Примерни задачи по Висша Алгебра 2, специалност Математика, II курс, 2013-2014 уч. г.

1 Идеали в комутативен пръстен. Китайска теорема за остатъците.

Лема 1. *Да се докаже, че ако I_α са идеали в пръстен R за всички $\alpha \in A$, то сечението $\cap_{\alpha\in A} I_\alpha$ е идеал в R.*

Доказателство: Ако $a, b \in I_\alpha$ за $\forall \alpha \in A$, то $a-b \in (I_\alpha, +) \leq (R, +)$ и $xa, ax \in I_\alpha \triangleleft R$ за $\forall \alpha \in A$ и произволен елемент $x \in R$.. Следователно $\cap_{\alpha\in A} I_\alpha$ е идеал в R.

Лема 2. *Ако I и J са идеали в пръстен R, то множеството*

$$I + J = \{\alpha + \beta \quad | \quad \alpha \in I, \quad \beta \in J\}$$

се нарича сума на I и J. Сумата $I + J$ на идеали I и J в пръстен R е идеал в R.

Доказателство: Ако $i_1 + j_1, i_2 + j_2 \in I + J$ с $i_s \in I$, $j_s \in J$, то

$$(i_1 + j_1) - (i_2 - j_2) = (i_1 - i_2) + (j_1 - j_2) \in I + J,$$

защото $i_1 - i_2 \in (I, +) \leq (R, +)$ и $j_1 - j_2 \in (J, +) \leq (R, +)$. За произволен елемент $x \in R$ имаме

$$x(i_1 + j_1) = xi_1 + xj_1 \in I + J, \quad (i_1 + j_1)x = i_1x + j_1x \in I + J,$$

съгласно $xi_1, i_1x \in I \triangleleft R$, $xj_1, j_1x \in J \triangleleft R$. Това доказва, че $I + J$ е идеал в R.

Лема 3. *Ако I и J са идеали в пръстен R, то множеството*

$$IJ = \left\{ \sum_{i=1}^{n} \alpha_i\beta_i \quad \Big| \quad \alpha_i \in I, \quad \beta_i \in J \right\}$$

се нарича произведение на идеалите I и J. Произведението IJ на идеали I и J в пръстен R е идеал в R.

Доказателство: Нека $\lambda = \sum\limits_{i=1}^{m} \alpha_i\beta_i, \lambda' = \sum\limits_{j=1}^{n} \alpha'_j\beta'_j \in IJ$ с $\alpha_i, \alpha'_j \in I$, $\beta_i, \beta'_j \in J$. Тогава $\lambda - \lambda' = \sum\limits_{i=1}^{m} \alpha_i\beta_i + \sum\limits_{j=1}^{n} (-\alpha'_j)\beta'_j \in IJ$, защото $-\alpha'_j \in (I, +) \leq (R, +)$. За произволен елемент $x \in R$ имаме $x\lambda = \sum\limits_{i=1}^{m} (x\alpha_i)\beta_i \in IJ$ с $x\alpha \in I \triangleleft R$ и $\lambda x = \sum\limits_{i=1}^{n} \alpha_i(\beta_i x) \in IJ$ с $\beta_i x \in J \triangleleft R$. Това доказва, че IJ е идеал в R.

Задача 4. *За произволни естествени числа $m, n \in \mathbb{Z}$ с най-голям общ делител $d = (m, n)$ и най-малко общо кратно $\mu = [m, n]$ е в сила:*

(i) $(m\mathbb{Z})(n\mathbb{Z}) = mn\mathbb{Z}$;

(ii) $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$;

(iii) $m\mathbb{Z} \cap n\mathbb{Z} = \mu\mathbb{Z}$.

Решение: (i) По определение,

$$(m\mathbb{Z})(n\mathbb{Z}) = \left\{ \sum_{i=1}^{k} (mx_i)(ny_i) = mn \left(\sum_{i=1}^{k} x_i y_i \right) \;\middle|\; k \in \mathbb{N}, \;\; x_i, y_i \in \mathbb{Z} \right\} \subseteq mn\mathbb{Z}.$$

Обратно, за $\forall z \in \mathbb{Z}$ имаме $mnz = (m.1)(n.z) \in (m\mathbb{Z})(n\mathbb{Z})$, така че $mn\mathbb{Z} \subseteq (m\mathbb{Z})(n\mathbb{Z})$ и $(m\mathbb{Z})(n\mathbb{Z}) = mn\mathbb{Z}$.

(ii) От една страна, $m, n \in d\mathbb{Z}$, защото d дели m и n. Идеалът $d\mathbb{Z}$ е затворен относно умножение с цели числа, така че $m\mathbb{Z} \subseteq d\mathbb{Z}$ и $n\mathbb{Z} \subseteq d\mathbb{Z}$. Следователно $m\mathbb{Z} + n\mathbb{Z} \subseteq d\mathbb{Z}$, защото $(d\mathbb{Z}, +)$ е подгрупа на $(\mathbb{Z}, +)$. За обратното включване $d\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$ използваме тъждеството на Безу $d = mu + nv$ с цели $u, v \in \mathbb{Z}$. По-точно, от $mu \in m\mathbb{Z}$ и $nv \in n\mathbb{Z}$ следва $d = mu + nv \in m\mathbb{Z} + n\mathbb{Z}$. Сумата $m\mathbb{Z} + n\mathbb{Z}$ на идеалите $m\mathbb{Z}$, $n\mathbb{Z}$ е идеал в $\mathbb{Z}$, така че $d\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$ и $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$.

(iii) Ако $\alpha \in m\mathbb{Z} \cap n\mathbb{Z}$, то m и n делят α, така че α е общо кратно на m и n. Оттук, най-малкото общо кратно μ на m и n дели α и $\alpha \in \mu\mathbb{Z}$. Това доказва включването $m\mathbb{Z} \cap n\mathbb{Z} \subseteq \mu\mathbb{Z}$. Обратно, общото кратно μ на m и n се дели както на m, така и на n. Следователно $\mu \in m\mathbb{Z}$ и $\mu \in n\mathbb{Z}$, откъдето $\mu \in m\mathbb{Z} \cap n\mathbb{Z}$. Сечението $m\mathbb{Z} \cap n\mathbb{Z}$ на идеалите $m\mathbb{Z}$ и $n\mathbb{Z}$ е идеал в $\mathbb{Z}$, така че $\mu\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$ и $\mu\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$.

Задача 5. *Идеалите $I_1, \ldots, I_n$ в комутативен пръстен с единица R са взаимно прости, ако $I_a + I_b = R$ за всички $a \neq b$. Да се докаже, че идеалите $m_1\mathbb{Z}, \ldots, m_n\mathbb{Z}$ в пръстена $\mathbb{Z}$ на целите числа са взаимно прости тогава и само тогава, когато числата m_a и m_b са взаимно прости за всички $a \neq b$.*

Теорема 6. (Китайска теорема за остатъците) *Нека $I_1, \ldots, I_n$ са два по два взаимно прости идеала в комутативен пръстен с единица R и $c_1, \ldots, c_n \in R$. Тогава съществува елемент $c \in R$, така че $c + I_j = c_j + I_j$ за $\forall 1 \leq j \leq n$.*

Доказателство: С индукция по $n \geq 2$, ако $I_1 + I_2 = R$, то съществуват $\alpha_1 \in I_1$ и $\alpha_2 \in I_2$ с $\alpha_1 + \alpha_2 = 1_R$. Непосредствено се проверява, че

$$c = c_1\alpha_2 + c_2\alpha_1 \in R$$

изпълнява условията $c + I_j = c_j + I_j$ за $\forall 1 \leq j \leq 2$.

В общия случай, от $I_1 + I_j = R$ за $\forall 2 \leq j \leq n$ следва съществуването на $\alpha_j \in I_1$ и $\beta_j \in I_j$ с $\alpha_j + \beta_j = 1_R$ за $\forall 2 \leq j \leq n$. Почленното умножение на тези равенства дава

$$1_R = (\alpha_2 + \beta_2)(\alpha_3 + \beta_3) \ldots (\alpha_n + \beta_n) = \alpha + \beta_2 \ldots \beta_n \in I_1 + I_2 \ldots I_n,$$

където $\alpha \in I_1$ е сумата на онези произведения, в които участва поне един множител $\alpha_j \in I_1$. Оттук $I_1 + I_2 \ldots I_n = R$. По индукционно предположение съществува $c' \in R$ с $c' + I_j = c_j + I_j$ за $\forall 2 \leq j \leq n$. Сега

$$c = c_1\beta_2 \ldots \beta_n + c'\alpha \in R$$

изпълнява равенствата $c + I_1 = c_1 + I_1$ и $c + I_2 \dots I_n = c' + I_2 \dots I_n$ за $\forall 2 \leq j \leq n$, откъдето и $c + I_j = c' + I_j = c_j + I_j$, съгласно $I_2 \dots I_n \subseteq I_j$ за $\forall 2 \leq j \leq n$, Q.E.D.

Следствие 7. *Ако R е комутативен пръстен с единица 1_R, а $I_1, \dots, I_n$ са два по два взаимно прости идеала в R, то произведението им*

$$I_1 \dots I_n = I_1 \cap \dots \cap I_n$$

съвпада със сечението.

Доказателство: За произволни идеали I_j в пръстен R имаме $I_1 \dots I_n \subseteq I_1 \cap \dots \cap I_n$. С индукция по $n \geq 2$ ще проверим, че ако $I_1, \dots, I_n$ са два по два взаимно прости идеала в комутативен пръстен с единица R, то

$$I_1 \cap \dots \cap I_n \subseteq I_1 \dots I_n,$$

откъдето $I_1 \cap \dots \cap I_n = I_1 \dots I_n$.

Наистина, от $I_1 + I_2 = R$ следва съществуването на $\alpha_1 \in I_1$ и $\alpha_2 \in I_2$ с $\alpha_1 + \alpha_2 = 1_R$. Оттук, за произволен елемент $\gamma \in I_1 \cap I_2$ имаме

$$\gamma = \gamma.1_R = \alpha_1\gamma + \gamma\alpha_2 \in I_1 I_2,$$

съгласно $\alpha_1 \in I_1$, $\gamma \in I_2$ и $\gamma \in I_1$, $\alpha_2 \in I_2$.

В общия случай, доказахме че ако $I_1, \dots, I_n$ са два по два взаимно прости идеала, то I_1 и произведението $I_2 \dots I_n$ на останалите идеали са взаимно прости, $I_1 + I_2 \dots I_n = R$. Оттук съществуват $\alpha_1 \in I_1$ и $\beta \in I_2 \dots I_n = I_2 \cap \dots \cap I_n$ с $\alpha_1 + \beta = 1_R$. За произволен елемент $\gamma \in I_1 \cap I_2 \cap \dots \cap I_n = I_1 \cap (I_2 \dots I_n)$ имаме

$$\gamma = \gamma.1_R = \alpha_1\gamma + \gamma\beta \in I_1(I_2 \dots I_n),$$

съгласно $\alpha_1 \in I_1$, $\gamma \in I_2 \dots I_n$ и $\gamma \in I_1$, $\beta \in I_2 \dots I_n$. Оттук следва включването

$$I_1 \cap \dots \cap I_n \subseteq I_1 \dots I_n$$

и съвпадението $I_1 \cap \dots \cap I_n = I_1 \dots I_n$, Q.E.D.

Теорема 8. *(i) Ако $a \in \mathbb{Z} \setminus \{0\}$ и $n \in \mathbb{N} \setminus \{1\}$ са взаимно прости, то сравнението $ax \equiv b (\mathrm{mod}\, n)$ има единствено решение $x \equiv x_0 (\mathrm{mod}\, n)$ за някое $0 \leq x_0 \leq n-1$.*

(ii) Ако най-големият общ делител $d = (a, n) \in \mathbb{N} \setminus \{1\}$ на $a \in \mathbb{Z} \setminus \{0\}$ и $n \in \mathbb{N} \setminus \{1\}$ не дели $b \in \mathbb{Z}$, то сравнението $ax \equiv b (\mathrm{mod}\, n)$ няма решение.

(iii) Ако най-големият общ делител $d = (a, n) \in \mathbb{N} \setminus \{1\}$ на $a \in \mathbb{Z} \setminus \{0\}$ и $n \in \mathbb{N} \setminus \{1\}$ дели $b \in \mathbb{Z}$, то сравнението $ax \equiv b (\mathrm{mod}\, n)$ има d решения

$$x_i \equiv x_0 + i\frac{n}{d} (\mathrm{mod}\ \ n), \quad 0 \leq i \leq d-1,$$

където $x_0 \left(\mathrm{mod}\, \frac{n}{d}\right)$ е единственото решение на редуцираното сравнение

$$\left(\frac{a}{d}\right) x \equiv \left(\frac{b}{d}\right) \left(\mathrm{mod}\, \frac{n}{d}\right)$$

с $\frac{a}{d} \in \mathbb{Z}$, $\frac{n}{d} \in \mathbb{N}$, $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$.

Доказателство: (i) По Тъждеството на Безу съществуват $u, v \in \mathbb{Z}$, така че

$$au + nv = 1.$$

След почленно умножение с b получаваме $abu+bnv = b$. Тогава $x \equiv bu(\mathrm{mod}\, n)$ е решение на $ax \equiv b(\mathrm{mod}\, n)$.

Произволно решение $x_1(\mathrm{mod}\, n)$ на $ax \equiv b(\mathrm{mod}\, n)$ дава решение $x_1 - bu(\mathrm{mod}\, n)$ на хомогенното линейно сравнение $ax \equiv 0(\mathrm{mod}\, n)$. Съгласно взаимната простота на a и n, от равенството $a(x_1 - bu) = nz$ за някое $z \in \mathbb{Z}$ следва, че n дели $x_1 - bu$ или $x_1 \equiv bu(\mathrm{mod}\, n)$. С други думи, $bu(\mathrm{mod}\, n)$ е единственото решение на $ax \equiv b(\mathrm{mod}\, n)$.

(ii) Ако съществува $x_0 \in \mathbb{Z}$ с $ax_0 \equiv b(\mathrm{mod}\, n)$, то $ax_0 - b = ny_0$ за някое $y_0 \in \mathbb{Z}$. Затова $d = (a, n)$ трябва да дели $b = ax_0 - ny_0$.

(iii) Ако

$$\frac{a}{d}x_0 - \frac{b}{d} = \frac{n}{d}y_0$$

за някои $x_0, y_0 \in \mathbb{Z}$, то за всяко $0 \leq i \leq d-1$ е в сила

$$a\left(x_0 + i\frac{n}{d}\right) = b + ny_0 + ai\frac{n}{d} \equiv b(\mathrm{mod}\, n)$$

и

$$x_i \equiv x_0 + i\frac{n}{d}\left(\mathrm{mod}\, \frac{n}{d}\right)$$

са решения на сравнението $ax \equiv b(\mathrm{mod}\, n)$. Тези решения са различни, защото n не дели $(i-j)\frac{n}{d}$ за $\forall 0 \leq i < j \leq d-1$.

Обратно, ако $ax_1 - b = ny_1$ за някои $x_1, y_1 \in \mathbb{Z}$, то

$$\left(\frac{a}{d}\right)x_1 - \frac{b}{d} = \frac{n}{d}y_1$$

и $x_1 \left(\mathrm{mod}\, \frac{n}{d}\right) \equiv x_0 \left(\mathrm{mod}\, \frac{n}{d}\right)$ е единственото решение на сравнението $\left(\frac{a}{d}\right) x \equiv \left(\frac{b}{d}\right) \left(\mathrm{mod}\, \frac{n}{d}\right)$. Условието

$$x_1 \equiv x_0 \left(\mathrm{mod}\, \frac{n}{d}\right)$$

е еквивалентно на $x_1 - x_0 = \frac{n}{d}z$ за някое $z \in \mathbb{Z}$ и остатъкът на $\frac{n}{d}z$ при деление с n зависи точно от остатъка на z при деление с d. По този начин,

$$x_1 \equiv x_0 + \frac{n}{d}z(\mathrm{mod}\, n) \quad \text{за някое} \quad 0 \leq z \leq d-1.$$

Задача 9. *Да се решат сравненията*

(i) $2x \equiv 3(\mathrm{mod}\, 5)$*;*

(ii) $2x \equiv 1(\mathrm{mod}\, 4)$*;*

(iii) $6x \equiv 3(\mathrm{mod}\, 9)$*;*

(iv) $11x \equiv 7(\mathrm{mod}\, 15)$.

