Задаци из Алгебре 2 - Решења

1. Доказати да је скуп R један комутативни прстен са јединицом у односу на операције сабирања и множења матрица, где је

$$R = \left\{ \begin{pmatrix} a & 0 & b \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}.$$

Означимо матрицу $\begin{pmatrix} a & 0 & b \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$ са $M_{a,b}$ и приметимо да је $M_{a,b} + M_{c,d} = M_{a+c,b+d}$. Како матрица $M_{a+c,b+d}$ припада R, видимо да је тај скуп затворен у односу на операцију сабирања матрица. За исту операцију важи закон асоцијативности у скупу $\mathrm{M}_3(\mathbb{R})$, па важи и у $R \subseteq \mathrm{M}_3(\mathbb{R})$ (исто је за асоцијативност множења матрица у R, као и дистрибутивност множења у односу на сабирање). Нула матрица $M_{0,0} \in R$ је неутрални елемент, а $M_{-a,-b} + M_{a,b} = M_{0,0} = M_{a,b} + M_{-a,-b}$, где $M_{-a,-b} \in R$. Такође је $M_{a,b} + M_{c,d} = M_{a+c,b+d} = M_{c,d} + M_{a,b}$, па је $(R, +)$ комутативна група.

Што се тиче операције множења матрица, имамо да је $M_{a,b} \cdot M_{c,d} = M_{ac,ad+bc} \in R$, па је R затворен и у односу на множење. Јединична матрица $M_{1,0}$ припада R, а како је $M_{a,b} \cdot M_{c,d} = M_{ac,ad+bc} = M_{c,d} \cdot M_{a,b}$, следи да је R један комутативни прстен са јединицом.

2. Нека је p прост број и $R = \{\frac{m}{n} \in \mathbb{Q} \mid p \nmid n\}$. Доказати да је R један потпрстен са јединицом од $\mathbb{Q}$.

Нека су $\frac{m}{n}, \frac{m_1}{n_1} \in R$. Како је $\frac{m}{n} + \frac{m_1}{n_1} = \frac{mn_1+m_1n}{nn_1}$ и како nn_1 није дељиво са p јер то нису ни n, n_1 а p је прост број, следи да $\frac{m}{n} + \frac{m_1}{n_1}$ припада R. Очигледно је да $-\frac{m}{n}, \frac{mm_1}{nn_1}, \frac{1}{1} \in R$, за $\frac{m}{n}, \frac{m_1}{n_1} \in R$, па R јесте потпрстен са јединицом од $\mathbb{Q}$.

3. Доказати да је I један идеал у прстену R из 1. задатка, где је

$$I = \left\{ \begin{pmatrix} 0 & 0 & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \;\middle|\; c \in \mathbb{R} \right\}.$$

$M_{0,c} + M_{0,c_1} = M_{0,c+c_1} \in I$, за $M_{0,c}, M_{0,c_1} \in I$. Такође је $M_{a,b} \cdot M_{0,c} = M_{0,ac} \in I$, за $M_{a,b} \in R$ и $M_{0,c} \in I$, па I јесте један идеал у R.

4. Нека је R комутативни прстен са јединицом. Доказати да скуп нилпотентних елемената овог прстена чини један идеал у R.

Нека је

$$N(R) = \{x \in R \mid x^n = 0, \text{ за } n \in \mathbb{N}\}$$

скуп нилпотентних елемената прстена R. Ако су $x, y \in N(R)$ тада постоје $n, m \in \mathbb{N}$ тако да $x^n = 0$ и $y^m = 0$. Због комутативности прстена R, важи да

$$(x+y)^{n+m} = \binom{n+m}{0} x^{n+m} + \binom{n+m-1}{1} x^{n+m-1} y + \binom{n+m-2}{2} x^{m+n-2} y^2 +$$

$$\cdots + \binom{n+m}{m} x^n y^m + \binom{n+m}{m+1} x^{n-1} y^{m+1} + \cdots + \binom{n+m}{n+m-1} x y^{n+m-1} + \binom{n+m}{n+m} y^{n+m}.$$

Са друге стране, ако су $x \in N(R), r \in R$ и $x^n = 0$, тада је, узимајући у обзир комутативност прстена за R: $(rx)^n = r^n x^n = r^n \cdot 0 = 0$.

5. Нека је $x \in R$ нилпотентан елемент комутативног прстена са јединицом R. Доказати да је $1 - x$ инвертибилан.

   Како је x нилпотентан, постоји $n \in \mathbb{N}$ тако да $x^n = 0$. Приметимо да је

   $$(1-x)(1+x+x^2+\cdots+x^{n-1}) = 1-x+x-x^2+x^2-x^3+\cdots-x^{n-1}+x^{n-1}+x^n = 1.$$

   Како је $1 + x + x^2 + \cdots + x^{n-1} \in R$, следи да је $1 - x$ инвертибилан.

6. Доказати да је $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ потпрстен од $\mathbb{C}$ у коме је сваки не-нула елемент инвертибилан.

   Приметимо прво да је $a + b\sqrt{2} = 0$ акко $a = b = 0$. Нека су $a + b\sqrt{2}, a_1 + b_1\sqrt{2} \in R$ и важи да $a + b\sqrt{2} + a_1 + b_1\sqrt{2} = (a + a_1) + (b + b_1)\sqrt{2} \in R$, јер $a + a_,b + b_1 \in \mathbb{Q}$. Такође је и $-a - b\sqrt{2} \in R$, као и $1 = 1 + 0 \cdot \sqrt{2} \in R$. Што се тиче производа, важи да

   $$(a + b\sqrt{2}) \cdot (a_1 + b_1\sqrt{2}) = (aa_1 + 2bb_1) + (ab_1 + a_1b)\sqrt{2} \in R,$$

   тако да R јесте један потпрстен са јединицом у $\mathbb{C}$.

   Нека је $a + b\sqrt{2} \in R \setminus \{0\}$. Треба доказати да је овај елемент инвертибилан. Ако је $(a + b\sqrt{2}) \cdot (a_1 + b_1\sqrt{2}) = 1$, тада је $(aa_1 + 2bb_1) + (ab_1 + a_1b)\sqrt{2} = 1$, то јест

   $$\begin{aligned} aa_1 + 2bb_1 &= 1 \\ ab_1 + a_1b &= 0. \end{aligned}$$

   Претпоставимо да $b \neq 0$. Тада из друге једнакости следи да $a_1 = -\frac{a}{b} \cdot b_1$, а потом из прве следи да $b_1(2b - \frac{a^2}{b}) = 1$. Следи да је $b_1 = \frac{b}{2b^2 - a^2}$, а онда је и $a_1 = -\frac{a}{2b^2 - a^2}$. Дакле, инверз је $-\frac{a}{2b^2 - a^2} + \frac{b}{2b^2 - a^2}\sqrt{2}$. Ако је $b = 0$, тада је инвез једнак $\frac{1}{a}$.

7. Нека је R комутативни прсен са јединицом и I, J су идеали у R. Ако важи да $R = I + J$, доказати да је $R = I^2 + J^2$.

   Јасно је да $I^2 + J^2 \subseteq R$. За обрнуту инклузију, довољно је доказати да $1 \in I^2 + J^2$. Из једнакости $R = I + J$ следи да $1 \in I + J$, па постоје $x \in I$ и $y \in J$ тако да $1 = x + y$. Пошто је

   $$1 = 1^3 = (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3, \qquad x^3, 3x^2y \in I^2, \qquad y^3, 3xy^2 \in J^2,$$

   следи да $1 \in I^2 + J^2$. Наиме, I^2 и J^2 су идеали којима припадају x^2 и y^2, редом. Тада је и $x^2y \in J^2$ и $xy^2 \in J^2$.

8. Нека је S потпрстен комутативног прстена са јединицом R и I идеал у R. Доказати да је $S + I$ потпрстен са јединицом од R.

   Нека су $x, y \in S + I$. Тада је $x = a + b$ и $y = a_1 + b_1$ за $a, a_1 \in S$ и $b, b_1 \in I$. Како је S потпрстен, важи да $a + a_1 \in S$, а како је I идеал, $b + b_1 \in I$. Тако да је $x + y \in S + I$. За $x \in S + I$, то јест, $a + b \in S + I$, важи да $-a \in S$ и $-b \in I$, па је $-x \in S + I$. Даље, ако су $a + b, a_1 + b_1 \in S + I$, важи да $(a + b)(a_1 + b_1) = aa_1 + ab_1 + ba_1 + bb_1$, где је $aa_1 \in S$ и $ab_1, ba_1, bb_1 \in I$, па је цео збир елемент у $S + I$. Коначно, $1 = 1 + 0 \in S + I$, па следи да $S + I$ јесте један комутативни прстен са јединицом.

9. Доказати да пресек два потпрстена са јединицом јесте потпрстен, као и да унија то не мора бити.

   Нека су S_1 и S_2 потпрстени од R. За $x, y \in S_1 \cap S_2$ важи да $x, y \in S_1$ и $x, y \in S_2$, па је $x + y, xy \in S_1$ и $x + y, xy \in S_2$, а тада $x + y$ и xy припадају и пресеку ова два потпрстена. Такође је $-x \in S_1 \cap S_2$ и $1 \in S_1 \cap S_2$.

   Ако је $S_1 \subseteq S_2$, тада је $S_1 \cup S_2 = S_2$, што јесте потпрстен од R. Слично ако је $S_2 \subseteq S_1$. Претпоставимо сада да постоје $x \in S_1 \setminus S_2$ и $y \in S_2 \setminus S_1$. Ако би

$S_1 \cup S_2$ био потпрстен, тада би $x+y \in S_1 \cup S_2$. Следило би да $x+y$ припада бар једном од S_1, S_2. Ако $x+y \in S_1$, следи и да $y = (x+y) - x$ припада S_1, што је контрадикција. Ако $x+y \in S_2$, следи да $x = (x+y) - y$ припада S_2; такође контрадикција. Дакле, $S_1 \cup S_2$ је потпрстен једино ако $S_1 \subseteq S_2$ или $S_2 \subseteq S_1$.

10. а) Доказати да је $K = \{p \in \mathbb{Z}[X] \mid p'(3) = 0\}$ потпрстен са јединицом у $\mathbb{Z}[X]$.
б) Доказати да је $I = \{p \in \mathbb{Z}[X] \mid p(3) = 0, p'(3) = 0\}$ идеал у $\mathbb{Z}[X]$.
в) Доказати да је $\varphi : \mathbb{Z}[X] \to \mathrm{M}_2(\mathbb{Z})$ један хомоморфизам наведених прстена, где је $\varphi(p) = \begin{pmatrix} p(3) & p'(3) \\ 0 & p(3) \end{pmatrix}$, за $p \in \mathbb{Z}[X]$. Одредити језгро од φ.

а) Нека су $p, q \in K$; тада је $p'(3) = q'(3) = 0$. Важи да $(p+q)'(3) = p'(3) + q'(3) = 0 + 0 = 0$, и како је $p+q$ полином са целобројним коефицијентима следи да $p+q \in K$. Такође је $(-p)'(3) = -p'(3) = 0$. Важи да $(pq)'(3) = (p'q + pq')(3) = p'(3)q(3) + p(3)q'(3) = 0$, па $pq \in K$. Како је $1' = 0$, следи да $1 \in K$. Дакле, K јесте потпрстен од $\mathbb{Z}[X]$.

б) За $p, q \in I$ важи да $(p+q)(3) = p(3) + q(3) = 0$ и $(p+q)'(3) = p'(3) + q'(3) = 0$, па $p+q \in I$. За $q \in \mathbb{Z}[X]$ и $p \in I$ је $(pq)(3) = p(3)q(3) = 0 \cdot q(3) = 0$ и $(pq)'(3) = p'(3)q(3) + p(3)q'(3) = 0 \cdot q(3) + 0 \cdot q'(3) = 0$, тако да $I \lhd \mathbb{Z}[X]$.

в) За $p, q \in \mathbb{Z}[X]$ је

$$\varphi(p+q) = \begin{pmatrix} p(3)+q(3) & p'(3)+q'(3) \\ 0 & p(3)+q(3) \end{pmatrix} = \begin{pmatrix} p(3) & p'(3) \\ 0 & p(3) \end{pmatrix} + \begin{pmatrix} q(3) & q'(3) \\ 0 & q(3) \end{pmatrix} = \varphi(p) + \varphi(q).$$

Такође је

$$\varphi(pq) = \begin{pmatrix} p(3)q(3) & p'(3)q(3)+p(3)q'(3) \\ 0 & p(3)q(3) \end{pmatrix} = \begin{pmatrix} p(3) & p'(3) \\ 0 & p(3) \end{pmatrix} \cdot \begin{pmatrix} q(3) & q'(3) \\ 0 & q(3) \end{pmatrix} = \varphi(p) \cdot \varphi(q).$$

Језгро пресликавања φ састоји се од полинома p тако да је $\varphi(p)$ нула-матрица, то јест, од полинома p тако да је $p(3) = 0, p'(3) = 0$. Следи да је $\mathrm{Ker}(\varphi) = I$.

11. Одредити $a \in \mathbb{Z}$ тако да је $\langle a \rangle = (\langle 9 \rangle \langle 5 \rangle + \langle 6 \rangle \langle 6 \rangle) \cap \langle 12 \rangle$.

Важи да

$$(\langle 9 \rangle \langle 5 \rangle + \langle 6 \rangle \langle 6 \rangle) \cap \langle 12 \rangle = (\langle 45 \rangle + \langle 36 \rangle) \cap \langle 12 \rangle = \langle \mathrm{nzd}(45, 36) \rangle \cap \langle 12 \rangle = \langle 9 \rangle \cap \langle 12 \rangle = \langle \mathrm{nzs}(9, 12) \rangle = \langle 36 \rangle,$$

па је $a = 36$.

12. Одредити праве делитеље нуле у $\mathbb{Z}_{21}$ и $\mathbb{Z}_{16}$.

Важи да је $n \in \mathbb{Z}_{21}$ делитељ нуле акко је $\mathrm{nzd}(n, 21) \neq 1$. Тако да су делитељи нуле у Z_{21} $\{0, 3, 6, 7, 9, 12, 14, 15, 18\}$, а прави су сви осим нуле. У Z_{16} делитељи нуле су $\{0, 2, 4, 6, 8, 10, 12, 14\}$.

13. Одредити инвертибилне елементе у $\mathbb{Z}_{15}$ и $\mathbb{Z}_{36}$ и наћи њихове инверзе.

Инвертибилни елементи $n \in \mathbb{Z}_{15}$ су они бројеви који су узајамно прости са 15. То су $\{1, 2, 4, 7, 8, 11, 13, 14\}$. Важи да

$$2 \cdot 8 \equiv 4 \cdot 4 \equiv 7 \cdot 13 \equiv 11 \cdot 11 \equiv 14 \cdot 14 \,(\mathrm{mod}\, 15).$$

14. Одредити све идеале у $\mathbb{Z}_{24}$ и $\mathbb{Z}_{16}$.

