + 8 = \\ &= x^4 - 8x^3 + (11 - 2\omega_3)x^2 + (12 + 2\omega_3)x + 8 = (x^2 - 3x + 2\omega_3)(x^2 - 5x - 4\omega_3 - 4) \end{aligned}$$

изпълняват равенствата

$$5(x_1 + x_2) = 5.3 = 3(x_3 + x_4), \quad (x_1 x_2)^2 = (2\omega_3)^2 = -4\omega_3 - 4 = x_3 x_4,$$

а корените $x_1, \dots, x_4$ на полинома

$$\begin{aligned} f(x) &= x^4 - 8x^3 + (12 + \sqrt{3}i)x^2 + (11 - \sqrt{3}i)x + 8 = \\ &= x^4 - 8x^3 + (13 + 2\omega_3)x^2 + (10 - 2\omega_3)x + 8 = (x^2 - 3x - 2\omega_3 - 2)(x^2 - 5x + 4\omega_3) \end{aligned}$$

изпълняват равенствата

$$5(x_1 + x_2) = 5.3 = 3(x_3 + x_4), \quad (x_1 x_2)^2 = (-2\omega_3 - 2)^2 = 4\omega_3 = x_3 x_4.$$

Окончателно, $(p, q) \in \{(21, -22), (12 + \sqrt{3}i, 11 - \sqrt{3}i), (12 - \sqrt{3}i, 11 + \sqrt{3}i)\}$.

СИМЕТРИЧНИ ПОЛИНОМИ

Задача 21. Да означим с $\sum x_1^{a_1} \dots x_m^{a_m}$ сумата на всички различни мономи, получени от $x_1^{a_1} \dots x_m^{a_m}$ с $a_1 \geq \dots \geq a_m$ чрез пермутация на променливите $x_1, \dots, x_n$, $n \geq m$. Да се представят симетричните полиноми

$$(i) \quad F_1(x_1, x_2, x_3) = \sum x_1^3 x_2^2 - 2 \sum x_1^2 x_2,$$

$$(ii) \quad F_2(x_1, x_2, x_3, x_4) = \sum x_1^3 x_2 x_3,$$

$$(iii) \quad F_3(x_1, x_2, x_3, x_4) = \sum x_1^3 x_2^2 x_3,$$

$$(iv) \quad F_4(x_1, \dots, x_n) = \sum x_1^2 \dots x_{n-1}^2 - 3 \sum x_1^2 \dots x_{n-2}^2 x_{n-1} \quad \text{за } n \geq 4,$$

$$(v) \quad F_5(x_1, \dots, x_n) = \sum x_1^3 x_2 x_3 \quad \text{за } n \geq 5,$$

като полиноми на елементарните симетрични полиноми $\sigma_1, \dots, \sigma_n$ на $x_1, \dots, x_n$

Решение: (i) Да означим с $F_1^{(5)}(x_1, x_2, x_3) = \sum x_1^3 x_2^2$ и $F_1^{(3)}(x_1, x_2, x_3) = \sum x_1^2 x_2$ хомогенните симетрични полиноми, за които

$$F_1(x_1, x_2, x_3) = F_1^{(5)}(x_1, x_2, x_3) - 2F_1^{(3)}(x_1, x_2, x_3).$$

По алгоритъма от основната теорема за симетричните полиноми, старшият член $LT(F_1^{(5)}) = x_1^3 x_2^2$ на $F_1^{(5)}$ отговаря на монома $\sigma_1^{3-2} \sigma_2^{2-0} \sigma_3^0 = \sigma_1 \sigma_2^2$ на елементарните симетрични полиноми $\sigma_1, \sigma_2, \sigma_3$ на x_1, x_2, x_3 . Мономите $x^\beta = x_1^{\beta_1} x_2^{\beta_2} x_3^{\beta_3}$, за които

$$(i) \quad x_1^3 x_2^2 >_{\text{lex}} x_1^{\beta_1} x_2^{\beta_2} x_3^{\beta_3},$$

$$(ii) \quad \beta_1 \geq \beta_2 \geq \beta_3 \quad \text{и}$$

$$(iii) \quad \beta_1 + \beta_2 + \beta_3 = 5$$

са $x_1^3 x_2 x_3$ и $x_1^2 x_2^2 x_3$. Те отговарят на мономите $\sigma_1^2 \sigma_3$ и $\sigma_2 \sigma_3$ на $\sigma_1, \sigma_2, \sigma_3$. Следователно

$$F_1^{(5)} = \sigma_1 \sigma_2^2 + A \sigma_1^2 \sigma_3 + B \sigma_2 \sigma_3$$

за някакви неопределени коефициенти A и B .