Решение: (i) По метода на Ойлер, остатъкът $x(\mathrm{mod}\, 5)$ е решение на $2x \equiv 3(\mathrm{mod}\, 5)$ точно когато съществува $y \in \mathbb{Z}$, така че $2x - 3 = 5y$. Коефициентът 2 на неизвестното x е по-малък по модул от коефициента 5 на неизвестното y и затова представяме уравнението във вида

$$x = \frac{5y+3}{2} = 2y + 1 + \frac{y+1}{2}. \tag{1}$$

Оттук 2 дели $y+1$ или $y=2z-1$ за $z\in\mathbb{Z}$ е нечетно цяло число. Заместваики в (1) получаваме $x=5z-1$ или $2x\equiv 3(\mathrm{mod}\,5)$ има единствено решение $x\equiv -1(\mathrm{mod}\,5)$.

(ii) Сравнението $2x\equiv 1(\mathrm{mod}\,4)$ е еквивалентно на уравнението $2x-1=4y$ с две неизвестни x и y, което се свежда до $1=2x-4y=2(x-2y)$ и няма решение в цели числа.

(iii) Сравнението $6x\equiv 3(\mathrm{mod}\,9)$ има три решения, защото коефициентът 6 на неизвестния остатък $x(\mathrm{mod}\,9)$ и модулът 9 имат най-голям общ делител $(6,9)=3$, който дели свободния член 3. Решаваното сравнение се свежда до уравнението $6x-3=9y$. След съкращаване на 3 получаваме $2x-1=3y$ или

$$x=\frac{3y+1}{2}=y+\frac{y+1}{2}. \tag{2}$$

Оттук $y+1$ е четно или $y=2z-1$ е нечетно. Заместваики в (2) получаваме $x=3z-1$ или

$$x\equiv -1+k\frac{9}{3}=3k-1(\mathrm{mod}\,9)\quad \text{за}\quad 0\leq k\leq 2.$$

С други думи, решенията на сравнението $6x\equiv 3(\mathrm{mod}\,9)$ са

$$x_1\equiv -1(\mathrm{mod}\,9),\quad x_2\equiv 2(\mathrm{mod}\,9)\quad \text{и}\quad x_3\equiv 5(\mathrm{mod}\,9).$$

(iv) Ако $11x-7=15y$ за цяло число y, то

$$x=\frac{15y+7}{11}=y+1+\frac{4y-4}{11}.$$

Полагаме

$$z:=\frac{4y-4}{11}$$

и изразяваме

$$y=\frac{11z+4}{4}=3z+1-\frac{z}{4}.$$

Въвеждаме

$$t:=\frac{z}{4}\in\mathbb{Z},$$

и получаваме $z=4t$, $y=11t+1$, $x=15t+2$. Следователно единственото решение на сравнението $11x\equiv 7(\mathrm{mod}\,15)$ е $x\equiv 2(\mathrm{mod}\,15)$.

Алгоритъм за решаване на системи линейни сравнения с едно неизвестно

(i) Нека m и n са взаимно прости естествени числа. За да решим системата сравнения

$$\left|\begin{array}{rcll} ax & \equiv & b & (\mathrm{mod}\,m)\\ cx & \equiv & d & (\mathrm{mod}\,n)\end{array}\right.,$$

започваме с решаване на всяко от сравненията поотделно. Ако някое от сравненията $ax\equiv b(\mathrm{mod}\,m)$ или $cx\equiv d(\mathrm{mod}\,n)$ няма решение, то и системата няма решение. Да предположим, че всяко от тези сравнения има решение. Тогава най-големият общ делител $\delta=(a,m)$ на a и m дели b и най-големият общ делител $\Delta=(c,n)$ на c и n дели d. Съществуват цели числа $x_o,y_o\in\mathbb{Z}$, така че $x_o+i\frac{m}{\delta}(\mathrm{mod}\,m)$ за $1\leq i\leq\delta$ са решенията на сравнението $ax\equiv b(\mathrm{mod}\,m)$, а $y_o+j\frac{n}{\Delta}(\mathrm{mod}\,n)$, $1\leq j\leq\Delta$ са решенията

на сравнението $cx \equiv d (\mathrm{mod}\, n)$. Първоначалната система сравнения има $\delta\Delta$ решения и всяко от тях е решение на система сравнения от вида

$$\left| \begin{array}{rcll} x & \equiv & x_o + i\frac{m}{\delta} & (\mathrm{mod}\, m) \\ x & \equiv & y_o + j\frac{n}{\Delta} & (\mathrm{mod}\, n) \end{array} \right. \tag{3}$$

за някои $1 \leq i \leq \delta$ и $1 \leq j \leq \Delta$. По тъждеството на Безу за взаимно простите естествени числа m и n съществуват $u, v \in \mathbb{Z}$, така че $mu + nv = 1$. Съгласно Теорема 6 - Китайска теорема за остатъците, цялото число

$$c = \left(x_o + i\frac{m}{\delta}\right) nv + \left(y_o + j\frac{n}{\Delta}\right) mu$$

изпълнява системата сравнения

$$\left| \begin{array}{rcll} c & \equiv & x_o + i\frac{m}{\delta} & (\mathrm{mod}\, m) \\ c & \equiv & y_o + j\frac{n}{\Delta} & (\mathrm{mod}\, n) \end{array} \right.$$

и е решение на (3). Обратно, всяко решение $x \in \mathbb{Z}$ на (3) изпълнява системата сравнения

$$\left| \begin{array}{rcll} x & \equiv & c & (\mathrm{mod}\, m) \\ x & \equiv & c & (\mathrm{mod}\, n) \end{array} \right. .$$

С други думи, $x - c \in \langle m \rangle \cap \langle n \rangle$ за идеалите $\langle m \rangle \lhd \mathbb{Z}$, $\langle n \rangle \lhd \mathbb{Z}$, породени съответно от m и n. Съгласно Задача 5, идеалите $\langle m \rangle$ и $\langle n \rangle$ са взаимно прости. Следователно $\langle m \rangle \cap \langle n \rangle = \langle m \rangle \langle n \rangle = \langle mn \rangle$ по Следствие 7. Оттук, $x \in \mathbb{Z}$ е решение на (3) тогава и само тогава, когато $x - c \in \langle mn \rangle$. С други думи, решенията на (3) образуват класа от остатъци $c + mn\mathbb{Z} \in \mathbb{Z}_{mn}$ при деление с mn.

(ii) Нека $m_1, \ldots, m_n \in \mathbb{N} \setminus \{1\}$ са две по две взаимно прости естествени числа, $a_j, b_j \in \mathbb{Z}$ за $1 \leq j \leq n$. За да решим системата сравнения

$$\left| \begin{array}{rcll} a_1 x & \equiv & b_1 & (\mathrm{mod}\, m_1) \\ \ldots & \ldots & \ldots & \ldots \\ a_n x & \equiv & b_n & (\mathrm{mod}\, m_n) \end{array} \right.$$

започваме с намиране на решенията $c_{ij} + m_1 m_2 \mathbb{Z} \in \mathbb{Z}_{m_1 m_2}$, $1 \leq i \leq (a_1, m_1)$, $1 \leq j \leq (a_2, m_2)$ на

$$\left| \begin{array}{rcll} a_1 x & \equiv & b_1 & (\mathrm{mod}\, m_1) \\ a_2 x & \equiv & b_2 & (\mathrm{mod}\, m_2) \end{array} \right. .$$

Това свежда първоначалната система от n сравнения спрямо два по два взаимно прости модула $m_1, m_2, \ldots, m_n$ към $(a_1, m_1)(a_2, m_2)$ системи сраднения

$$\left| \begin{array}{rcll} x & \equiv & c_{ij} & (\mathrm{mod}\, m_1 m_2) \\ a_3 x & \equiv & b_3 & (\mathrm{mod}\, m_3) \\ \ldots & \ldots & \ldots & \ldots \\ a_n x & \equiv & b_n & (\mathrm{mod}\, m_n) \end{array} \right.$$

от $n - 1$ сравнения спрямо два по два взаимно прости модула $m_1 m_2, m_3, \ldots, m_n$. С индукция по n решаваме тези системи сравнения, обединяваме решенията им и получаваме решенията на първоначалната система сравнения.

Задача 10. *Да се намерят всички цели решения на системите сравнения*

$$(i)\left|\begin{array}{lll} 2x & \equiv -1 & (\mathrm{mod}\,3) \\ 3x & \equiv -1 & (\mathrm{mod}\,5) \end{array}\right. ;(ii)\left|\begin{array}{lll} 5x & \equiv 1 & (\mathrm{mod}\,6) \\ 5x & \equiv 6 & (\mathrm{mod}\,7) \end{array}\right. ;(iii)\left|\begin{array}{lll} 2x & \equiv 1 & (\mathrm{mod}\,3) \\ 3x & \equiv 4 & (\mathrm{mod}\,5) \\ 5x & \equiv -2 & (\mathrm{mod}\,7) \end{array}\right. .$$

Решение: (i) Първо решаваме всяко от сравненията в системата. От $2x-(-1)=3y_1$ с $y_1 \in \mathbb{Z}$ изразяваме

$$x = \frac{3y_1-1}{2} = y_1 + \frac{y_1-1}{2}.$$

Полагаме

$$z_1 := \frac{y_1-1}{2} \in \mathbb{Z}$$

и получаваме $y_1 = 2z_1+1$, $x = 3z_1+1$. Следователно $2x \equiv -1(\mathrm{mod}\,3)$ има единствено решение $x \equiv 1(\mathrm{mod}\,3)$. Аналогично, представяме $3x+1=5y_2$ с $y_2 \in \mathbb{Z}$ във вида

$$x = \frac{5y_2-1}{3} = 2y_2 + \frac{(-y_2-1)}{3}.$$

Ако

$$z_2 := \frac{-y_2-1}{3} \in \mathbb{Z},$$

то $y_2 = -3z_2-1$ и $x = -5z_2-2$. Оттук $3x \equiv -1(\mathrm{mod}\,5)$ има решение $x \equiv -2(\mathrm{mod}\,5)$. С това сведохме системата сравнения (i) към системата

$$\left|\begin{array}{lll} x & \equiv 1 & (\mathrm{mod}\,3) \\ x & \equiv -2 & (\mathrm{mod}\,5) \end{array}\right. . \tag{4}$$

За да намерим едно решение $c \in \mathbb{Z}$ на тази система ще използваме доказателството на Китайската теорема за остатъците. По-точно, съгласно $1 = 6+(-5)$ с $6 \in 3\mathbb{Z}$, $(-5) \in 5\mathbb{Z}$, цялото число $c = 6(-2)+(-5).1 = -17$ е решение на (4). Съгласно взаимната простота на 3 и 5, всички решения на (i) са $-17+15\mathbb{Z} = 13+15\mathbb{Z}$.

Втори начин за решаване на (4) е чрез заместване на решението $x = 3y+1$, $y \in \mathbb{Z}$ на първото сравнение на системата във второто сравнение. Това дава $3y+1 = 5z-2$, откъдето

$$y = 2z-1-\frac{z}{3} \in \mathbb{Z}$$

за някои $y, z \in \mathbb{Z}$. В резултат, $z = 3t$ за някое цяло $t \in \mathbb{Z}$, откъдето $y = 5t-1$ и $x = 15t-2$. С други думи, решенията на системата са целите числа с остатък -2 или 13 при деление на 15.

(ii) Решаваме поотделно дадените сравнения и свеждаме системата (ii) към

$$\left|\begin{array}{lll} x & \equiv 5 & (\mathrm{mod}\,6) \\ x & \equiv 4 & (\mathrm{mod}\,7) \end{array}\right. . \tag{5}$$

Съгласно $1 = 7+(-6)$ с $7 \in 7\mathbb{Z}$, $(-6) \in 6\mathbb{Z}$, цялото число $c = 7.5+(-6).4 = 11$ е решение на системата (5). Понеже 6 и 7 са взаимно прости естествени числа, всички решения на (ii) образуват съседния клас $11+42\mathbb{Z} \in \mathbb{Z}_{42}$.

Можем да решим (5) пряко чрез полагане на $x = 6y + 5$ за някое $y \in \mathbb{Z}$ от първото сравнение. Заместването във второто сравнение дава $6y + 5 = 7z + 4$ за някое $z \in \mathbb{Z}$. Сега

$$y = z + \frac{z-1}{6} \in \mathbb{Z}$$

изисква $t := \frac{z-1}{6} \in \mathbb{Z}$. Следователно $z = 6t + 1$, $y = 7t + 1$, $x = 42t + 11$ за някое $t \in \mathbb{Z}$ или $x \equiv 11 (\mathrm{mod}\, 42)$.

(iii) Поотделното решаване на всяко от дадените сравнения свежда системата (iii) към

$$\left| \begin{array}{lll} x & \equiv -1 & (\mathrm{mod}\, 3) \\ x & \equiv 3 & (\mathrm{mod}\, 5) \\ x & \equiv 1 & (\mathrm{mod}\, 7) \end{array} \right. . \tag{6}$$

Първо решаваме системата сравнения

$$\left| \begin{array}{lll} x & \equiv -1 & (\mathrm{mod}\, 3) \\ x & \equiv 3 & (\mathrm{mod}\, 5) \end{array} \right. \tag{7}$$

като представяме $1 = 6 + (-5)$ с $6 \in 3\mathbb{Z}$, $(-5) \in 5\mathbb{Z}$ и намираме едно решение

$$c = (-1)(-5) + 6.3 = 23.$$

Всички решения на (7) образуват съседния клас $23 + 15\mathbb{Z} = 8 + 15\mathbb{Z}$.

Сега системата (6) е еквивалентна на системата

$$\left| \begin{array}{lll} x & \equiv 8 & (\mathrm{mod}\, 15) \\ x & \equiv 1 & (\mathrm{mod}\, 7) \end{array} \right. . \tag{8}$$

Представяме $1 = 15 + (-14)$ с $15 \in 15\mathbb{Z}$, $(-14) \in 7\mathbb{Z}$ и намираме едно решение

$$c = 15.1 + (-14).8 = -97.$$

Поради взаимната простота на 15 и 7, всички решения са

$$-97 + 15.7\mathbb{Z} = -97 + 105\mathbb{Z} = 8 + 105\mathbb{Z}.$$

Можем да решим непосредствено системата (6), полагайки $x = 3y - 1$ за някое $y \in \mathbb{Z}$ от първото сравнение. Тогава $3y - 1 = 3 + 5z$ за някое $z \in \mathbb{Z}$ от второто сравнение дава

$$y = 2z + 1 + \frac{1-z}{3} \in \mathbb{Z}.$$

Това изисква

$$t := \frac{1-z}{3} \in \mathbb{Z},$$

откъдето $z = 1 - 3t$, $y = 3 - 5t$, $x = 8 - 15t$. Заместваики в третото сравнение получаваме $8 - 15t = 7u + 1$ за $u \in \mathbb{Z}$ или

$$u = 1 - 2t - \frac{t}{7} \in \mathbb{Z}.$$

Въвеждаме $v := \frac{t}{7} \in \mathbb{Z}$ и изразяваме $t = 7v$, $x = 8 - 105v$. Следователно решението на (6) е $x \equiv 8 (\mathrm{mod}\, 105)$.