Одредимо прво скуп $Z(\mathbb{Z}_{24})$ свих делитеља нуле овог прстена, као и скуп инвертибилних елемената $U(\mathbb{Z}_{24})$.

$$Z(\mathbb{Z}_{24}) = \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22\}$$

$$U(\mathbb{Z}_{24}) = \{1, 5, 7, 11, 13, 17, 19, 23\}$$

Сваки идеал у $\mathbb{Z}_{24}$ је главни и генератори идеала у овом прстену могу бити само делитељи нуле. Пошто је

$$2 \cdot 5 = 10, \qquad 2 \cdot 7 = 14, \qquad 2 \cdot 11 = 22 \qquad (\mathrm{mod}\, 24),$$

следи да $\langle 2\rangle = \langle 10\rangle = \langle 14\rangle = \langle 22\rangle$. Слично, множењем броја 3 неким од инвертибилних елемената добијамо да је $\langle 3\rangle = \langle 15\rangle = \langle 21\rangle = \langle 9\rangle$. Имамо и да је $\langle 4\rangle = \langle 20\rangle$, $\langle 8\rangle = \langle 16\rangle$, $\langle 6\rangle = \langle 18\rangle$. Тако да су нетривијални идеали које разматрамо у $\mathbb{Z}_{24}$ само

$$\langle 2\rangle,\ \langle 3\rangle,\ \langle 4\rangle,\ \langle 6\rangle,\ \langle 8\rangle,\ \langle 12\rangle.$$

Можемо се лако уверити да

$$\langle 8\rangle \subseteq \langle 4\rangle \subseteq \langle 2\rangle,\ \langle 12\rangle \subseteq \langle 6\rangle \subseteq \langle 3\rangle,\ \langle 12\rangle \subseteq \langle 4\rangle,\ \langle 6\rangle \subseteq \langle 2\rangle,$$

као и да су ови идеали међусобно различити. Наиме, ако би $\langle 2\rangle \subseteq \langle 4\rangle$, тада би било $2 = 4 \cdot m \pmod{24}$, што би значило да у скупу $\mathbb{Z}$ важи да $2 = 4m + 24s$, то јест, $1 = 2m + 12s$ а то је немогуће. На сличан начин се може доказати да су и сви остали идеали међусобно различити. Дакле, различити идеали у $\mathbb{Z}_{24}$ су:

$$\mathbb{Z}_{24},\ \langle 2\rangle,\ \langle 3\rangle,\ \langle 4\rangle,\ \langle 6\rangle,\ \langle 8\rangle,\ \langle 12\rangle,\ \{0\}.$$

Што се тиче прстена $\mathbb{Z}_{16}$, можемо се уверити на сличан начин да су ту идеали:

$$\mathbb{Z}_{16} \ \supseteq\ \langle 2\rangle \ \supseteq\ \langle 4\rangle \ \supseteq\ \langle 8\rangle \ \supseteq\ \{0\}.$$

15. Доказати да је са $f(x) = \rho(x, 9)$ дефинисан један хомоморфизам $f : \mathbb{Z}_{36} \longrightarrow \mathbb{Z}_9$ и одредити његово језгро.

Приметимо прво да је пресликавање f добро дефинисано, јер $\rho(x, 9) \in \mathbb{Z}_9$ за све $x \in \mathbb{Z}_{36}$. Видимо одмах да је $f(1) = \rho(1, 9) = 1$, па остаје још да се докаже да $f(x +_{36} y) = f(x) +_9 f(y)$ и $f(x \cdot_{36} y) = f(x) \cdot_9 f(y)$. Нека су $x = 9a + b$ и $y = 9c + d$, где $0 \leq b, d < 9$. Узмимо у обзир да је $\rho(\rho(x + y, 36), 9) = \rho(x + y, 9)$. Како је $x + y = 9(a + c) + b + d = 9(a + c) + 9s + \rho(b + d, 9)$, следи да

$$f(x +_{36} y) = \rho(x +_{36} y, 9) = \rho(x + y, 9) = \rho(b + d, 9) = b +_9 d = f(x) +_9 f(y).$$

Са друге стране, $xy = 81ac + 9ad + 9bc + bd = 81ac + 9ad + 9bc + 9t + \rho(bd, 9)$, па

$$f(x \cdot_{36} y) = \rho(x \cdot_{36} y, 9) = \rho(xy, 9) = \rho(bd, 9) = b \cdot_9 d = f(x) \cdot_9 f(y).$$

Овим смо доказали да је f хомоморфизам наведених прстена, а његово језгро је једнако

$$\mathrm{Ker}(f) = \{x \in \mathbb{Z}_{36} \mid f(x) = 0\} = \{x \in \mathbb{Z}_{36} \mid \rho(x, 9) = 0\} = \{0, 9, 18, 27\}.$$

16. а) Доказати да је $R = \left\{ \begin{pmatrix} m & -n \\ n & m \end{pmatrix} \mid m, n \in \mathbb{Z} \right\}$ комутативни прстен са јединицом у односу на операција сабирања и множхења матрица.
б) Доказати да је $\pi : \mathbb{Z} \to R$ један мономорфизам наведених прстена, где је $\pi(m) = \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}$, за $m \in \mathbb{Z}$.

Нека је $M_{m,n} = \begin{pmatrix} m & -n \\ n & m \end{pmatrix}$. Тада је $M_{m,n} + M_{p,q} = M_{m+p,n+q} \in R$, као и $M_{m,n} \cdot M_{p,q} = M_{mp-nq,mq+np} \in R$. Операција $+$ је асоцијативна и комутативна у $\mathrm{M}_2(\mathbb{Z})$, операција $\cdot$ је асоцијативна у истом прстену и важи дистрибутивност $\cdot$ у односу на $+$. Како су нула-матрица $M_{0,0}$ и јединична

матрица $M_{1,0}$ елементи у R, као и $M_{-m,-n} \in R$, остаје још да се уверимо да важи комутативност множења:

$$M_{m,n} \cdot M_{p,q} = M_{mp-nq,mq+np} = \begin{pmatrix} mp-nq & -mq-np \\ mq+np & mp-nq \end{pmatrix} =$$

$$= \begin{pmatrix} pm-qn & -qm-pn \\ qm+pn & pm-qn \end{pmatrix} = M_{p,q} \cdot M_{m,n}.$$

б) Приметимо да је $\pi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Како је

$$\pi(m_1 + m_2) = M_{m_1+m_2,0} = M_{m_1,0} + M_{m_2,0} = \pi(m_1) + \pi(m_2)$$

$$\pi(m_1 m_2) = M_{m_1 m_2,0} = M_{m_1,0} \cdot M_{m_2,0} = \pi(m_1)\pi(m_2),$$

следи да је π један хомоморфизам. Из $\mathrm{Ker}(\pi) = \{m \in \mathbb{Z} \mid \pi(m) = 0\} = \{0\}$ следи да је π инјективно, па је и мономорфизам.

17. Користећи Еуклидов алгоритам доказати да су полиноми $p(X) = X^3 - X^2 + 2X + 3$ и $q(X) = X^2 + 1 \in \mathbb{Q}[X]$ узајамно прости.

Важи да:

$$\begin{aligned} p(X) &= q(X)(X-1) + (X+4) \\ q(X) &= (X+4)(X-4) + 17 \\ X+4 &= 17\Big(\frac{1}{17}X + \frac{4}{17}\Big). \end{aligned}$$

Последњи не-нула остатак је 17, па је $\mathrm{nzd}(p,q) = \frac{1}{17} \cdot 17 = 1$.

18. Користећи Еуклидов алгоритам наћи $f \in \mathbb{R}[X]$ тако да $\langle f \rangle = \langle p, q \rangle$, где су $p(X) = X^6 - 1$ и $q(X) = X^4 + 2X^3 + 2X^2 - 2X - 3$. Наћи полиноме $u(X)$ и $v(X)$ тако да $pu + qv = \mathrm{nzd}(p,q)$.

$$\begin{aligned} p(X) &= q(X)(X^2 - 2X + 2) + (2X^3 - 5X^2 - 2X + 5) \\ q(X) &= (2X^3 - 5X^2 - 2X + 5)\Big(\frac{1}{2}X + \frac{9}{4}\Big) + \Big(\frac{57}{4}X^2 - \frac{57}{4}\Big) \\ 2X^3 - 5X^2 - 2X + 5 &= \Big(\frac{57}{4}X^2 - \frac{57}{4}\Big)\Big(\frac{8}{57}X - \frac{20}{57}\Big). \end{aligned}$$

Следи да је $\mathrm{nzd}(p,q) = \frac{4}{57}\Big(\frac{57}{4}X^2 - \frac{57}{4}\Big) = X^2 - 1$. Такође је

$$\begin{aligned} X^2 - 1 &= \frac{4}{57}\Big(\frac{57}{4}X^2 - \frac{57}{4}\Big) = \frac{4}{57}\Big(q - (2X^3 - 5X^2 - 2X + 5)\Big(\frac{1}{2}X + \frac{9}{4}\Big)\Big) \\ &= \frac{4}{57}\Big(q - (p - q(X^2 - 2X + 2))\Big)\Big(\frac{1}{2}X + \frac{9}{4}\Big) \\ &= \Big(-\frac{2}{57}X - \frac{9}{57}\Big)p + \Big(\frac{2}{57}X^3 + \frac{5}{57}X^2 - \frac{12}{57}X + \frac{27}{57}\Big)q. \end{aligned}$$

19. Одредити $\mathrm{nzd}(p,q)$ где су $p(X) = X^4 + 1, q(X) = X^3 + 2X^2 + 3X + 1 \in \mathbb{Z}_5[X]$.

$$\left(\begin{array}{c|cc} X^4+1 & 1 & 0 \\ X^3+2X^2+3X+1 & 0 & 1 \end{array}\right) \xrightarrow{V_1 \mapsto V_1 + 4XV_2} \left(\begin{array}{c|cc} 3X^3+2X^2+4X+1 & 1 & 4X \\ X^3+2X^2+3X+1 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{V_1 \mapsto V_1 + 2V_2} \left(\begin{array}{c|cc} X^2+3 & 1 & 4X+2 \\ X^3+2X^2+3X+1 & 0 & 1 \end{array}\right) \xrightarrow{V_2 \mapsto V_2 + 4XV_1}$$

$$\left(\begin{array}{c|cc} X^2+3 & 1 & 4X+2 \\ 2X^2+1 & 4X & X^2+3X+1 \end{array}\right) \xrightarrow{V_2 \mapsto V_2 + 3V_1} \left(\begin{array}{c|cc} X^2+3 & 1 & 4X+2 \\ 0 & * & * \end{array}\right)$$

Следи да је $\mathrm{nzd}(p,q) = X^2 + 3 = p \cdot 1 + q \cdot (4X + 2)$.

20. Одредити полиноме $f, u_1, u_2, u_3 \in \mathbb{Z}_3[X]$ тако да $\langle f \rangle = \langle p, q, r \rangle$ и $pu_1 + qu_2 + ru_3 = f$, где су $p, q, r \in \mathbb{Z}_3[X]$:

$$\begin{aligned} p(X) &= X^3 + 2X \\ q(X) &= X^4 + 2X^3 + X + 2 \\ r(X) &= 2X^5 + X^4 + 2X^3. \end{aligned}$$

$$\left(\begin{array}{c|ccc} X^3+2X & 1 & 0 & 0 \\ X^4+2X^3+X+2 & 0 & 1 & 0 \\ 2X^5+X^4+2X^3 & 0 & 0 & 1 \end{array}\right) \xrightarrow[V_3 \mapsto V_3 + X^2 V_1]{V_2 \mapsto V_2 + 2XV_1} \left(\begin{array}{c|ccc} X^3+2X & 1 & 0 & 0 \\ 2X^3+X^2+X+2 & 2X & 1 & 0 \\ X^4+X^3 & X^2 & 0 & 1 \end{array}\right)$$

$$\xrightarrow[V_3 \mapsto V_3 + 2XV_1]{V_2 \mapsto V_2 + V_1} \left(\begin{array}{c|ccc} X^3+2X & 1 & 0 & 0 \\ X^2+2 & 2X+1 & 1 & 0 \\ X^3+X^2 & X^2+2X & 0 & 1 \end{array}\right) \xrightarrow[V_3 \mapsto V_3 + 2XV_2]{V_1 \mapsto V_1 + 2XV_2}$$

$$\left(\begin{array}{c|ccc} 0 & X^2+2X+1 & 2X & 0 \\ X^2+2 & 2X+1 & 1 & 0 \\ X^2+X & 2X^2+X & 2X & 1 \end{array}\right) \xrightarrow{V_3 \mapsto V_3 + 2V_2} \left(\begin{array}{c|ccc} 0 & * & * & * \\ X^2+2 & 2X+1 & 1 & 0 \\ X+1 & 2X^2+2X+2 & 2X+2 & 1 \end{array}\right)$$

$$\xrightarrow{V_2 \mapsto V_2 + 2XV_3} \left(\begin{array}{c|ccc} 0 & * & * & * \\ 2X+2 & X^3+X^2+X+1 & X^2+X+1 & 2X \\ X+1 & 2X^2+2X+2 & 2X+2 & 1 \end{array}\right) \xrightarrow{V_2 \mapsto V_2 + V_3}$$

$$\left(\begin{array}{c|ccc} 0 & * & * & * \\ 0 & * & * & * \\ X+1 & 2X^2+2X+2 & 2X+2 & 1 \end{array}\right)$$

Следи да је $f = X + 1, u_1 = 2X^2 + 2X + 2, u_2 = 2X + 2, u_3 = 1$.

21. Доказати да за идеале I, J, K комутативног прстена са јединицом R важи $I(J + K) = IJ + IK$.

Елемент a из $I(J + K)$ је облика $a = x_1(y_1 + z_1) + \cdots + x_k(y_k + z_k)$ за $x_1, \ldots, x_k \in I$, $y_1, \ldots, y_k \in J$ и $z_1, \ldots, z_k \in K$. Важи дистрибутивност множења у односу на сабирање тако да је дати елемент једнак $x_1y_1 + x_1z_1 + \cdots + x_ky_k + x_kz_k$. Пошто је $x_iy_i \in IJ$ и $x_iz_i \in IK$, следи да је $a \in IJ + IK$.

Са друге стране, како је $J \subseteq J + K$, важи и $IJ \subseteq I(J + K)$. Слично је и $IK \subseteq I(J + K)$. Тако да је $IJ + IK \subseteq I(J + K)$.

22. Ако је $I + J = R$, где је R комутативни прстен са јединицом и I, J идеали у R, доказати да је $IJ = I \cap J$.

За $a \in IJ$, важи $a = x_1y_1 + \cdots + x_ky_k$, где је $x_1, \ldots, x_k \in I$, $y_1, \ldots, y_k \in J$. Како је I идеал и $x_i \in I$ важи да $x_iy_i \in I$. Тако је и $a \in I$. Слично, пошто је J идеал и $y_i \in J$, следи да $x_iy_i \in J$, па и $a \in J$. Дакле, $a \in I \cap J$.

Са друге стране је

$$I \cap J = (I \cap J) \cdot R = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J.$$

Овде смо користили претпоставку задатка и претходни задатак. Како је $I \cap J \subseteq J$, следи да је $(I \cap J)I \subseteq JI = IJ$, јер је прстен комутативан. Слично је и $(I \cap J)J \subseteq IJ$. Дакле, $I \cap J$ је садржано у $IJ + IJ = IJ$, што је и требало доказати.

23. Доказати да за идеале I, J, K комутативног прстена са јединицом R важи: $I \cap (J + K) = (I \cap J) + K$ ако и само ако $K \subseteq I$.

Претпоставимо прво да је $K \subseteq I$. Нека је $a \in (I \cap J) + K$, тада је $a = b + c$, за $b \in I \cap J$, $c \in K$. Како је $b \in I$ и $c \in K \subseteq I$, то је и $a = b + c \in I$. Са друге стране, $b + c \in J + K$, па је $a \in J + K$. Следи да је $a \in I \cap (J + K)$.

Ако је $a \in I \cap (J+K)$, тада је $a \in I$ и $a = b + c \in J + K$, за $b \in J$ и $c \in K$. Пошто је $K \subseteq I$, онда је $c \in I$ и $b = a - c \in I$. Тако да је $b \in I \cap J$. Следи да $a = b + c \in (I \cap J) + K$, чиме смо доказали да $I \cap (J+K) = (I \cap J) + K$.

