SBÍRKA ÚLOHA Z ALGEBRY, VERZE 2022

DAVID STANOVSKÝ

Jde o narychlo spíchnutý kompilát ze starší sbírky. Její struktura už dávno neodpovídá současnému kurzu. S ohledem na poptávku po početních úlohách dávám ven to, co zrovna mám, snad je lepší tohle, než vůbec nic. Prosím, mějte na paměti, že

- ne všechna témata a typové úlohy jsou zde zastoupeny,
- některá témata jsou zastoupena zbytečně mnoho, některá jsme ani nedělali (ne vše jsem zvládl promazat),
- řazení úplně neodpovídá sledu přednášky,
- spousta úloh má marginální smysl (ale nemám to teď čas třídit),
- některé úlohy mohou být chybně zadané, řešení taky nemusí být správně.

I. Dělitelnost

1. Elementární teorie čísel

1. Dokažte, že $7 \mid n^7 - n$.

2. Dokažte, že $9 \mid 4^n + 6n - 1$.

3. Dokažte, že $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

4. Dokažte, že $1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$.

5. * Sečtěte řadu $1^2 + 2^2 + \ldots + n^2$. [N]

6. * Sečtěte řadu $1^3 + 2^3 + \ldots + n^3$. [N]

7. Dokažte, že $\frac{1}{2} - \frac{2}{2^2} + \frac{3}{2^3} - \frac{4}{2^4} + \ldots + (-1)^{n+1}\frac{n}{2^n} = \frac{1}{9}(2 + (-1)^{n+1}\frac{3n+2}{2^n})$.

8. Spočtěte $\mathrm{NSD}(1023, 96)$ a $\mathrm{NSD}(168, 396)$. V obou případech najděte koeficienty z Bézoutovy rovnosti. [Ř]

9. Spočtěte poslední cifru čísla $99^{98^{97}}$. [Ř]

10. Dokažte, že $13 \mid 16^{20} + 29^{21} + 42^{22}$.

11. Najděte všechna $x \in \mathbb{Z}$ splňující a) $6x \equiv 9 \pmod{21}$, b) $10x \equiv 5 \pmod{21}$, c) $26^5 x \equiv 16 \pmod{11}$. [Ř]

12. Generál Chuan-wen poslal do bitvy tisíc vojáků. Po bitvě chtěl zjistit, kolik se jich vrátilo. Nechal je tedy nastoupit do řad po pěti a zjistil, že tři zbyli stranou. Pak je nechal nastoupit do řad po šesti, to zbyli také tři, a pak ještě po sedmi, to zbylo šest. Nakonec je nechal nastoupit po jedenácti a nezbyl žádný. Kolik vojáků přežilo bitvu? [Ř]

13. Skupině třinácti pirátů se podařilo uloupit bednu zlatých mincí. Zkusili je rozdělit rovným dílem na třináct hromádek, ale deset mincí jim zbylo. O zbylé mince se strhla rvačka, při níž jednoho piráta propíchli. Přestali tedy bojovat a zkusili mezi sebe znovu rozdělit mince rovným dílem. Tentokrát zbyly tři mince, o které opět začali bojovat. V boji zahynul další pirát a tak si ostatní opět zkusili mince spravedlivě rozdělit, tentokrát úspěšně. Kolik bylo nejméně mincí, které piráti ukradli? [Ř]

14. Najděte všechna (celočíselná) řešení soustavy $x \equiv 3 \pmod{11}$, $x \equiv 6 \pmod{8}$, $x \equiv 14 \pmod{15}$. [Ř]

15. Najděte všechna řešení soustavy $2x \equiv -1 \pmod{3}$, $3x \equiv 2 \pmod{5}$, $3x \equiv 6 \pmod{8}$. [Ř]

16. Najděte všechna řešení soustavy $2x \equiv 3 \pmod{6}$, $2x \equiv 1 \pmod{5}$. [Ř]

17. Najděte všechna řešení soustavy $2x \equiv 4 \pmod{6}$, $2x \equiv 1 \pmod{5}$. [Ř]

18. * Buď $a_1, \ldots, a_k$, n, b přirozená čísla, položme $d = \mathrm{NSD}(a_1, \ldots, a_k, n)$. Dokažte, že kongruence $a_1x_1 + \ldots + a_kx_k \equiv b \pmod{n}$ má řešení právě tehdy, když $d \mid b$.

19. Dokažte, že $11 \mid 3^{2000} + 4^{2002} + 5^{2001}$. [Ř]

20. Dokažte, že $13 \mid 2^{60} + 7^{30}$. [Ř]

21. Spočtěte $121^{121} \bmod 18$ a $127^{217} \bmod 129$. [Ř]

22. Spočtěte $13^{13^{13}} + 15^{15^{15}} \bmod 17$.

23. Spočtěte $2^\ell \bmod 13$, kde ℓ je současný letopočet.

24. Spočtěte $2^{3^{4^{5^{6^7}}}} \mod 9$. [Ř]

25. Spočtěte $3^{3^{3^{3^{3^3}}}} \mod 28$. [Ř]

26. Spočtěte $3^{5^{7^{9^{11}}}} \mod 35$. [Ř]

27. Spočtěte poslední cifru čísla $2^{3^{2^{3^{2^3}}}}$. [Ř]

28. Spočtěte poslední dvě cifry čísla $87^{85^{83}}$. [Ř]

29. Spočtěte $a^{101} \bmod 125$ v závislosti na $a \in \mathbb{Z}$. [Ř]

30. * Dokažte, že pro libovolné n je číslo $2^{2^{2n+1}} + 3$ složené. [N]

31. Dokažte, že $5 \mid n^9 + 2n^7 + 3n^3 + 4n$ pro každé $n \in \mathbb{N}$. [Ř]

32. Řešte v $\mathbb{Z}$ rovnici $x^6 + x + xy \equiv 1 \pmod 7$. [Ř]

33. ** Nechť $n = pq$, kde p, q jsou lichá prvočísla. Dokažte, že pro každé a nesoudělné s n má rovnice $x^2 \equiv a \pmod n$ žádné nebo právě čtyři řešení. (Jinými slovy, existuje-li nějaká druhá odmocnina z a modulo n, pak jsou tyto odmocniny právě čtyři.) [?]

34. Buď p prvočíslo a $a \in \mathbb{Z}$. Dokažte, že pokud $a^2 \equiv 1 \pmod p$, pak $a \equiv 1 \pmod p$ nebo $a \equiv -1 \pmod p$.

35. * Dokažte, že číslo p je prvočíslo právě tehdy, když

$$(p-1)! \equiv -1 \pmod p.$$

[Wilsonovo kritérium] [N]

2. Obory polynomů

36. Najděte v oboru $\mathbb{Z}[x]$ ideál, který není hlavní. [Ř]

37. Buď $\mathbf{R}$ obor integrity. Najděte v oboru $\mathbf{R}[x, y]$ ideál, který není hlavní. [Ř]

38. Uvažujte obor $\mathbb{Z}[x]$. Proč zobrazení $f \mapsto 1 + \deg f$ není Eukleidovská norma? Uveďte protipříklad na Bezoutovu rovnost. [Ř]

39. Zjistěte, za jakých podmínek v $\mathbb{Z}[x]$ platí $x^m - 1 \mid x^n - 1$. [Ř]

40. Spočtěte v oboru $\mathbb{Z}[x]$ zbytek po dělení polynomů $x^n - 1$ a $x^m - 1$. [Ř]

41. Spočtěte v oboru $\mathbb{Z}[x]$ NSD polynomů $x^n - 1$ a $x^m - 1$. [Ř]

42. * Zjistěte, zda platí následující tvrzení pro libovolný obor integrity $\mathbf{R}$ a $f \in R[x]$: jestliže $x - 1 \mid f(x^n)$, pak $x^n - 1 \mid f(x^n)$. [N] [Ř]