Твърдение 11. *Декартовото произведение $R = R_1 \times \ldots \times R_n$ на пръстените $R_1, \ldots, R_n$ е пръстен относно покомпонентно определените операции събиране*

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

и умножение

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$

Пръстенът R има единица тогава и само тогава, когато всички множители R_i имат единици 1_{R_i} и $1_R = (1_{R_1}, \ldots, 1_{R_n})$. В такъв случай, мултипликативната група

$$R^* = R_1^* \times \ldots \times R_n^*$$

на R е директно произведение на мултипликативните групи R_i^* на R_i.

Пръстенът $R = R_1 \times \ldots \times R_n$ се нарича директно произведение на $R_1, \ldots, R_n$.

Директното произведение $R = R_1 \times \ldots \times R_n$ на R_i е комутативен пръстен тогава и само тогава, когато всички множители R_i са комутативни.

Доказателство: За произволни $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n), z = (z_1, \ldots, z_n)$ от $R = R_1 \times \ldots \times R_n$ е в сила асоциативният закон за събиране

$$(x+y)+z = ((x_1+y_1)+z_1, \ldots, (x_n+y_n)+z_n) = (x_1+(y_1+z_1), \ldots, x_n+(y_n+z_n)) = x+(y+z).$$

От комутативността на събирането в R_i за $\forall 1 \leq i \leq n$ получаваме комутативността на събирането

$$x + y = (x_1 + y_1, \ldots, x_n + y_n) = (y_1 + x_1, \ldots, y_n + x_n) = y + x$$

в R. Ако 0_{R_i} е нулевият елемент на R_i, то $0_R = (0_{R_1}, \ldots, 0_{R_n})$ е нула на R, съгласно

$$x + 0_R = (x_1 + 0_{R_1}, \ldots, x_n + 0_{R_n}) = (x_1, \ldots, x_n) = x \quad \text{за} \quad \forall x \in R = R_1 \times \ldots \times R_n.$$

Всеки елемент $x_i \in R_i$ има противоположен $-x_i \in R_i$, така че $x = (x_1, \ldots, x_n) \in R = R_1 \times \ldots \times R_n$ има противоположен $-x = (-x_1, \ldots, -x_n) \in R$, изпълняващ равенството

$$x + (-x) = (x_1 + (-x_1), \ldots, x_n + (-x_n)) = (0_{R_1}, \ldots, 0_{R_n}) = 0_R.$$

С това проверихме, че $R = R_1 \times \ldots \times R_n$ е абелева група относно покомпоненнтното събиране.

Покомпонентното умножение в $R = R_1 \times \ldots \times R_n$ е асоциативно, съгласно асоциативността на умножението в R_i за $\forall 1 \leq i \leq n$. По-точно,

$$(xy)z = ((x_1y_1)z_1, \ldots, (x_ny_n)z_n) = (x_1(y_1z_1), \ldots, x_n(y_nz_n)) = x(yz) \quad \text{за} \quad \forall x, y, z \in R.$$

Дистрибутивните закони за събиране и умножение в R са директно следствие от дистрибутивните закони за събиране и умножение в R_i,

$$(x + y)z = ((x_1 + y_1)z_1, \ldots, (x_n + y_n)z_n) = (x_1z_1 + y_1z_1, \ldots, x_nz_n + y_nz_n) =$$

$$= (x_1z_1, \ldots, x_nz_n) + (y_1z_1, \ldots, y_nz_n) = xz + yz \quad \text{за} \quad \forall x, y, z \in R,$$

$$x(y+z) = (x_1(y_1+z_1), \ldots, x_n(y_n+z_n)) = (x_1y_1 + x_1z_1, \ldots, x_ny_n + x_nz_n) =$$
$$= (x_1y_1, \ldots, x_ny_n) + (x_1z_1, \ldots, x_nz_n) = xy + xz \quad \text{за} \quad \forall x, y, z \in R.$$

Следователно $R = R_1 \times \ldots \times R_n$ е пръстен относно покомпонентно определените събиране и умножение.

Елементът $1_R = (e_1, \ldots, e_n) \in R = R_1 \times \ldots \times R_n$ е единица в R точно когато

$$1_R x = x = x 1_R \quad \text{за} \quad \forall x \in R = R_1 \times \ldots \times R_n,$$

$$(e_1x_1, \ldots, e_nx_n) = (x_1, \ldots, x_n) = (x_1e_1, \ldots, x_ne_n) \quad \text{за} \quad \forall x \in R = R_1 \times \ldots \times R_n.$$

Последното е еквивалентно на $e_ix_i = x_i = x_ie_i$ за $\forall x_i \in R_i$, така че $1_R = (e_1, \ldots, e_n)$ е единица в $R = R_1 \times \ldots \times R_n$ тогава и само тогава, когато $e_i = 1_{R_i}$ са единиците на R_i за $\forall 1 \leq i \leq n$.

Ако R и R_i имат единици, то мултипликативната група R^* на R се състои от онези $x = (x_1, \ldots, x_n) \in R = R_1 \times \ldots \times R_n$, за които съществува $y = (y_1, \ldots, y_n) \in R = R_1 \times \ldots \times R_n$ с

$$xy = yx = 1_R,$$

$$(x_1y_1, \ldots, x_ny_n) = (y_1x_1, \ldots, y_nx_n) = (1_{R_1}, \ldots, 1_{R_n}).$$

Последното е равносилно на $x_iy_i = y_ix_i = 1_{R_i}$ за $\forall 1 \leq i \leq n$, така че $x = (x_1, \ldots, x_n) \in R^*$ тогава и само тогава, когато $x_i \in R_i^*$ за $\forall 1 \leq i \leq n$. По този начин доказахме, че

$$R^* = R_1^* \times \ldots \times R_n^*.$$

Пръстенът R е комутативен, ако

$$xy = yx \quad \text{за} \quad \forall x, y \in R,$$

$$(x_1y_1, \ldots, x_ny_n) = (y_1x_1, \ldots, y_nx_n) \quad \text{за} \quad \forall x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in R.$$

Последното е в сила тогава и само тогава, когато $x_iy_i = y_ix_i$ за $\forall x_i, y_i \in R_i$. Това доказва, че R е комутативен пръстен точно тогава, когато всички множители R_i са комутативни пръстени, Q.E.D.

Следствие 12. *Ако $I_1, \ldots, I_n$ са два по два взаимно прости идеала в комутативен пръстен с единица R, то съществува изоморфизъм на пръстени*

$$R/I_1 \ldots I_n \simeq (R/I_1) \times \ldots \times (R/I_n).$$

Решение: Изображението

$$\varphi : R \longrightarrow (R/I_1) \times \ldots \times (R/I_n),$$

$$\varphi(r) = (r + I_1, \ldots, r + I_n) \quad \text{за} \quad \forall r \in R$$

е хомоморфизъм на пръстени съгласно

$$\varphi(r+s) = (r+s+I_1, \ldots, r+s+I_n) = (r+I_1, \ldots, r+I_n) + (s+I_1, \ldots, s+I_n) = \varphi(r) + \varphi(s)$$

и

$$\varphi(rs) = (rs + I_1, \ldots, rs + I_n) = (r + I_1, \ldots, r + I_n)(s + I_1, \ldots, s + I_n) = \varphi(r)\varphi(s)$$

за $\forall r, s \in R$. Съгласно Китайската теорема за остатъците, φ е епиморфизъм, т.е. $\mathrm{im}(\varphi) = (R/I_1) \times \ldots \times (R/I_n)$.

По определение, ядрото $\ker(\varphi) = I_1 \cap \ldots \cap I_n$. Вземайки предвид Следствие 7, получаваме, че $\ker(\varphi) = I_1 \ldots I_n$. Сега теоремата за хомоморфизмите на пръстени дава

$$R/I_1 \ldots I_n = R/\ker(\varphi) \simeq \mathrm{im}(\varphi) = (R/I_1) \times \ldots \times (R/I_n)\,,$$

Q.E.D.

Следствие 13. *Ако $n = p_1^{a_1} \ldots p_k^{a_k}$ е разлагането на естественото число $n \geq 2$ в произведение на прости множители p_i с естествени степенни показатели a_i, то пръстенът $\mathbb{Z}_n$ на остатъците при деление с n се разлага в директно произведение*

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}. \tag{9}$$

Следствие 13 се получава непосредствено от Следствие 12, вземайки предвид $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$, $\mathbb{Z}_{p_i^{a_i}} = \mathbb{Z}/\langle p_i^{a_i}\rangle$ за $\forall 1 \leq i \leq k$ и $\langle p_1^{a_1}\rangle \ldots \langle p_k^{a_k}\rangle = \langle n\rangle$.

От разлагането (9) на $\mathbb{Z}_n$ в директно произведение на пръстени получаваме разлагането

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{a_1}}^* \times \ldots \times \mathbb{Z}_{p_k^{a_k}}^*$$

на мултипликативната група $\mathbb{Z}_n^*$ на $\mathbb{Z}_n$ в директно произведение на мултипликативните групи $\mathbb{Z}_{p_i^{a_i}}^*$ на $\mathbb{Z}_{p_i^{a_i}}$. За нечетно просто p и произволно естествено m може да се докаже, че мултипликативната група $\mathbb{Z}_{p^m}^* \simeq (\mathbb{Z}_{p^{m-1}(p-1)}, +)$ е циклична. За произволно естествено $m \geq 3$ мултипликативната група $\mathbb{Z}_{2^m}^* \simeq (\mathbb{Z}_2, +) \times (\mathbb{Z}_{2^{m-2}}, +)$ е директно произведение на две циклични групи.

2 Характеристика на поле. Прости полета.

Задача 14. *Да се докаже, че:*

(i) множеството $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ е подполе на полето $\mathbb{R}$ на реалните числа;

(ii) полето $\mathbb{Q}(\sqrt{2})$ е двумерно линейно пространство над простото си подполе.

Задача 15. *Нека F е поле с проста характеристика p, a и b са елементи на F, а n е естествено число. Да се докаже, че:*

(i) $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$.

(ii) изображението $\Phi_{p^n} : F \to \mathrm{im}\Phi_{p^n}$, $\Phi_{p^n}(a) = a^{p^n}$ е изоморфизъм на пръстени.

(iii) ако F е крайно поле с p^m елемента, то $\Phi_{p^n} : F \to F$, $\Phi_{p^n}(a) = a^{p^n}$ е изоморфизъм на полета.

Упътване: (i) Докажете, че биномните коефициенти $\binom{p}{i}$ с $1 \leq i \leq p-1$ се делят на p, за да изведете $(a \pm b)^p = a^p \pm b^p$. Продължете с индукция по $n \in \mathbb{N}$.

(ii) За съгласуваността на Φ_{p^n} със събирането използвайте (i). Ако $\Phi_{p^n}(a) = \Phi_{p^n}(b)$, то $0 = a^{p^n} - b^{p^n} = (a-b)^{p^n}$, откъдето $a = b$. Това доказва взаимната еднозначност на $\Phi_{p^n} : F \to \mathrm{im}\Phi_{p^n}$.

(iii) За крайно поле F с $|F| = p^m$ елемента, щом образът $\mathrm{im}\Phi_{p^n} \subseteq F$ се състои от p^m различни елемента, то $\mathrm{im}\Phi_{p^n} = F$ съвпада с цялото поле F.

Задача 16. *Ако F е поле с характеристика* $\mathrm{char}(F) = p$ *и $a_1, \ldots, a_m \in F$, то за $\forall n \in \mathbb{N}$ е в сила*

$$(a_1 + \ldots + a_m)^{p^n} = a_1^{p^n} + \ldots + a_m^{p^n}.$$

Решение: С индукция по $m \in \mathbb{N}$, случаят $m = 2$ съвпада със Задача 15 (i). Ако допуснем, че $(a_1 + \ldots + a_m)^{p^n} = a_1^{p^n} + \ldots + a_{m-1}^{p^n}$, то

$$(a_1+\ldots+a_m)^{p^n} = [(a_1+\ldots+a_{m-1})+a_m]^{p^n} = (a_1+\ldots+a_{m-1})^{p^n}+a_m^{p^n} = a_1^{p^n}+\ldots+a_{m-1}^{p^n}+a_m^{p^n},$$

съгласно Задача 15 (i) и индукционното предположение.

Задача 17. *Да се докаже, че ако F е поле с проста характеристика* $\mathrm{char}F = p$, *то за произволни елементи $x, y \in F$ е в сила*

$$(x+y)^{p-1} = \sum_{i=0}^{p-1} (-1)^i x^{p-1-i} y^i.$$

Упътване: Ако $y = 0$, то $(x+y)^{p-1} = x^{p-1}$. Отсега нататък предполагаме, че $y \neq 0$ и представяме

$$\begin{aligned}(x+y)^{p-1} = \left\{(-y)\left[\left(-\frac{x}{y}\right)-1\right]\right\}^{p-1} = (-1)^{p-1}y^{p-1}\left[\left(-\frac{x}{y}\right)-1\right]^{p-1} = \\ = (-1)^{p-1}y^{p-1}\sum_{i=0}^{p-1}(-1)^i\binom{p-1}{i}\left(-\frac{x}{y}\right)^{p-1-i}.\end{aligned} \tag{10}$$

От равенството на полиноми

$$\sum_{i=0}^{p-1}(-1)^i\binom{p-1}{i}x^{p-1-i} = (x-1)^{p-1} = \frac{(x-1)^p}{x-1} = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\ldots+x+1$$

с коефициенти от простото подполе $\mathbb{Z}_p$ на F следва $(-1)^i\binom{p-1}{i} = 1$ за $\forall 0 \leq i \leq p-1$. Заместваики в (10) получаваме

$$(x+y)^{p-1} = (-1)^{p-1}y^{p-1}\sum_{i=0}^{p-1}\left(-\frac{x}{y}\right)^{p-1-i} = \sum_{i=0}^{p-1}(-1)^i x^{p-1-i}y^i.$$

Задача 18. *За произволно просто число p да се докаже, че полето*

$$\mathbb{Z}_p(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in \mathbb{Z}_p[x], \quad g(x) \not\equiv 0 \right\}$$

на рационалните функции на x с коефициенти от простото поле $\mathbb{Z}_p$ с p елемента е безкрайно поле с характеристика $\mathrm{char}(\mathbb{Z}_p(x)) = p$.

Упътване: Аксиомите за поле се проверяват непосредствено. За безкрайността на полето $\mathbb{Z}_p(x)$ може да използвате, например, безкрайността на множеството

$$\{x^n \,|\, n \in \mathbb{N} \cup \{0\}\} \subset \mathbb{Z}_p(x)$$

на всички мономи на x.

3 Кратни корени.

Определение 19. *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 20. *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

$$f' + g' = \sum_{i=1}^{n} i a_i x^{i-1} + \sum_{j=1}^{m} j b_j x^{j-1} = \sum_{i=1}^{\max(n,m)} i(a_i + b_i) x^{i-1} =$$

$$= \left(\sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i \right)' = (f+g)'.$$

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

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

$$= \sum_{i=0}^{n-1+m} \left(\sum_{p=0}^{i} (p+1) a_{p+1} b_{i-p} \right) x^i + \sum_{i=0}^{n+m-1} \left(\sum_{q=0}^{i} (i-q+1) a_q b_{i-q+1} \right) x^i =$$

$$= \sum_{i=0}^{n+m-1} \left(\sum_{p=0}^{i} (p+1) a_{p+1} b_{i-p} + \sum_{q=0}^{i} (i-q+1) a_q b_{i-q+1} \right) x^i.$$

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

$$f'g + fg' = \sum_{i=0}^{n+m-1} \left(\sum_{s=1}^{i+1} s a_s b_{i+1-s} + \sum_{q=0}^{i} (i-q+1) a_q b_{i-q+1} \right) x^i =$$

$$= \sum_{i=0}^{n+m-1} \left((i+1) a_0 b_{i+1} + \sum_{s=1}^{i} (i+1) a_s b_{i+1-s} + (i+1) a_{i+1} b_0 \right) x^i =$$

$$= \sum_{i=0}^{n+m-1} (i+1) \left(\sum_{s=0}^{i+1} a_s b_{i+1-s} \right) x^i.$$

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

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

Q.E.D.