Претпоставимо сада да важи једнакост $I \cap (J+K) = (I \cap J) + K$. Нека је $a \in K$. Тада је $a = 0 + a \in (I \cap J) + K$, па је $a \in I \cap (J+K)$. Следи да $a \in I$, па је $K \subseteq I$.

24. Конструисати поље са 4 елемента.

Приметимо да је полином $X^2 + X + 1$ нерастављив над $\mathbb{Z}_2$. Тада је $\mathbb{Z}_2[X]/\langle X^2 + X + 1\rangle$ поље, а посматрано као векторски прсотор над $\mathbb{Z}_2$ изоморфно је са $\mathbb{Z}_2 \times \mathbb{Z}_2$ (димензија векторског простора је $\deg(X^2 + X + 1) = 2$). Тако да ово поље има 4 елемента. Ако са α означимо $X + \langle X^2 + X + 1\rangle$, тада су сви елементи у овом пољу $\mathbb{F}_4$: $0, 1, \alpha$ и $\alpha + 1$ (0 је заправо $0 + \langle X^2 + X + 1\rangle$, а 1 је $1 + \langle X^2 + X + 1\rangle$). Такође важи да је

$$\alpha^2 = X^2 + \langle X^2 + X + 1\rangle = X + 1 + \langle X^2 + X + 1\rangle = \alpha + 1.$$

25. Наћи све нерастављиве полиноме степена 2 над $\mathbb{Z}_3$.

Можемо разматрати само моничне полиноме. Таквих над $\mathbb{Z}_3$ има 9. За полиноме $X^2, X^2 + X, X^2 + 2X, X^2 + 2X + 1, X^2 + 2, X^2 + X + 1$ се лако можемо уверити да су растављиви над $\mathbb{Z}_3$. Што се тиче полинома $X^2 + 1, X^2 + X + 2, X^2 + 2X + 2$, видимо да ниједан од бројева $0, 1, 2$ није нула ниједног полинома, па су они нерастављиви над $\mathbb{Z}_3$.

26. Конструисати поље са 9 елемената.

За било који нерастављиви полином p из претходног задатка важи да је $\mathbb{Z}_3[X]/\langle p\rangle$ тражено поље. За $p = X^2 + 1$ имамо да је то поље $\mathbb{F}_9 = \{0, 1, 2, \beta, \beta + 1, \beta + 2, 2\beta, 2\beta + 1, 2\beta + 2\}$, где је β класа елемента X у $\mathbb{Z}_3[X]/\langle X^2 + 1\rangle$.

27. а) Одредити све нерастављиве моничне полиноме степена 3 у прстену $\mathbb{Z}_3[X]$.
б) Конструисати поље са 27 елемената.
в) Написати све елементе тог поља и наћи инверзе за нека три одабрана елемента.

а) Директном провером можемо се уверити да су тражени полиноми:

$$X^3 + 2X + 1,\ X^3 + 2X + 2,\ X^3 + X^2 + 2,\ X^3 + 2X^2 + 1,$$

$$X^3 + X^2 + X + 2,\ X^3 + X^2 + 2X + 1,\ X^3 + 2X^2 + X + 1,\ X^3 + 2X^2 + 2X + 2.$$

Остали монични полиноми степена 3 над $\mathbb{Z}_3$ су растављиви.

б) Тражено поље је, на пример, $\mathbb{Z}_3[X]/\langle X^3 + 2X + 1\rangle$.

в) Елементи тог поља су

$$\begin{aligned}\mathbb{F}_{27} \;=\; \{&0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2, \alpha^2, \alpha^2 + 1, \alpha^2 + 2, \alpha^2 + \alpha, \alpha^2 + 2\alpha,\\ &\alpha^2 + \alpha + 1, \alpha^2 + \alpha + 2, \alpha^2 + 2\alpha + 1, \alpha^2 + 2\alpha + 2, 2\alpha^2, 2\alpha^2 + 1, 2\alpha^2 + 2,\\ &2\alpha^2 + \alpha, 2\alpha^2 + \alpha + 1, 2\alpha^2 + \alpha + 2, 2\alpha^2 + 2\alpha, 2\alpha^2 + 2\alpha + 1, 2\alpha^2 + 2\alpha + 2\}.\end{aligned}$$

Користећи релацију $\alpha^3 = \alpha + 2$ добијамо да $\alpha \cdot (2\alpha^2 + 1) = 1$. Тривијално важи да $1 \cdot 1 = 1$ и $2 \cdot 2 = 1$.

28. Одредити све нерастављиве моничне полиноме степена 4 у прстену $\mathbb{Z}_2[X]$.

Моничних полинома степена 4 над $\mathbb{Z}_2$ је укупно 16. Полиноми X^4, $X^4 + X^3$, $X^4 + X^2$, $X^4 + X$, $X^4 + X^3 + X^2$, $X^4 + X^3 + X$, $X^4 + X^2 + X$, $X^4 + X^3 + X^2 + X$ су очигледно дељиви са X, па су растављиви. Такође је очигледно да су полиноми $X^4 + 1$, $X^4 + X^3 + X^2 + 1$, $X^4 + X^3 + X + 1$, $X^4 + X^2 + X + 1$ дељиви са $X + 1$. Преостало је испитати да ли су нерастављиви полиноми

X^4+X^3+1, X^4+X^2+1, X^4+X+1, $X^4+X^3+X^2+X+1$. Ни 0 ни 1 нису нуле ових полинома. Да ли је могуће написати

$$X^4+X^3+1=(X^2+aX+b)(X^2+cX+d),$$

за $a,b,c,d\in\mathbb{Z}_2$? Изједначавањем коефицијената уз одговарајуће степене уз X, добијамо систем:

$$\begin{aligned} a+c &= 1\\ b+ac+d &= 0\\ ad+bc &= 0\\ bd &= 1. \end{aligned}$$

Како систем решавамо над $\mathbb{Z}_2$, из последње једнакости следи да $b=d=1$. Заменом ових вредности у трећу једнакост, добијамо да $a+c=0$, што је у контрадикцији са првом једнакошћу. Следи да полином X^4+X^3+1 није растављив над $\mathbb{Z}_2$. Сличном анализом добијамо да то важи и за полиноме X^4+X+1 и $X^4+X^3+X^2+X+1$. Са друге стране, систем

$$\begin{aligned} a+c &= 0\\ b+ac+d &= 1\\ ad+bc &= 0\\ bd &= 1 \end{aligned}$$

добијен из једнакости

$$X^4+X^2+1=(X^2+aX+b)(X^2+cX+d)$$

има решење у $\mathbb{Z}_2$. То је $a=b=c=d=1$ и
$X^4+X^2+1=(X^2+X+1)(X^2+X+1)$.

29. Наћи $f\in\mathbb{F}_4[Y]$ тако да $\langle f\rangle=\langle p,q\rangle$, где су $p(Y)=Y^4+\alpha Y^2+\alpha+1$, $q(Y)=Y^4+\alpha Y^3+\alpha Y^2+(\alpha+1)Y$ и $\mathbb{F}_4$ је поље са 4 елемента.

$$\begin{pmatrix} Y^4+\alpha Y^2+\alpha+1\\ Y^4+\alpha Y^3+\alpha Y^2+(\alpha+1)Y\end{pmatrix}\xrightarrow{V_2\mapsto V_2+V_1}\begin{pmatrix} Y^4+\alpha Y^2+\alpha+1\\ \alpha Y^3+(\alpha+1)Y+(\alpha+1)\end{pmatrix}$$

$$\xrightarrow{V_1\mapsto V_1+(\alpha+1)YV_2}\begin{pmatrix} \alpha Y+\alpha+1\\ \alpha Y^3+(\alpha+1)Y+(\alpha+1)\end{pmatrix}\xrightarrow{V_2\mapsto V_2+Y^2V_1}$$

$$\begin{pmatrix} \alpha Y+\alpha+1\\ (\alpha+1)Y^2+(\alpha+1)Y+(\alpha+1)\end{pmatrix}\xrightarrow[V_2\mapsto\alpha V_2]{V_1\mapsto(\alpha+1)V_1}\begin{pmatrix} Y+\alpha\\ Y^2+Y+1\end{pmatrix}\xrightarrow{V_2\mapsto V_2+YV_1}$$

$$\begin{pmatrix} Y+\alpha\\ (\alpha+1)Y+1\end{pmatrix}\xrightarrow{V_2\mapsto\alpha V_2}\begin{pmatrix} Y+\alpha\\ Y+\alpha\end{pmatrix}\xrightarrow{V_2\mapsto V_2+V_1}\begin{pmatrix} Y+\alpha\\ 0\end{pmatrix}$$

Следи да је $f=Y+\alpha$.

30. Нека је I идеал у $\mathbb{F}_8[Y]$ генерисан са:

$$\begin{aligned} p(Y) &= Y^4+(\beta^2+\beta+1)Y^3+\beta Y^2+Y+(\beta^2+1)\\ q(Y) &= Y^5+(\beta^2+\beta+1)Y^4+Y^3+(\beta^2+\beta+1)Y^2+\beta Y+(\beta^2+1)\\ r(Y) &= Y^6+(\beta+1)Y^4+(\beta^2+\beta+1)Y^2+(\beta^2+1), \end{aligned}$$

где је β ознака за класу елемента X у стандардној конструкцији поља са 8 елемената $\mathbb{F}_8=\mathbb{Z}_2[X]/\langle X^3+X+1\rangle$. Одредити полином $f\in\mathbb{F}[Y]$ тако да $I=\langle f\rangle$.

После дужег рачуна добијамо да је $f=1$.

31. Доказати да поља $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt{3})$ нису изоморфна.

Претпоставимо да постоји изоморфизам $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Тада је

$$2 = \varphi(2) = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(\sqrt{2}) \cdot \varphi(\sqrt{2}) = (\varphi(\sqrt{2}))^2.$$

Дакле, имамо да је $\varphi(\sqrt{2})$ елемент у $\mathbb{Q}(\sqrt{3})$ чији квадрат је једнак 2. Нека је $\varphi(\sqrt{2}) = a + b\sqrt{3}$, за $a, b \in \mathbb{Q}$. Ако квадрирамо ову једнакост, добијамо $2 = a^2 + 2ab\sqrt{3} + 3b$. То значи да је $\sqrt{3} = (2 - a^2 - 3b) \cdot \frac{1}{2ab} \in \mathbb{Q}$, а ово је контрадикција.

32. Показати да је $\alpha = i + \sqrt{3}$ алгебарски над $\mathbb{Q}$. Наћи минимални полином за α и одредити $\frac{1}{\alpha^2-2}$ у облику $p(\alpha)$, где је $p(X)$ полином из $\mathbb{Q}[X]$.

Квадрирањем једнакости $\alpha - \sqrt{3} = i$, добијамо да је $\alpha^2 + 4 = 2\sqrt{3}\alpha$. Поновним квадрирањем последње једнакости добијамо да је $\alpha^4 - 4\alpha^2 + 16 = 0$. То значи да је α нула полинома $f(X) = X^4 - 4X^2 + 16 \in \mathbb{Q}[X]$, па јесте алгебарски елемент над $\mathbb{Q}$.

С обзиром на то да је f моничан и да је α његова нула, да бисмо доказали да је то заправо минимални полином за α, довољно је доказати да је f нерастављив над $\mathbb{Q}$. Из теореме о рационалним нулама полинома следи да су могуће целобројне нуле $\frac{a}{b}$ за f елементи скупа $\{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$. Директном провером можемо се уверити да ниједан од наведених елемената није нула за f. Да ли је f производ два полинома степена 2? Ако важи:

$$X^4 - 4X^2 + 16 = (X^2 + aX + b)(X^2 + cX + d),$$

за $a, b, c, d \in \mathbb{Q}$, тада добијамо да

$$X^4 - 4X^2 + 16 = X^4 + (a + c)X^3 + (b + ac + d)X^2 + (ad + bc)X + bd.$$

Изједначавањем коефицијената уз одговарајуће степене уз X, добијамо систем:

$$\begin{aligned} a + c &= 0 \\ b + ac + d &= -4 \\ ad + bc &= 0 \\ bd &= 16 \end{aligned}$$

Из треће једначине имамо да је $a(b - d) = 0$, па је $a = 0$ или $b = d$. У првом случају, добијамо да

$$\begin{aligned} c &= 0 \\ b + d &= -4 \\ bd &= 16 \end{aligned}$$

Заменом $b = \frac{16}{d}$ у другу једначину, добијамо да је $d^2 + 4d + 16 = 0$, што је немогуће, јер $d \in \mathbb{Q}$. У другом случају, када $b = d$, имамо да $d^2 = 16$. Приметимо да је $c = -a$. Ако је $d = b = 4$, тада из друге једначине следи да $-a^2 = -12$. Ако је $b = d = -4$, следи да $-a^2 = 4$. У оба случаја добијамо контрадикцију, јер је a из $\mathbb{Q}$. Дакле, f није могуће написати ни као производ два полинома степена два, па је он нерастављив над $\mathbb{Q}$, то јест, $f = \mu_\alpha$.

Даље, како базу за $\mathbb{Q}(\alpha)$ над $\mathbb{Q}$ чине $1, \alpha, \alpha^2, \alpha^3$, то је елемент $\frac{1}{\alpha^2-2}$ могуће написати у облику

$$\frac{1}{\alpha^2 - 2} = a + b\alpha + c\alpha^2 + d\alpha^3,$$

за $a, b, c, d \in \mathbb{Q}$. Помножимо ову једнакост са $\alpha^2 - 2$ и искористимо чињеницу да је $\alpha^4 = 4\alpha^2 - 16$ (јер је α нула полинома f), као и да онда $\alpha^5 = 4\alpha^3 - 16\alpha$. Сређивањем те једнакости, добијамо да је

$$1 = (-2a - 16c) + (-2b - 16d)\alpha + (a + 2c)\alpha^2 + (b + 2d)\alpha^3.$$

Због линеарне независности елемената $1, \alpha, \alpha^2, \alpha^3$ над $\mathbb{Q}$, следи да је

$$\begin{aligned} -2a - 16c &= 1 \\ -2b - 16d &= 0 \\ a + 2c &= 0 \\ b + 2d &= 0 \end{aligned}$$

Можемо одмах уочити да је $b = d = 0$, а затим и да је $c = -\frac{1}{12}$, а $a = \frac{1}{6}$.

Дакле, ако је полином $p(X) = \frac{1}{6} - \frac{1}{12}X^2$ (који очигледно припада $\mathbb{Q}[X]$), тада је $\frac{1}{\alpha^2-2} = p(\alpha)$, па је p тражени полином.

33. Урадити све из претходног задатка за елемент $\alpha = \sqrt{5} - \sqrt{3}$.