43. * Dokažte, že pro žádné $n > 2$ neexistují nenulové polynomy $f, g, h \in \mathbb{Z}[x]$ splňující $f^n + g^n = h^n$. V řešení můžete využít Velkou Fermatovu větu, která říká, že neexistují žádná nenulová celá čísla s touto vlastností. [Ř]

44. Určete takové $a \in \mathbb{C}$, pro než má polynom $f = 2x^6 - x^5 - 11x^4 - x^3 + ax^2 + 2ax + 8 \in \mathbb{C}[x]$ kořen 2. [Ř]

45. Najděte polynom v $\mathbb{Z}[x]$, mezi jehož kořeny jsou čísla $\frac{1}{2}$, i a $2 - i$. [Ř]

46. Najděte polynom f v $\mathbb{Z}[x]$ stupně 3 splňující $x - 1 \mid f$ a $f(2) = f(3) = f(4)$. [Ř]

47. Najděte komutativní okruh $\mathbf{R}$ a polynom $f \in R[x]$ stupně 2 s více než dvěma kořeny v $\mathbf{R}$. [Ř]

48. Uvažujte nekomutativní těleso kvaternionů $\mathbb{H}$ a najděte polynom $f \in \mathbb{H}[x]$ stupně 2, který má více než dva kořeny. [Ř]

49. * Spočtěte determinant matice $A = (a_{ij})_{i,j=1}^{n}$, kde $a_{ij} = u_i^{j-1}$ a $u_1, \ldots, u_n \in \mathbb{R}$. Návod: uvažujte determinant jako polynom nad proměnnými $u_1, \ldots, u_n$. [tzv. Vandermondův determinant] [N] [Ř]

50. Najděte všechny racionální kořeny polynomů

(a) $2x^3 - x^2 + 3$,
(b) $12x^6 + 8x^5 - 85x^4 + 15x^3 + 55x^2 + x - 6$,
(c) $4x^7 - 16x^6 + x^5 + 55x^4 - 35x^3 - 38x^2 + 12x + 8$.

[Ř]

51. Je polynom $2x^3 + 4$ ireducibilní v oborech $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$, $\mathbb{Z}_5[x]$? [Ř]

52. Jsou polynomy $x^3 + 3x - 2$, $4x^2 - 1$ a $x^7 + 2$ ireducibilní v oboru $\mathbb{Z}[x]$? [Ř]

53. Najděte všechny ireducibilní polynomy a) v $\mathbb{C}[x]$, b) v $\mathbb{R}[x]$. [Ř]

54. Najděte všechny ireducibilní polynomy a) v $\mathbb{Z}_2[x]$ stupně ≤ 5, b) v $\mathbb{Z}_3[x]$ stupně ≤ 4.

55. * Buď p prvočíslo. Dokažte, že je-li a generátor grupy $\mathbb{Z}_p^*$, pak je polynom $x^p - x + a$ ireducibilní v $\mathbb{Z}_p[x]$. [?] [N]

56. Zjistěte, zda platí následující tvrzení pro každé $f \in \mathbb{Q}[x]$ a $a \in \mathbb{Q}$: jestliže f je ireducibilní, pak $f(x + a)$ je ireducibilní. [Ř]

57. * Dokažte, že pro každé prvočíslo p je polynom $\frac{x^p-1}{x-1}$ ireducibilní v $\mathbb{Z}[x]$. [N]

58. Rozložte polynom $x^4 - x^2 - 2$ na součin ireducibilních prvků v oborech $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_5[x]$, $\mathbb{Z}_3[x]$. [Ř]

59. Rozložte na součin ireducibilních prvků v oboru $\mathbb{Z}[x]$ následující polynomy: $x^4 + 1$, $x^4 + x^2 + 1$, $x^4 + x^3 + x^2 + x + 1$, $2x^2 + 9x + 10$. [Ř]

60. Rozložte na součin ireducibilních prvků v oborech $\mathbb{Z}[x]$ a $\mathbb{Q}[x]$ následující polynomy: $2x^3 + 4x^2 - 2x + 4$, $2x^3 + 3x^2 + 2x + 3$. [Ř]

61. Rozložte na součin ireducibilních prvků polynom $x^5 + 3x^3 + x + 3$ v oboru $\mathbb{Z}_5[x]$. [Ř]

62. Rozložte na součin ireducibilních prvků v oboru $\mathbb{Z}_3[x]$ následující polynomy: $x^3 + x^2 + 2$, $x^5 + x^2 - x + 1$, $x^6 + 1$. [Ř]

63. Rozložte na součin ireducibilních prvků polynom $2x^5 + x^4 - 2x^3 - x^2 - 4x - 2$ v oborech $\mathbb{Z}[x]$ a $\mathbb{Z}_5[x]$. [Ř]

64. * Rozložte na součin ireducibilních prvků a) polynom $x^{15} - 1$ v oboru $\mathbb{Z}_2[x]$, b) polynom $x^8 - 1$ v $\mathbb{Z}_3[x]$. [Ř]

65. Spočtěte $\mathrm{NSD}(x^4 + 2x^3 + x^2 + 2x, 2x^5 + x^4 + x + 2)$ a koeficienty z Bézoutovy rovnosti v oboru $\mathbb{Z}_3[x]$. [Ř]

66. Spočtěte a) $\mathrm{NSD}(x^4 + 3x^2 + 4x, 2x^2 - 2x - 4)$, b) $\mathrm{NSD}(x^4 + 1, x^3 - 1)$, c) $\mathrm{NSD}(x^4 - 3x^2 - 2x + 4, x^3 - x^2 - x + 1)$ v oboru $\mathbb{Q}[x]$. [Ř]

67. Spočtěte $\mathrm{NSD}(2x^3 + 1, x^4 - x^3 + 2x^2 - x - 1)$ v oborech $\mathbb{Q}[x]$ a $\mathbb{Z}_3[x]$. [Ř]

68. Spočtěte a) $\mathrm{NSD}(x^4 - 2x^3 + x^2 + 1, x^3 - x + 2)$, b) $\mathrm{NSD}(x^5 + x^3 + x^2 - 2x + 2, x^6 + x^5 + 2x^4 + x^3 + 2x^2 - 2x - 1)$ v oboru $\mathbb{Z}_5[x]$. [Ř]

69. Spočtěte $\mathrm{NSD}(x^6 - x^4 - x^2 + 1, x^4 + 3x^3 + 3x^2 + 3x + 2)$ v oborech $\mathbb{Q}[x]$ a $\mathbb{Z}_5[x]$. [Ř]

70. Zjistěte násobnost kořene -1 polynomu $x^5 - ax^2 - ax + 1 \in \mathbb{Q}[x]$ v závislosti na parametru $a \in \mathbb{Q}$. [Ř]

71. Najděte všechna $a, b \in \mathbb{Q}$ taková, že polynom $(x - 1)^2$ dělí v $\mathbb{Q}[x]$ polynom $ax^{n+1} + bx^n - 1$. [Ř]

72. Najděte všechna $a, b \in \mathbb{Q}$ taková, že polynom $x^5 + ax^3 + b$ má dvojnásobný kořen v $\mathbb{Q}$. [Ř]

73. Zjistěte násobnost

(a) kořene 1 v polynomu $x^4 + 2x^3 + x^2 + 3x + 3 \in \mathbb{Z}_5[x]$;
(b) kořene 6 v polynomu $x^4 + 3x^3 - x^2 + 3x - 1 \in \mathbb{Z}_7[x]$;
(c) kořene 1 v polynomu $x^4 + x^3 + 2x + 2 \in \mathbb{Z}_3[x]$.