Задача 21. *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 22. *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 23. *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: $r(x) = 3^{n-2}x^2 - 3^{n-1}x + 1$

4 Основна теорема за симетричните полиноми.

Задача 24. *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*

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

$$(ii)\quad F_2(x_1,x_2,x_3,x_4) = \sum x_1^3x_2x_3,$$

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

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

$$(v)\quad F_5(x_1,\dots,x_n) = \sum x_1^3x_2x_3 \quad \text{за} \quad n \geq 5,$$

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

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

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

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

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

са $x_1^3x_2x_3$ и $x_1^2x_2^2x_3$. 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 $LT(F_1^{(3)}) = x_1^2x_2$ на $F_1^{(3)}$ отговаря на монома $\sigma_1\sigma_2$ на $\sigma_1,\sigma_2,\sigma_3$. Единственият моном $x_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3} <_{\text{lex}} x_1^2x_2$ с $\beta_1 \geq \beta_2 \geq \beta_3$, $\beta_1+\beta_2+\beta_3 = 3$ е $x_1x_2x_3$, 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:

$$\sum x_1^2x_2 = \left(\sum x_1x_2\right)\left(\sum x_1\right) - 3\left(\sum x_1x_2x_3\right) = \sigma_1\sigma_2 - 3\sigma_3 \quad \text{за} \quad \forall n \geq 3, \tag{11}$$

$$F_1^{(5)}(x_1,x_2,x_3) = \sum x_1^3x_2^2 = \left(\sum x_1^2x_2\right)\left(\sum x_1x_2\right) - 2\left(\sum x_1^3x_2x_3\right) - 2\left(\sum x_1^2x_2^2x_3\right) =$$

$$= (\sigma_1\sigma_2 - 3\sigma_3)\,\sigma_2 - 2\sigma_3\left(\sum x_1^2\right) - 2\sigma_3\left(\sum x_1x_2\right),$$

$$\sum x_1^2 = (x_1)^2 - 2\left(\sum x_1x_2\right) = \sigma_1^2 - 2\sigma_2 \quad \text{за} \quad \forall n \geq 2. \tag{12}$$

$$(ii)\quad F_2(x_1,x_2,x_3,x_4) = \sum x_1^3x_2x_3 = \left(\sum x_1x_2x_3\right)\left(\sum x_1^2\right) - \sum x_1^2x_2x_3x_4 =$$

$$= \sigma_3(\sigma_1^2 - 2\sigma_2) - \sigma_4\sigma_1.$$

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 $\sigma_1, \ldots, \sigma_4$. 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

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

$$= \left(\sum x_1x_2x_3\right)\left(\sum x_1^2x_2\right) - 3\left(\sum x_1^3x_2x_3x_4\right) - 2\sum x_1^2x_2^2x_3x_4 =$$

$$= \sigma_3\left(\sum x_1^2x_2\right) - 3\sigma_4\left(\sum x_1^2\right) - 2\sigma_4\left(\sum x_1x_2\right) \quad \text{за} \quad n = 4,$$

(11) и (12) 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

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

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

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) Възоснова на

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

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 $x_1 = x_2 = x_3 = 1$, $x_4 = \ldots = x_n = 0$ имаме $\sigma_1 = 3$, $\sigma_2 = 3$, $\sigma_3 = 1$ и $\sigma_i = 0$ за $\forall 4 \leq i \leq n$. В резултат, $3 = F_5(1,1,1,0,\ldots,0) = 9 + 3A$ и $A = -2$. За $x_1 = x_2 = x_3 = x_4 = 1$, $x_5 = \ldots = x_n = 0$ 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 $12 = 4.3 = F_5(1,1,1,1,0,\ldots,0) = 64 - 48 + 4B$ определяме $B = -1$. Накрая, за $x_1 = x_2 = x_3 = x_4 = x_5 = 1$, $x_6 = \ldots = 0$ 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 $30 = 3\binom{5}{3} = F_5(1,1,1,1,1,0,\ldots,0) = 250 - 200 - 25 + C$. Следователно $C = 5$.

Задача 25. *Нека* $f(x) = \prod_{i=1}^{n}(x - x_i) \in \mathbb{R}[x]$ *е полином със старши коефициент 1 и корени* $x_1, \ldots, x_n$. *Да се докаже, че:*

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

Задача 26. *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*

$$(i)\, \Sigma_1(x_1,x_2,x_3) = (x_1^2 - x_2x_3)(x_2^2 - x_3x_1)(x_3^2 - x_1x_2);$$

$$(ii)\, \Sigma_2(x_1,x_2,x_3) = \frac{x_1x_2}{(x_2 + x_3 - x_1)(x_1 + x_3 - x_2)} +$$

$$+ \frac{x_2x_3}{(x_1 + x_3 - x_2)(x_1 + x_2 - x_3)} + \frac{x_3x_1}{(x_1 + x_2 - x_3)(x_2 + x_3 - x_1)};$$

$$(iii)\, \Sigma_3(x_1,x_2,x_3) = \frac{x_1^2 + 2}{x_2 + x_3} + \frac{x_2^2 + 2}{x_1 + x_3} + \frac{x_3^2 + 2}{x_1 + x_2}.$$

Отговор:

$$(i)\ \ \Sigma_1(x_1,x_2,x_3) = p^3r - q^3;$$

$$(ii)\ \ \Sigma_2 = \frac{6r - pq}{p^3 - 4pq + 8r};$$

$$(iii)\ \ \Sigma_3(x_1,x_2,x_3) = \frac{p^4 - 3p^2q + 4pr + 2p^2 + 2q}{r - pq}.$$

Задача 27. *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*

$$(i)\, \Sigma_1(x_1,x_2,x_3) = \frac{x_1^2}{(1 + x_2)(1 + x_3)} + \frac{x_2^2}{(1 + x_3)(1 + x_1)} + \frac{x_3^2}{(1 + x_1)(1 + x_2)};$$

$$(ii)\, \Sigma_2(x_1,x_2,x_3) = \ = \frac{x_3}{x_1^2 + 4x_1x_2 + x_2^2} + \frac{x_2}{x_1^2 + 4x_1x_3 + x_3^2} + \frac{x_1}{x_2^2 + 4x_2x_3 + x_3^2}\,.$$

$$(iii)\, \Sigma_3(x_1,x_2,x_3) = \frac{x_1}{(1 + x_1)^2} + \frac{x_2}{(1 + x_2)^2} + \frac{x_3}{(1 + x_3)^2}$$

$$(iv)\, \Sigma_4(x_1,x_2,x_3) = \frac{x_1^2}{(1 + x_1)^2} + \frac{x_2^2}{(1 + x_2)^2} + \frac{x_3^2}{(1 + x_3)^2}$$

Отговор:

$$(i)\ \ \Sigma_1(x_1,x_2,x_3)=\frac{-2p-3q}{p-q+1};$$

$$(ii)\ \ \Sigma_2(x_1,x_2,x_3)=\frac{9pq}{2p^3+27q^2};$$

$$(iii)\ \ \Sigma_3(x_1,x_2,x_3)=\frac{4p-9q-pq}{(q-p-1)^2};$$

$$(iv)\ \ \Sigma_4(x_1,x_2,x_3)=\frac{2p^2-4pq+3q^2-2p+6q}{(q-p-1)^2}.$$

5 Дискриминанта и резултанта.

Задача 28. *Да се намери резултантата $R(f,g)$ на полиномите*

$$f(x)=x^4+3px^2+x+3 \quad и \quad g(x)=x^3+px^2+1\in\mathbb{C}[x]..$$

Решение: Ако $g(x)=\prod\limits_{i=1}^{3}(x-\alpha_i)$, то

$$R(f,g)=(-1)^{3.4}R(g,f)=\prod_{i=1}^{3}f(\alpha_i)=\prod_{i=1}^{3}[(p+3)(p\alpha_i^2+1)]=(p+3)^3\prod_{i=1}^{3}(p\alpha_i^2+1),$$

съгласно $\alpha_i^3=-p\alpha_i^2-1$ и $\alpha_i^4=-p(-p\alpha_i^2-1)-\alpha_i=p^2\alpha_i^2-\alpha_i+p$. Следователно

$$R(f,g)=(p+3)^3\left[p^3(\alpha_1\alpha_2\alpha_3)^2+p^2\left(\sum\alpha_1^2\alpha_2^2\right)+p\left(\sum\alpha_1^2\right)+1\right].$$

Вземайки предвид

$$\alpha_1\alpha_2\alpha_3=-1,$$

$$\sum\alpha_1^2\alpha_2^2=\left(\sum\alpha_1\alpha_2\right)^2-2\left(\sum\alpha_1^2\alpha_2\alpha_3\right)=\sigma_2^2-2\sigma_1\sigma_3=-2p,$$

$$\sum\alpha_1^2=\sigma_1^2-2\sigma_2=p^2,$$

получаваме $R(f,g)=(p+3)^3$.

Задача 29. *Да се намери резултантата на полиномите*

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n \quad и \quad g(x)=a_0x^{n-1}+a_1x^{n-2}+\ldots a_{n-1}$$

с комплексни коефициенти и $a_0\neq 0$.

Решение: Забелязваме, че $f(x)=xg(x)+a_n$. Ако $\beta_1,\ldots,\beta_{n-1}$ са корените на $g(x)=0$, то $f(\beta_j)=a_n$ за $\forall 1\leq j\leq n-1$. Следователно

$$R(f,g)=(-1)^{n(n-1)}R(g,f)=R(g,f)=a_0^n\prod_{j=1}^{n-1}f(\beta_j)=a_0^na_n^{n-1}.$$

Задача 30. *Да се намери резултантата на полиномите*

$$(i)\quad f(x)=x^{n+1}-ax^n-x+a,\quad g(x)=x^n+x^{n-1}+\ldots+x+1,$$

$$(ii)\quad f(x)=x^{2n+1}-1,\quad g(x)=x^{4n+3}+x^{2n+2}+2.$$

Решение: (i) Ако $\omega=\cos\left(\frac{2\pi}{n}\right)+i\sim\left(\frac{2\pi}{n}\right)$, то полиномът $f(x)$ има разлагане $f(x)=(x-a)(x^n-1)=(x-a)\prod\limits_{i=1}^{n}(x-\omega^i)$. Вземайки предвид $\frac{x^n-1}{x-1}=x^{n-1}+x^{n-2}+\ldots+x+1$ и $\omega^i\neq 1$ за $\forall 1\leq i\leq n-1$, пресмятаме, че

$$\omega^{i(n-1)}+\omega^{i(n-2)}+\ldots+\omega^i+1=\frac{\omega^{in}-1}{\omega^i-1}=0\quad\text{за}\quad\forall 1\leq i\leq n-1.$$

Следователно

$$R(f,g)=g(a)\prod_{i=1}^{n}g(\omega^i)=(a^n+a^{n-1}+\ldots+a+1)(n+1),$$

защото $g(\omega^i)=\omega^{in}=1$ за $\forall 1\leq i\leq n-1$.

(ii) Ако $\omega=\cos\left(\frac{2\pi}{2n+1}\right)+i\sin\left(\frac{2\pi}{2n+1}\right)$, то $f(x)=\prod\limits_{i=1}^{2n+1}(x-\omega^i)$ и $\omega^{i(2n+1)}=1$ за $\forall 1\leq i\leq 2n+1$. Пресмятаме

$$g(\omega^i)=\omega^{i(4n+3)}+\omega^{i(2n+2)}+2=\omega^{2i(2n+1)}\omega^i+\omega^{i(2n+1)}\omega^i+2=\omega^i+\omega^i+2=2(\omega^i+1)$$

и получаваме, че

$$R(f,g)=\prod_{i=1}^{2n+1}g(\omega^i)=2^{2n+1}\prod_{i=1}^{2n+1}(1+\omega^i)=$$

$$=-2^{2n+1}\prod_{i=1}^{2n+1}(-1-\omega^i)=-2^{2n+1}f(-1)=-2^{2n+1}(-2)=2^{2n+2}.$$

Задача 31. *Нека $f(x),g(x),h(x)$ са полиноми с коефициенти от поле F, $t(x)=f(x-c)$. Да се докаже, че:*

(i) $R(f,gh)=R(f,g)R(f,h)$;
(ii) $D(fg)=D(f)D(g)R(f,g)^2$;
(iii) $D(t)=D(f)$;
(iv) $D((x-c)f)=D(f)f(c)^2$.

Решение: Нека

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n=a_0\prod_{i=1}^{n}(x-\alpha_i),$$

$$g(x)=b_0x^m+b_1x^{m-1}+\ldots b_m=b_0\prod_{j=1}^{m}(x-\beta_j),$$

$$h(x) = c_0x^k + c_1x^{k-1} + \ldots + c_k = c_0\prod_{s=1}^{k}(x-\gamma_s)$$

за корените $\alpha_1, \ldots, \alpha_n$ на $f(x)$, корените $\beta_1, \ldots, \beta_m$ на $g(x)$ и корените $\gamma_1, \ldots, \gamma_k$ на $h(x)$ от позходящо разширение на F. Тогава, по определение

$$(i)\ \ R(f,gh) = a_0^{m+k}(b_0c_0)^n\left[\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j)\right]\left[\prod_{i=1}^{n}\prod_{s=1}^{k}(\alpha_i-\gamma_s)\right] =$$

$$= \left[a_0^m b_0^n\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j)\right]\left[a_0^k c_0^n\prod_{i=1}^{n}\prod_{s=1}^{k}(\alpha_i-\gamma_k)\right] = R(f,g)R(f,h).$$

Отново по определение,

$$(ii)\ \ D(fg) = (a_0b_0)^{2(n+m)}\prod_{n\geq i>j\geq 1}(\alpha_i-\alpha_j)^2\prod_{m\geq i>j\geq 1}(\beta_i-\beta_j)^2\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j)^2 =$$

$$\left[a_0^{2n-2}\prod_{n\geq i>j\leq 1}(\alpha_i-\alpha_j)^2\right]\left[b_0^{2m-2}\prod_{m\geq i>j\geq 1}(\beta_i-\beta_j)^2\right]\left[a_0^m b_0^n\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j)\right]^2 =$$

$$= D(f)D(g)R(f,g)^2.$$

Ако полиномът $f(x) = a_0\prod_{i=1}^{n}(x-\alpha_i)$ има корени $\alpha_1, \ldots, \alpha_n$, то полиномът $t(x) = f(x-c) = a_0\prod_{i=1}^{n}(x-c-\alpha_i)$ има корени $\alpha_1+c, \ldots, \alpha_n+c$ и дискриминантата

$$(iii)\ \ D(t) = a_0^{2n-2}\prod_{n\geq i>j\geq 1}[(\alpha_i+c)-(\alpha_j+c)]^2 = a_0^{2n-2}\prod_{n\geq i>j\geq 1}(\alpha_i-\alpha_j)^2 = D(f).$$

За полинома $f(x) = a_0\prod_{i=1}^{n}(x-\alpha_i)$ имаме

$$(iv)\ \ D((x-c)f) = a_0^{2(n+1)-2}\prod_{n\geq i>j\geq 1}(\alpha_i-\alpha_j)^2\prod_{i=1}^{n}(c-\alpha_i)^2 =$$

$$= \left[a_0^{2n-2}\prod_{n\geq i>j\geq 1}(\alpha_i-\alpha_j)^2\right]\left[a_0\prod_{i=1}^{n}(c-\alpha_i)\right]^2 = D(f)f(c)^2.$$

Задача 32. *Да се пресметне дискриминантата на полинома* $f(x) = x^3 + px + q$.