При полагането $x_1 = x_2 = 1, x_3 = -1$ имаме $\sigma_1 = 1, \sigma_2 = -1, \sigma_3 = -1$, откъдето $2 = F_1^{(5)}(1, 1, -1) = 1 - A + B$. Ако $x_1 = x_2 = x_3 = 1$, то $\sigma_1 = 3, \sigma_2 = 3, \sigma_3 = 1$ и $6 = F_1^{(5)}(1, 1, 1) = 27 + 9A + 3B$. В резултат, $A = -2, B = -1$ или $F_1^{(5)} = \sigma_1 \sigma_2^2 - 2\sigma_1^2 \sigma_3 - \sigma_2 \sigma_3$.

Старшият член $LT(F_1^{(3)}) = x_1^2 x_2$ на $F_1^{(3)}$ отговаря на монома $\sigma_1 \sigma_2$ на $\sigma_1, \sigma_2, \sigma_3$. Единственият моном $x_1^{\beta_1} x_2^{\beta_2} x_3^{\beta_3} <_{\text{lex}} x_1^2 x_2$ с $\beta_1 \geq \beta_2 \geq \beta_3, \beta_1 + \beta_2 + \beta_3 = 3$ е $x_1 x_2 x_3$, а съответният му моном на $\sigma_1, \sigma_2, \sigma_3$ е σ_3 . Следователно

$$F_1^{(3)} = \sigma_1 \sigma_2 + C \sigma_3$$

за някакъв неопределен коефициент C .

Полагаме $x_1 = x_2 = x_3 = 1$ и пресмятаме, че $\sigma_1 = 3$, $\sigma_2 = 3$, $\sigma_3 = 1$, откъдето $6 = F_1^{(3)}(1, 1, 1) = 9 + C$, т.е. $C = -3$ и $F_1^{(3)} = \sigma_1\sigma_2 - 3\sigma_3$. В резултат,

$$F_1 = \sigma_1\sigma_2^2 - 2\sigma_1^2\sigma_3 - \sigma_2\sigma_3 - 2\sigma_1\sigma_2 + 6\sigma_3.$$

Хомогенните симетрични полиноми $F_1^{(5)} = \sum x_1^3x_2^2$ и $F_1^{(3)} = \sum x_1^2x_2$ могат да се пресметнат и по метода на симетричните суми:

$$\sum x_1^2x_2 = \left(\sum x_1x_2\right) \left(\sum x_1\right) - 3 \left(\sum x_1x_2x_3\right) = \sigma_1\sigma_2 - 3\sigma_3 \quad \text{за } \forall n \geq 3, \quad (6)$$

$$\begin{aligned} F_1^{(5)}(x_1, x_2, x_3) &= \sum x_1^3x_2^2 = \left(\sum x_1^2x_2\right) \left(\sum x_1x_2\right) - 2 \left(\sum x_1^3x_2x_3\right) - 2 \left(\sum x_1^2x_2^2x_3\right) = \\ &= (\sigma_1\sigma_2 - 3\sigma_3) \sigma_2 - 2\sigma_3 \left(\sum x_1^2\right) - 2\sigma_3 \left(\sum x_1x_2\right), \\ \sum x_1^2 &= (x_1)^2 - 2 \left(\sum x_1x_2\right) = \sigma_1^2 - 2\sigma_2 \quad \text{за } \forall n \geq 2. \end{aligned} \quad (7)$$

$$\begin{aligned} (ii) \quad F_2(x_1, x_2, x_3, x_4) &= \sum x_1^3x_2x_3 = \left(\sum x_1x_2x_3\right) \left(\sum x_1^2\right) - \sum x_1^2x_2x_3x_4 = \\ &= \sigma_3(\sigma_1^2 - 2\sigma_2) - \sigma_4\sigma_1. \end{aligned}$$