Квадрирањем једнакости $\alpha + \sqrt{3} = \sqrt{5}$, добијамо $\alpha^2 - 2 = -2\sqrt{3}\alpha$. А поновним квадрирањем овога и $\alpha^4 - 16\alpha^2 + 4 = 0$. Дакле, α је алгебарски елемент над $\mathbb{Q}$, а кандидат за минимални полином је $f(X) = X^4 - 16X^2 + 4$. Да ли је он нерастављив над $\mathbb{Q}$? Рационалне нула полинома f могле би бити неки од $\{\pm 1, \pm 2, \pm 4\}$. Директном провером се уверавамо да ниједан од ових бројева није нула од f. Написавши f као производ полинома $(X^2 + aX + b)(X^2 + cX + d)$, за $a, b, c, d \in \mathbb{Q}$, добијамо систем:

$$\begin{aligned} a + c &= 0 \\ b + ac + d &= -16 \\ ad + bc &= 0 \\ bd &= 4 \end{aligned}$$

Из треће једначине следи да је $a = 0$ или $b = d$. Ако је $a = 0$, тада је и $c = 0$, па је $b + d = -16$. Како је и $bd = 4$, добијамо да је $d^2 + 16d + 4 = 0$, што је немогуће јер $d \in \mathbb{Q}$. Ако је $b = d$, тада из $b^2 = 4$, следи да је $b = d = 2$ или $b = d = -2$. У првом случају је $-a^2 = 20$, а у другом $-a^2 = -12$. Ни једно ни друго није могуће, јер $a \in \mathbb{Q}$. Следи да је f нерастављив, па је $f = \mu_\alpha$.

Множењем једанкости

$$\frac{1}{\alpha^2 - 2} = a + b\alpha + c\alpha^2 + d\alpha^3,$$

за $a, b, c, d \in \mathbb{Q}$ са $\alpha^2 - 2$ и коришћењем $\alpha^4 = 16\alpha^2 - 4$, добијамо да

$$1 = (-2a - 4c) + (-2b - 4d)\alpha + (a + 14c)\alpha^2 + (b + 14d)\alpha^3.$$

Решавањем система добија се $b = d = 0$, $a = \frac{7}{16}$ и $c = -\frac{1}{32}$, па је тражени полином $p(X) = -\frac{1}{32}X^2 + \frac{7}{16}$, то јест $\frac{1}{\alpha^2-2} = -\frac{1}{32}\alpha^2 + \frac{7}{16}$.

34. Урадити све из претходног задатка за елемент $\alpha = \sqrt{2 + \sqrt{3}}$.

Како је $\alpha^2 = 2 + \sqrt{3}$, квадрирањем $\alpha^2 - 2 = \sqrt{3}$ добијамо $\alpha^4 - 4\alpha^2 + 1 = 0$. Дакле, α је алгебарски и нека је $f(X) = X^4 - 4X^2 + 1$. Бројеви 1 и -1 нису нуле од f. Ако би било $f = X^2 + aX + b)(X^2 + cX + d)$, добили бисмо систем над $\mathbb{Q}$:

$$\begin{aligned} a + c &= 0 \\ b + ac + d &= -4 \\ ad + bc &= 0 \\ bd &= 1 \end{aligned}$$

За $a=0$, добија се $d^2+4d+1=0$, што је немогуће. За $b=d$, имамо $b=1$ или $b=-1$. У првом случају је $a^2=6$ а у другом $a^2=2$. Контрадикција. Дакле, f је нерастављив над $\mathbb{Q}$, а како је моничан и $f(\alpha)=0$, следи да $f=\mu_\alpha$.

Понављајући исти поступак као у претходном задатку, добијамо да је $p(X)=\frac{1}{3}X^2-\frac{2}{3}$.

35. Наћи α тако да је $\mathbb{Q}(i,\sqrt{5})=\mathbb{Q}(\alpha)$.

Да ли је $\alpha=i+\sqrt{5}$? Како $i+\sqrt{5}\in\mathbb{Q}(i,\sqrt{5})$, имамо да $\mathbb{Q}(i+\sqrt{5})\subseteq\mathbb{Q}(i,\sqrt{5})$. Из

$$(i+\sqrt{5})^3=2\sqrt{5}+14i=14(i+\sqrt{5})-12\sqrt{5},$$

следи да је

$$\sqrt{5}=\frac{-(i+\sqrt{5})^3+14(i+\sqrt{5})}{12}=-\frac{1}{12}(i+\sqrt{5})^3+\frac{14}{12}(i+\sqrt{5})\in\mathbb{Q}(i+\sqrt{5}).$$

Тада је и $i=(i+\sqrt{5})-\sqrt{5}\in\mathbb{Q}(i+\sqrt{5})$. Па је и најмање поље $\mathbb{Q}(i,\sqrt{5})$ које садржи i и $\sqrt{5}$ такође садржано у $\mathbb{Q}(i+\sqrt{5})$. Следи да $\mathbb{Q}(i+\sqrt{5})=\mathbb{Q}(i,\sqrt{5})$, то јест $\alpha=i+\sqrt{5}$.

36. Наћи α тако да је $\mathbb{Q}(\sqrt{5},\sqrt{7})=\mathbb{Q}(\alpha)$.

Да ли $\alpha=\sqrt{5}+\sqrt{7}$? Како је

$$(\sqrt{5}+\sqrt{7})^3=26\sqrt{5}+22\sqrt{7}=22(\sqrt{5}+\sqrt{7})+4\sqrt{5},$$

следи да

$$\sqrt{5}=\frac{(\sqrt{5}+\sqrt{7})^3-22(\sqrt{5}+\sqrt{7})}{4}\in\mathbb{Q}(\sqrt{5}+\sqrt{7}).$$

Такође, $\sqrt{7}=(\sqrt{5}+\sqrt{7})-\sqrt{5}\in\mathbb{Q}(\sqrt{5}+\sqrt{7})$. Дакле, $\mathbb{Q}(\sqrt{5},\sqrt{7})\subseteq\mathbb{Q}(\sqrt{5}+\sqrt{7})$.

37. Наћи коренско поље K полинома $X^4+2X^2-15\in\mathbb{Q}[X]$ и одредити елемент α за који је $K=\mathbb{Q}(\alpha)$.

Приметимо да је

$$X^4+2X^2-15=(X^2+1)^2-16=((X^2+1)+4)((X^2+1)-4)=$$
$$=(X^2+5)(X^2-3)=(X-\sqrt{3})(X+\sqrt{3})(X-i\sqrt{5})(X+i\sqrt{5}).$$

Дакле, коренско поље K је једнако $\mathbb{Q}(\sqrt{3},i\sqrt{5})$. Одредимо примитивни елемент α овог раширења. Пошто је

$$(\sqrt{3}+i\sqrt{5})^3=4(\sqrt{3}+i\sqrt{5})-16\sqrt{3},$$

следи да се $\sqrt{3}$ може написати као $\mathbb{Q}$-линеарна комбинација степена елемента $\sqrt{3}+i\sqrt{5}$, дакле $\sqrt{3}\in\mathbb{Q}(\sqrt{3}+i\sqrt{5})$. Слично је и $i\sqrt{5}\in\mathbb{Q}(\sqrt{3}+i\sqrt{5})$. Следи да је $\alpha=\sqrt{3}+i\sqrt{5}$.

38. Наћи коренско поље K полинома $X^4-12X^2+9\in\mathbb{Q}[X]$ и одредити елемент α за који је $K=\mathbb{Q}(\alpha)$.

Како је

$$X^4-12X^2+9=(X^2-6)^2-27=(X^2-6-3\sqrt{3})(X^2-6+3\sqrt{3})=$$
$$=(X^2-(6+3\sqrt{3}))(X^2-(6-3\sqrt{3}))=$$
$$=(X-\sqrt{6+3\sqrt{3}})(X+\sqrt{6+3\sqrt{3}})(X-\sqrt{6-3\sqrt{3}})(X+\sqrt{6-3\sqrt{3}}),$$

коренско поље K датог полинома је једнако $\mathbb{Q}(\sqrt{6+3\sqrt{3}},\sqrt{6-3\sqrt{3}})$. Како је

$$\sqrt{6+3\sqrt{3}}\cdot\sqrt{6-3\sqrt{3}}=9,$$

следи да је $K=\mathbb{Q}(\sqrt{6+3\sqrt{3}})$, јер је $\sqrt{6-3\sqrt{3}}=9\cdot(\sqrt{6+3\sqrt{3}})^{-1}$, што припада $\mathbb{Q}(\sqrt{6+3\sqrt{3}})$. Одавде је јасно да је примитивни елемент за раширење K над $\mathbb{Q}$ једнак $\sqrt{6+3\sqrt{3}}$.

39. Нека је α елемент који генерише раширење од $\mathbb{Q}$ степена 5. Доказати да α^2 генерише исто раширење.

Дакле, имамо да је $[\mathbb{Q}(\alpha):\mathbb{Q}]=5$, а како је $\mathbb{Q}(\alpha^2)\subseteq\mathbb{Q}(\alpha)$, важи и

$$5=[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^2)]\cdot[\mathbb{Q}(\alpha^2):\mathbb{Q}].$$

С обзиром на то је да је степен раширења неког поља природан број, а 5 је прост број, следи да је број $[\mathbb{Q}(\alpha^2):\mathbb{Q}]$ једнак 1 или 5. Ако би био једнак 1, то би значило да је $\mathbb{Q}(\alpha^2)=\mathbb{Q}$, то јест $\alpha^2\in\mathbb{Q}$. У том случају, полином $p(X)=X^2-\alpha^2$ је са коефицијентима у $\mathbb{Q}$, моничан је и α је његова нула. Такође је нерастављив, јер би у супротном $\alpha\in\mathbb{Q}$. Добијамо тада да је $p=\mu_\alpha$, а онда и да је $[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg(\mu_\alpha)=2$, што је немогуће. Следи да је $[\mathbb{Q}(\alpha^2):\mathbb{Q}]=5$, а тиме је $[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^2)]=1$, па су поља $\mathbb{Q}(\alpha)$ и $\mathbb{Q}(\alpha^2)$ једнака.

40. Одредити степен раширења поља $\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{5})$ над $\mathbb{Q}$.

Важи да

$$(*)\qquad [\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{5}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{5}):\mathbb{Q}(\sqrt[3]{2})]\cdot[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}].$$

Минимални полином за елемент $\sqrt[3]{2}$ над $\mathbb{Q}$ је X^3-2 (нерастављив је над $\mathbb{Q}$), па је $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$. Дакле, $[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{5}):\mathbb{Q}]$ је дељив са 3. Дељив је и са 4. Наиме,

$$[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{5}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{5}):\mathbb{Q}(\sqrt[4]{5})]\cdot[\mathbb{Q}(\sqrt[4]{5}):\mathbb{Q}],$$

а минимални полином за $\sqrt[4]{5}$ над $\mathbb{Q}$ је X^4-5 (нерастављив је: нема нула у $\mathbb{Q}$, а и није производ два полинома степена 2).

Пошто су 3 и 4 узајамно прости, сада следи да је $[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{5}):\mathbb{Q}]$ дељив са 12. Са друге стране, ако се вратимо на $(*)$, видимо да полином X^4-5 припада $\mathbb{Q}(\sqrt[3]{2})[X]$ као и да га $\sqrt[4]{5}$ поништава. Дакле, минимални полином за $\sqrt[4]{5}$ над $\mathbb{Q}(\sqrt[3]{2})$ дели X^4-5, па је степен раширења $[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{5}):\mathbb{Q}(\sqrt[3]{2})]\leq 4$. Из $(*)$ следи да је $[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{5}):\mathbb{Q}]\leq 12$. Пошто је и дељив са 12, следи да је $[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{5}):\mathbb{Q}]=12$.

41. Нека су $\alpha=e^{\frac{2\pi i}{7}}$ и $\beta=e^{\frac{2\pi i}{5}}$. Доказати да $\beta\notin\mathbb{Q}(\alpha)$.

Одредимо прво минималне полиноме за α и β над $\mathbb{Q}$. Елемент $\alpha=e^{\frac{2\pi i}{7}}=cos\frac{2\pi}{7}+i\,sin\frac{2\pi}{7}$ је седми корен из јединице па је нула полинома $p(X)=X^7-1$, за који важи да

$$p(X)=(X-1)(X^6+X^5+X^4+X^3+X^2+X+1).$$

Како $\alpha\neq 1$, следи да је нула полинома $X^6+X^5+X^4+X^3+X^2+X+1$. Сваки полином облика

$$X^{p-1}+X^{p-2}+\cdots+X+1,\qquad p\ \text{прост број}$$

је нерастављив над $\mathbb{Q}$, па је $p(X)=\mu_\alpha(X)$. Слично је $\mu_\beta=X^4+X^3+X^2+X+1$.

Ако би $\beta\in\mathbb{Q}(\alpha)$, тада би $\mathbb{Q}(\beta)\subseteq\mathbb{Q}(\alpha)$, па добијамо

$$6=[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\beta)]\cdot[\mathbb{Q}(\beta):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\beta)]\cdot 4,$$

што је немогуће.

42. Нека је $\alpha_n=e^{\frac{2\pi i}{n}}$. Наћи минимални полином μ_{α_n} над $\mathbb{Q}$ за:

а) $n=4$;

б) $n=6$;

в) $n=8$;

г) $n = 9$;

д) $n = 12$.

Како је $\alpha_4 = cos\frac{\pi}{2} + i\, sin\frac{\pi}{2} = i$, онда је $\mu_{\alpha_4} = X^2 + 1$.

За $\alpha_6 = cos\frac{\pi}{3} + i\, sin\frac{\pi}{3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, после квадрирања $\alpha_6 - \frac{1}{2} = i\frac{\sqrt{3}}{2}$, добијамо да $\alpha_6^2 - \alpha_6 + 1 = 0$. Полином $X^2 - X + 1$ је нерастављив над $\mathbb{Q}$, па је једнак μ_{α_6}.

Како је $X^8 - 1 = (X^4 - 1)(X^4 + 1)$ и α_8 није и четврти корен јединице, следи да је α_8 нула полинома $X^4 + 1$. На стандардни начин доказујемо да је $X^4 + 1$ нерастављив над $\mathbb{Q}$.

Пошто је $\alpha_9 = cos\frac{2\pi}{9} + i\, sin\frac{2\pi}{9}$, применом Моаврове формуле добијамо да је

$$\alpha_9^3 = cos\frac{2\pi}{3} + i\, sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Квадрирањем $\alpha_9^3 + \frac{1}{3} = i\frac{\sqrt{3}}{2}$, добија се да $\alpha_9^6 + \alpha_9^3 + 1 = 0$. Дакле, од значаја је полином $f(X) = X^6 + X^3 + 1$. Када у f уведемо смену $X := X + 1$, добијамо полином

$$g(X) = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3.$$

Применимо Ајзенштајнов критеријум на полином g, за прост број $p = 3$. Наиме, ако је $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$, и p прост број тако да

- p дели сваки од $a_{n-1}, \ldots, a_0$;
- p не дели a_n;
- p^2 не дели a_0;

тада је полином f нерастављив над $\mathbb{Q}$.

Следи да је $g(X)$ нерастављив над $\mathbb{Q}$. Како је $f(X) = g(X - 1)$, да је $f(X) = f_1(X)f_2(X)$ за неке $f_1, f_2 \in \mathbb{Q}[X]$, тада би и $g(X) = f(X + 1) = f_1(X + 1)f_2(X + 1)$ био растављив. Дакле, f је нерастављив над $\mathbb{Q}$, па је $f = \mu_{\alpha_9}$.

Како је $\alpha_{12} = cos\frac{2\pi}{12} + i\, sin\frac{2\pi}{12} = \frac{\sqrt{3}}{2} + i\frac{1}{2}$, квадрирањем једнакости, као и раније, закључујемо да је $\alpha_{12}^4 - \alpha_{12}^2 + 1 = 0$. Полином $X^4 - X^2 + 1$ је нерастављив над $\mathbb{Q}$, па је једнак $\mu_{\alpha_{12}}$.

43. Да ли $i \in \mathbb{Q}(i\sqrt{2})$?