Решение: Ако α_i, $1 \leq i \leq 2$ е корен на $f'(x) = 3x^2 + p = 3\prod_{i=1}^{2}(x-\alpha_i) = 0$, то $f(\alpha_i) = \frac{1}{3}(2p\alpha_i + 3q)$ и

$$D(f) = (-1)^{\frac{3.2}{2}}R(f,f') = -R(f',f) = -3^3\prod_{i=1}^{2}f(\alpha_i) = -3\prod_{i=1}^{2}(2p\alpha_i+3q) =$$

$$= -(2p)^2 \left[3 \prod_{i=1}^{2} \left(-\frac{3q}{2p} - \alpha_i \right) \right] = -4p^2 f' \left(-\frac{3q}{2p} \right) = -4p^3 - 27q^2.$$

Задача 33. *За кои стойности на параметъра* $\lambda \in \mathbb{C}$ *полиномът* $f(x) \in \mathbb{C}[x]$ *има кратни корени, ако*

$$(i) \quad f(x) = x^3 + 3x^2 + \lambda - 2; \quad (ii) f(x) = x^4 - 4x + \lambda.$$

Решение: (i) Производната $f'(x) = 3x^2 + 6x = 3x(x+2)$ има корени $x_1 = 0$ и $x_2 = -2$, така че дискриминантата

$$D(f) = (-1)^{\frac{3.2}{2}} F(f', f) = -3^3 f(0) f(-2) = -27(\lambda - 2)(\lambda + 2).$$

Полиномът $f(x) \in \mathbb{C}[x]$ има кратен корен тогава и само тогава, когато дискриминантата му $D(f) = 0$ се анулира. В случая, $f(x)$ има кратен корен за $\lambda_1 = 2$ или $\lambda_2 = -2$.

(ii) Производната $f'(x) = 4x^3 - 4 = 4(x^3 - 1) = 4(x-1)(x-\omega)(x-\omega^2)$ за

$$\omega = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2} i.$$

Дискриминантата

$$D(f) = (-1)^{\frac{4.3}{2}} F(f', f) = R(f', f) = 4^4 f(1) f(\omega) f(\omega^2) = 256(\lambda - 3)(\lambda - 3\omega)(\lambda - 3\omega^2),$$

вземайки предвид, че $\omega^3 = (\omega^2)^3 = 1$. Полиномът $f(x)$ има кратен корен точно когато $D(f) = 0$ и това е в сила за $\lambda_1 = 3$, $\lambda_2 = 3\omega$ или $\lambda_3 = 3\omega^2$.

Задача 34. *Нека* F *е поле с характеристика* $\mathrm{char}(F) = 0$ *или* $\mathrm{char}(F) = p > n$. *Да се намерят дискриминантите на полиномите*

$$f(x) = x^n + a \quad u \quad g(x) = n! \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!} \right)$$

с коефициенти от F.

Решение: Формалната производна $f'(x) = nx^{n-1}$ има $(n-1)$-кратен корен 0, така че

$$D(f) = (-1)^{\frac{n(n-1)}{2}} R(f', f) = (-1)^{\frac{n(n-1)}{2}} n^n f(0)^{n-1} = (-1)^{\frac{n(n-1)}{2}} n^n a^{n-1}.$$

Забелязваме, че $g'(x) = g(x) - x^n$. Ако $g(x) = \prod_{i=1}^{n} (x - \alpha_i)$, то $g'(\alpha_i) = -\alpha_i^n$ и

$$D(g) = (-1)^{\frac{n(n-1)}{2}} R(g, g') = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} g'(\alpha_i) =$$

$$= (-1)^{\frac{n(n-1)}{2}} (-1)^n (\alpha_1 \ldots \alpha_n)^n = (-1)^{\frac{n(n-1)}{2}} (-1)^n [(-1)^n n!] = (-1)^{\frac{n(n-1)}{2}} (n!)^n,$$

съгласно формулата на Виет $\alpha_1 \ldots \alpha_n = (-1)^n g(0) = (-1)^n n!$ за $g(x)$.

6 Действие на група върху множество. Теореми на Силов.

Задача 35. (Теорема на Поанкаре) *Нека G е група, а H е подгрупа на G с индекс $[G:H]=m$. Да се докаже, че съществува хомоморфизъм на групи $\Phi: G \to S_m$ в симетричната група S_m с ядро $N=\ker\Phi \subseteq H$, така че индексът $[G:N]$ се дели на m и дели $m!$.*

В частност, за $H=\{1\}$ получаваме теоремата на Кейли, съгласно която всяка крайна група G от ред m е изоморфна на подгрупа на симетричната група S_m.

Решение: Множеството $G/H=\{gH \,|\, g\in G\}$ на левите съседни класове на G относно H се състои от $[G:H]=m$ елемента. Непосредствено се проверява, че изображението

$$G\times(G/H)\longrightarrow(G/H),$$
$$(x,gH)\mapsto xgH$$

е действие на групата G върху G/H. Това действие отговаря на хомоморфизъм на групи

$$\Phi: G\longrightarrow S(G/H)=S_m.$$

Ядрото

$$N=\ker\Phi=\{x\in G\,|\,xgH=gH,\,\forall gH\in G/H\}=$$
$$=\{x\in G\,|\,g^{-1}xgH=H,\forall g\in G\}=$$
$$=\{x\in G\,|\,g^{-1}xg\in H,\,\forall g\in G\}=$$
$$=\{x\in G\,|\,x\in gHg^{-1},\,\forall g\in G\}=\cap_{g\in G}\ \ gHg^{-1}$$

е сечението на всики спрегнати с H подгрупи на G. От $N\subseteq H\subseteq G$ следва $[G:N]=[G:H][H:N]$, защото по Теоремата на Лагранж имаме

$$[G:N]=\frac{|G|}{|N|},\ \ [G:H]=\frac{|G|}{|H|},\ \ [H:N]=\frac{|H|}{|N|}.$$

Следователно $m=[G:H]$ дели индекса $[G:N]$ на N в G. От друга страна, по Теоремата за хомоморфизмите на групи, $\mathrm{im}\Phi\simeq G/\ker\Phi=G/N$. Редът $[G:N]=|G/N|=|\mathrm{im}\Phi|$ на подгрупата $\mathrm{im}\Phi$ на S_m дели реда $|S_m|=m!$ на симетричната група S_m.

Ако $H=\{1\}$, то $m=[G:H]=|G|$ и действието

$$G\times G\longrightarrow G,$$
$$(x,g)\mapsto xg$$

на G върху себе си отговаря на хомоморфизъм на групи

$$\Phi: G\longrightarrow S(G)=S_m.$$

Ядрото

$$N=\ker\Phi=\cap_{g\in G}\ \ g\{1\}g^{-1}=\cap_{g\in G}\ \ \{1\}=\{1\},$$

така че $\Phi: G\to\mathrm{im}\Phi$ е изоморфизъм върху образа си и групата G е изоморфна на подгрупата $\mathrm{im}\Phi$ на $S_m=S_{|G|}$.

Задача 36. *Нека G е група, а H е такава подгрупа на G, чийто индекс $[G:H]=p$ е най-малкият прост делител на реда $|G|$ на G. Да се докаже, че H е нормална подгрупа на G.*

Решение: Съгласно Задача 35, ако $[G:H]=p$, то съществува хомоморфизъм на групи $\Phi: G \to S_p$ с ядро $N = \ker\Phi = \cap_{g\in G}\ gHg^{-1}$, чийто индекс $[G:N]$ се дели на p и дели $p!$. По Теоремата на Лагранж, $[G:N]$ дели реда $|G|$ на групата G.

Ако $[G:N]$ има прост делител $q \neq p$, то q дели $|G|$ и $q > p$. От друга страна, q дели $p!$, защото q дели $[G:N]$ и $[G:N]$ дели $p!$. Но за просто число p, простите делители на $p!$ са не по-големи от p, така че $[G:N]$ няма друг прост делител освен p.

Ако допуснем, че $[G:N]=p^r$ за някое $r\in\mathbb{N}$, $r\geq 2$, то p^r не може да дели $p!=(p-1)!p$, защото простите делители на $(p-1)!$ са строго по-малки от p и p не дели $(p-1)!$. Това доказва $[G:N]=p=[G:H]$ и

$$[H:N]=\frac{[G:N]}{[G:H]}=1 \quad \text{за} \quad N\subseteq H.$$

Следователно $H=N$ е нормална подгрупа на G.

Теорема 37. (Теореми на Силов) *Нека G е крайна група и p е такова просто число, че p^r дели реда $|G|$ на G, а p^{r+1} не дели $|G|$. Тогава:*

(i) за всяко $1\leq i\leq r$ съществува подгрупа на G от ред p^i;

(ii) всички подгрупи на G от ред p^r са спрегнати в G;

(iii) броят n_p на подгрупите на G от ред p^r дели реда $|G|$ на G и изпълнява сравнението $n_p\equiv 1(\mathrm{mod}\, p)$.

Подгрупите на G от ред p^r се наричат силови p-подгрупи.

Задача 38. *Нека G е крайна група, а H е нормална p-подгрупа на G. Да се докаже, че H се съдържа във всяка силова p-подгрупа на G.*

Решение: В доказателството на втората теорема на Силов установихме, че всяка p-подгрупа H на G се съдържа в някоя силова p-подгрупа Q. Съгласно същата теорема, всяка силова p-подгрупа на G е от вида gQg^{-1} за някое $g\in G$. Сега от $H\subseteq Q$ следва $H=gHg^{-1}\subseteq gQg^{-1}$ за нормалната подгрупа H на G.

Задача 39. *Нека p е прост делител на реда $|G|$ на крайна група G, а H е нормална подгрупа на G, която съдържа някоя силова p-подгрупа P на G. Да се докаже, че H съдържа всички силови p-подгрупи на G.*

Решение: Нека $P\subseteq H$ за някоя силова p-подгрупа P на G. Тогава всяка силова p-подгрупа на G е от вида gPg^{-1} за някое $g\in G$ и $gPg^{-1}\subseteq gHg^{-1}=H$ за нормалната подгрупа H на G.

Задача 40. *Нека G е крайна група, P е силова p-подгрупа на G, а H е подгрупа на G, съдържаща нормализатора $N_G(P):=\{g\in G\,|\,gPg^{-1}\}$ на P в G. Да се докаже, че нормализаторът $N_G(H)=H$ на H в G се изчерпва от H.*

Решение: Включването $H \subseteq N_G(H)$ следва непосредствено от $hHh^{-1} = H$ за всеки елемент $h \in H$.

Ако $g \in N_G(H)$, то $gHg^{-1} = H$. Вземайки предвид $P \subseteq N_G(P) \subseteq H$, получаваме, че $gPg^{-1} \subseteq gHg^{-1} = H$. Редът $|G|$ на G се дели на реда $|P| = p^r$, $r \in \mathbb{N}$ на P и не се дели на p^{r+1}. От $P \subseteq H$ следва, че редът $|H|$ на H се дели на p^r. Редът $|H|$ на H дели реда $|G|$ на G и не се дели на p^{r+1}. Следователно P е силова p-подгрупа на H и силовата p-подгрупа gPg^{-1} на H е спрегната с P в H. С други думи, съществува $h \in H$, така че $gPg^{-1} = hPh^{-1}$. Оттук $(h^{-1}g)P(h^{-1}g)^{-1} = P$ и $h^{-1}g \in N_G(P) \subseteq H$. В резултат, $g = h(h^{-1}g) \in hH = H$, което трябваше да се докаже.

Задача 41. *Да се намерят всички силови подгрупи на симетричната група S_3 и на алтернативната група A_4.*

Решение: Симетричната група S_3 е от ред $3! = 6$. Следователно силовите подгрупи на S_3 са от ред 2 или от ред 3. Силовите 2-подгрупи са

$$\{\varepsilon, (12)\}, \quad \{\varepsilon, (13)\}, \quad \{\varepsilon, (23)\},$$

където ε е тъждествената пермутация на $1, 2, 3$. Ако P_3 е силова 3-подгрупа на S_3, то индексът на P_3 е $[S_3 : P_3] = \frac{|S_3|}{|P_3|} = \frac{6}{3} = 2$ и P_3 е нормална подгрупа на S_3. С други думи, S_3 има единствена силова 3-подгрупа и това е алтернативната група

$$P_3 = A_3 = \{\varepsilon, (123), (132)\}.$$

Алтебрнативната група A_4 е от ред $|A_4| = \frac{|S_4|}{2} = \frac{4!}{2} = 12$. Силовите 3-подгрупи на A_4 са циклични от ред 3 и се пораждат от тройните цикли. Това са

$$\{\varepsilon, (123), (132)\}, \quad \{\varepsilon, (124), (142)\}, \quad \{\varepsilon, (134), (143)\}, \quad \{\varepsilon, (234), (243)\}.$$

Ако P_2 е силова 2-подгрупа на A_4, то P_2 е от ред 4. Четворните цикли са нечетни пермутации и не принадлежат на A_4. Единствената подгрупа на A_4 от ред 4 е групата на Клайн

$$P_2 = K_4 = \{\varepsilon, (12)(34), (13)(24), (14)(23)\}.$$

Задача 42. *За произволно просто число $p \geq 3$ да се намери броя n_p на силовите p-подгрупи на симетричната група S_p.*

Решение: Симетричната група S_p е от ред $|S_p| = p!$, който се дели на p и не се дели на p^2 за просто p. Следователно силовите p-подгрупи P на S_p са циклични от ред p и се пораждат от циклите $(i_1 i_2 \dots i_p)$ с дължина p. Броят на циклите с дължина p в симетричната група S_p е $(p-1)!$, защото всеки такъв цикъл може да се записва с начало $i_1 = 1$. Произволна силова p-подгрупа P на S_p се състои от $p-1$ цикъла с дължина p и тъждествената пермутация ε. Всеки цикъл с дължина p поражда силовата p-подгрупа, на която принадлежи, така че произволни две различни силови p-подгрупи на S_p се пресичат само в тъждествената пермутация ε. Оттук, броят на силовите p-подгрупи на S_p е равен на частното

$$\frac{(p-1)!}{p-1} = (p-2)!$$

на броя $(p-1)!$ на циклите с дължина p и броя $p-1$ на циклите с дължина p в коя и да е силова p-подгрупа на S_p.

Задача 43. *Нека p и q са различни прости числа, а G е група от ред $|G| = pq$. Да се докаже, че:*

(i) G има нормална силова подгрупа;

(ii) ако p не дели $q-1$ и q не дели $p-1$, то G е циклична група.

Решение: (i) Без ограничение на общността можем да считаме, че $p < q$. Тогава броят n_q на силовите q-подгрупи на G не може да е равен на p, защото q не може да дели $p - 1 < q - 1$. Следователно $n_q = 1$ и съществува единствена нормална силова q-подгрупа Q на G.

(ii) Ако p не дели $q-1$ и q не дели $p-1$, то $n_q = 1$ и $n_p = 1$. С други думи, съществуват единствена нормална силова p-подгрупа P на G и единствена нормална q-подгрупа Q на G. Подгрупите P и Q от прост ред p, съответно q, са циклични. Нека $P = \langle a \rangle = \{1, a, \ldots, a^{p-1}\}$ се поражда от a, $Q = \langle b \rangle = \{1, b, \ldots, b^{q-1}\}$ се поражда от b. Твърдим, че $ab = ba$. Наистина, от $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in P \triangleleft G$ и $aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in Q \triangleleft G$ следва $aba^{-1}b^{-1} \in P \cap Q = \{1\}$, откъдето $ab = ba$. Достатъчно е да докажем, че елементът $ab \in G$ е от ред pq, за да получим, че G съвпада с цикличната група, породена от ab. По-точно, ако ab е от ред r, то $1 = (ab)^{pr} = (a^p)^r b^{pr} = b^{pr}$, защото $a \in G$ е от ред p. Следователно редът q на b дели pr. Различните прости числа p и q са взаимно прости, така че q дели r. Аналогично, от $1 = (ab)^{qr} = a^{qr}(b^q)^r = a^{qr}$ следва, че p дели qr, откъдето p дели r. Щом взаимно простите числа p и q делят поотделно r, то и произведението им pq дели r. Обратно, от $(ab)^{pq} = (a^p)^q(b^q)^p = 1$ получаваме, че редът r на ab дели pq и $r = pq$ за $pq, r \in \mathbb{N}$.

