Задаци из Алгебре 2

1. Доказати да је скуп R један комутативни прстен са јединицом у односу на операције сабирања и множења матрица, где је
$$R = \left\{ \begin{pmatrix} a & 0 & b \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \;\Big|\; a, b \in \mathbb{R} \right\}.$$

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 $\mathbb{Q}$.

3. Доказати да је I један идеал у прстену R из 1. задатка, где је
$$I = \left\{ \begin{pmatrix} 0 & 0 & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \;\Big|\; c \in \mathbb{R} \right\}.$$

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

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

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

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

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

10. а) Доказати да је $K = \{p \in \mathbb{Z}[X] \,|\, p'(3) = 0\}$ потпрстен са јединицом у $\mathbb{Z}[X]$.
б) Доказати да је $I = \{p \in \mathbb{Z}[X] \,|\, p(3) = 0, p'(3) = 0\}$ 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.

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

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

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

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

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.

16. а) Доказати да је $R = \left\{ \begin{pmatrix} m & -n \\ n & m \end{pmatrix} \,\Big|\, m, n \in \mathbb{Z} \right\}$ 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 $m \in \mathbb{Z}$.

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.

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 $pu + qv = \mathrm{nzd}(p, q)$.

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

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 $p, q, r \in \mathbb{Z}_3[X]$:

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

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

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

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 $K \subseteq I$.

24. Конструисати поље са 4 елемента.

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

26. Конструисати поље са 9 елемената.

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.

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

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

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 $f \in \mathbb{F}_8[Y]$ тако да $I = \langle f \rangle$.

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

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 $\mathbb{Q}[X]$.

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

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

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

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

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

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

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

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

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

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) $n = 12$.

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

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

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.

46. Изразити $cos 15^\circ$ преко квадратних корена.

47. Доказати да је правилни петоугао конструктибилан.

48. Да ли је правилни деветоугао конструктибилан?

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

50. Наћи полином четвртог степена $p(X) \in \mathbb{Z}[X]$ чија нула је $e^{\frac{2\pi i}{10}}$. Помоћу њега, наћи полином 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?

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.

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 $X_1 > X_2 > X_3$.

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 $Z > Y > X$.

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

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

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

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 $LP(f) = X^4Y^5$.

58. Нека је $f \in K[x_1, \dots, X_n]$, 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 $X_n \,|\, f$ ако и само ако $X_n \,|\, LP(f)$.

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.

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 $f = u_1f_1 + u_2f_2 + r$.
<u>Алгоритам за дељење полинома</u> f са $F = \{f_1, \dots, f_k\}$, то јест одређивање полинома $u_1, \dots, u_n, r$ тако да $f = u_1f_1 + \cdots u_nf_n + r$. Поставимо све тражене полиноме на нулу и уведемо помоћни полином h:

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

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

<u>ако</u> постоји индекс i тако да $LP(f_i) \,|\, LP(h)$
онда наћи најмање такво i и

$$u_i := u_i + \frac{LM(h)}{LM(f_i)}$$

$$h := h - \frac{LM(h)}{LM(f_i)} f_i$$

<u>иначе</u>

$$r := r + LM(h)$$

$$h := h - LM(h)$$

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 $f = u_1f_1 + u_2f_2 + u_3f_3 + u_4f_4 + r$.

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 $\langle f_1, f_2 \rangle$.

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 $W > X > Y > Z$.

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

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 $X > Y > Z > W$.

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 $f_1 = X^2Y + Z, f_2 = XZ + Y \in \mathbb{Q}[X, Y, Z]$.

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

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 $Y > X$.

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 $J \subset I$.

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.

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.

72. Доказати да је векторски простор $\mathbb{Q}[X, Y, Z]/I$, где је I из 66. задатка, 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 $\alpha \neq 0$.

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

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

76. Доказати да је елемент $XY + I \in \mathbb{Q}[X, Y]/I$ делитељ нуле (задатак 68).

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