[Ř]

74. Najděte všechny aspoň dvojnásobné kořeny polynomu $x^6+7x^5+18x^4+25x^3+25x^2+8x-12$ v $\mathbb{Q}$. [Ř]

75. Najděte všechny aspoň dvojnásobné kořeny polynomu $x^4 - x^3 - x^2 + x + 1$ v $\mathbb{C}$. [Ř]

76. * Najděte všechny aspoň dvojnásobné kořeny polynomu $x^6+6x^5+15x^4+20x^3+12x^2-4$ v $\mathbb{Q}$. [N]

77. Polynom $x^4 + 2ix^3 + x^2 + 2ix + 1 \in \mathbb{C}[x]$ má v $\mathbb{C}$ dvojnásobný kořen. S využitím této vlastnosti jej rozložte na ireducibilní činitele. [?]

3. Číselné obory

78. Spočtěte prvky grup $\mathbb{Z}[i]^*$, $\mathbb{Z}[i\sqrt{2}]^*$ a rozložte tyto grupy na součin cyklických grup. [Ř]

79. Všimněte si, že grupa $\mathbb{Z}[\sqrt{2}]^*$ je nekonečná a najděte v ní prvek nekonečného řádu. [Ř]

80. ** Je grupa $\mathbb{Z}[\sqrt{2}]^*$ konečně generovaná? [?] [N]

81. Rozložte v $\mathbb{Z}[i]$ na součin ireducibilních prvků následující čísla: $4 + 2i$, $5i$, $1 - 5i$, 6, 11. [Ř]

82. * Dokažte, že číslo $a + bi$, $a, b \neq 0$, je ireducibilní v oboru $\mathbb{Z}[i]$ právě tehdy, když je $a^2 + b^2$ prvočíslo. [N] [Ř]

83. Dokažte, že pokud je p prvočíslo a $p \equiv 3 \pmod 4$, pak je ireducibilní v oboru $\mathbb{Z}[i]$. [Ř]

84. ** Dokažte, že pokud je p prvočíslo a $p \equiv 1 \pmod 4$, pak není ireducibilní v oboru $\mathbb{Z}[i]$. [N]

85. Rozložte v $\mathbb{Z}[i\sqrt{2}]$ na součin ireducibilních prvků následující čísla: $1 + 3i\sqrt{2}$, 5, $2 + 2i\sqrt{2}$. [Ř]

86. Ověřte, že prvky $2, \sqrt{5}+1, \sqrt{5}-1$ jsou ireducibilní v oboru integrity $\mathbb{Z}[\sqrt{5}]$ a že $2 \nmid \sqrt{5} \pm 1$. Protože $4 = 2 \cdot 2 = (\sqrt{5}+1) \cdot (\sqrt{5}-1)$, obor $\mathbb{Z}[\sqrt{5}]$ není Gaussovský.

87. S využitím předešlé úlohy najděte v oboru $\mathbb{Z}[\sqrt{5}]$ a) ireducibilní prvek, který není prvočinitel, b) prvky a, b, pro něž neexistuje $\mathrm{NSD}(a, b)$. [Ř]

88. Dokažte, že obor $\mathbb{Z}[i\sqrt{3}]$ není Gaussovský. [Ř]

89. Dokažte, že právě definovaná q, r splňují $a = bq + r$ a $\nu(r) < \nu(b)$. (Tedy že ν je skutečně Eukleidovská norma na $\mathbb{Z}[i]$.) [Ř]

90. Dokažte, že obory $\mathbb{Z}[i\sqrt{2}]$ a $\mathbb{Z}[\omega]$ jsou Eukleidovské. Zde $\omega = e^{2\pi i/3}$ značí komplexní třetí odmocninu z jedné. [Ř]

91. * Dokažte, že obory $\mathbb{Z}[\sqrt{2}]$ a $\mathbb{Z}[\sqrt{3}]$ jsou Eukleidovské. [N]

92. Spočtěte v $\mathbb{Z}[i]$ NSD a NSN čísel a) $3 + i, 4 + 2i$, b) $3 + 6i, 12 - 3i$, c) $5 + 3i, 13 + 18i$ d) $85, 1 + 13i$. [Ř]

93. Zjistěte, zda je množina $\{a \in \mathbb{Z}[i] : 3+6i \mid a \text{ a } 12-3i \mid a\}$ a) ideál, b) hlavní ideál oboru $\mathbb{Z}[i]$. Pokud ano, najděte generátor. [Ř]

94. Zjistěte, zda je množina $\{a \in \mathbb{Z}[i] : 4 \mid \nu(a) \text{ a } 7-3i \mid a\}$ a) ideál, b) hlavní ideál oboru $\mathbb{Z}[i]$. Pokud ano, najděte generátor. [N] [Ř]

4. Konečná tělesa

95. Napište tabulku sčítání a násobení čtyřprvkového, osmiprvkového a devítiprvkového tělesa.

96. Uvažujme těleso $\mathbb{F}_{125} = \mathbb{Z}_5[x]/x^3+x+1$. Spočtěte $[3x^2+4x+1]+[2x^2+4]$, $[3x^2+4x+1]\cdot[2x^2+4]$ a $[x]^{-1}$. [Ř]

97. Uvažujme těleso $\mathbb{F}_{81} = \mathbb{Z}_3[x]/x^4+x^2+x+1$. Spočtěte $[x^3+2x^2]+[2x^2+1]$, $[x^3+2x^2]\cdot[2x^2+1]$ a $[x+1]^{-1}$. (Ověřte, že je polynom x^4+x^2+x+1 skutečně ireducibilní v $\mathbb{Z}_3[x]$.) [Ř]

98. Najděte primitivní prvky tělesa $\mathbb{F}_8 = \mathbb{Z}_2[x]/x^3+x+1$. [Ř]

99. Najděte primitivní prvky tělesa $\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2+1$. [Ř]

100. Najděte primitivní prvky tělesa $\mathbb{F}_{16} = \mathbb{Z}_2[x]/x^4+x+1$.

101. Kolik podtěles má těleso $\mathbb{F}_{p^2}$? [?] [Ř]

II. Grupy

1. Příklady a základní vlastnosti

102. Rozhodněte, zda pro danou množinu A a danou operaci (označme ji zatím $*$) existují operace $'$ a konstanta e tak, aby $(A, *, ', e)$ byla grupa. Které z těchto grup jsou abelovské?

(1) $A = \mathbb{Q}$, operace $\cdot$.
(2) $A = \mathbb{Q}$, operace $-$.
(3) $A = \mathbb{Q}$, operace $*$ definovaná $a * b = |a \cdot b|$.
(4) $A = \mathbb{Q} \setminus \{0\}$, operace $\circ$ definovaná $a \circ b = a \cdot b$ pro $a > 0$ a $a \circ b = \frac{a}{b}$ pro $a < 0$.
(5) $A = \mathbb{Z}$, operace $*$ definovaná $a * b = a + (-1)^a b$.
(6) $A = M_n(\mathbb{Q})$, operace $+$.
(7) $A = M_n(\mathbb{Q})$, operace $\cdot$.
(8) $A = GL_n(\mathbb{Z})$, operace $\cdot$.
(9) $A = P(X)$, operace $\cap$.
(10) $A = P(X)$, operace $\cup$.
(11) $A = P(X)$, operace $\triangle$ definovaná $U \triangle V = (U \setminus V) \cup (V \setminus U)$.