Задача 44. *Нека p, q, r са различни прости числа, а G е група от ред $|G| = pqr$. Да се докаже, че G има нормална силова подгрупа.*

Решение: Без ограничение на общността считаме, че $p < q < r$. Да допуснем, че G няма нормална силова подгрупа, т.е. $n_p > 1$, $n_q > 1$, $n_r > 1$ за броя n_p, n_q, n_r на силовите p-подгрупи, съответно, q-подгрупи и r-подгрупи на G. Както в решението на Задача 43, делителят n_r на pq е различен от p и q, защото r не може да дели $p-1$ и $q-1$. Следователно $n_r = pq$. Аналогично, делителят n_q на pr е различен от p, защото q не може да дели $p-1$. Затова $n_q = r$ или $n_q = pr$. И в двата случая, $n_q \geq r$. Накрая, за делителя $n_p > 1$ на qr имаме $n_p \in \{q, r, qr\}$ или $n_p \geq q$. Силовите подгрупи на G са циклични от прост ред и се пораждат от кой и да е свой нетривиален елемент. Следователно произволни две различни силови подгрупи на G от един и същи ред или от различен ред се пресичат само в неутралния елечент на G. В резултат, групата G съдържа поне $q(p-1)$ елемента от ред p, поне $r(q-1)$ елемента от ред q и $pq(r-1$ елемента от ред r. Общият броя на тези елементи е по-голям или равен на

$$q(p-1) + r(q-1) + pq(r-1) = pqr + pq + qr - pr - q - r > pqr,$$

защото

$$pq + qr - pr - q - r = q(p-1) + r(q-p-1) \geq q(p-1) > 0$$

за прости $p < q < r$.

Задача 45. *Да се докаже, че крайната група G има нормална силова подгрупа, ако редът $|G|$ на G е:*

$$(i)\ \ |G| = 80, \quad (ii)\ \ |G| = 280, \quad (iii)\ \ |G| = 495.$$

Решение: В кой и да е от случаите да допуснем, че групата G няма нормална силова подгрупа. Тогава за всеки прост делител p на реда $|G|$ на G броят n_p на силовите p-подгрупи на G е строго по-голям от 1.

(i) Ако $|G| = 80 = 2^4.5$, то n_2 е нечетен делител на 5, $n_2 > 1$. Следователно $n_2 = 5$. Броят n_5 на силовите 5-подгрупи на G е делител на $2^4 = 16$, изпълняващ сравнението $n_5 \equiv 1 (\mathrm{mod}\, 5)$. Следователно $n_5 = 16$. Силовите 5-подгрупи са циклични от прост ред и се пресичат две по две само в неутралния елемент на G. Следователно G съдържа $16.4 = 64$ елемента от ред 5. Останалите 16 елемента образуват единствена силова 2-подгрупа на G. Това противоречи на $n_2 = 5$ и доказва, че всяка група от ред 80 има нормална силова подгрупа.

(ii) Ако $|G| = 280 = 2^3.5.7$, то броят n_7 на силовите 7-подгрупи на G е делител на $2^3.5 = 40$ и $n_7 \equiv 1 (\mathrm{mod}\, 7)$. Следователно $n_7 = 8$. Броят n_5 на силовите 5-подгрупи на G дава остатък 1 при деление на 5 и дели $2^3.7 = 56$. Оттук, $n_5 = 56$. За $p = 5$ или $p = 7$, всеки две силови p-подгрупи се пресичат само в неутралния елемент на G. Следователно групата G съдържа $56 = 4 = 224$ елемента от ред 5 и $8.6 = 48$ елемента от ред 7. Останалите 8 елемента на G могат да образуват само една силова 2-подгрупа. Това доказва, че всяка група G от ред 280 има нормална силова подгрупа.

(iii) Нека $|G| = 495 = 3^2.5.11$. Тогава броят n_{11} на силовите 11-подгрупи на G дели $3^2.5 = 45$ и $n_{11} \equiv 1 (\mathrm{mod}\, 11)$. Предположението $n_{11} > 1$ изисква $n_{11} = 45$. За $n_5 > 1$ знаем, че $n_5 \equiv 1 (\mathrm{mod}\, 5)$ и n_5 дели $3^2.11 = 99$. Оттук $n_5 = 11$. Вземайки предвид, че произволни две различни силови 11-подгрупи се пресичат сами в неутралния елемент, стигаме до извода, че G има $45.10 = 450$ елемента от ред 11. Аналогично, G съдържа $11.4 = 44$ елемента от ред 5. Следователно G е обединение на елементите си от ред 5, елементите си от ред 11 и неутралния си елемент. Това противоречи на съществуването на силова 3-подгрупа на G от ред 9 и доказва наличието на нормална силова подгрупа на G.

7 Алгебрични разширения на полета. Поле на разлагане. Теорема за примитивния елемент.

Задача 46. *Нека $K \supset F$ е крайно разширение на полета и $\alpha \in K$. Да се докаже, че α е алгебричен над F и степента на алгебричност $\deg_F \alpha$ на α над F дели степента $[K : F]$ на разширението $K \supset F$.*

Упътване: Ако $[K : F] \in \mathbb{N}$ и $\alpha \in K$, то редицата от разширения $F \subseteq F(\alpha) \subseteq K$ има степен $[K : F] = [K : F(\alpha)][F(\alpha) : F]$ за някои естествени $[K : F(\alpha)]$ и $[F(\alpha) : F]$. Оттук, α е алгебричен над F и степента на алгебричност $\deg_F \alpha = [F(\alpha) : F]$ на α над F дели $[K : F]$.

Задача 47. *Нека $F \subseteq K \subseteq L$ е редица от разширения на полета и $\alpha \in L$. Да се докаже, че ако α е алгебричен над F, то α е алгебричен над K и минималният полином на α над K дели минималния полином на α над F в пръстена $K[x]$.*

Упътване: Нека $f(x) \in F[x]$ е минималният полином на α над F. Тогава $f(x) \in K[x]$ и неразложимият над K множител $g(x) \in K[x]$ на $f(x)$ с корен α и старши коефициент 1 е минималният полином на α над K.

Задача 48. *Нека F е числово поле, а $\alpha \in \mathbb{C}$ е алгебрично над F комплексно число с нечетна степен на алгебричност $\deg_F \alpha$. Да се докаже, че полетата $F(\alpha) = F(\alpha^2)$ съвпадат.*

Решение: Ако в редицата от разширения $F \subseteq F(\alpha^2) \subseteq F(\alpha)$ има нечетна степен $[F(\alpha^2) : F][F(\alpha) : F(\alpha^2)] = [F(\alpha) : F] = \deg_F \alpha = 2n + 1$, то $[F(\alpha) : F(\alpha_2)]$ е нечетно естествено число. Елементът $\alpha \in F(\alpha) = F(\alpha^2)(\alpha)$ е корен на полинома $x^2 - \alpha^2 \in F(\alpha^2)[x]$, така че степента на алгебричност $\deg_{F(\alpha^2)} \alpha = [F(\alpha) : F(\alpha^2)] \leq 2$. Единственото нечетно естествено $[F(\alpha) : F(\alpha^2)]$, ненадминаващо 2 е $[F(\alpha) : F(\alpha^2)] = 1$, откъдето $F(\alpha) = F(\alpha^2)$.

Задача 49. *Нека $K \supset F$ е разширение на полета от степен $[K : F] = 2$ с характеристика $\mathrm{char}(F) = \mathrm{char}(K) \neq 2$. Да се докаже, че съществува примитивен елемент $\theta \in K$ на $K = F(\theta)$ с $\theta^2 \in F$.*

Решение: За произволен елемент $\alpha \in K \setminus F$ разглеждаме редицата от разширения $F \subset F(\alpha) \subseteq K$. Съгласно $2 = [K : F] = [K : F(\alpha)][F(\alpha) : F]$ степента $[F(\alpha) : F] \in \mathbb{N}$ е делител на 2. Ако $[F(\alpha) : F] = 1$, то $F(\alpha) = F$ и $\alpha \in F$, противно на избора на $\alpha \notin F$. Следователно $\deg_F \alpha = [F(\alpha) : F] = 2$ и минималният полином $f(x) \in F[x]$ на α над F е от степен 2. Освен това, $[K : F(\alpha)] = 1$ показва, че $K = F(\alpha)$. Квадратният тричлен $f(x) = x^2 + bx + c \in F[x]$ има дискриминанта $D = b^2 - 4c \in F$. Ако $\mathrm{char} F \neq 2$, то корените на $f(x)$ са

$$\alpha_1, 2 = (-b \pm \sqrt{D})2^{-1} \in F(\sqrt{D}).$$

Следователно $F(\theta) \subseteq F(\sqrt{D})$, доколкото полето $F(\sqrt{D})$ е затворено относно събиране, изваждане, умножение и деление с ненулев елемент. От друга страна, $\sqrt{D} = 2\alpha + b \in F(\alpha)$ дава $F(\sqrt{D}) \subseteq F(\alpha)$, откъдето $F(\alpha) = F(\sqrt{D})$. Примитивният елемент $\theta := \sqrt{D}$ на $K = F(\alpha)$ има квадрат $\theta^2 = D \in F$.

Следствие 50. (от Теоремата за примитивния елемент) *Нека $F \subset \mathbb{C}$ е числово поле, α и β са алгебрични над F комплексни числа. Нека $f(x) \in F[x]$ е минималният полином на α над F с различни корени $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$, а $g(x) \in F[x]$ е минималният полином на β над F с различни корени $\beta_1 = \beta, \beta_2, \ldots, \beta_m$. Образуваме комплексните числа*

$$\gamma_{ij} = -\frac{\alpha_i - \alpha_1}{\beta_j - \beta_1} \quad \textit{за} \quad \forall 1 \leq i \leq n, \quad \forall 2 \leq j \leq m$$

и избираме $c \in F \setminus \{\gamma_{ij} \,|\, 1 \leq i \leq n, 2 \leq j \leq m\}$. По Теоремата за примитивния елемент, $F(\alpha, \beta) = F(\theta)$ за $\theta = \alpha + c\beta$. Нека

$$h(x) = f(x - c\beta_1)f(x - c\beta_2)\ldots f(x - c\beta_m).$$

Тогава:

(i) $h(x)$ е полином с коефициенти от F;

(ii) минималният полином $f_\theta(x) \in F[x]$ на θ над F дели $h(x)$;

(iii) ако $[F(\alpha, \beta) : F] = [F(\alpha) : F][F(\beta) : F]$, то $f_\theta(x) = h(x)$ съвпадат.

Доказателство: (i) По определение, полиномът $h(x) \in F[\beta_1, \ldots, \beta_m][x]$ е симетричен относно $\beta_1, \ldots, \beta_m$. Съгласно Основната теорема за симетричните полиноми и формулите на Виет за $g(x)$, $F[\beta_1, \ldots, \beta_m]^{S_m} = F$ и $h(x) \in F[x]$.

(ii) Числото θ е корен на полинома $f(x - c\beta_1)$, защото $f(\theta - c\beta_1) = f(\alpha) = 0$. Следователно $h(\theta) = 0$ и минималният полином $f_\theta(x) \in F[x]$ на θ над F дели $h(x)$.

(iii) Ако $\deg_F \theta = [F(\theta) : F] = [F(\alpha, \beta) : F] = [F(\alpha) : F][F(\beta) : F] = nm$, то $\deg f_\theta(x) = nm = \deg h(x)$ и $f_\theta(x) = h(x)$, защото $h(x)$ има старши коефициент 1.

Задача 51. *Нека α е корен на полинома $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$ и $K = \mathbb{Q}(\alpha)$. Да се докаже, че степента $[K : \mathbb{Q}] = 3$ и числата $1, \alpha, \alpha^2$ образуват базис на K над $\mathbb{Q}$. Да се изразят чрез този базис числата α^5, $\beta = \alpha^6 - 3\alpha^5 - 2\alpha^4 + \alpha + 1$ и $\gamma = \frac{1}{\alpha^2 - 1}$.*

Решение: Достатъчно е да докажем неразложимостта на $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$ над $\mathbb{Q}$, за да твърдим, че $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg_{\mathbb{Q}} \alpha = 3$. Ако $f(x) = x^3 - 3x - 1 \in \mathbb{Z}[x]$ от степен $\deg(f) = 3$ е разложим над $\mathbb{Q}$, то $f(x)$ е разложим над $\mathbb{Z}$ и има цял корен s. Коренът $s \in \{1, -1\}$ в качеството си на делител на свободния член -1 на $f(x)$. От $f(1) = -3 \neq 0$ и $f(-1) = 1 \neq 0$ следва, че $f(x) \in \mathbb{Z}[x]$ е неразложим над $\mathbb{Z}$ и над $\mathbb{Q}$. Още повече, $f(x) \in \mathbb{Q}[x]$ е минималният полином на α над $\mathbb{Q}$ и $1, \alpha, \alpha^2$ са линейно независими над $\mathbb{Q}$. Всеки три линейно независими вектора от тримерно линейно пространство образуват базис на това пространство.

От $f(\alpha) = 0$ получаваме, че $\alpha^3 = 3\alpha + 1$. Почленното умножение с α дава $\alpha^4 = 3\alpha^2 + \alpha$. Сега

$$\alpha^5 = \alpha^4.\alpha = 3\alpha^3 + \alpha^2 = 3(3\alpha + 1) + \alpha^2 = \alpha^2 + 9\alpha + 3.$$

По-нататък,

$$\alpha^6 = \alpha^5.\alpha = \alpha^3 + 9\alpha^2 + 3\alpha = 9\alpha^2 + 6\alpha + 1.$$

Следователно

$$\beta = \alpha^6 - 3\alpha^5 - 2\alpha^4 + \alpha + 1 = -22\alpha - 7.$$

Полиномът $g(x) = x^2 - 1 \in \mathbb{Q}[x]$ е взаимно прост с полинома $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$, защото корените ± 1 на $g(x)$ не са корени на $f(x)$. По алгоритъма на Евклид за намиране на най-голям общ делител и реализация на тъждеството на Безу, извършваме последователно деление

$$f(x) = xg(x) + (-2x - 1),$$

$$g(x) = (-2x - 1)\left(-\frac{1}{2}x + \frac{1}{4}\right) - \frac{3}{4}.$$

След почленно умножение на второто равенство с $-\frac{4}{3}$ имаме

$$-\frac{4}{3}g(x) = (-2x - 1)\left(\frac{2}{3}x - \frac{1}{3}\right) + 1.$$

Оттук,

$$1 = (-2x - 1)\left(-\frac{2}{3}x + \frac{1}{3}\right) - \frac{4}{3}g(x) = [f(x) - xg(x)]\left(-\frac{2}{3}x + \frac{1}{3}\right) - \frac{4}{3}g(x) =$$

$$= \left(-\frac{2}{3}x + \frac{1}{3}\right) f(x) + \left(\frac{2}{3}x^2 - \frac{1}{3}x - \frac{4}{3}\right) g(x).$$

Заместването с α в последното равенство дава $1 = \left(\frac{2}{3}\alpha^2 - \frac{1}{3}\alpha - \frac{4}{3}\right) g(\alpha)$. Следователно

$$\gamma = \frac{1}{g(\alpha)} = \frac{2\alpha^2 - \alpha - 4}{3}.$$

Задача 52. *Нека* $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(i) Да се докаже, че степента $[K : \mathbb{Q}] = 4$ *и числата* $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ *образуват базис на* K *над* $\mathbb{Q}$.