По втори начин, съгласно основната теорема за симетричните полиноми, старшият член $LT(F_2) = x_1^3x_2x_3$ отговаря на монома $\mu = \sigma_1^2\sigma_3$ на $\sigma_1, \dots, \sigma_4$. Търсим мономите $x_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3}x_4^{\beta_4} <_{\text{lex}} x_1^3x_2x_3$ с $\beta_1 \geq \beta_2 \geq \beta_3 \geq \beta_4$ и $\beta_1 + \beta_2 + \beta_3 + \beta_4 = 5$. Това са $x_1^2x_2^2x_3$ и $x_1^2x_2x_3x_4$, отговарящи съответно на $\sigma_2\sigma_3$ и $\sigma_1\sigma_4$. Следователно хомогенният симетричен полином

$$F_2(x_1, x_2, x_3, x_4) = \sigma_1^2\sigma_3 + A\sigma_2\sigma_3 + B\sigma_1\sigma_4$$

за някакви неопределени коефициенти A и B .

Ако $x_1 = x_2 = x_3 = x_4 = 1$, то $\sigma_1 = 4$, $\sigma_2 = 6$, $\sigma_3 = 4$, $\sigma_4 = 1$ и $12 = F_2(1, 1, 1, 1) = 64 + 24A + 4B$. За $x_1 = x_2 = x_3 = 1$, $x_4 = 0$ получаваме $\sigma_1 = 3$, $\sigma_2 = 3$, $\sigma_3 = 1$, $\sigma_4 = 0$ и $3 = F_2(1, 1, 1, 0) = 9 + 3A$. Следователно $A = -2$ и $B = -1$.

(iii) От

$$\begin{aligned} F_3(x_1, x_2, x_3, x_4) &= \sum x_1^3x_2^2x_3 = \\ &= \left(\sum x_1x_2x_3\right) \left(\sum x_1^2x_2\right) - 3 \left(\sum x_1^3x_2x_3x_4\right) - 2 \sum x_1^2x_2^2x_3x_4 = \\ &= \sigma_3 \left(\sum x_1^2x_2\right) - 3\sigma_4 \left(\sum x_1^2\right) - 2\sigma_4 \left(\sum x_1x_2\right) \quad \text{за } n = 4, \end{aligned}$$

(6) и (7) получаваме, че

$$F_3(x_1, x_2, x_3, x_4) = \sigma_1\sigma_2\sigma_3 - 3\sigma_3^2 - 3\sigma_1^2\sigma_4 + 4\sigma_2\sigma_4.$$

(iv) Съгласно

$$\sum x_1^2 \dots x_{n-1}^2 = \left(\sum x_1 \dots x_{n-1}\right)^2 - 2 \left(\sum x_1^2 \dots x_{n-2}^2 x_{n-1} x_n\right) = \sigma_{n-1}^2 - 2\sigma_{n-2}\sigma_n \quad \text{и}$$

$$\sum x_1^2 \dots x_{n-2}^2 x_{n-1} = \left(\sum x_1 \dots x_{n-2} x_{n-1} \right) \left(\sum x_1 \dots x_{n-2} \right) - \\ - 3 \left(\sum x_1^2 \dots x_{n-3}^2 x_{n-2} x_{n-1} x_n \right) = \sigma_{n-2} \sigma_{n-1} - 3 \sigma_{n-3} \sigma_n \quad \text{за } \forall n \geq 4$$

пресмятаме, че $F_4(x_1, \dots, x_n) = \sigma_{n-1}^2 - 2\sigma_{n-2}\sigma_n - 3\sigma_{n-2}\sigma_{n-1} + 9\sigma_{n-3}\sigma_n$.

По алгоритъма от основната теорема за симетричните полиноми, старшият член $x_1^2 \dots x_{n-1}^2$ на $F_4^{(2n-2)}(x_1, \dots, x_n) = \sum x_1^2 \dots x_{n-1}^2$ отговаря на монома σ_{n-1}^2 на $\sigma_1, \dots, \sigma_n$. Мономите $x^\beta = x_1^{\beta_1} \dots x_n^{\beta_n} <_{\text{lex}} x_1^2 \dots x_{n-1}^2$ с $\beta_1 \geq \beta_2 \geq \dots \geq \beta_n$, $\beta_1 + \dots + \beta_n = 2n - 2$ се изчерпват с $x_1^2 \dots x_{n-2}^2 x_{n-1} x_n$, който съответства на $\sigma_{n-2}\sigma_n$. Затова

$$F_4^{(2n-2)}(x_1, \dots, x_n) = \sigma_{n-1}^2 + A\sigma_{n-2}\sigma_n$$

за някакъв неопределен коефициент A и $\forall n \geq 3$.