Zde $P(X)$ značí množinu všech podmnožin dané množiny X. [Ř]

103. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $a \in G$. Definujme novou operaci na $\mathbf{G}$ předpisem $x \circ y = x * a * y$. Dokažte, že existují operace $''$ a konstanta u tak, aby $(G, \circ, '', u)$ byla grupa. [Ř]

104. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $a, b, c \in G$. Spočtěte všechny $x \in G$ takové, že $c * ((a^2 * x) * b') = c' * b^2$. [Ř]

105. Dokažte, že $\mathbb{Z}_n^*$ je skutečně grupa. Najděte a) prvek 10^{-1} v grupě $\mathbb{Z}_{47}^*$, b) prvek 20^{-1} v grupě $\mathbb{Z}_{97}^*$. [N] [Ř]

106. Dokažte, že v každé grupě sudého řádu existuje prvek řádu 2.

107. Dokažte, že každá grupa, ve které mají všechny prvky řád 1 nebo 2, je abelovská.

108. * Buď $\mathbf{G} = (G, *, ', e)$ grupa a a její prvek řádu mn, kde m, n jsou nesoudělné. Pak existuje $b, c \in G$ takové že $a = b * c$ a $|b|$ dělí m a $|c|$ dělí n. [N] [Ř]

109. Buď $\mathbf{G} = (G, *, ', e)$ grupa a a, b její prvky konečného řádu splňující $a * b = b * a$. a) Dokažte, že $a * b$ je konečného řádu a $|a * b|$ dělí NSN$(|a|, |b|)$. b) * Jsou-li $|a|$, $|b|$ nesoudělné, dokažte, že $|a * b| = |a| \cdot |b|$.

110. Dokažte, že podmnožina $H \subseteq G$ tvoří podgrupu grupy $\mathbf{G} = (G, *, ', e)$ právě tehdy, když $a * b' \in H$ pro každé $a, b \in H$. [Ř]

111. Dokažte, že *konečná* podmnožina $H \subseteq G$ tvoří podgrupu grupy $\mathbf{G} = (G, *, ', e)$ právě tehdy, když $a * b \in H$ pro každé $a, b \in H$.

112. Je pravda, že prvky konečného řádu vždy tvoří podgrupu dané grupy? [Ř]

113. Je pravda, že prvky konečného řádu vždy tvoří podgrupu dané *abelovské* grupy? [Ř]

114. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $\mathbf{A}$,$\mathbf{B}$ její podgrupy. Dokažte, že a) $A \cap B$ tvoří podgrupu, b) $A \cup B$ tvoří podgrupu právě tehdy, když $A \subseteq B$ nebo $B \subseteq A$; c) $AB = \{a * b : a \in A, b \in B\}$ tvoří podgrupu právě tehdy, když $AB = BA$.

115. * Buď $\mathbf{G}$ konečná grupa a $\mathbf{A}$,$\mathbf{B}$ její podgrupy. Dokažte, že $|A| \cdot |B| = |A \cap B| \cdot |AB|$.

116. Buď $\mathbf{G}$ grupa velikosti p^k, p prvočíslo. Dokažte, že $\mathbf{G}$ obsahuje prvek řádu p. [Ř]

117. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $\mathbf{A}$, $\mathbf{B}$ její podgrupy. Dokažte, že

$$\langle A \cup B \rangle = \{a_1 * b_1 * \ldots * a_n * b_n : a_1, \ldots, a_n \in A,\ b_1, \ldots, b_n \in B\}.$$

118. Buď $\mathbf{G}, \mathbf{G}_1, \ldots, \mathbf{G}_n$ abelovské grupy a $f_i : \mathbf{G}_i \to \mathbf{G}$, $i = 1, \ldots, n$, homomorfismy. Dokažte, že zobrazení

$$f : \mathbf{G}_1 \times \ldots \times \mathbf{G}_n \to \mathbf{G}, \quad (a_1, \ldots, a_n) \mapsto f_1(a_1) * \ldots * f_n(a_n)$$

je také homomorfismus.

119. Buď $\mathbf{G} = (G, *, ', e)$ grupa. Dokažte, že zobrazení $G \times G \to G$, $(x, y) \mapsto x * y$, je homomorfismus právě tehdy, když je $\mathbf{G}$ abelovská.

120. Dokažte, že zobrazení $x \mapsto x'$ je automorfismus grupy $\mathbf{G} = (G, *, ', e)$ právě tehdy, když je $\mathbf{G}$ abelovská.

121. Dokažte, že zobrazení $x \mapsto x * x$ je endomorfismus grupy $\mathbf{G} = (G, *, ', e)$ právě tehdy, když je $\mathbf{G}$ abelovská.

122. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $\psi : G \to G$ zobrazení. Dokažte, že $\psi(x*y) = \psi(y)*\psi(x)$ pro každé $x, y \in G$ právě tehdy, když existuje endomorfismus φ grupy $\mathbf{G}$ takový, že $\psi(x) = \varphi(x')$ pro všechna $x \in G$. [N]

123. Buď $\mathbf{A}$ a $\mathbf{B}$ normální podgrupy grupy $\mathbf{G}$. Dokažte, že $AB = \{ab : a \in A, b \in B\}$ tvoří normální podgrupu grupy $\mathbf{G}$. Dále dokažte, že pokud $A \cap B = \{1\}$ a $AB = G$, pak $\mathbf{G} \simeq \mathbf{G}/\mathbf{A} \times \mathbf{G}/\mathbf{B}$. Návod: Uvažujte homomorfismus $x \mapsto (xA, xB)$. Obtížné je dokázat, že je toto zobrazení na. K tomu se hodí pozorování, že pro každé $x \in G$ existuje $b \in B$ takové, že $xA = bA$ a analogicky pro xB.

124. Dokažte, že grupa $\mathbb{Z}^*_{2^k}$ není cyklická pro žádné $k > 2$. [N]

125. Nechť $\varphi : \mathbf{G} \to \mathbf{H}$ je izomorfismus grup. Dokažte, že pro každé $a \in G$ platí $|a| = |\varphi(a)|$. [N]

126. Najděte dvě *neizomorfní* grupy, které mají stejný počet prvků všech řádů. [Ř]

127. * Najděte dvě *konečné neizomorfní* grupy, které mají stejný počet prvků všech řádů. [?]

128. Dokažte, že grupy uvedené v tabulce malých grup jsou navzájem neizomorfní.

129. Dokažte, že neexistují jiné dvou, tří a čtyřprvkové grupy (až na izomorfismus). [N]

130. * Dokažte, že neexistují jiné šestiprvkové grupy (až na izomorfismus). [N]

131. ** Dokažte, že neexistují jiné osmi a devítiprvkové grupy (až na izomorfismus).

132. Dokažte, že relace definovaná $x \sim y \ \Leftrightarrow\ x, y$ jsou konjugované, je ekvivalence na množině G. Jak vypadá v případě, že je $\mathbf{G}$ abelovská?

133. Spočtěte a) řád prvku 60 v grupě $\mathbb{Z}_{64}$, b) řád prvku 18 v grupě $\mathbb{Z}_{37}$, c) řád prvku 11 v grupě $\mathbb{Z}_{122}^*$, d) řád prvku 7 v grupě $\mathbb{Z}_{17}^*$. [Ř]

134. Určete, kolik prvků kterého řádu obsahují grupy a) $\mathbb{Z}_{16}$, b) $\mathbb{Z}_{16}^*$.

135. Určete, kolik prvků kterého řádu obsahují grupy a) $\mathbb{Z}_{24}$, b) $\mathbb{Z}_{24}^*$.

136. Pro každé $n \in \mathbb{N} \cup \{\infty\}$ najděte v grupě $\mathbb{C}^*$ prvek řádu n. [Ř]

137. * Dokažte, že pokud $k \mid n$, pak grupa $\mathbb{Z}_n$ obsahuje právě $\varphi(k)$ prvků řádu k, kde φ je Eulerova funkce.