Важи да је $[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$, јер је $\mu_{i\sqrt{2}} = X^2 + 2$. Ако би $i \in \mathbb{Q}(i\sqrt{2})$, онда би

$$[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}],$$

па следи $[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}(i)] = 1$. Дакле, $\mathbb{Q}(i\sqrt{2}) = \mathbb{Q}(i)$. Али није могуће написати $i\sqrt{2}$ у облику $a + ib$, за $a, b \in \mathbb{Q}$, како знамо да изгледају елементи у $\mathbb{Q}(i)$. Значи да i не припада $\mathbb{Q}(i\sqrt{2})$.

44. Да ли $i \in \mathbb{Q}(\alpha)$, где важи да $\alpha^3 + \alpha + 1 = 0$?

Полином $X^3 + X + 1$ је нерастављив над $\mathbb{Q}$, тако да је степен раширења $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Ако би i припадало том раширењу, слично као горе имали бисмо да 2 дели 3, што је немогуће.

45. Нека су $\alpha, \beta \in \mathbb{C}$. Ако су $\alpha + \beta$ и $\alpha\beta$ алгебарски елементи над $\mathbb{Q}$, доказати да су то онда и α и β.

Како су $\alpha + \beta$ и $\alpha\beta$ алгебарски елементи над $\mathbb{Q}$, постоје $f_1, f_2 \in \mathbb{Q}[X]$ тако да $f_1(\alpha + \beta) = 0$ и $f_2(\alpha\beta) = 0$. Важи да је

$$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \beta, \alpha + \beta, \alpha\beta) = \mathbb{Q}(\alpha, \alpha + \beta, \alpha\beta),$$

тако да имамо

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha+\beta) \subseteq \mathbb{Q}(\alpha+\beta, \alpha\beta) \subseteq \mathbb{Q}(\alpha, \alpha+\beta, \alpha\beta),$$

а тиме и

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\alpha+\beta,\alpha\beta):\mathbb{Q}(\alpha+\beta,\alpha\beta)]\cdot[\mathbb{Q}(\alpha+\beta,\alpha\beta):\mathbb{Q}(\alpha+\beta)]\cdot[\mathbb{Q}(\alpha+\beta):\mathbb{Q}].$$

Пошто је

$$p(X) = (X-\alpha)(X-\beta) = X^2 - (\alpha+\beta)X + \alpha\beta \in \mathbb{Q}(\alpha+\beta,\alpha\beta)[X],$$

следи да је $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha+\beta,\alpha\beta)] \leq 2$. Такође је $f_2 \in \mathbb{Q}(\alpha+\beta)[X]$, па $[\mathbb{Q}(\alpha+\beta,\alpha\beta):\mathbb{Q}(\alpha+\beta)] \leq \deg(f_2)$. Као и $[\mathbb{Q}(\alpha+\beta):\mathbb{Q}] \leq \deg(f_1)$. Следи да је $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \leq 2\deg(f_1)\deg(f_2)$, па је раширење $\mathbb{Q}(\alpha,\beta)$ коначно над $\mathbb{Q}$. Тада је онда и алгебарско, то јест, α и β су алгебарски над $\mathbb{Q}$.

46. Изразити $cos15°$ преко квадратних корена.

$$(cos15°)^2 = \frac{cos30°+1}{2} = \frac{\sqrt{3}}{4} + \frac{1}{2} \Rightarrow cos15° = \sqrt{\frac{\sqrt{3}}{4} + \frac{1}{2}}$$

Можемо закључити да је $cos15°$ конструктибилан број.

47. Доказати да је правилни петоугао конструктибилан.

Довољно је доказати да се може конструисати $cos\frac{2\pi}{5}$. Минимални полином за $\alpha = e^{\frac{2\pi i}{5}}$ је $X^4+X^3+X^2+X+1$. Имамо да

$$\begin{aligned}\alpha+\alpha^4 &= cos\frac{2\pi}{5} + i\,sin\frac{2\pi}{5} + cos\frac{8\pi}{5} + i\,sin\frac{8\pi}{5} \\ &= cos\frac{2\pi}{5} + i\,sin\frac{2\pi}{5} + cos\frac{2\pi}{5} - i\,sin\frac{2\pi}{5} = 2cos\frac{2\pi}{5}\end{aligned}$$

$$\begin{aligned}\alpha^2+\alpha^3 &= cos\frac{4\pi}{5} + i\,sin\frac{4\pi}{5} + cos\frac{6\pi}{5} + i\,sin\frac{6\pi}{5} \\ &= cos\frac{4\pi}{5} + i\,sin\frac{4\pi}{5} + cos\frac{4\pi}{5} - i\,sin\frac{4\pi}{5} = 2cos\frac{4\pi}{5} = 2(2cos^2\frac{2\pi}{5} - 1)\end{aligned}$$

$$\alpha^4+\alpha^3+\alpha^2+\alpha+1 = 0 \Rightarrow 2cos\frac{2\pi}{5} + 2(2cos^2\frac{2\pi}{5} - 1) + 1 = 0$$

Дакле, $4t^2+2t-1=0$, за $t = cos\frac{2\pi}{5}$. Решења ове квадратне једначине по t су $\frac{-1\pm\sqrt{5}}{4}$, а како је $cos\frac{2\pi}{5} > 0$ следи да је $cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$. Значи да се $cos\frac{2\pi}{5}$ може изразити преко квадратних корена, па је конструктибилан.

48. Да ли је правилни деветоугао конструктибилан?

Да ли је конструктибилан број $cos\frac{2\pi}{9} = cos40°$? Важи да је

$$cos\frac{\pi}{9} = \sqrt{\frac{1+cos\frac{2\pi}{9}}{2}}.$$

Одатле следи да ако би био конструктибилан $cos40°$, онда би био конструктибилан и $cos20°$, што знамо да није тачно. Дакле, правилни деветоугао није конструктибилан.

2. начин:

$$\begin{aligned}-\frac{1}{2} = cos(120°) = cos(40°+80°) &= cos40°cos80° - sin40°sin80° \\ &= cos40°(2cos^240° - 1) - sin40°2sin40°cos40° \\ &= 2cos^340° - cos40° - 2sin^240°cos40° \\ &= 2cos^340° - cos40° - 2(1-cos^240°)cos40° \\ &= 4cos^340° - 3cos40°\end{aligned}$$

Број $cos40°$ је нула полинома $4t^3 - 3t + \frac{1}{2}$, то јест $8t^3 - 6t + 1$. Тај полином је нерастављив над $\mathbb{Q}$, што повлачи да је $[\mathbb{Q}(cos40°) : \mathbb{Q}] = 3$. Дакле, степен раширења није једнак степену двојке, па није конструктибилан елемент.

49. Да ли је могуће конструисати квадрат чија је површина једнака површини датог троугла?

Јесте, зато што бисмо страницу тог квадрата добили као $\sqrt{P} = \sqrt{\frac{ah}{2}}$, где је a дужина странице троугла, а h његова висина.

50. Наћи полином четвртог степена $p(X) \in \mathbb{Z}[X]$ чија нула је $e^{\frac{2\pi i}{10}}$. Помоћу њега, наћи полином $q(X)$ другог степена над $\mathbb{Z}$ чија нула је $cos\frac{2\pi}{10}$, а затим тај број написати преко квадратних корена. Да ли је могуће конструисати правилни десетоугао?

$$\text{Из } X^{10} - 1 = (X^5 - 1)(X^5 + 1) = (X^5 - 1)(X + 1)(X^4 - X^3 + X^2 - X + 1)$$

следи да је тражени полином четвртог степена $p(X) = X^4 - X^3 + X^2 - X + 1$. Наиме, $e^{\frac{2\pi i}{10}}$ је десети корен јединице, али није пети корен јединице, а није ни -1. Сређивањем израза

$$0 = p(e^{\frac{2\pi i}{10}}) = cos\frac{8\pi}{10} + i\,sin\frac{8\pi}{10} - cos\frac{6\pi}{10} - i\,sin\frac{6\pi}{10} + cos\frac{4\pi}{10} + i\,sin\frac{4\pi}{10} - cos\frac{2\pi}{10} - i\,sin\frac{2\pi}{10} + 1,$$

добијамо да је

$$4cos^2\frac{2\pi}{10} - 2cos\frac{2\pi}{10} - 1 = 0.$$

Значи, $q(X) = 4X^2 - 2X - 1$. Пошто су нуле овог полинома $\frac{1\pm\sqrt{5}}{4}$ и $cos\frac{2\pi}{10} > 0$, следи да је $cos\frac{2\pi}{10} = \frac{1+\sqrt{5}}{4}$. На основу тога закључујемо и да је правилан десетоугао конструктибилан.

51. Испитати да ли полином $p(X) = X^5 + X^3 + X^2 - 7$ припада идеалу $I = \langle X^6 - 1, X^4 + 2X^3 + 2X^2 - 2X - 3\rangle$ у прстену полинома $\mathbb{R}[X]$. Доказати да $q(X) = X^4 + 2X^2 - 3$ припада I и написати га преко датих генератора овог идеала.

Нека су f_1 и f_2 дати генератори идеала I. На вежбама смо већ одредили да је $\text{nzd}(f_1, f_2) = X^2 - 1$, као и да

$$X^2 - 1 = \Big(-\frac{2}{57}X - \frac{9}{57}\Big)f_1 + \Big(\frac{2}{57}X^3 + \frac{5}{57}X^2 - \frac{12}{57}X + \frac{27}{57}\Big)f_2.$$

Дакле, $I = \langle X^2 - 1\rangle$ и неки полином g припада идеалу I акко $X^2 - 1$ дели g. Како је $p(X) = (X^2 - 1)(X^3 + 2X + 1) + (2X - 6)$, то јест, остатак при дељењу p са $X^2 - 1$ није нула, то p не припада I. Са друге стране, $q(X) = (X^2 - 1)(X^2 + 3) \in I$. Такође је

$$q = \left(-\frac{2}{57}X - \frac{9}{57}\right)(X^2 + 3)f_1 + \left(\frac{2}{27}X^3 + \frac{5}{57}X^2 - \frac{14}{57}X + \frac{22}{57}\right)(X^2 + 3)f_2.$$

52. Поређати у односу на лексикографски, степенасти лексикографски и обрнути степенасти лексикографски мономни поредак следеће мономе:

$$X_1, X_2, X_3, X_1^2, X_1X_2, X_1X_3, X_1X_2^2, X_3^3, X_1X_2X_3, X_2^2X_3$$

где је у сваком случају $X_1 > X_2 > X_3$.

За лексикографски поредак, то јест *lex* важи:

$$X_3 < X_3^3 < X_2 < X_2^2X_3 < X_1 < X_1X_3 < X_1X_2 < X_1X_2X_3 < X_1X_2^2 < X_1^2.$$

За степенасти лексикографски поредак, то јест *grlex* важи:

$$X_3 < X_2 < X_1 < X_1X_3 < X_1X_2 < X_1^2 < X_3^3 < X_2^2X_3 < X_1X_2X_3 < X_1X_2^2.$$

За обрнути степенасти лексикографски поредак, то јест *grrevlex*, који се дефинише на следећи начин:

$$X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n} \prec_{grrevlex} X_1^{\beta_1}X_2^{\beta_2}\cdots X_n^{\beta_n} \Leftrightarrow \left(\sum_{i=1}^{n}\alpha_i < \sum_{i=1}^{n}\beta_i\right) \text{ или}$$

$$\left(\sum_{i=1}^{n}\alpha_i = \sum_{i=1}^{n}\beta_i \text{ и } (\exists i \in \{1,\ldots,n\})((\forall j > i)(\alpha_j = \beta_j) \wedge \alpha_i > \beta_i)\right),$$

важи:

$$X_3 < X_2 < X_1 < X_1X_3 < X_1X_2 < X_1^2 < X_3^3 < X_2^2X_3 < X_1X_2X_3 < X_1X_2^2.$$

53. Одредити водећи производ, водећи коефицијент и водећи моном за полином

$$f(X,Y,Z) = 3X^4Z - 2X^3Y^4 + 7X^2Y^2Z^3 - 8XY^3Z^3 \in \mathbb{Q}[X,Y,Z]$$

у односу на $lex, grlex$ и $grrevlex$, где је $X > Y > Z$. Поновити за $Z > Y > X$.

$LM(f) = 3X^4Z$ у односу на lex ($LP(f) = X^4Z$, $LC(f) = 3$), а у односу на $grlex$ и $grrevlex$ је исти $LM(f) = -2X^3Y^4$. Ако је сада $Z > Y > X$, онда је $LM(f) = -8XY^3Z^3$ за сва три поретка.

54. Доказати да за било који мономни поредак $<$ на $K[X]$, где је K поље важи $1 < X < X^2 < X^3 \cdots$

Из прве особине за мономни поредак следи да $1 < X$. Множењем са X, то јест, коришћењем друге особине за мономни поредак следи да $X < X^2$. Даљим множењем добијамо да $X^2 < X^3$ и тако даље.

55. Доказати да је сваки од *lex*, *grlex* и *grrevlex* мономни поредак.

Проверићемо само за *grlex*, остало се доказује слично. Такође, прескачемо проверу да је *grlex* релација парцијалног уређења. Ако су $X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n}$ и $X_1^{\beta_1}X_2^{\beta_2}\cdots X_n^{\beta_n}$ два производа, тада су бројеви $\sum_{i=1}^n \alpha_i$ и $\sum_{i=1}^n \beta_i$ упоредиви. Ако је $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$, тада је $X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n} < X_1^{\beta_1}X_2^{\beta_2}\cdots X_n^{\beta_n}$. Слично, ако је прва сума већа од друге. Ако су суме једнаке, упоређујемо редом α_i и β_i. Свакако постоји индекс i тако да су $\alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}$ и $\alpha_i \neq \beta_i$, или, сви одговарајући степени су једнаки, а тиме су једнаки и полазни производи $X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n}$ и $X_1^{\beta_1}X_2^{\beta_2}\cdots X_n^{\beta_n}$. Ако је $\alpha_i < \beta_i$, онда је $X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n} < X_1^{\beta_1}X_2^{\beta_2}\cdots X_n^{\beta_n}$, и обрнуто. Дакле, *grlex* је линеаро уређење, то јест, свака два елемента су упоредива.

За доказ да је $1 < \boldsymbol{X}^{\boldsymbol{\alpha}}$ за све $\boldsymbol{\alpha} \neq \mathbf{0}$, приметимо да је тотални степен за $1 = X_1^0\cdots X_n^0$ једнак 0. Тотални степен, са друге стране за $\boldsymbol{X}^{\boldsymbol{\alpha}}$ је строго већи од нуле јер је $\boldsymbol{\alpha} \neq \mathbf{0}$.

За доказ друге особине, претпоставимо да је $X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n} < X_1^{\beta_1}X_2^{\beta_2}\cdots X_n^{\beta_n}$ и нека је $\boldsymbol{X}^{\boldsymbol{\gamma}}$ било који производ. Ако је $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$, тада је и

$$\sum_{i=1}^{n}\alpha_i + \sum_{i=1}^{n}\gamma_i < \sum_{i=1}^{n}\beta_i + \sum_{i=1}^{n}\gamma_i \Rightarrow \sum_{i=1}^{n}(\alpha_i+\gamma_i) < \sum_{i=1}^{n}(\beta_i+\gamma_i).$$

Следи да $\boldsymbol{X}^{\boldsymbol{\alpha}}\boldsymbol{X}^{\boldsymbol{\gamma}} < \boldsymbol{X}^{\boldsymbol{\beta}}\boldsymbol{X}^{\boldsymbol{\gamma}}$.