При $x_1 = \dots = x_n = 1$ получаваме $\sigma_i = \binom{n}{i}$ за $\forall 1 \leq i \leq n$ и $n = \binom{n}{n-1} = F_4^{(2n-2)}(1, \dots, 1) = n^2 + A \frac{n(n-1)}{2}$, откъдето $A = -2$.

Старшият член $x_1^2 \dots x_{n-2}^2 x_{n-1}$ на $F_4^{(2n-3)}(x_1, \dots, x_n) = \sum x_1^2 \dots x_{n-2}^2 x_{n-1}$ отговаря на монома $\sigma_{n-2}\sigma_{n-1}$ на $\sigma_1, \dots, \sigma_n$. Единственият моном $x_1^{\beta_1} \dots x_n^{\beta_n} <_{\text{lex}} x_1^2 \dots x_{n-2}^2 x_{n-1}$ с $\beta_1 \geq \beta_2 \geq \dots \geq \beta_n$ и $\beta_1 + \dots + \beta_n = 2n - 3$ е $x_1^2 \dots x_{n-3}^2 x_{n-2} x_{n-2} x_n$, съответстващ на $\sigma_{n-3}\sigma_n$. Оттук

$$F_4^{(2n-3)}(x_1, \dots, x_n) = \sigma_{n-2}\sigma_{n-1} + B\sigma_{n-3}\sigma_n.$$

За определяне на неизвестния коефициент B избираме $x_1 = \dots = x_n = 1$ и пресмятаме, че $\sigma_i = \binom{n}{i}$ за $\forall 1 \leq i \leq n$,

$$n(n-1) = (n-1) \binom{n}{n-1} = F_4^{(2n-3)}(1, \dots, 1) = \frac{n^2(n-1)}{2} + B \frac{n(n-1)(n-2)}{6}.$$

В резултат, $B = -3$.

(v) Въз основа на

$$\sum x_1^3 x_2 x_3 = \left(\sum x_1 x_2 x_3 \right) \left(\sum x_1^2 \right) - \left(\sum x_1^2 x_2 x_3 x_4 \right), \\ \sum x_1^2 x_2 x_3 x_4 = \left(\sum x_1 x_2 x_3 x_4 \right) \left(\sum x_1 \right) - 5 \left(\sum x_1 \dots x_5 \right) = \\ = \sigma_1 \sigma_4 - 5 \sigma_5 \quad \text{за } \forall n \geq 5$$

намираме

$$F_5(x_1, \dots, x_n) = \sigma_1^2 \sigma_3 - 2\sigma_2 \sigma_3 - \sigma_1 \sigma_4 + 5\sigma_5.$$

По алгоритъма от основната теорема за симетричните полиноми, $LT(F_5) = x_1^3 x_2 x_3$ отговаря на монома $\sigma_1^2 \sigma_3$ на $\sigma_1, \dots, \sigma_n$. Мономите $x_1^{\beta_1} \dots x_n^{\beta_n} <_{\text{lex}} x_1^3 x_2 x_3$, изпълняващи условията $\beta_1 \geq \beta_2 \geq \dots \geq \beta_n$, $\beta_1 + \dots + \beta_n = 5$ са $x_1^2 x_2^2 x_3$, $x_1^2 x_2 x_3 x_4$ и $x_1 x_2 x_3 x_4 x_5$. Те отговарят съответно на мономите $\sigma_2 \sigma_3$, $\sigma_1 \sigma_4$ и σ_5 на $\sigma_1, \dots, \sigma_n$, така че

$$F_5(x_1, \dots, x_n) = \sigma_1^2 \sigma_3 + A\sigma_2 \sigma_3 + B\sigma_1 \sigma_4 + C\sigma_5$$

за подходящи коефициенти A, B, C .