138. Sečtěte $\sum_{k|n} \varphi(k)$. [N] [Ř]

139. Rozhodněte, zda množina $\{z \in \mathbb{C} : |z| = 1\}$ tvoří podgrupu grupy a) $\mathbb{C}$, b) $\mathbb{C}^*$. [Ř]

140. Rozhodněte, zda iracionální čísla tvoří podgrupu grupy a) $\mathbb{R}$, b) $\mathbb{R}^*$. [Ř]

141. Dokažte, že libovolné dvě vlastní podgrupy grupy $\mathbb{Q}$ mají netriviální průnik. Platí toto tvrzení i pro grupu $\mathbb{R}$? [Ř]

142. Dokažte, že $\mathbb{Q} = \langle \{\frac{1}{n} : n \in \mathbb{N}\} \rangle$. Existuje nějaká konečná množina generátorů této grupy? [Ř]

143. Spočtěte prvky podgrup $\langle 28, 63 \rangle_{\mathbb{Z}}$ a $\langle 15, 18, 40 \rangle_{\mathbb{Z}}$. [Ř]

144. Spočtěte prvky podgrup $\langle 18, 33, 69 \rangle_{\mathbb{Q}}$, $\langle \frac{3}{4} \rangle_{\mathbb{Q}}$, $\langle \frac{3}{4}, \frac{2}{7} \rangle_{\mathbb{Q}}$ a $\langle \frac{2}{3}, \frac{2}{5} \rangle_{\mathbb{Q}}$. [Ř]

145. Spočtěte prvky grup $\langle i \rangle_{\mathbb{C}^*}$, $\langle -\frac{1}{2} + \frac{\sqrt{3}}{2} i \rangle_{\mathbb{C}^*}$ a $\langle 2, i \rangle_{\mathbb{C}^*}$. [Ř]

146. Dokažte, že $\mathbb{Z}_n = \langle a \rangle$ právě tehdy, když jsou a, n nesoudělné. [N]

147. * Užitím předchozího cvičení dokažte, že grupa $\mathbb{Z}_n$ obsahuje právě $\varphi(k)$ prvků řádu k, pro každé $k \mid n$.

148. Užitím předchozího cvičení sečtěte řadu $\sum_{k|n} \varphi(k)$. [Ř]

149. * Spočtěte všechny podgrupy grupy $\mathbb{Z}$.

150. Spočtěte všechny podgrupy grup $\mathbb{Z}_8$, $\mathbb{Z}_{12}$ a $\mathbb{Z}_{54}$.

151. Spočtěte všechny podgrupy grup $\mathbb{Z}_5^*$, $\mathbb{Z}_7^*$ a $\mathbb{Z}_8^*$.

152. Dokažte, že podgrupa $a\mathbb{Z}_n = \{ax \bmod n : x = 0, \ldots, n-1\}$ grupy $\mathbb{Z}_n$ je generovaná prvkem $\mathrm{NSD}(a, n)$. [N]

153. Užitím předchozího cvičení dokažte, že podgrupy grupy $\mathbb{Z}_n$ jsou právě $a\mathbb{Z}_n$, $a \mid n$.

154. Která z následujících zobrazení jsou homomorfismy $\mathbb{Z} \to \mathbb{Z}$?

$$x \mapsto 3x; \quad x \mapsto x + 3; \quad x \mapsto x^3; \quad x \mapsto 1; \quad x \mapsto 0$$

[Ř]

155. Která z následujících zobrazení jsou homomorfismy $\mathbb{C}^* \to \mathbb{R}^*$?

$$x \mapsto 3|x|; \quad x \mapsto |x| + 3; \quad x \mapsto |x|^3; \quad x \mapsto 1; \quad x \mapsto 1/|x|$$

[Ř]

156. Která z následujících zobrazení jsou homomorfismy?

$$\mathbb{Z}_4 \to \mathbb{C}^*,\ a \mapsto i^a; \qquad \mathbb{Z}_5 \to \mathbb{C}^*,\ a \mapsto i^a; \qquad \mathbb{Z} \to \mathbb{C}^*,\ a \mapsto i^a$$

[Ř]

157. Která z následujících zobrazení jsou homomorfismy?

$$\mathbb{Z}_3^* \times \mathbb{Z}_5 \to \mathbb{Z}_5,\ (a, b) \mapsto b^a; \qquad \mathbb{Z}_3 \to \mathbf{A}_4,\ a \mapsto (1\ 2\ 4) \circ (1\ 3\ 2)^a \circ (1\ 4\ 2)$$

[Ř]

158. Rozhodněte, pro která celá čísla n je zobrazení $z \mapsto z^n$ endomorfismus grupy $\mathbb{Q}^*$. Pro která n je toto zobrazení prosté a pro která je na? [Ř]

159. Rozhodněte, zda je zobrazení $\varphi : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}^*$, $(x, y, z) \mapsto 2^x 3^y 12^z$ homomorfismus. Pokud ano, spočtěte jeho jádro a obraz. [Ř]

160. Najděte všechny homomorfismy a) $\mathbb{Z} \to \mathbb{Z}$, b) $\mathbb{Z} \to \mathbb{Z}_n$, c) $\mathbb{Z}_n \to \mathbb{Z}$. [Ř]

161. Najděte všechny homomorfismy a) $\mathbb{Z}_{15} \to \mathbb{Z}_6$, b) $\mathbb{Z}_6 \to \mathbb{Z}_{15}$ c) * $\mathbb{Z}_m \to \mathbb{Z}_n$. [Ř]

162. Najděte všechny homomorfismy a) $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$, b) $\mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$.

163. Najděte a) všechny endomorfismy grupy $\mathbb{Q}$, b) všechny spojité endomorfismy grupy $\mathbb{R}$, c) * nějaký nespojitý endomorfismus grupy $\mathbb{R}$. [N] [Ř]

164. Existuje prostý homomorfismus $\mathbb{Z} \to \prod_{p \text{ prvoč.}} \mathbb{Z}_p$? [Ř]

165. Dokažte, že $\varphi_n : \mathbb{Z}_n \to \mathbb{C}^*$, $k \mapsto \cos(2\pi k/n) + i \sin(2\pi k/n)$ je prostý homomorfismus. Co je jeho obrazem? [Ř]

166. Dokažte, že $\mathbb{C} \simeq \mathbb{R} \times \mathbb{R}$ a $\mathbb{C}^* \simeq \mathbb{R}^+ \times \mathbf{S}$, kde $\mathbb{R}^+$ značí podgrupu $\mathbb{R}^*$ sestávající z kladných čísel a $\mathbf{S}$ značí podgrupu $\mathbb{C}^*$ sestávající z čísel s absolutní hodnotou 1. [Ř]

167. Dokažte, že grupy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ jsou izomorfní právě tehdy, když jsou m, n nesoudělné. [N]

168. Zjistěte, které z následujících grup jsou izomorfní: $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q}$. [Ř]

169. Zjistěte, které z následujících grup jsou izomorfní: $\mathbb{Q}$, $\mathbb{Q}^*$, $\mathbb{Q}^+$ (jako podgrupa $\mathbb{Q}^*$). [Ř]

170. Zjistěte, které z následujících grup jsou izomorfní: $\mathbb{R}$, $\mathbb{R}^*$, $\mathbb{R}^+$ (jako podgrupa $\mathbb{R}^*$). [Ř]

171. * Dokažte, že grupy $\mathbb{Q}^+$ a $(\mathbb{Z}[x], +, -, 0)$ jsou izomorfní (zde $\mathbb{Z}[x]$ značí množinu všech celočíselných polynomů). [N] [Ř]

172. * Buď $\mathbf{H}$ podgrupa grupy $\mathbb{R}$ taková, že v každém omezeném intervalu reálných čísel se nachází pouze konečné množství prvků grupy $\mathbf{H}$. Dokažte, že $\mathbf{H} \simeq \mathbb{Z}$. [N] [Ř]

173. Rozhodněte, zda jsou grupy $\mathbb{Z}_8^*$, $\mathbb{Z}_{14}^*$, $\mathbb{Z}_{16}^*$ cyklické. Pokud ano, najděte nějaký generátor.