(ii) Да се намери примитивен елемент θ *на разширението* $\mathbb{Q} \subset K$ *и минималният полином на* θ *над* $\mathbb{Q}$. *Да се изразят числата* $\sqrt{2}, \sqrt{3}, \sqrt{6}$ *чрез базиса* $1, \theta, \theta^2, \theta^3$ *на полето* K *над полето* $\mathbb{Q}$ *на рационалните числа.*

Решение: (i) Редицата от разширения $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ има степен $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[K : \mathbb{Q}(\sqrt{2})]$, защото $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ е ирационално число. Твърдим, че разширението $K = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \supset \mathbb{Q}(\sqrt{2})$ е от степен 2. По-точно, $\sqrt{3}$ е корен на полинома $x^2 - 3 \in \mathbb{Q}[x] \subset \mathbb{Q}(\sqrt{2})[x]$, така че $[K : \mathbb{Q}(\sqrt{2})] = \deg_{\mathbb{Q}(\sqrt{2})} \sqrt{3} \leq 2$. Допускането $\deg_{\mathbb{Q}(\sqrt{2})} \sqrt{3} = 1$ води до $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Тогава $\sqrt{3} = a + b\sqrt{2}$ за подходящи $a, b \in \mathbb{Q}$ и $3 = (\sqrt{3})^2 = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$. При $ab \neq 0$ получаваме $\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}$, което е проитворечие. Ако $a = 0$, то $b = \sqrt{\frac{3}{2}} \in \mathbb{Q}$ е противоречие. За $b = 0$ имаме $\sqrt{3} \in \mathbb{Q}$, което не е вярно и доказва, че $[K : \mathbb{Q}(\sqrt{2})] = \deg_{\mathbb{Q}(\sqrt{2})} \sqrt{3} = 2$.

Твърдим, че числата $1, \sqrt{2}, \sqrt{3}, \sqrt{6} \in K$ са линейно независими над $\mathbb{Q}$. Да допуснем, че $a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} = 0$ за някои $a_i \in \mathbb{Q}$. Ако $(a_2, a_3) \neq (0, 0)$, то $\sqrt{3} = \frac{-a_0 - a_1\sqrt{2}}{a_2 + a_3\sqrt{2}} \in \mathbb{Q}(\sqrt{2})$ е противоречие. За $a_2 = a_3 = 0$ получаваме $a_0 + a_1\sqrt{2} = 0$, откъдето $a_0 = a_1 = 0$ съгласно $\sqrt{2} \notin \mathbb{Q}$. Линейно независимите над $\mathbb{Q}$ числа $1, \sqrt{2}, \sqrt{3}, \sqrt{6} \in K$ образуват базис на четиримерното линейно пространство K над $\mathbb{Q}$.

(ii) Минималният полином на $\sqrt{2}$ над $\mathbb{Q}$ е $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ с корени $\alpha = \alpha_1 = \sqrt{2}$ и $\alpha_2 = -\sqrt{2}$. Минималният полином на $\sqrt{3}$ над $\mathbb{Q}$ е $g(x) = x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$ с корени $\beta = \beta_1 = \sqrt{3}$ и $\beta_2 = -\sqrt{3}$. Избираме

$$c \in \mathbb{Q} \setminus \left\{ -\frac{\alpha_1 - \alpha_1}{\beta_2 - \beta_1}, \quad -\frac{\alpha_2 - \alpha_1}{\beta_2 - \beta_1} \right\} = \mathbb{Q} \setminus \left\{ 0, \quad -\sqrt{\frac{2}{3}} \right\},$$

например $c = 1$ и получаваме примитивен елемент $\theta = \alpha + c\beta = \sqrt{2} + \sqrt{3}$ на K над $\mathbb{Q}$. Съгласно

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4 = 2.2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}],$$

можем да приложим Следствие 50 и да получим, че

$$h(x) = f(x - c\beta_1) f(x - c\beta_2) = f(x - \sqrt{3}) f(x + \sqrt{3}) = (x^2 - 2\sqrt{3}x + 1)(x^2 + 2\sqrt{3}x + 1) =$$

$$= (x^2 + 1)^2 - (2\sqrt{3}x)^2 = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$$

е минималният полином на $\theta = \sqrt{2} + \sqrt{3}$ над $\mathbb{Q}$.

За да изразим $\sqrt{2}, \sqrt{3}, \sqrt{6}$ чрез базиса $1, \theta, \theta^2, \theta^3$ на $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\theta)$ над $\mathbb{Q}$ пресмятаме

$$\theta^2 = 5 + 2\sqrt{6} \quad \text{и} \quad \theta^3 = 11\sqrt{2} + 9\sqrt{3}.$$

Елиминирането на $\sqrt{3}$ от

$$\theta = \sqrt{2} + \sqrt{3}$$
$$\theta^3 = 11\sqrt{2} + 9\sqrt{3}$$

дава $\theta^3 - 9\theta = 2\sqrt{2}$, откъдето

$$\sqrt{2} = \frac{1}{2}\theta^3 - \frac{9}{2}\theta.$$

Елиминирането на $\sqrt{2}$ от същите равенства води до $\theta^3 - 11\theta = -2\sqrt{3}$ и

$$\sqrt{3} = -\frac{1}{2}\theta^3 + \frac{11}{2}\theta.$$

Накрая, от $\theta^2 = 5 + 2\sqrt{6}$ изразяваме

$$\sqrt{6} = \frac{1}{2}\theta^2 - \frac{5}{2}.$$

8 Циклотомични полиноми и крайни полета.

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. Полиномът $\Phi_n(x) \in \mathbb{Z}[x]$ е неразложим над $\mathbb{Z}$ и над $\mathbb{Q}$.

Задача 53. *Да се намерят циклотомичните полиноми:*
(i) $\Phi_p(x)$ *за просто число* p; *(ii)* $\Phi_4(x)$; *(iii)* $\Phi_8(x)$; *(iv)* $\Phi_{15}(x)$.

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

Задача 54. *Нека* $\mathbb{Q}_n$ *е полето на разлагане на циклотомочния полином* $\Phi_n(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ *над полето* $\mathbb{Q}$ *на рационалните числа. Да се докаже, че степента*

$$[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$$

е равна на функцията на Ойлер $\varphi(n)$*, която по определение е броят на взаимно простите с* n *естествени числа от* 1 *до* n *включително.*

Решение: Ако $\omega = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$, то корените на $\Phi_n(x)$ образуват множеството $R_n = \{\omega^k \mid 1 \leq k \leq n,\ (k,n) = 1\}$. Полето на разлагане

$$\mathbb{Q}_n = \mathbb{Q}(\omega^k \mid 1 \leq k \leq n,\ (k,n) = 1) = \mathbb{Q}(\omega)$$

на Φ_n над $\mathbb{Q}$ се поражда от ω, защото $\omega^k \in \mathbb{Q}(\omega)$ за $\forall k \in \mathbb{N}$. Степента

$$[\mathbb{Q}_n : \mathbb{Q}] = \deg_{\mathbb{Q}} \omega = \deg \Phi_n = \varphi(n),$$

защото циклотомичният полином $\Phi_n(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ е минималният полином на ω над $\mathbb{Q}$ в качеството си на неразложим над $\mathbb{Q}$ полином със старши коефициент 1 и корен ω.

Задача 55. *Нека α е корен на полинома $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ и $K = \mathbb{Q}(\alpha)$. Да се докаже, че степента $[K : \mathbb{Q}] = 4$ и числата $1, \alpha, \alpha^2, \alpha^3$ образуват базис на K над $\mathbb{Q}$. Да се изрази чрез този бази числото $\beta = \frac{\alpha^2}{\alpha^2+\alpha+1}$.*

Решение: Известно е, че $\deg_{\mathbb{Q}} \alpha = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}] = 4$ точно когато полиномът $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}[x]$ е неразложим над $\mathbb{Q}$. Понеже $f(x) = \Phi_5(x) \in \mathbb{Z}[x]$ е циклотомичният полином на примитивните пети корени на единицата, $f(x)$ е неразложим над $\mathbb{Z}$ и над $\mathbb{Q}$. В резултат, $f(x)$ е минималният полином на α над $\mathbb{Q}$, $1, \alpha, \alpha^2, \alpha^3$ са линейно независими над $\mathbb{Q}$ и образуват базис на $K = \mathbb{Q}(\alpha)$ над $\mathbb{Q}$.

Циклотомичният полином $g(x) = x^2 + x + 1 = \Phi_3(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ на примитивните трети степени на единицата е взаимно прост с $f(x) = \Phi_5(x)$. По алгоритъма на Евклид за намиране на най-голям общ делител на два полинома и реализиране на тъждеството на Безу за тях, делим последователно

$$\Phi_5(x) = x^2\Phi_3(x) + x + 1,$$

$$\Phi_3(x) = (x + 1)x + 1.$$

Оттук,

$$1 = \Phi_3(x) - x(x + 1) = \Phi_3(x) - x[\Phi_5(x) - x^2\Phi_3(x)] = -x\Phi_5(x) + (x^3 + 1)\Phi_3(x).$$

Заместваме с корена α на $\Phi_5(x)$ и получаваме, че $1 = (\alpha^3 + 1)\Phi_3(x)$. Следователно

$$\frac{1}{\Phi_3(\alpha)} = \frac{1}{\alpha^2 + \alpha + 1} = \alpha^3 + 1$$

и

$$\beta = \frac{\alpha^2}{\alpha^2 + \alpha + 1} = \alpha^2(\alpha^3 + 1) = \alpha^5 + \alpha^2 = \alpha^2 + 1,$$

защото α е корен на полинома $(x - 1)\Phi_5(x) = x^5 - 1$.

Задача 56. *Нека K е полето на разлагане на полинома $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ над полето $\mathbb{Q}$ на рационалните числа.*

(i) Да се докаже, че $K = \mathbb{Q}(\alpha, \omega)$, където $\alpha \in \mathbb{R}$, $\alpha^3 = 2$, а ω е примитивен трети корен на единицата.

(ii) Да се намери примитивен елемент θ на разширението $\mathbb{Q} \subset K$ и минималният полином на θ над $\mathbb{Q}$.

Решение: (i) Ако $\alpha = \sqrt[3]{2} \in \mathbb{R}$ и $\omega = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, то корените на $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ са $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ и полето на разлагане на $f(x)$ над $\mathbb{Q}$ е $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Разглеждаме редицата от разширения

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega).$$

От една страна, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, защото полиномът $x^3 - 2 \in \mathbb{Q}[x]$ с корен $\sqrt[3]{2}$ е неразложим над $\mathbb{Q}$, т.е. няма рационален корен. От друга страна, ω е корен на циклотомичния полином $\Phi_3(x) = x^2 + x + 1 \in \mathbb{Z}[x]$, така че $\deg_{\mathbb{Q}(\sqrt[3]{2})} \omega \leq \deg_{\mathbb{Q}} \omega = 2$. Ако $\deg_{\mathbb{Q}(\sqrt[3]{2})} \omega = 1$, то $\omega \in \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, което е противоречие. Следователно $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = \deg_{\mathbb{Q}(\sqrt[3]{2})} \omega = 2$ и

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 3.2 = 6.$$

(ii) Минималният полином на $\sqrt[3]{2} \in \mathbb{R}$ над $\mathbb{Q}$ е $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ с корени $\alpha_1 = \alpha = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\omega$, $\alpha_3 = \sqrt[3]{2}\omega^2$. Минималният полином на ω над $\mathbb{Q}$ е $\Phi_3(x)$ с корени $\beta_1 = \beta = \omega$ и $\beta_2 = \omega^2$. Разглеждаме числата

$$-\frac{\alpha_1 - \alpha_1}{\beta_2 - \beta_1} = 0, \quad -\frac{\alpha_2 - \alpha_1}{\beta_2 - \beta_1} = -\sqrt[3]{2}\omega^2, \quad -\frac{\alpha_3 - \alpha_1}{\beta_2 - \beta_1} = \sqrt[3]{2}\omega$$

и избираме $c = 1 \in \mathbb{Q} \setminus \{0, -\sqrt[3]{2}\omega^2, \sqrt[3]{2}\omega\}$, $\theta = \alpha + c\beta = \sqrt[3]{2} + \omega$. Вземайки предвид $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6 = 3.2 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][\mathbb{Q}(\omega) : \mathbb{Q}]$, прилагаме Следствие 50 и получаваме, че минималният полином на $\theta = \sqrt[3]{2} + \omega$ над $\mathbb{Q}$ е

$$h(x) = f(x - c\beta_1)f(x - c\beta_2) = f(x - \omega)f(x - \omega^2) =$$

$$= (x^3 - 3\omega x^2 + 3\omega^2 x - 3)(x^3 - 3\omega^2 x^2 + 3\omega x - 3) =$$

$$= (x^3 - 3)^2 + (x^3 - 3)(-3\omega x^2 + 3\omega^2 x - 3\omega^2 x^2 + 3\omega x) + 3\omega x(\omega - x)3\omega x(1 - \omega x) =$$

$$= (x^3 - 3)^2 + (x^3 - 3)(3x^2 - 3x) + 9\omega^2 x^2 \omega(x^2 + x + 1) =$$

$$= x^6 - 6x^3 + 9 + 3x^5 - 3x^4 - 9x^2 + 9x + 9x^4 + 9x^3 + 9x^2 = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9$$

Задача 57. *Нека K е полето на разлагане на полинома $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ над $\mathbb{Q}$.*

(i) Да се докаже, че $K = \mathbb{Q}(\alpha, i)$ за $\alpha \in \mathbb{R}$ с $\alpha^4 = 2$ и имагинерната единица i, а степента $[K : \mathbb{Q}] = 8$.

(ii) Да се намери примитивен елемент на разширението $\mathbb{Q} \subset K$ и минималният полином на θ над $\mathbb{Q}$.

Решение: (i) Ако $\sqrt[4]{2} \in \mathbb{R}$, то корените на полинома $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ са $\sqrt[4]{2}, -\sqrt[4]{2}$, $\sqrt[4]{2}i$, $-\sqrt[4]{2}i$, където i е имагинерната единица, $i^2 = -1$. Следователно $K = \mathbb{Q}(\sqrt[4]{2}, i)$ е полето на разлагане на $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ над $\mathbb{Q}$. Редицата от разширения

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$$

има степен $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = \deg_{\mathbb{Q}} \sqrt[4]{2} = 4$, съгласно неразложимостта на $f(x) = x^4 - 2$ над $\mathbb{Q}$. Минималният полином на имагинерната единица i над $\mathbb{Q}$ е $\Phi_4(x) = x^2 + 1 \in$

$\mathbb{Z}[x] \subset \mathbb{Q}[x]$, така че $\deg_{\mathbb{Q}(\sqrt[4]{2})} i \leq \deg_{\mathbb{Q}} i \leq 2$. Ако $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = \deg_{\mathbb{Q}(\sqrt[4]{2})} i = 1$, то $i \in \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ е противоречие. Следователно $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$ и

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 4.2 = 8.$$

(ii) Минималният полином на $\sqrt[4]{2} \in \mathbb{R}$ над $\mathbb{Q}$ е $f(x) = x^4 - 2$ с корени $\alpha_1 = \alpha = \sqrt[4]{2}$, $\alpha_2 = -\sqrt[4]{2}$, $\alpha_3 = \sqrt[4]{2}i$, $\alpha_4 = -\sqrt[4]{2}i$. Минималният полином на i над $\mathbb{Q}$ е $\Phi_4(x) = x^2 + 1$ с корени $\beta_1 = \beta = i$, $\beta_2 = -i$. Разглеждаме комплексните числа

$$-\frac{\alpha_1 - \alpha_1}{\beta_2 - \beta_1} = 0, \quad -\frac{\alpha_2 - \alpha_1}{\beta_2 - \beta_1} = \sqrt[4]{2}i, \quad -\frac{\alpha_3 - \alpha_1}{\beta_2 - \beta_1} = \frac{\sqrt[4]{2}}{2}(1 + i), \quad -\frac{\alpha_4 - \alpha_1}{\beta_2 - \beta_1} = \frac{\sqrt[4]{2}}{2}(-1 + i)$$

и избираме $c = 1 \in \mathbb{Q} \setminus \left\{0,\ \sqrt[4]{2}i,\ \frac{\sqrt[4]{2}}{2}(1 + i),\ \frac{\sqrt[4]{2}}{2}(-1 + i)\right\}$, $\theta = \alpha + c\beta = \sqrt[4]{2} + i$. Съгласно $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}][\mathbb{Q}[i] : \mathbb{Q}]$, минималният полином на $\theta = \sqrt[4]{2} + i$ над $\mathbb{Q}$ е

$$h(x) = f(x - c\beta_1)f(x - c\beta_2) = f(x - i)f(x + i) =$$

$$= (x^4 - 4ix^3 - 6x^2 + 4ix - 1)(x^4 + 4ix^3 - 6x^2 - 4ix - 1) = (x^4 - 6x^2 - 1)^2 - [4ix(x^2 - 1)]^2 =$$

$$= x^8 + 36x^4 + 1 - 12x^6 - 2x^4 + 12x^2 + 16x^2(x^4 - 2x^2 + 1) = x^8 + 4x^6 + 2x^4 + 28x^2 + 1.$$

Задача 58. *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*

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

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

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

Упътване: Използвайте, че

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

Задача 59. *Да се докаже, че полиномите*

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

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 60. *Да се докаже, че полиномите*

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

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.