При полагането $x_1 = x_2 = x_3 = 1$, $x_4 = \dots = x_n = 0$ имаме $\sigma_1 = 3$, $\sigma_2 = 3$, $\sigma_3 = 1$ и $\sigma_i = 0$ за $\forall 4 \leq i \leq n$. В резултат, $3 = F_5(1, 1, 1, 0, \dots, 0) = 9 + 3A$ и $A = -2$. За $x_1 = x_2 = x_3 = x_4 = 1$, $x_5 = \dots = x_n = 0$ пресмятаме, че $\sigma_1 = 4$, $\sigma_2 = 6$, $\sigma_3 = 4$, $\sigma_4 = 1$, $\sigma_i = 0$ за $\forall 5 \leq i \leq n$. От $12 = 4.3 = F_5(1, 1, 1, 1, 0, \dots, 0) = 64 - 48 + 4B$ определяме $B = -1$. Накрая, за $x_1 = x_2 = x_3 = x_4 = x_5 = 1$, $x_6 = \dots = 0$ са в сила $\sigma_1 = 5$, $\sigma_2 = \binom{5}{2} = 10$, $\sigma_3 = \binom{5}{3} = 10$, $\sigma_4 = 5$, $\sigma_5 = 1$, $\sigma_i = 0$ за $\forall 6 \leq i \leq n$ и $30 = 3\binom{5}{3} = F_5(1, 1, 1, 1, 1, 0, \dots, 0) = 250 - 200 - 25 + C$. Следователно $C = 5$.

Задача 22. Нека $f(x) = \prod_{i=1}^n (x - x_i) \in \mathbb{R}[x]$ е полином със старши коефициент 1 и корени $x_1, \dots, x_n$. Да се докаже, че:

$$\frac{f'(x)}{f(x)} = \sum_{i=1}^n \frac{1}{x - x_i} \quad u \quad \left(\frac{f'(x)}{f(x)} \right)' = - \sum_{i=1}^n \frac{1}{(x - x_i)^2}.$$

Задача 23. Нека x_1, x_2 и x_3 са корените на полинома

$$f(x) = x^3 + px^2 + qx + r.$$

Да се изразят чрез p и q (когато има смисъл) симетричните рационални функции

$$\begin{aligned} (i) \quad \Sigma_1(x_1, x_2, x_3) &= (x_1^2 - x_2x_3)(x_2^2 - x_3x_1)(x_3^2 - x_1x_2); \\ (ii) \quad \Sigma_2(x_1, x_2, x_3) &= \frac{x_1x_2}{(x_2 + x_3 - x_1)(x_1 + x_3 - x_2)} + \\ &+ \frac{x_2x_3}{(x_1 + x_3 - x_2)(x_1 + x_2 - x_3)} + \frac{x_3x_1}{(x_1 + x_2 - x_3)(x_2 + x_3 - x_1)}; \\ (iii) \quad \Sigma_3(x_1, x_2, x_3) &= \frac{x_1^2 + 2}{x_2 + x_3} + \frac{x_2^2 + 2}{x_1 + x_3} + \frac{x_3^2 + 2}{x_1 + x_2}. \end{aligned}$$

Отговор:

$$\begin{aligned} (i) \quad \Sigma_1(x_1, x_2, x_3) &= p^3r - q^3; \\ (ii) \quad \Sigma_2 &= \frac{6r - pq}{p^3 - 4pq + 8r}; \\ (iii) \quad \Sigma_3(x_1, x_2, x_3) &= \frac{p^4 - 3p^2q + 4pr + 2p^2 + 2q}{r - pq}. \end{aligned}$$

Задача 24. Нека x_1, x_2, x_3 са корените на полинома

$$f(x) = x^3 + px + q.$$

Да се изразят чрез p и q (когато има смисъл) симетричните рационални функции

$$\begin{aligned} (i) \quad \Sigma_1(x_1, x_2, x_3) &= \frac{x_1^2}{(1 + x_2)(1 + x_3)} + \frac{x_2^2}{(1 + x_3)(1 + x_1)} + \frac{x_3^2}{(1 + x_1)(1 + x_2)}; \\ (ii) \quad \Sigma_2(x_1, x_2, x_3) &= \frac{x_3}{x_1^2 + 4x_1x_2 + x_2^2} + \frac{x_2}{x_1^2 + 4x_1x_3 + x_3^2} + \frac{x_1}{x_2^2 + 4x_2x_3 + x_3^2}; \\ (iii) \quad \Sigma_3(x_1, x_2, x_3) &= \frac{x_1}{(1 + x_1)^2} + \frac{x_2}{(1 + x_2)^2} + \frac{x_3}{(1 + x_3)^2} \\ (iv) \quad \Sigma_4(x_1, x_2, x_3) &= \frac{x_1^2}{(1 + x_1)^2} + \frac{x_2^2}{(1 + x_2)^2} + \frac{x_3^2}{(1 + x_3)^2} \end{aligned}$$