174. Dokažte, že grupa $\mathbb{Q}$ není cyklická, ale každá její konečně generovaná podgrupa je cyklická.

175. Rozhodněte, zda je každá *konečná* podgrupa grupy $\mathbb{C}^*$ cyklická. [Ř]

176. Dokažte, že grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ je cyklická právě tehdy, když jsou m, n nesoudělné. [N]

177. * Dokažte, že každá podgrupa cyklické grupy je cyklická. [N]

178. Buď $\mathbf{G}$ abelovská grupa taková, že každá její podgrupa je cyklická. Musí být $\mathbf{G}$ cyklická? [Ř]

179. Dokažte, že konečná n-prvková cyklická grupa má právě jednu podgrupu velikosti k pro každé $k \mid n$.

180. Buď $\mathbf{G} = (G, *, ', e)$ konečná n-prvková cyklická grupa a $a, b \in G$. Dokažte, že pokud $k \times a = k \times b$ pro nějaké k nesoudělné s n, pak $a = b$.

181. * Buď $\mathbf{G} = (G, *, ', e) = \langle a \rangle$ konečná n-prvková cyklická grupa. Dokažte, že $\mathbf{G} = \langle k \times a \rangle$ právě tehdy, když je k nesoudělné s n.

182. Buď $\mathbf{G} = (G, *, ', e) = \langle a \rangle$ cyklická grupa. Dokažte, že a) endomorfismy grupy $\mathbf{G}$ jsou právě všechna zobrazení $x \mapsto k \times x$, $k \in \mathbb{Z}$; b) automorfismy grupy $\mathbf{G}$ jsou právě všechna zobrazení $x \mapsto k \times x$ taková, že $\mathbf{G} = \langle k \times a \rangle$.

183. Buď $\mathbf{G}$ konečná abelovská grupa a p prvočíslo takové, že $p \mid |G|$. Dokažte, že grupa $\mathbf{G}$ obsahuje prvek řádu p.

184. Rozložte následující grupy na součin cyklických grup: $\mathbb{Z}_5^*$, $\mathbb{Z}_{12}^*$, $\mathbb{Z}_{24}^*$, $\mathbb{Z}_{25}^*$, $\mathbb{Z}_{21}^*$, $\mathbb{Z}_{33}^*$. [Ř]

185. Spočtěte všechny podgrupy grup $\mathbb{Z}_{11}^*$ a $\mathbb{Z}_{24}^*$.

186. Najděte $m \neq n$ taková, že $\mathbb{Z}_m^* \simeq \mathbb{Z}_n^*$. [Ř]

187. * Dokažte, že pro $k > 1$ je $\mathbb{Z}_{2^k}^* \simeq \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_2$. [N] [?]

3. Permutační grupy

188. Rozložte na cykly permutace $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 7 & 1 & 6 & 5 \end{pmatrix}$ a $(2\ 3\ 4) \circ (1\ 2\ 5) \circ (3\ 6\ 1\ 7)$. [Ř]

189. Řešte v S_5 rovnici $(1\ 3\ 2) \circ \pi \circ (3\ 5\ 2)(1\ 4) = (2\ 4)(1\ 5)$. [Ř]

190. Najděte všechny permutace $\pi \in S_7$ takové, že a) $\pi^2 = (1\ 2\ 3)(4\ 5\ 6)$, b) $\pi^4 = (1\ 2\ 3\ 4\ 5\ 6\ 7)$, c) $\pi^2 = (1\ 2\ 3\ 4)$. [Ř]

191. * Charakterizujte všechny permutace $\pi \in S_n$ takové, že existuje $\sigma \in S_n$ tak, aby $\pi = \sigma^2$. [Ř]

192. Buď $(a_1\ a_2\ \ldots\ a_m)$ a $(b_1\ b_2\ \ldots\ b_n)$ dva cykly, které mají společný právě jeden prvek. Dokažte, že jejich složení je také cyklus.

193. Buď $\pi = (a_1\ a_2\ \ldots\ a_n) \in S_n$. Najděte všechny permutace σ takové, že $\pi \circ \sigma = \sigma \circ \pi$.

194. * Buď $\pi = (a_1\ a_2\ \ldots\ a_m) \in S_n$, $1 \leq m \leq n$. Dokažte, že pokud $\pi \circ \sigma = \sigma \circ \pi$, pak $\sigma = \pi^k \circ \tau$ pro nějaké $k \in \mathbb{N}$ a permutaci τ takovou, že $\tau(a_i) = a_i$ pro všechna $i = 1, \ldots, m$.

195. * Nechť $\pi \in S_{26}$. Dokažte, že existují permutace ρ, σ sestávající z třinácti cyklů délky 2 splňující $\pi = \rho \circ \sigma$ právě tehdy, když π má sudý počet cyklů každé délky. [Jde o tzv. Rejewského větu, užitou při řešení Enigmy; číslo 26 zde zastupuje počet písmen německé abecedy.]

196. Označme $\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ n & n-1 & \ldots & 1 \end{pmatrix}$ a $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$. Spočtěte π^r a σ^r, kde r je současný letopočet. [Ř]

197. Buď $\pi \in S_n$ libovolná permutace. Popište, co je nejmenší $k > 0$ takové, že π^k je identita (tj. řád π v grupě $\mathbf{S}_n$). [Ř]

198. Obsahuje a) grupa $\mathbf{S}_8$ prvek řádu 15? b) grupa $\mathbf{S}_9$ prvek řádu 16? c) grupa $\mathbf{A}_7$ prvek řádu 10? d) grupa $\mathbf{A}_8$ prvek řádu 6? Pokud ano, uveďte příklad. [Ř]

199. Jaký je největší možný řád v grupě a) $\mathbf{S}_4$, b) $\mathbf{S}_7$, c) $\mathbf{S}_{10}$? Uveďte příklady takových permutací! [Ř]

200. Určete, kolik prvků kterého řádu obsahují grupy a) $\mathbf{D}_{12}$, b) $\mathbf{A}_4$, c) * $\mathbf{D}_{2n}$. [N] [Ř]

201. * Obsahuje grupa $\mathbf{S}_n$ více prvků lichého řádu, nebo sudého řádu? [?]

202. * Dokažte oba vzorce na výpočet znaménka permutace.

203. Najděte a, b tak, aby permutace $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & a & 6 & b & 1 & 5 \end{pmatrix}$ byla lichá. [Ř]

204. Uvažujte permutaci $\pi \in S_n$ danou vzorcem $\pi(i) = ((i+1) \bmod n) + 1$. Rozložte tuto permutaci na cykly a spočtěte její znaménko pomocí obou uvedených vzorců. [Ř]

205. Spočtěte znaménko permutací

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & 3n-2 & 3n-1 & 3n \\ 2 & 3 & 1 & 5 & 6 & 4 & \dots & 3n-1 & 3n & 3n-2 \end{pmatrix}$,

b) $\begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & n+2 & \dots & 2n \\ 2 & 4 & 6 & \dots & 2n & 1 & 3 & \dots & 2n-1 \end{pmatrix}$.

[Ř]

206. Buď

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 7 & 2 & 1 & 9 & 8 & 6 & 5 \end{pmatrix},$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 1 & 4 & 3 & 8 & 7 & 6 & 9 \end{pmatrix},$$
$$\upsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 4 & 6 & 3 & 7 & 5 & 9 & 2 \end{pmatrix}.$$

Spočtěte permutace $(\sigma^{120} \circ \tau^{-3})^{17} \circ \upsilon^{23}$ a $(\upsilon^{-23} \circ \sigma)^{134} \circ \tau^4$ a spočtěte znaménko permutace $(\sigma^3 \circ \tau^{-17})^{18} \circ \sigma^{10} \circ (\upsilon^9 \circ \tau)^{-2}$.

207. Rozhodněte, zda existuje permutace $\sigma \in S_9$ taková, že $(\sigma \circ (1\ 2\ 3))^2 \circ (\sigma \circ (2\ 3\ 4))^2 = (1\ 2\ 3\ 4)$. [Ř]

208. Dokažte, že je každá permutace řádu 20 v $\mathbf{S}_{10}$ lichá.

209. * Charakterizujte řešitelné a neřešitelné pozice hry „15“ (nápověda: znaménko permutace).