Ако је $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ и $\alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}$ и $\alpha_i < \beta_i$, за неко i. Тада је и

$$\alpha_1 + \gamma_1 = \beta_1 + \gamma_1, \ldots, \alpha_{i-1} + \gamma_{i-1} = \beta_{i-1} + \gamma_{i-1} \text{ и } \alpha_i + \gamma_i < \beta_i + \gamma_i.$$

Опет следи $\boldsymbol{X}^{\boldsymbol{\alpha}}\boldsymbol{X}^{\boldsymbol{\gamma}} < \boldsymbol{X}^{\boldsymbol{\beta}}\boldsymbol{X}^{\boldsymbol{\gamma}}$.

56. Доказати да у $K[X,Y]$, где је K поље, *grlex* и *grrevlex* представљају исти мономни поредак.

Нека је $X > Y$. Докажимо да из $X^aY^b \prec_{grlex} X^cY^d$ следи да $X^aY^b \prec_{grrevlex} X^cY^d$, затим и обрнуто. Ако $X^aY^b \prec_{grlex} X^cY^d$, у првом случају је $a+b < c+d$. Тада је и $X^aY^b \prec_{grrevlex} X^cY^d$. У другом случају је $a+b = c+d$. Такође је, због лексикографског поретка где $X > Y$, $a < c$ или $a = c, b < d$. Ако је $a < c$, због једнакости тоталног степена мора бити $b > d$, а тиме је $X^aY^b \prec_{grrevlex} X^cY^d$. Да су a и c једнаки, а $b < d$, је немогуће. Дакле, у оба случаја добијамо да $X^aY^b \prec_{grrevlex} X^cY^d$.

Са друге стране, нека је $X^aY^b \prec_{grrevlex} X^cY^d$. Први случај је опет $a+b < c+d$, када је и $X^aY^b \prec_{grlex} X^cY^d$. Други случај, када $a+b = c+d$, повлачи да, или $b > d$ (када мора бити $a < c$, па $X^aY^b \prec_{grlex} X^cY^d$), или $b = d$ и $a < c$, што није могуће.

57. Нека је $f(X,Y) = 2X^4Y^5 + 3X^5Y^2 + X^3Y^9 \in \mathbb{Q}[X,Y]$. Показати да не постоји мономни поредак на $\mathbb{Q}[X,Y]$ тако да $LP(f) = X^4Y^5$.

Претпоставимо супротно, постоји такав мономни поредак. Тада мора бити

$$X^5Y^2 < X^4Y^5, \qquad X^3Y^9 < X^4Y^5.$$

Због друге особине мономног поретка, смемо да помножимо прву релацију са производом Y^4, а другу са X. Добијамо

$$X^5Y^6 < X^4Y^9, \qquad X^4Y^9 < X^5Y^5.$$

Одатле имамо да $X^5Y^6 < X^5Y^5$. Али пошто $1 < Y$ повлачи да $X^5Y^5 < X^5Y^6$, имамо контрадикцију.

58. Нека је $f \in K[x_1, \ldots, X_n]$, где је K поље, хомогени полином. (Хомогени полином је полином чији сваки члан има исти тотални степен.) Нека је мономни поредак *grrevlex* где $X_1 > \cdots > X_n$. Доказати да $X_n \mid f$ ако и само ако $X_n \mid LP(f)$.

Ако X_n дели f, онда X_n мора да дели сваки моном у f, па и водећи моном.

Са друге стране, нека $X_n \mid LP(f)$ и нека је $LP(f) = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. Ако је $bX_1^{\beta_1} \cdots X_n^{\beta_n}$ било који други моном у f, тада је $X_1^{\alpha_1} \cdots X_n^{\alpha_n} > X_1^{\beta_1} \cdots X_n^{\beta_n}$. Како је f хомогени полином, следи да $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$. Због задатог поретка следи да је $\beta_n = \alpha_n$ или $\beta_n > \alpha_n$. Пошто X_n дели водећи члан, мора бит $\alpha_n \geq 1$. Тада је и $\beta_n \geq 1$, па $X_n \mid bX_1^{\beta_1} \cdots X_n^{\beta_n}$, а тиме X_n дели f.

59. Нека су $f = Y^2X + 4YX - 3X^2$ и $g = 2Y + X + 1$ елементи у $\mathbb{Q}[X,Y]$ и нека је задат степенасти лексикографски мономни поредак, где је $Y > X$. Ако је могуће, редуковати f помоћу g.

Како је $LP(f) = Y^2X$, а $LP(g) = Y$ и $Y \mid Y^2X$, f се може редуковати са g:

$$\begin{aligned} f_1 = f - \frac{LM(f)}{LM(g)}g &= Y^2X + 4YX - 3X^2 - \frac{Y^2X}{2Y}(2Y + X + 1) \\ &= Y^2X + 4YX - 3X^2 - Y^2X - \frac{1}{2}YX^2 - \frac{1}{2}YX \\ &= -\frac{1}{2}YX^2 + \frac{7}{2}YX - 3X^2. \end{aligned}$$

Како је $LP(f_1) = YX^2$ што је дељиво са $LP(g) = Y$, можемо наставити редукцију:

$$\begin{aligned} f_2 = f_1 - \frac{LM(f_1)}{LM(g)}g &= -\frac{1}{2}YX^2 + \frac{7}{2}YX - 3X^2 - \frac{-\frac{1}{2}YX^2}{2Y}(2Y + X + 1) \\ &= \frac{1}{4}X^3 + \frac{7}{2}YX - \frac{11}{4}X^2. \end{aligned}$$

Сада је $LP(f_2) = X^3$, што није дељиво са $LP(g) = Y$. Тако да се овде заустављамо са редукцијом, иако можемо приметити да се може извршити још једна редукција (јер је моном $\frac{7}{2}YX$ у f_2 дељив са Y):

$$\begin{aligned} f_3 = f_2 - \frac{\frac{7}{2}YX}{2Y}g &= \frac{1}{4}X^3 + \frac{7}{2}YX - \frac{11}{4}X^2 - \frac{7}{2}YX - \frac{7}{4}X^2 - \frac{7}{4}X \\ &= \frac{1}{4}X^3 - \frac{9}{2}X^2 - \frac{7}{4}X. \end{aligned}$$

60. Нека су $f = X^3Y^3 + 2Y^2, f_1 = 2XY^2 + 3X + 4Y^2, f_2 = Y^2 - 2Y - 2 \in \mathbb{Q}[X, Y]$ и задат је лексикографски мономни поредак где $X > Y$. Користећи алгоритам за дељење, наћи $u_1, u_2, r \in \mathbb{Q}[X, Y]$ тако да $f = u_1f_1 + u_2f_2 + r$.
Алгоритам за дељење полинома f са $F = \{f_1, \ldots, f_k\}$, то јест одређивање полинома $u_1, \ldots, u_n, r$ тако да $f = u_1f_1 + \cdots u_nf_n + r$. Поставимо све тражене полиноме на нулу и уведемо помоћни полином h:

$$u_1 := 0, \qquad \ldots \qquad u_n := 0, \qquad r := 0, \qquad h := f.$$

Док је $h \neq 0$, примењујемо следеће:

ако постоји индекс i тако да $LP(f_i) \mid LP(h)$
онда наћи најмање такво i и
$$u_i := u_i + \frac{LM(h)}{LM(f_i)}$$
$$h := h - \frac{LM(h)}{LM(f_i)}f_i$$
иначе
$$r := r + LM(h)$$
$$h := h - LM(h)$$

Према алгоритму, имамо да $LP(f_1) = XY^2$ и $LP(f_2) = Y^2$, као и

$$u_1 := 0,\ u_2 := 0,\ r := 0,\ h := X^3Y^3 + 2Y^2.$$

$h \neq 0$ и $XY^2 \mid X^3Y^3$ повлачи да:

$$\begin{aligned} u_1 &= 0 + \frac{LM(h)}{LM(f_1)} = \frac{X^3Y^3}{2XY^2} = \frac{1}{2}X^2Y \\ h &= h - \frac{LM(h)}{LM(f_1)}f_1 = X^3Y^3 + 2Y^2 - \frac{X^3Y^3}{2XY^2}(2XY^2 + 3X + 4Y^2) = -\frac{3}{2}X^3Y - 2X^2Y^3 + 2Y^2 \end{aligned}$$

$h \neq 0$; $XY^2 \nmid X^3Y$ и $XY^2 \nmid Y^2$ повлачи да:

$$\begin{aligned} r &= 0 + LM(h) - \frac{3}{2}X^3Y \\ h &= -2X^2Y^3 + 2Y^2 \end{aligned}$$

$h \neq 0$ и $XY^2 \mid X^2Y^3$ повлачи да:

$$\begin{aligned} u_1 &= \frac{1}{2}X^2Y + \frac{-2X^2Y^3}{2XY^2} = \frac{1}{2}X^2Y - XY \\ h &= -2X^2Y^3 + 2Y^2 - \frac{-2X^2Y^3}{2XY^2}(2XY^2 + 3X + 4Y^2) = 3X^2Y + 4XY^3 + 2Y^2 \end{aligned}$$

$h \neq 0$; $XY^2 \nmid X^2Y$ и $Y^2 \nmid X^2Y$ повлачи да:

$$\begin{aligned} r &= -\frac{3}{2}X^3Y + 3X^2Y \\ h &= 4XY^3 + 2Y^2 \end{aligned}$$

$h \neq 0$ и $XY^2 \mid XY^3$ повлачи да:

$$\begin{aligned} u_1 &= \frac{1}{2}X^2Y - XY + \frac{4XY^3}{2XY^2} = \frac{1}{2}X^2Y - XY + 2Y \\ h &= 4XY^3 + 2Y^2 - \frac{4XY^3}{2XY^2}(2XY^2 + 3X + 4Y^2) = -6XY - 8Y^3 + 2Y^2 \end{aligned}$$

$h \neq 0$; $XY^2 \nmid XY$ и $Y^2 \nmid XY$ повлачи да:

$$\begin{aligned} r &= -\frac{3}{2}X^3Y + 3X^2Y - 6XY \\ h &= -8Y^3 + 2Y^2 \end{aligned}$$

$h \neq 0$; $XY^2 \nmid Y^3$ и $Y^2 \mid Y^3$ повлачи да:

$$\begin{aligned} u_2 &= 0 + \frac{LM(h)}{LM(f_2} = \frac{-8Y^3}{Y^2} = -8Y \\ h &= -8Y^3 + 2Y^2 - \frac{-8Y^3}{Y^2}(Y^2 - 2Y - 2) = -14Y^2 - 16Y \end{aligned}$$

$h \neq 0$; $XY^2 \nmid Y^2$ и $Y^2 \mid Y^2$ повлачи да:

$$\begin{aligned} u_2 &= -8Y + \frac{-14Y^2}{Y^2} = -8Y - 14 \\ h &= -14Y^2 - 16Y - \frac{-14Y^2}{Y^2}(Y^2 - 2Y - 2) = -44Y - 28 \end{aligned}$$

$h \neq 0$; $XY^2 \nmid Y$ и $Y^2 \nmid Y$ повлачи да:

$$\begin{aligned} r &= -\frac{3}{2}X^3Y + 3X^2Y - 6XY - 44Y \\ h &= -28 \end{aligned}$$

$h \neq 0$; $XY^2 \nmid 1$ и $Y^2 \nmid 1$ повлачи да:

$$\begin{aligned} r &= -\frac{3}{2}X^3Y + 3X^2Y - 6XY - 44Y - 28 \\ h &= 0 \end{aligned}$$

Дакле, добијамо да

$$u_1 = \frac{1}{2}X^2Y - XY + 2Y,\ u_2 = -8Y - 14,\ r = -\frac{3}{2}X^3Y + 3X^2Y - 6XY - 44Y - 28.$$

61. Нека су $f = X^2Y^2 - W^2, f_1 = X - Y^2W, f_2 = Y - ZW, f_3 = Z - W^3, f_4 = W^3 - W \in \mathbb{Q}[X, Y, Z, W]$ и задат је лексикографски мономни поредак где $X > Y > Z > W$. Користећи алгоритам за дељење, наћи $u_1, u_2, u_3, u_4, r \in \mathbb{Q}[X, Y, Y, W]$ тако да $f = u_1f_1 + u_2f_2 + u_3f_3 + u_4f_4 + r$.

$$\begin{aligned} u_1 &= XY^2 + Y^4W \\ u_2 &= Y^5W^2 + Y^4ZW^3 + Y^3Z^2W^4 + Y^2Z^3W^5 + YZ^4W^6 + Z^5W^7 \\ u_3 &= Z^5W^8 + Z^4W^{11} + Z^3W^{14} + Z^2W^{17} + ZW^{20} + W^{23} \\ u_4 &= W^{23} + W^{21} + W^{19} + \cdots + W^3 + W \\ r &= 0 \end{aligned}$$

62. Нека су $f_1 = 2XY^2 + 3X + 4Y^2, f_2 = Y^2 - 2Y - 2 \in \mathbb{Q}[X, Y]$ са лексикографским мономним поретком где $X > Y$, као у задатку 60. Прво одредити остатак при дељењу полинома $f = X^3Y^3 + 2Y^2$ са $g_1 = f_2$ и $g_2 = f_1$, а затим искористити тај задатак и доказати да $\{f_1, f_2\}$ није Гребнерова база за идеал $\langle f_1, f_2\rangle$.

Примењујући алгоритам за дељење полинома f са g_1 и g_2 добијамо да је остатак једнак $6X^3Y + 4X^3 + 4Y + 4$. Из задатка 29. имамо да је остатак при дељењу f са f_1 и f_2 (приметимо да алгоритам зависи од поретка полинома којима се дели!) једнак $-\frac{3}{2}X^3Y + 3X^2Y - 6XY - 44Y - 28$. Пошто остатак при дељењу са $\{f_1, f_2\}$ није јединствен, следи да тај скуп не може чинити Гребнерову базу за идеал који генерише.

63. Доказати да полиноми f_1, f_2, f_3, f_4 из 61. задатка не чине Гребнерову базу за идеал који генеришу у односу на лексикографски поредак где $W > X > Y > Z$.

Приметимо да $f_3 + f_4 = -W + Z \in \langle f_1, f_2, f_3, f_4\rangle$. Водећи производ за овај полином је W, а

$$LP(f_1) = WY^2,\ LP(f_2) = WZ,\ LP(f_3) = W^3,\ LP(f_4) = W^3$$

у односу на овај мономни поредак. Како ниједан од водећих производа за f_1, f_2, f_3, f_4 не дели $LP(f_3 + f_4) = W$, следи да они не чине Гребнерову базу за $\langle f_1, f_2, f_3, f_4\rangle$.

64. Израчунати S-полиноме следећих парова у односу на *lex*, *grlex*, *grrevlex*, где $X > Y > Z$:

а) $f = 3X^2YZ - Y^3Z^3$, $g = XY^2 + Z^2$;

б) $f = 3X^2YZ - XY^3$, $g = XY^2 + Z^2$;

в) $f = 3X^2Y - YZ$, $g = XY^2 + Z^4$.

а) У односу на лексикографски поредак је $LP(f) = X^2YZ$ и $LP(g) = XY^2$, па је

$$\begin{aligned} S(f,g) &= \frac{X^2Y^2Z}{3X^2YZ}(3X^2YZ - Y^3Z^3) - \frac{X^2Y^2Z}{XY^2}(XY^2 + Z^2) \\ &= X^2Y^2Z - \frac{1}{3}Y^4Z^3 - X^2Y^2Z - XZ^3 = -XZ^3 - \frac{1}{3}Y^4Z^3. \end{aligned}$$

У односу на степенасти лексикографски поредак је $LP(f) = Y^3Z^3$ и $LP(g) = XY^2$, па је

$$\begin{aligned} S(f,g) &= \frac{XY^3Z^3}{-Y^3Z^3}(3X^2YZ - Y^3Z^3) - \frac{XY^3Z^3}{XY^2}(XY^2 + Z^2) \\ &= -3X^3YZ - YZ^5. \end{aligned}$$

У односу на обрнути степенасти лексикографски поредак је $LP(f) = Y^3Z^3$ и $LP(g) = XY^2$, па је S-полином исти као у претходном случају.