Задача 61. *Нека p е просто числ, $n \in \mathbb{N}$ е естествено число, $q = p^n$ и $\mathbb{F}_q$ е полето с q елемента. Да се докаже, че:*

(i) за всяко естествено число m полето $\mathbb{F}_{q^m}$ е полето на разлагане на полинома $f(x) = x^{q^m} - x \in \mathbb{F}_q[x]$ над $\mathbb{F}_q$ и съвпада с множеството на кореният на $f(x)$;

(ii) всяко крайно разширение $\mathbb{F}_q \subset K$ има примитивен елемент;

(iii) за всяко естествено число m съществува неразложим над $\mathbb{F}_q$ полином $g(x) \in \mathbb{F}_q[x]$ от степен m;

(iv) полето $\mathbb{F}_{q^m}$ е поле на разлагане на кой и да е неразложим над $\mathbb{F}_q$ полином $g(x) \in \mathbb{F}_q[x]$ от степен m;

(v) ако $g(x) \in \mathbb{F}_q[x]$ е неразложим над $\mathbb{F}_q$ полином от степен $m \in \mathbb{N}$ и $\alpha \in \mathbb{F}_{q^m}$ е корен на $g(x)$, то $\alpha^q \in \mathbb{F}_{q^m}$ е корен на $g(x)$;

(vi) ако $m, t \in \mathbb{N}$ и $g(x) \in \mathbb{F}_q[x]$ е неразложим над $\mathbb{F}_q$ полином от степен m, то $g(x)$ дели полинома $x^{q^t} - x$ тогава и само тогава, когато естественото число m дели естественото число t.

Решение: (i) Полето $\mathbb{F}_{q^m}$ съвпада с множеството $\{\alpha_1, \ldots, \alpha_{q^m}\}$ на кореният на полинома $f(x) = x^{q^m} - x \in \mathbb{F}_p[x] \subset \mathbb{F}_q[x]$ и с полето на разлагане $\mathbb{F}_p(\alpha_1, \ldots, \alpha_{q^m})$ на $f(x)$ над простото подполе $\mathbb{F}_p = \mathbb{Z}_p$ на $\mathbb{F}_{q^m}$. Подполето $\mathbb{F}_q$ на $\mathbb{F}_{q^m}$ съдържа простото поле $\mathbb{F}_p$, така че

$$\mathbb{F}_q(\alpha_1, \ldots, \alpha_{q^m}) \supseteq \mathbb{F}_p(\alpha_1, \ldots, \alpha_{q^m}) = \{\alpha_1, \ldots, \alpha_{q^m}\} = \mathbb{F}_{q^m}.$$

От друга страна, от $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ и $\alpha_1, \ldots, \alpha_{q^m} \in \mathbb{F}_{q^m} = \{\alpha_1, \ldots, \alpha_{q^m}\}$ получаваме включването $\mathbb{F}_q(\alpha_1, \ldots, \alpha_{q^m}) \subseteq \mathbb{F}_{q^m}$, защото полето $\mathbb{F}_{q^m}$ е затворено относно събиране, изваждане, умножение и деление с ненулев елемент. Следователно полето на разлагане $\mathbb{F}_q(\alpha_1, \ldots, \alpha_{q^m}) = \mathbb{F}_{q^m}$ на $f(x)$ над $\mathbb{F}_q$ съвпада с множеството $\mathbb{F}_{q^m} = \{\alpha_1, \ldots, \alpha_{q^m}\}$ на кореният на $f(x)$.

(ii) По определение, всяко крайно разширение K на $\mathbb{F}_q$ е крайномерно линейно пространство над $\mathbb{F}_q$, а оттам и крайно поле $K = \mathbb{F}_{q^m}$ за $m = \dim_{\mathbb{F}_q} K = [K : \mathbb{F}_q]$. Мултипликативната група K^* на K е циклична. Ако $\theta \in K^*$ е пораждащ на K^*, то $K = \{0, \theta, \theta^2, \ldots, \theta^{q^m-1} = 1\} \subseteq \mathbb{F}_q(\theta)$. Обратно, $\mathbb{F}_q(\theta) \subseteq K$, защото $\mathbb{F}_q$ е подполе на K, $\theta \in K$ и полето K е затворено относно събиране, изваждане, умножение и деление с ненулев елемент. Следователно полето $K = \mathbb{F}_q(\theta)$ има примитивен елемент θ над $\mathbb{F}_q$.

(iii) За произволно естествено число m да изберем пораждащ θ на мултипликативната група $\mathbb{F}^*_{q^m}$ на полето $\mathbb{F}_{q^m}$ с q^m елемента. Съгласно (ii), θ е примитивен елемент на $\mathbb{F}_{q^m} = \mathbb{F}_q(\theta)$ над $\mathbb{F}_q$. Следователно $m = [\mathbb{F}_{q^m} : \mathbb{F}_q] = \deg_{\mathbb{F}_q} \theta$ съвпада със степента на алгебричност на θ над $\mathbb{F}_q$. Оттук, минималният полином $f_\theta(x) \in \mathbb{F}_q[x]$ на θ над $\mathbb{F}_q$ е от степен $\deg f_\theta(x) = \deg_{\mathbb{F}_q} \theta = m$. Полиномът $f_\theta(x)$ е неразложим над $\mathbb{F}_q$, защото в противен случай степента на алгебричност на θ над $\mathbb{F}_q$ е строго по-малка от m.

(iv) Нека $g(x) \in \mathbb{F}_q[x]$ е неразложим над $\mathbb{F}_q$ полином от степен $\deg(g) = m$ и α е корен на $g(x)$ в подходящо разширение на $\mathbb{F}_q$. Тогава

$$[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg_{\mathbb{F}_q} \alpha = \deg(g) = m$$

и полето $\mathbb{F}_q(\alpha)$ има q^m елемента. С точност до изоморфизъм, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Нека $\alpha_1 = \alpha$, $\alpha_2, \ldots, \alpha_m$ са всички корени на $g(x)$ в подходящо разширение на $\mathbb{F}_q$. Горните разглеждания доказват, че произволен корен α_i, $1 \leq i \leq m$ се съдържа в полето $\mathbb{F}_{q^m}$. Следователно

полето на разлагане $\mathbb{F}_q(\alpha_1,\ldots,\alpha_m) \subseteq \mathbb{F}_{q^m}$ на $g(x)$ над $\mathbb{F}_q$ се съдържа в $\mathbb{F}_{q^m}$. От друга страна,

$$\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha) = \mathbb{F}_q(\alpha_1) \subseteq \mathbb{F}_q(\alpha_1,\ldots,\alpha_m),$$

така че $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha_1,\ldots,\alpha_m)$ е полето на разлагане на $g(x)$ над $\mathbb{F}_q$.

(v) Ако $g(x) = \sum\limits_{i=0}^{m} a_i x^i \in \mathbb{F}_q[x]$, то $a_i^q = a_i$ за $\forall 0 \leq i \leq m$, защото полето $\mathbb{F}_q$ се състои от корените на полинома $x^q - x$. Условието $0 = g(\alpha) = \sum\limits_{i=0}^{m} a_i \alpha^i$ води до

$$0 = g(\alpha)^q = \left(\sum_{i=0}^{m} a_i \alpha^i\right)^q = \sum_{i=0}^{m} a_i^q \alpha^{iq} = \sum_{i=0}^{m} a_i (\alpha^q)^i = g(\alpha^q),$$

съгласно Задача 16.

(vi) От условие (iv) знаем, че ако $g(x) \in \mathbb{F}_q[x]$ е неразложим над $\mathbb{F}_q$ полином от степен m, то $\mathbb{F}_{q^m}$ е полето на разлагане на $g(x)$ над $\mathbb{F}_q$. Полиномът $g(x)$ дели полинома $x^{q^t} - x$ точно когато всички корени $\alpha_1,\ldots,\alpha_m$ на $g(x)$ принадлежат на множеството $\mathbb{F}_{q^t}$ на корените на $x^{q^t} - x$. Понеже $\mathbb{F}_q$ е подполе на $\mathbb{F}_{q^t}$, условието $\alpha_1,\ldots,\alpha_m \in \mathbb{F}_{q^t}$ е еквивалентно на $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha_1, \ddots, \alpha_m) \subseteq \mathbb{F}_{q^t}$. Крайното поле $\mathbb{F}_{q^m}$ е подполе на крайното поле $\mathbb{F}_{q^t}$ тогава и само тогава, когато естественото число m дели есетственото число t.

Задача 62. *Нека p е просто число, а $\overline{\mathbb{F}_p} = \cup_{m=1}^{\infty} \mathbb{F}_{p^m}$ е обединението на крайните полета с халактеристика p. Да се докаже, че $\overline{\mathbb{F}_p}$ е алгебрично затворено поле с халактеристика p.*

Решение: Ако $x, y \in \overline{\mathbb{F}_p}$, то съществуват $m, n \in \mathbb{N}$, така че $x \in \mathbb{F}_{p^m}$, $y \in \mathbb{F}_{p^n}$. Съгласно $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{mn}}$ и $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^{mn}}$ имаме $x, y \in \mathbb{F}_{p^{mn}}$, токъдето $x + y, xy \in \mathbb{F}_{p^{mn}} \subset \overline{\mathbb{F}_p}$. По този начин, събирането и умножението в $\mathbb{F}_{p^k}$ за $\forall k \in \mathbb{N}$ задава събиране и умножение в $\overline{\mathbb{F}_p}$. Аксиомите за полето $\overline{\mathbb{F}_p}$ се свеждат до съответните аксиоми за подходящи крайни полета $\mathbb{F}_{p^k} \subset \overline{\mathbb{F}_p}$.

Произволен неконстантен полином $g(x) = \sum\limits_{i=0}^{n} a_i x^i \in \overline{\mathbb{F}_p}[x] \setminus \overline{\mathbb{F}_p}$ има краен брой коефициенти $a_i \in \mathbb{F}_{p^{m_i}}$, $0 \leq i \leq n$. За $m = m_0 m_1 \ldots m_n$ имаме $a_0, a_1, \ldots, a_n \in \mathbb{F}_{p^m}$, така че $g(x) \in \mathbb{F}_{p^m}[x]$. Нека $g(x) = g_1(x) \ldots g_k(x)$ е разлагането на $g(x)$ в произведение от неразложими над $\mathbb{F}_{p^m}$ множители $g_j(x) \in \mathbb{F}_{p^m}[x]$ от степен $\deg(g_j) = d_j \in \mathbb{N}$. Съгласно Задача 61 (iv), полето на разлагане на $g_j(x)$ над $\mathbb{F}_{p^m}$ е $\mathbb{F}_{p^{md_j}} \subset \overline{\mathbb{F}_p}$, така че всички корени на $g_j(x)$ се съдържат в $\overline{\mathbb{F}_p}$. Оттук, всички корени на $g(x)$ се съдържат в $\overline{\mathbb{F}_p}$ и полето $\overline{\mathbb{F}_p}$ е алгебрично затворено.

Задача 63. *Да се докоже, че:*

(i) за произволни $a \in \mathbb{F}_q \setminus \{1\}$ и $b \in \mathbb{F}_q$ полиномът $f(x) = x^q - ax + b \in \mathbb{F}_q[x]$ има единствен корен в $\mathbb{F}_q$;

(ii) полиномът $g(x) = x^q - x + b \in \mathbb{F}_q[x]$ с $b \neq 0$ няма корен в $\mathbb{F}_q$.

Решение: (i) Ако $x_o \in \mathbb{F}_q$ е корен на $f(x)$, то $x_o^q = x_o$ и

$$0 = f(x_o) = x_o^q - ax_o + b = x_o(1 - a) + b.$$

Оттук, $x_o = b(a-1)^{-1}$.

(ii) Ако допуснем, че $y_o \in \mathbb{F}_q$ е корен на $g(x)$, то $0 = g(y_o) = y_o^q - y_o + b = b$ води до противоречие с предположението $b \neq 0$.

Задача 64. *За произволно естествено число m да се докаже, че полиномът $g(x) = x^q - x + b \in \mathbb{F}_q[x]$ дели полинома $h(x) = x^{q^m} - x + mb \in \mathbb{F}_q[x]$.*

Решение: Полиномът $g(x)$ няма кратни корени, защото формалната производна $g'(x) = qx^{q-1} - 1 = -1 \in \mathbb{F}_q[x]$ няма общ корен с $g(x)$. Затова е достатъчно да проверим, че всеки корен α на $g(x)$ е корен на $h(x)$, за да твърдим, че $g(x)$ дели $h(x)$. Наистина, ако $\alpha^q = \alpha - b$, то

$$(\alpha^q)^q = (\alpha - b)^q = \alpha^q - b^q = (\alpha - b) - b = \alpha - 2b,$$

съгласно Задача 15 (i) и $b^q = b$ за $\forall b \in \mathbb{F}_q$. С индукция по $i \leq m$, ако $\alpha^{q^i} = \alpha - ib$, то

$$\alpha^{q^{i+1}} = (\alpha^{q^i})^q = (\alpha - ib)^q = \alpha^q - (ib)^q = (\alpha - b) - (ib) = \alpha - (i+1)b.$$

Следващата задача разглежда пример за безкрайно тяло, което не е поле.

Задача 65. *Дадено е множеството от матрици*

$$\mathbb{H} = \left\{ \begin{pmatrix} x & y \\ -\overline{y} & \overline{x} \end{pmatrix} \;\mid\; x, y \in \mathbb{C} \right\} \subset \mathbb{C}_{2\times 2}.$$

Да се докаже, че:

(i) $\mathbb{H}$ е некомутативно тяло относно обичайните операции събиране и умножение на матрици, което се нарича тяло на кватернионите;

(ii) $\mathbb{H}$ е линейно пространство над $\mathbb{R}$ с базис

$$E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix};$$

(iii) матриците $\pm E_2, \pm I, \pm J, \pm K$ образуват подгрупа на общата линейна група $Gl_2(\mathbb{C}) = \{X \in \mathbb{C}_{2\times 2} \;\mid\; \det(A) \neq 0\}$, наречена група на кватернионите $\mathbb{Q}_8$ със съотношения

$$I^2 = J^2 = K^2 = -E_2, \quad IJ = -JI = K, \quad JK = -KJ = I, \quad KI = -IK = J.$$

Упътване: Използвайти изброените съотношения, за да обосновете, че подмножеството $\mathbb{Q}_8 = \{\pm E_2, \pm I, \pm J, \pm K\} \subset Gl_2(\mathbb{C})$ е затворено относно умножение и обръщане.