210. Označme $\pi = (1\ 2\ 3)(4\ 5\ 6\ 8)$ a $\sigma = (8\ 2\ 1\ 4\ 3)(7\ 5)$. Spočtěte $\pi \circ \sigma \circ \pi^{-1}$. [Ř]

211. Označme $\pi = (8\ 7\ 4\ 3\ 1\ 2)(5\ 6)$ a $\sigma = (1\ 3\ 4)(2\ 9\ 5\ 7)(8\ 6)$. Spočtěte $\pi^2 \circ \sigma \circ \pi^{-2}$. [Ř]

212. Jsou permutace $(1\ 2\ 3)$ a $(1\ 2\ 4)$ konjugované v grupě $\mathbf{S}_4$? Jsou konjugované také v grupě $\mathbf{A}_4$? Pokud ano, nalezněte příslušnou permutaci, která je konjuguje. [Ř]

213. Jsou permutace $(1\ 3)(2\ 8\ 6)(4\ 7)$ a $(1\ 2\ 8)(3\ 7)(5\ 4)$ konjugované v grupě $\mathbf{S}_8$? Jsou konjugované také v grupě $\mathbf{A}_7$? Pokud ano, nalezněte příslušnou permutaci, která je konjuguje. [Ř]

214. Napište permutaci $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 1 & 7 & 3 & 4 & 6 \end{pmatrix}$ jako složení transpozic. [Ř]

215. Napište permutaci $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 7 & 3 & 4 & 6 \end{pmatrix}$ jako složení a) transpozice, b) trojcyklů.

216. Dokažte, že každou permutaci lze rozložit na transpozice. [Ř]

217. Dokažte, že každou sudou permutaci lze rozložit na součin trojcyklů. [Ř]

218. Dokažte, že $\mathbf{S}_4 = \langle (1\ 2), (2\ 3), (3\ 4) \rangle$ a $\mathbf{S}_n = \langle (1\ 2), \dots, (n-1\ n) \rangle$.

219. Dokažte, že $\mathbf{S}_4 = \langle (1\ 2), (1\ 3), (1\ 4) \rangle$ a $\mathbf{S}_n = \langle (1\ 2), \dots, (1\ n) \rangle$.

220. Dokažte, že $\mathbf{S}_4 = \langle (1\ 2), (1\ 2\ 3\ 4) \rangle$ a $\mathbf{S}_n = \langle (1\ 2), (1\ 2\ \dots\ n) \rangle$.

221. Dokažte, že $\mathbf{S}_4 \neq \langle (1\ 3), (1\ 2\ 3\ 4) \rangle$.

222. Dokažte, že $\mathbf{S}_n = \langle (1\ 2\ \dots\ n-1), (1\ 2\ \dots\ n) \rangle$.

223. * Buď $T \subset S_n$ množina $n-1$ transpozic. Označme $\mathbf{G}_T$ graf s množinou vrcholů $\{1,\ldots,n\}$, kde vrcholy i,j spojuje hrana právě tehdy, když $(i\ j) \in T$. Dokažte, že $\mathbf{S}_n = \langle T\rangle$ právě tehdy, když $\mathbf{G}_T$ je strom.

224. Dokažte, že $\mathbf{A}_4 = \langle (1\ 2\ 3), (1\ 2\ 4)\rangle$ a $\mathbf{A}_n = \langle (1\ 2\ 3), (1\ 2\ 4), \ldots, (1\ 2\ n)\rangle$.

225. Dokažte, že $\mathbf{A}_n = \langle (1\ 2\ 3), (1\ 2\ \ldots\ n)\rangle$ pro n liché a $\mathbf{A}_n = \langle (1\ 2\ 3), (2\ 3\ \ldots\ n)\rangle$ pro n sudé.

226. Dokažte, že $\mathbf{D}_{10} = \langle (1\ 2\ 3\ 4\ 5), (1\ 4)(2\ 3)\rangle$ a $\mathbf{D}_{2n} = \langle (1\ 2\ \ldots\ n), \pi\rangle$, kde π je libovolná z osových symetrií. (Uvažujte $\mathbf{D}_{2n}$ jako grupu automorfismů n-úhelníka s vrcholy označenými postupně 1, 2, …, n.) [Ř]

227. * Buď

$$\mathbf{G} = \langle (a_1\ a_2\ \ldots\ a_m\ a_{m+1}), (a_1\ a_2\ \ldots\ a_m\ a_{m+2}), \ldots, (a_1\ a_2\ \ldots\ a_m\ a_n)\rangle_{\mathbf{S}_n},$$

kde $1 \le m < n-1$. Dokažte, že $\mathbf{G} = \mathbf{S}_n$ pro m liché a $\mathbf{G} = \mathbf{A}_n$ pro m sudé.

228. Obsahuje grupa a) $\mathbf{S}_4$, b) $\mathbf{A}_4$ šestiprvkovou podgrupu? [Ř]

229. Rozhodněte, zda a) všechny osové symetrie, b) všechna otočení tvoří podgrupu grupy $\mathbf{D}_{2n}$. [Ř]

230. Najděte všechny podgrupy grup $\mathbf{S}_3$, $\mathbf{A}_4$, $\mathbf{D}_8$ a kvaternionové grupy $\mathbf{Q}$. [Ř]

231. Dokažte, že sgn je homomorfismus $\mathbf{S}_n \to \mathbb{Z}_3^*$. (Uvažujte $-1 \equiv 2 \pmod 3$.)

232. Dokažte, že libovolný automorfismus grupy $\mathbf{S}_n$ zachovává znaménko permutace.

233. Buď $\mathbf{G} = (G, *, ', e)$ grupa. Dokažte, že $\varphi : \mathbf{G} \to \mathbf{S}_G$, $a \mapsto L_a$ je vnoření (tj. prostý homomorfismus). Zde $L_a : x \mapsto a * x$ značí levou translaci prvku a. [Tzv. *Cayleyova reprezentace* grup.]

234. * Nechť $n = 2^k m$, $k \neq 0$, m liché. Najděte vnoření a) $\mathbf{D}_n \hookrightarrow \mathbf{D}_{2^k} \times \mathbf{D}_m$, b) $\mathbf{D}_{2^k} \hookrightarrow \mathbf{D}_n$, c) $\mathbf{D}_m \hookrightarrow \mathbf{D}_n$. [N] [?]

235. ** Buď $\mathbf{G}$ grupa a $a \in G$. Vnořte $\mathbf{G}$ do nějaké grupy $\mathbf{H}$ tak, aby v $\mathbf{H}$ existoval prvek b takový, že b^2 je roven obrazu a. [N]

236. Dokažte, že je podgrupa $\langle (1\ 2\ 3\ 4)(5\ 6\ 7\ 8), (1\ 5\ 3\ 7)(2\ 8\ 4\ 6)\rangle_{\mathbf{S}_8}$ izomorfní kvaternionové grupě $\mathbf{Q}$. [N]

Automorfismy dané struktury $\mathbf{X}$ (algebry, grafu, uspořádané množiny, apod.) tvoří podgrupu grupy $\mathbf{S}_X$, značí se $\mathbf{Aut}(\mathbf{X})$.

Automorfismem grafu $\mathbf{G} = (V, E)$ rozumíme permutaci $\varphi \in S_V$ takovou, že

$$\{x, y\} \in E \quad \Leftrightarrow \quad \{\varphi(x), \varphi(y)\} \in E.$$

Automorfismem uspořádané množiny $\mathbf{X} = (X, \le)$ rozumíme permutaci $\varphi \in S_X$ takovou, že

$$x \le y \quad \Leftrightarrow \quad \varphi(x) \le \varphi(y).$$

237. Dokažte, že množina všech automorfismů dané algebry $\mathbf{A}$ skutečně tvoří podgrupu grupy $\mathbf{S}_A$. Analogické tvrzení dokažte pro automorfismy grafů a uspořádaných množin.