65. Користећи S-полиноме доказати да полиноми f_1, f_2, f_3, f_4 из 61. задатка чине Гребнерову базу за идеал који генеришу у односу на лексикографски поредак где $X > Y > Z > W$.

$$\begin{aligned} S(f_1, f_2) &= -Y^3W + XZW \xrightarrow{f_1} -Y^3W + Y^2ZW^2 \xrightarrow{f_2} 0 \\ S(f_1, f_3) &= -Y^2ZW + XW^3 \xrightarrow{f_1} -Y^2ZW + Y^2W^4 \xrightarrow{f_2} Y^2W^4 - YZ^2W^2 \\ &\xrightarrow{f_2} -YZ^2W^2 + YZW^5 \xrightarrow{f_2} YZW^5 - Z^3W^3 \xrightarrow{f_2} \\ &-Z^3W^3 + Z^2W^6 \xrightarrow{f_3} 0 \end{aligned}$$

$$\begin{aligned}
S(f_1,f_4) &= -Y^2W^4+XW \xrightarrow{f_1} -Y^2W^4+Y^2W^2 \xrightarrow{f_2} Y^2W^2-YZW^5 \\
&\xrightarrow{f_2} -YZW^5+YZW^3 \xrightarrow{f_2} YZW^3-Z^2W^6 \xrightarrow{f_2} \\
&-Z^2W^6+Z^2W^4 \xrightarrow{f_3} Z^2W^4-ZW^9 \xrightarrow{f_3} -ZW^9+ZW^7 \\
&\xrightarrow{f_3} ZW^7-W^{12} \xrightarrow{f_3} -W^{12}+W^{10} \xrightarrow{f_4} 0 \\
S(f_2,f_3) &= -Z^2W+YW^3 \xrightarrow{f_2} -Z^2W+ZW^4 \xrightarrow{f_3} 0 \\
S(f_2,f_4) &= -ZW^4+YW \xrightarrow{f_2} -ZW^4+ZW^2 \xrightarrow{f_3} ZW^2-W^7 \\
&\xrightarrow{f_3} -W^7+W^5 \xrightarrow{f_4} 0 \\
S(f_3,f_4) &= -W^6+ZW \xrightarrow{f_3} -W^6+W^4 \xrightarrow{f_4} 0
\end{aligned}$$

Пошто се сви S-полиноми редукују до нуле, следи да f_1, f_2, f_3, f_4 чине Гребнерову базу.

66. Наћи Гребнерову базу за $I = \langle f_1, f_2\rangle$ у односу на степенасти лексикографски поредак где $X > Y > Z$ и где су $f_1 = X^2Y + Z, f_2 = XZ + Y \in \mathbb{Q}[X, Y, Z]$.

Овде је $LP(f_1) = X^2Y$ и $LP(f_2) = XZ$. Како је S-полином $S(f_1, f_2) = -XY^2 + Z^2$ и не може се редуковати помоћу f_1 и f_2, назваћемо га f_3 и додати у скуп који ће постати Гребнерова база $G = \{f_1, f_2, f_3\}$. Треба израчунати $S(f_1, f_3)$ и $S(f_2, f_3)$. Ако се они редукују до нуле помоћу G онда је G Гребнерова база. А у супротном се скуп G повећава.

$$\begin{aligned}
S(f_1,f_3) &= XZ^2+YZ \xrightarrow{f_2} 0 \\
S(f_2,f_3) &= Y^3+Z^3
\end{aligned}$$

Како се S-полином за f_2 и f_3 не може редуковати до нуле, назваћемо га f_4 и додати у скуп G. Сада је $G = \{f_1, f_2, f_3, f_4\}$.

Треба израчунати $S(f_1, f_4), S(f_2, f_4)$ и $S(f_3, f_4)$.

$$\begin{aligned}
S(f_1,f_4) &= -X^2Z^3+Y^2Z \xrightarrow{f_2} Y^2Z+XYZ^2 \xrightarrow{f_2} 0 \\
S(f_2,f_4) &= Y^4-XZ^4 \xrightarrow{f_2} Y^4+YZ^3 \xrightarrow{f_4} 0 \\
S(f_3,f_4) &= -YZ^2-XZ^3 \xrightarrow{f_2} 0
\end{aligned}$$

Овиме добијамо да је Гребнерова база за идеал I једнака $\{f_1, f_2, f_3, f_4\}$.

67. Наћи Гребнерову базу за $I = \langle f_1, f_2\rangle$ у односу на лексикографски поредак где $X > Y$ и где су $f_1 = X^2 + Y^2 + 1, f_2 = X^2Y + 2XY + X \in \mathbb{Z}_5[X, Y]$.

Приметимо прво да се f_2 може редуковати помоћу f_1:

$$f_2 \xrightarrow{f_1} X^2Y + 2XY + X - Y(X^2 + Y^2 + 1) = 2XY + X + 4Y^3 + 4Y = f_2'.$$

Ради лакшег рачуна, а користећи чињеницу да $\langle f_1, f_2\rangle = \langle f_1, f_2'\rangle$, поступак одређивања Гребнерове базе примењујемо на полиноме f_1 и f_2'.

$$\begin{aligned}
S(f_1,f_2') &= \frac{X^2Y}{X^2}(X^2+Y^2+1)-\frac{X^2Y}{2XY}(2XY+X+4Y^3+4Y) \\
&= Y^3+Y-3X^2-+3XY^3+3XY = 2X^2+3XY^3+3XY+Y^3+Y \xrightarrow{f_1} \\
&\quad 3XY^3+3XY+Y^3+3Y^2+Y+3 \xrightarrow{f_2'} \\
&\quad 3XY^3+3XY+Y^3+3Y^2+Y+3+Y^2(2XY+X+4Y^3+4Y) \\
&= XY^2+3XY+4Y^5+3Y^2+Y+3 \xrightarrow{f_2'} \\
&\quad XY^2+3XY+4Y^5+3Y^2+Y+3+2Y(2XY+X+4Y^3+4Y) \\
&= 4Y^5+3Y^4+Y^2+Y+3 = f_3
\end{aligned}$$

Полином $f_3 = 4Y^5 + 3Y^4 + Y^2 + Y + 3$ се не може даље редуковати помоћу $\{f_1, f_2^{'}\}$, па га додајемо у Гребнерову базу. Доказаћемо још да се $S(f_1, f_3)$ и $S(f_2^{'}, f_3)$ редукују до нуле, одакле следи да је $\{f_1, f_2^{'}, f_3\}$ Гребнерова база за идеал I.

$$\begin{aligned}
S(f_1, f_3) &= Y^5(X^2 + Y^2 + 1) + X^2(4Y^5 + 3Y^4 + Y^2 + Y + 3) \\
&= Y^7 + Y^5 + X^2(3Y^4 + Y^2 + Y + 3) \xrightarrow{f_1} \\
&\quad Y^7 + Y^5 + X^2(3Y^4 + Y^2 + Y + 3) - (3Y^4 + Y^2 + Y + 3)(X^2 + Y^2 + 1) \\
&= Y^7 + 2Y^6 + Y^5 + Y^4 + 4Y^3 + Y^2 \xrightarrow{f_3} Y^5 + 2Y^4 + 4Y^2 + 4Y + 2 \xrightarrow{f_3} 0
\end{aligned}$$

$$\begin{aligned}
S(f_2^{'}, f_3) &= 3Y^4(2XY + X + 4Y^3 + 4Y) + X(4Y^5 + 3Y^4 + Y^2 + Y + 3) \\
&= XY^4 + XY^2 + XY + 3X + 2Y^7 + 2Y^5 \xrightarrow{f_2^{'}} \\
&\quad XY^4 + XY^2 + XY + 3X + 2Y^7 + 2Y^5 + (2Y^3 + 2Y + 2)(2XY + X + 4Y^3 + 4Y) \\
&= 2XY^3 + 2XY + 2Y^7 + 3Y^6 + 2Y^5 + Y^4 + 3Y^3 + 3Y^2 + 3Y \xrightarrow{f_2^{'}} \\
&\quad 2XY^3 + 2XY + 2Y^7 + 3Y^6 + 2Y^5 + 3Y^3 + 3Y^2 + 3Y \\
&\quad -(Y^2 + 1)(2XY + X + 4Y^3 + 4Y) = \\
&= 4XY^2 + 4X + 2Y^7 + 3Y^6 + 3Y^5 + Y^4 + 3Y^2 + 4Y \xrightarrow{f_2^{'}} \\
&\quad 3XY + 4X + 2Y^7 + 3Y^6 + 3Y^5 + 3Y^4 + 4Y \xrightarrow{f_2^{'}} \\
&\quad 2Y^7 + 3Y^6 + 3Y^5 + 3Y^4 + 4Y^3 + 3Y \xrightarrow{f_3} \\
&\quad 4Y^6 + 3Y^5 + Y^3 + Y^2 + 3Y \xrightarrow{f_3} 0
\end{aligned}$$

68. Одредити редуковану Гребнерову базу за идеал $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[X, Y]$, где су $f_1 = X^2Y - Y + X$ и $f_2 = XY^2 - X$, а задати мономни поредак је *grlex* где $Y > X$.

На стандардни начин одредимо Гребнерову базу $G = \{f_1, f_2, f_3, f_4, f_5\}$ за I, где су

$$f_3 = -Y^2 + XY + X^2,\ f_4 = X^4 + XY - 2X^2,\ f_5 = X^3 + Y - 2X.$$

Од ове базе добијамо минималну базу у два корака. Први је да од датих полинома направимо моничне, делећи сваки са његовим водећим коефицијентом. То се овде своди на то да само поделимо f_3 са -1 и добијемо полином $f_3^{'} = Y^2 - XY - X^2$. Други корак у формирању минималне базе је да избацимо све оне елементе из $\{f_1, f_2, f_3^{'}, f_4, f_5\}$ за које важи да је његов водећи производ дељив неким другим водећим производом полинома из тог скупа. Видимо да $LP(f_3^{'}) \,|\, LP(f_2)$, па избацујемо полином f_2. Такође, $LP(f_5) \,|\, LP(f_4)$, и избацујемо f_4. Дакле, минимална база је $G^{'} = \{f_1, f_3^{'}, f_5\}$. Редуковану базу добијамо од минималне тако што сваки полином g из $G^{'}$ редукујемо у односу на $G^{'} \setminus \{g\}$. Ниједан производ у $f_1 = X^2Y - Y + X$ није дељив водећим прозводима $LP(f_3^{'}) = Y^2$ и $LP(f_5) = X^3$, тако да је f_1 већ редукован у односу на $G^{'} \setminus \{f_1\}$. Слично, ниједан производ у $f_3^{'} = Y^2 - XY - X^2$ није дељив са $LP(f_1) = X^2Y$ и $LP(f_5) = X^3$, па је и $f_3^{'}$ редукован у односу на $G^{'} \setminus \{f_3^{'}\}$. Редукован је и f_5 у односу на $G^{'} \setminus \{f_5\}$, што значи да је $G^{'} = \{f_1, f_3^{'}, f_5\}$ редукована Гребнерова база за I.

69. Дати су идеали $I = \langle X^2 + Z, XY + Y^2 + Z, XZ - Y^3 - 2YZ, Y^4 + 3Y^2Z + Z^2 \rangle$ и $J = \langle X^2 + Z, XY + Y^2 + Z, X^3 - YZ \rangle$ у $\mathbb{Q}[X, Y, Z]$. Испитати да ли важи нека од следећих релација: $I = J$, $I \subset J$ или $J \subset I$.

Важи да су нека два идеала једнака ако и само ако су једнаке њихове редуковане Гребнерове базе. Назовимо генераторе идеала I редом

f_1, f_2, f_3, f_4. Можемо се уверити да је $F = \{f_1, f_2, f_3, f_4\}$ редукована Гребнерова база за I у односу на лексикографски поредак где је $X > Y > Z$.

Гребнерова база G за J у односу на исти поредак је једнака $G = \{g_1, g_2, g_3, g_4, g_5, g_6\}$ где су

$$g_1 = X^2+Z,\ g_2 = XY+Y^2+Z,\ g_3 = XZ+YZ,\ g_4 = Y^3+3YZ,\ g_5 = Y^2Z+2Z^2,\ g_6 = Z^2.$$

Она јесте минимална база, а редуковану добијемо када редукујемо g_5 са g_6: $g_5 \xrightarrow{g_6} Y^2Z = g_5^{'}$. Дакле, $G^{'} = \{g_1, g_2, g_3, g_4, g_5^{'}, g_6\}$ је редукована Гребнерова база за J.

Како је $F \neq G^{'}$, следи да I и J нису једнаки. Са друге стране,

$$f_1 = g_1,\ f_2 = g_2,\ f_3 = g_3 - g_4,\ f_4 = Yg_4 + g_6,$$

што значи да је $I \subset J$. Наиме, можемо се уверити да се f_i редукује до нуле помоћу $G^{'}$ за свако $i \in \{1, 2, 3, 4\}$, што значи да су ти елементи садржани у J, а тиме је и цело I садржано у J.

70. Нека је $I = \langle f_1, f_2\rangle \subseteq \mathbb{Q}[X, Y]$, где су $f_1 = X^2Y - Y + X$ и $f_2 = XY^2 - X$, а задати мономни поредак је *grlex* где $Y > X$ (као у задатку 68). Одредити базу векторског простора $\mathbb{Q}[X, Y]/I$ и написати таблицу множења базних елемената.

Као што смо се већ уверили, редуковану Гребнерову базу за I чине

$$g_1 = X^2Y - Y + X,\ g_2 = Y^2 - XY - X^2,\ g_3 = X^3 + Y - 2X.$$

Важи да се база за K-векторски простор $K[X_1, \ldots, X_n]/I$ састоји од свих

$$X_1^{\alpha_1} \ldots X_n^{\alpha_n} + I \text{ тако да } LP(g_i) \nmid X_1^{\alpha_1} \ldots X_n^{\alpha_n}, \qquad \forall i \in \{1, \ldots, k\},$$

где је $\{g_1, \ldots, g_k\}$ Гребнерова база за I.

Дакле, овде је потребно наћи све производе $X^\alpha Y^\beta$ који нису дељиви ниједним од

$$LP(g_1) = X^2Y,\ LP(g_2) = Y^2,\ LP(g_3) = X^3.$$

То ће бити $1, X, X^2, Y$ и XY. Следи да је база за $\mathbb{Q}$-векторски простор $\mathbb{Q}[X, Y]/I$ једнака

$$1 + I,\ X + I,\ X^2 + I,\ Y + I,\ XY + I,$$

а димензија $dim_{\mathbb{Q}}(\mathbb{Q}[X, Y]/I) = 5$. Напишимо још таблицу множења базних елемената. Објаснимо зашто је, на пример $(Y + I)(XY + I) = X + I$:

$$Y \cdot XY = XY^2 \xrightarrow{g_2} X^2Y + X^3 \xrightarrow{g_1} X^3 + Y - X \xrightarrow{g_3} X.$$

И остали производи се слично рачунају, користимо редукције елементима Гребнерове базе да бисмо резултат изразили преко елемената нађене базе за $\mathbb{Q}[X, Y]/I$.