Отговор:

$$\begin{aligned}
 (i) \quad \Sigma_1(x_1, x_2, x_3) &= \frac{-2p - 3q}{p - q + 1}; \\
 (ii) \quad \Sigma_2(x_1, x_2, x_3) &= \frac{9pq}{2p^3 + 27q^2}; \\
 (iii) \quad \Sigma_3(x_1, x_2, x_3) &= \frac{4p - 9q - pq}{(q - p - 1)^2}; \\
 (iv) \quad \Sigma_4(x_1, x_2, x_3) &= \frac{2p^2 - 4pq + 3q^2 - 2p + 6q}{(q - p - 1)^2}.
 \end{aligned}$$

ЦИКЛОТОМИЧНИ ПОЛИНОМИ И КРАЙНИ ПОЛЕТА

Определение 25. За произволно естествено число n полиномът

$$\Phi_n(x) = \prod_{k \in \mathbb{Z}_n^*} \left(x - \cos\left(\frac{2k\pi}{n}\right) - i \sin\left(\frac{2k\pi}{n}\right) \right),$$

чиито корени са елементите на $\mathbb{C}^*$ от ред n се нарича n -ти циклотомичен полином.

Задача 26. Да се намерят циклотомичните полиноми:

$$(i) \quad \Phi_p(x) \text{ за просто число } p; \quad (ii) \quad \Phi_4(x); \quad (iii) \quad \Phi_8(x); \quad (iv) \quad \Phi_{15}(x).$$

$$\begin{aligned}
 \text{Отговор: } (i) \quad \Phi_p(x) &= x^{p-1} + x^{p-2} + \dots + x^2 + x + 1; & (ii) \quad \Phi_4(x) &= x^2 + 1; \\
 (iii) \quad \Phi_8(x) &= x^4 + 1; & (iv) \quad \Phi_{15}(x) &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.
 \end{aligned}$$

Задача 27. Нека p е просто число, $n \in \mathbb{N}$, α е пораждащ на мултипликативната група $\mathbb{F}_{p^n} \simeq (\mathbb{Z}_{p^n-1}, +)$ на полето $\mathbb{F}_{p^n}$ с p^n елемента, а

$$\Pi_p : \mathbb{Z}[x] \rightarrow \mathbb{F}_p[x] = \mathbb{Z}_p[x],$$

$$\Pi_p \left(\sum_{i=0}^n a_i x^i \right) = \sum_{i=0}^n (a_i + p\mathbb{Z}) x^i$$

е редукцията по модул p . Да се докаже, че α е корен на полинома $\Pi_p(\Phi_{p^n-1}(x)) \in \mathbb{Z}_p[x]$.

Упътване: Използвайте, че

$$\Pi_p(\Phi_{p^n-1}(x)) = \frac{\Pi_p(x^{p^n-1} - 1)}{\prod_{d/p^n-1, d < p^n-1} \Pi_p(\Phi_d(x))}.$$

Задача 28. Да се докаже, че полиномите

$$f(x) = x^2 + x - 1 \in \mathbb{Z}_3[x] \quad \text{и} \quad g(x) = x^2 - x - 1 \in \mathbb{Z}_3[x]$$

са неразложими над $\mathbb{Z}_3$ и произволен пораждащ α на мултипликативната група $\mathbb{F}_9^*$ на полето $\mathbb{F}_9$ е корен на точно един от тях.

Упътване: Проверете, че $\Pi_3(\Phi_8(x)) = f(x)g(x)$.

Задача 29. Да се докаже, че полиномите

$$f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x] \quad \text{и} \quad g(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$$

са неразложими над $\mathbb{Z}_2$ и произволен пораждащ α на мултипликативната група $\mathbb{F}_8^*$ на полето $\mathbb{F}_8$ е корен на точно един от тях.