	$1+I$	$X+I$	X^2+I	$Y+I$	$XY+I$
$1+I$	$1+I$	$X+I$	X^2+I	$Y+I$	$XY+I$
$X+I$	$X+I$	X^2+I	$-Y+2X+I$	$XY+I$	$Y-X+I$
X^2+I	X^2+I	$-Y+2X+I$	$-XY+2X^2+I$	$Y-X+I$	$XY-X^2+I$
$Y+I$	$Y+I$	$XY+I$	$Y-X+I$	$XY+X^2+I$	$X+I$
$XY+I$	$XY+I$	$Y-X+I$	$XY-X^2+I$	$X+I$	X^2+I

71. Наћи базу векторског простора $\mathbb{Z}_5[X,Y]/I$ (67. задатак) и написати таблицу множења базних елемената. Да ли елементи Y^2+I и $X+I$ имају инверзе у прстену $\mathbb{Z}_5[X,Y]/I$? Ако да, наћи те инверзе.

Сетимо се да је Гребнерова база (редукована) за идеал I једнака

$$g_1 = X^2+Y^2+1,\ g_2 = XY+3X+2Y^3+2Y,\ g_3 = Y^5+2Y^4+4Y^2+4Y+2.$$

Ово је рачунато у односу на лексикографски поредак, где $X>Y$, тако да су водећи производи

$$LP(g_1)=X^2,\ LP(g_2)=XY,\ LP(g_3)=Y^5.$$

Сви производи $X^\alpha Y^\beta$ који нису дељиви ниједним од ових су $1, X, Y, Y^2, Y^3, Y^4$, па је тражена база

$$\{1+I,\ X+I,\ Y+I,\ Y^2+I,\ Y^3+I,\ Y^4+I\},$$

и $dim_{\mathbb{Z}_5}(\mathbb{Z}_5[X,Y]/I)=6$. Представимо и таблицу множења ових елемената.

	1	x	y	y^2	y^3	y^4
1	1	x	y	y^2	y^3	y^4
x	x	$4y^2+4$	$2x+3y^3$ $+3y$	$4x+3y^4+y^3$ $+3y^2+y$	$3x+4y^2$ $+4$	$x+3y^3$ $+3y$
y	y	$2x+3y^3$ $+3y$	y^2	y^3	y^4	$3y^4+y^2$ $+y+3$
y^2	y^2	$4x+3y^4+y^3$ $+3y^2+y$	y^3	y^4	$3y^4+y^2$ $+y+3$	$4y^4+y^3+$ $4y^2+y+4$
y^3	y^3	$3x+4y^2$ $+4$	y^4	$3y^4+y^2$ $+y+3$	$4y^4+y^3+$ $4y^2+y+4$	$3y^4+4y^3$ $+4y+1$
y^4	y^4	$x+3y^3$ $+3y$	$3y^4+y^2$ $+y+3$	$4y^4+y^3+$ $4y^2+y+4$	$3y^4+4y^3$ $+4y+1$	$3y^4+y^2$ $+3y+3$

Овде је уведена ознака $x=X+I$ и $y=Y+I$ ради краћег записа.

Питамо се да ли постоји $g+I\in\mathbb{Z}_5[X,Y]$ тако да $(Y^2+I)(g+I)=1+I$. Тај елемент мора бити облика

$$g+I = a+bX+cY+dY^2+eY^3+fY^4+I,$$

за неке $a,b,c,d,e,f\in\mathbb{Z}_5$. После одговарајућег множења уз коришћење таблице, добијамо:

$$\begin{aligned}
1+I &= (Y^2+I)(a+bX+cY+dY^2+eY^3+fY^4+I)\\
&= aY^2+b(4X+3Y^4+Y^3+3Y^2+Y)+cY^3+dY^4+e(3Y^4+Y^2+Y+3)\\
&\quad +f(4Y^4+Y^3+4Y^2+Y+4)+I\\
&= (3e+4f)\cdot 1+4b\cdot X+(b+e+f)\cdot Y+\\
&\quad (a+3b+e+4f)Y^2+(b+c+f)Y^3+(3b+d+3e+4f)Y^4+I\\
&= (3e+4f)(1+I)+4b(X+I)+(b+e+f)(Y+I)+\\
&\quad (a+3b+e+4f)(Y^2+I)+(b+c+f)(Y^3+I)+(3b+d+3e+4f)(Y^4+I)
\end{aligned}$$

Сетимо се да је база векторског простора и линеарно независан скуп, па можемо изједначити одговарајуће коефицијенте. Следи да полазни елемент

има инверз ако и само ако следећи систем има решење у $\mathbb{Z}_5$:

$$\begin{aligned} 3e+4f &= 1\\ 4b &= 0\\ b+e+f &= 0\\ a+3b+e+4f &= 0\\ b+c+f &= 0\\ 3b+d+3e+4f &= 0 \end{aligned}$$

Лако се закључује да је $b=0$ и $d=4$, а наставком решавања добијамо и да $a=2$, $c=4$, $e=4$ и $f=1$. Дакле, инверз за полазни елемент постоји и једнак је $2+4Y+4Y^2+4Y^3+Y^4+I$.

72. Доказати да је векторски простор $\mathbb{Q}[X,Y,Z]/I$, где је I из 66. задатка, бесконачне димензије.

Гребнерова база за I је:

$$f_1 = X^2Y+Z,\ f_2 = XZ+Y,\ f_3 = XY^2-Z^2,\ f_4 = Y^3+Z^3,$$

а њихови водећи чланови су

$$LP(f_1) = X^2Y,\ LP(f_2) = XZ,\ LP(f_3) = XY^2,\ LP(f_4) = Y^3.$$

Приметимо да је сваки степен X^k+I, $k\in\mathbb{N}$, елемент те базе за $\mathbb{Q}[X,Y,Z]/I$, јер није дељив ниједним водећим чланом. То управо значи да је $\mathbb{Q}[X,Y,Z]/I$ бесконачне димензије.

73. Нека је $\mathbb{Q}[X,Y]/I$, где $I=\langle X^2+Y, Y^2+X\rangle$ и $\alpha\in\mathbb{Q}$. Доказати да елемент $XY+Y+\alpha+I\in\mathbb{Q}[X,Y]/I$ има инверз ако и само ако $\alpha\neq 0$.

Нека су $f_1 = X^2+Y, f_2 = Y^2+X$ и мономни поредак *grlex* где $X>Y$. Како је

$$S(f_1,f_2) = Y^3 - X^3 \xrightarrow{f_1,f_2} 0,$$

следи да ови полиноми чине Греброву базу за I, а да се база за векторски простор $\mathbb{Q}[X,Y]/I$ састоји из

$$1+I,\ X+I,\ Y+I,\ XY+I.$$

Имамо да је

$$(X+I)(X+I) = -Y+I, \qquad (Y+I)(Y+I) = -X+I,$$

као и

$$(X+I)(XY+I) = X+I, \qquad (Y+I)(XY+I) = Y+I, \qquad (XY+I)(XY+I) = XY+I.$$

Важи да $(XY+Y+\alpha+I)(a+bX+cY+dXY+I) = 1+I$, то јест,

$$\alpha a\cdot 1 + (b-c+\alpha b)X + (a+c+\alpha c+d)Y + (a+b+d+\alpha d)XY = 1+I$$

ако и само ако систем

$$\begin{aligned} \alpha a &= 1\\ (1+\alpha)b-c &= 0\\ a+(1+\alpha)c+d &= 0\\ a+b+(1+\alpha)d &= 0 \end{aligned}$$

има решење, где су $a, b, c, d \in \mathbb{Q}$. Ако систем има решење, тада је $\alpha \neq 0$. Ако је $\alpha \neq 0$, тада је $a = \frac{1}{\alpha}$, и остаје нам систем:

$$\begin{array}{rcrcrcl} (1+\alpha)b & - & c & & & = & 0 \\ & & (1+\alpha)c & + & d & = & -\frac{1}{\alpha} \\ b & + & & & (1+\alpha)d & = & -\frac{1}{\alpha} \end{array}$$

Множењем треће једначине са $-(1+\alpha)$ и додавањем првој, добијамо

$$\begin{array}{rcrcrcl} - & c & - & (1+\alpha)^2 d & = & \frac{1+\alpha}{\alpha} \\ & (1+\alpha)c & + & d & = & -\frac{1}{\alpha} \\ b & + & & (1+\alpha)d & = & -\frac{1}{\alpha} \end{array}$$

Множењем прве са $1+\alpha$ и додавањем другој, добијамо

$$\begin{array}{rcrcrcl} - & c & - & (1+\alpha)^2 d & = & \frac{1+\alpha}{\alpha} \\ & & & -\alpha(\alpha^2+3\alpha+3)d & = & \alpha+2 \\ b & + & & (1+\alpha)d & = & -\frac{1}{\alpha} \end{array}$$

Како је $\alpha(\alpha^2+3\alpha+3) \neq 0$, следи да је

$$d = -\frac{\alpha+2}{\alpha(\alpha^2+3\alpha+3)},\ c = -\frac{\alpha+1}{\alpha(\alpha^2+3\alpha+3)},\ b = -\frac{1}{\alpha(\alpha^2+3\alpha+3)}.$$

Значи да систем има решење.

74. Користећи теорију Гребнерових база, рационалисати израз $\frac{1}{i+\sqrt{3}+2}$.

Уочимо идеал $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[X,Y]$, где $f_1 = X^2+1$ и $f_2 = Y^2-3$. Приметимо да су прстени $\mathbb{Q}[i,\sqrt{3}]$ и $\mathbb{Q}[X,Y]/I$ изоморфни, при чему броју i одговара $X+I$, а броју $\sqrt{3}$ одговара $Y+I$. Тако да се питање рационалисања полазног израза своди на одређивање инверза елемента $X+Y+2+I$ у прстену $\mathbb{Q}[X,Y]/I$.

Можемо се уверити да f_1 и f_2 јесу Гребенрова база за I, као и да базу за простор $\mathbb{Q}[X,Y]/I$ чине $1+I, X+I, Y+I, XY+I$. Одредимо $a, b, c, d \in \mathbb{Q}$ тако да

$$(X+Y+2+I)(a+bX+cY+dXY+I) = 1+I.$$

Коришћењем релација $X^2+I = -1+I$ и $Y^2+I = 3+I$, добијамо систем:

$$\begin{array}{rcrcrcrcl} 2a & - & b & + & 3c & & & = & 1 \\ a & + & 2b & & & + & 3d & = & 0 \\ a & & & + & 2c & - & d & = & 0 \\ & & b & + & c & + & 2d & = & 0 \end{array}$$

Решење је:

$$a = \frac{1}{4}, \qquad b = -\frac{1}{2}, \qquad c = 0, \qquad d = \frac{1}{4},$$

па је инверз за $X+Y+2+I$ једнак $\frac{1}{4} - \frac{1}{2}X + \frac{1}{4}XY + I$. Дакле,

$$\frac{1}{i+\sqrt{3}+2} = \frac{1}{4} - \frac{1}{2}i + \frac{1}{4}i\sqrt{3}.$$

75. Користећи теорију Гребнерових база, рационалисати израз $\frac{1}{x+\sqrt{3}+\sqrt{5}}$.

Сада посматрамо прстен $\mathbb{Q}(x)[X_1, X_2]$ и идеал $I = \langle f, g \rangle$ у њему, где је $f = X_1^2 - 3$ и $g = X_2^2 - 5$. Када пређемо на количнички прстен $\mathbb{Q}(x)[X_1, X_2]/I$, елементу $X_1 + I$ одговара $\sqrt{3}$, а елементу $X_2 + I$ број $\sqrt{5}$. Дакле, занима нас како да $(x + X_1 + X_2 + I)^{-1}$ напишемо као комбинацију базних елемената са коефицијентима у $\mathbb{Q}(x)$.

Како се S-полином за f и g редукује до 0 (у односу на мономни поредак *grlex*, $X_1 > X_2$, на пример), следи да они чине Гребнерову базу за I, па је база за $\mathbb{Q}(x)$-векторски простор $\mathbb{Q}(x)[X_1, X_2]/I$ једнака $\{1 + I, X_1 + I, X_2 + I, X_1X_2 + I\}$.

Из

$$(x + X_1 + X_2 + I)(a + bX_1 + cX_2 + dX_1X_2 + I) = 1 + I,$$

за $a, b, c, d \in \mathbb{Q}(x)$, добијамо систем

$$\begin{array}{rcrcrcrcl} xa & + & 3b & + & 5c & & & = & 1 \\ a & + & xb & & & + & 5d & = & 0 \\ a & & & + & xc & + & 3d & = & 0 \\ & & b & + & c & + & xd & = & 0 \end{array}$$

Овај систем има решење над $\mathbb{Q}(x)$ које је једнако:

$$a = \frac{x^3 - 8x}{x^4 - 16x^2 + 4}, b = \frac{-x^2 - 2}{x^4 - 16x^2 + 4}, c = \frac{2 - x^2}{x^4 - 16x^2 + 4}, d = \frac{2x}{x^4 - 16x^2 + 4}.$$

Следи да је

$$\frac{1}{x + \sqrt{3} + \sqrt{5}} = \frac{x^3 - 8x}{x^4 - 16x^2 + 4} + \frac{-x^2 - 2}{x^4 - 16x^2 + 4}\sqrt{3} + \frac{2 - x^2}{x^4 - 16x^2 + 4}\sqrt{5} + \frac{2x}{x^4 - 16x^2 + 4}\sqrt{15}.$$

76. Доказати да је елемент $XY + I \in \mathbb{Q}[X, Y]/I$ делитељ нуле (задатак 70).

Докажимо да постоје $a, b, c, d, e \in \mathbb{Q}$ тако да

$$(XY + I)(a + bX + cX^2 + dY + eXY + I) = 0 + I.$$

Уз коришћење таблице за множење базних елемената, следи да

$$aXY + b(Y - X) + c(XY - X^2) + dX + eX^2 + I = 0 + I.$$

Сређивањем добијамо систем

$$\begin{array}{rcl} -b + d & = & 0 \\ -c + e & = & 0 \\ b & = & 0 \\ a + c & = & 0 \end{array}$$

Следи да је $b = d = 0$, као и да је $a = 1, c = e = -1$ једно решење система, то јест, важи да

$$(XY + I)(1 - X^2 - XY + I) = 0 + I.$$

77. Испитати да ли полином $f = -X^2 + Y + 1$ припада радикалу идеала $I = \langle XY^2 + 2Y^2, X^4 - 2X^2 + 1\rangle \subseteq \mathbb{Q}[X, Y]$.

Радикал неког идеала J у прстену R дефинишемо на следећи начин:

$$\sqrt{J} = \{a \in R \mid a^k \in J, \text{ за неко } k \in \mathbb{N}\}.$$

Имамо теорему која каже да полином f припада радикалу идеала $\langle f_1, \ldots, f_s\rangle \subseteq K[X_1, \ldots, X_n]$ ако и само ако $1 \in \langle f_1, \ldots, f_s, 1 - Zf\rangle$, при чему је идеал $\langle f_1, \ldots, f_s, 1 - Zf\rangle$ садржан у $K[X_1, \ldots, X_n, Z]$ и Z је нова неодређена.

Овде посматрамо идеал $\langle XY^2 + 2Y^2, X^4 - 2X^2 + 1, 1 - Z(-X^2 + Y + 1)\rangle$ у прстену $\mathbb{Q}[X, Y, Z]$. Лако се можемо уверити да је његова Гребнерова база једнака $\{1\}$. Тако да је

$$1 \in \langle XY^2 + 2Y^2, X^4 - 2X^2 + 1, 1 - Z(-X^2 + Y + 1)\rangle = \langle 1\rangle,$$

што значи да је полином f елемент радикала полазног идеала.