238. Vypište prvky grup automorfismů tříprvkových grafů, domečku, prasátka, * Petersenova grafu. S kterými malými grupami jsou izomorfní?

239. Vypište prvky grup automorfismů čtverce, pětiúhelníka a obecně pravidelného n-úhelníka (tj. grupy $\mathbf{D}_8$, $\mathbf{D}_{10}$, resp. $\mathbf{D}_{2n}$).

240. Najděte graf na alespoň dvou vrcholech, který má triviální grupu automorfismů. [Ř]

241. Vypište prvky grup a) $\mathbf{Aut}(\mathbb{N}, \le)$, b) $\mathbf{Aut}(\mathbb{Z}, \le)$. [Ř]

242. * Uvědomte si, že $\mathbf{Aut}(\mathbb{R}, \le)$ obsahuje právě všechny striktně rostoucí spojité reálné funkce. Spočtěte prvky grupy $\mathbf{Aut}(\mathbb{Q}, \le)$. [N] [Ř]

243. Vypište prvky grupy všech symetrií čtyřstěnu, krychle, * osmistěnu a ** dvanáctistěnu.

244. Dokažte, že grupa symetrií čtyřstěnu je izomorfní s $\mathbf{S}_4$, krychle s $\mathbb{Z}_2 \times \mathbf{S}_4$ a ** dvanáctistěnu s $\mathbb{Z}_2 \times \mathbf{A}_5$.

245. Vypište prvky grupy všech otočení čtyřstěnu, krychle, * osmistěnu a ** dvanáctistěnu.

246. Najděte všechny automorfismy grupy a) $\mathbb{Z}$, b) $\mathbb{Q}$, c) $\mathbb{Z}_2 \times \mathbb{Z}_2$, d) $\mathbb{Z}_4 \times \mathbb{Z}_2$, e) * $\mathbf{S}_3$. S kterými známými grupami jsou izomorfní? [Ř]

247. Dokažte, že $\mathbf{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$. [Ř]

248. Dokažte, že pokud jsou m, n nesoudělné, pak $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. (Toto tvrzení se dá interpretovat jako $\mathbf{Aut}(\mathbb{Z}_m \times \mathbb{Z}_n) \simeq \mathbf{Aut}(\mathbb{Z}_m) \times \mathbf{Aut}(\mathbb{Z}_n)$.)

249. * Dokažte, že pokud jsou řády grup $\mathbf{G}, \mathbf{H}$ nesoudělné, pak $\mathbf{Aut}(\mathbf{G} \times \mathbf{H}) \simeq \mathbf{Aut}(\mathbf{G}) \times \mathbf{Aut}(\mathbf{H})$.

250. Dokažte, že $\mathbf{Aut}((\mathbb{Z}_p)^d) \simeq \mathbf{GL}(d, \mathbb{Z}_p)$.

251. Buď $\mathbf{G} = (G, *, ', e)$ grupa, $a \in G$ a označme ψ_a zobrazení $G \to G$, $x \mapsto a * x * a'$. Dokažte, že je ψ_a automorfismus grupy $\mathbf{G}$.

Zobrazení ψ_a, $a \in G$, z předchozího cvičení se nazývají *vnitřní automorfismy* grupy $\mathbf{G}$. Tvoří podgrupu grupy $\mathbf{Aut}(\mathbf{G})$, značí se $\mathbf{Inn}(\mathbf{G})$.

252. Dokažte, že $\mathbf{Inn}(\mathbf{G})$ je skutečně podgrupa grupy $\mathbf{Aut}(\mathbf{G})$.

253. Najděte všechny automorfismy grupy $\mathbf{S}_4$. Se kterou známou grupou je $\mathbf{Aut}(\mathbf{S}_4)$ izomorfní? [?] [Ř]

254. ** Dokažte, že pro $n \neq 6$ jsou všechny automorfismy $\mathbf{S}_n$ vnitřní. Návod: ??? [?]

255. ** Dokažte, že $\mathbf{S}_6$ má automorfismus, který není vnitřní. Návod: ??? [?]

256. * Buď $\mathbf{G}$ neabelovská grupa. Dokažte, že $\mathbf{Inn}(\mathbf{G})$ nemůže být konečná cyklická. [?]

257. * Buď $\mathbf{G}$ grupa. Dokažte, že $\mathbf{Aut}(\mathbf{G})$ nemůže být cyklická lichého řádu. [?] [N]

4. Maticové a geometrické grupy

258. Buď $\mathbf{T}$ těleso. Rozhodněte, zda a) $\mathbf{SL}_n(\mathbf{T}) \leq \mathbf{GL}_n(\mathbf{T})$, b) $\mathbf{GO}_n(\mathbf{T}) \leq \mathbf{GL}_n(\mathbf{T})$, c) $\mathbf{GO}_n(\mathbf{T}) \leq \mathbf{SL}_n(\mathbf{T})$. [Ř]

259. Dokažte, že $\mathbf{GL}_2(\mathbb{Z}_2) = \langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \rangle$. Je tato grupa cyklická? [Ř]

260. Dokažte, že $\mathbf{GL}_n(\mathbb{Q}) = \langle T_{ij}(a), E_i(a) : \ i, j = 1, \ldots, n, \ a \in \mathbb{Q} \rangle$, kde $T_{ij}(a)$ je matice s jedičkami na diagonále, a na pozici ij a nulami jinde, a $E_i(\alpha)$ je matice s jedničkami na diagonále s vyjímkou pozice ii, kde je prvek a a jinde nuly.

261. * Dokažte, že $\mathbf{SL}_2(\mathbb{Z}) = \langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \rangle$.

262. * Dokažte, že $\mathbf{SL}_n(\mathbb{Z}) = \langle T_{ij} : \ i, j = 1, \ldots, n \rangle$, kde T_{ij} je matice s jedičkami na diagonále a na pozici ij a nulami jinde.

263. Označme $\mathbf{G}$ grupu všech regulárních horních trojúhelníkových matic $n \times n$ nad $\mathbb{Q}$ a uvažujme zobrazení φ přiřazující matici A diagonální matici se stejnými prvky na diagonále. Je φ homomorfismus $\mathbf{G} \to \mathbf{GL}_n(\mathbb{Q})$? [Ř]

264. Buď $\mathbf{T}$ těleso. Dokažte, že $\varphi : \mathbf{S}_n \to \mathbf{GL}_n(\mathbf{T})$, $\pi \mapsto \left(\delta_{i,\sigma(j)}\right)_{i,j=1}^n$, kde $\delta_{u,v} = 1$ pokud $u = v$ a $\delta_{u,v} = 0$ v opačném případě, je prostý homomorfismus. Dokažte, že obraz tohoto homomorfismu je podgrupa $\mathbf{O}_n(\mathbf{T})$. [Tzv. *lineární reprezentace* grup.]

265. Najděte vnoření grupy $\mathbb{C}^*$ do $\mathbf{GL}_2(\mathbb{R})$. [Ř]

266. * Najděte vnoření kvaternionové grupy $\mathbf{Q}$ a) do $\mathbf{GL}_2(\mathbb{C})$, b) do $\mathbf{GL}_4(\mathbb{R})$. Rozšiřte tato zobrazení na celou multiplikativní grupu nekomutativního tělesa kvaternionů. [N] [Ř]

267. Dokažte, že $\mathbf{GL}_2(\mathbb{Z}_2) \simeq \mathbf{S}_3$.

Izometrií Eukleidovského prostoru $\mathbb{R}^n$ rozumíme zobrazení φ takové, že $|\varphi(x)| = |x|$. Příklady izometrií jsou otočení (rotace), posunutí (translace) a osové symetrie (reflexe).

Nadále budeme uvažovat především izometrie, které zachovávají počátek souřadnic, tj. bod $(0,\dots,0)$. (Ostatní izometrie dostanem složením s vhodným posunutím.)

268. Dokažte, že grupa všech posunutí v prostoru $\mathbb{R}^n$ je izomorfní s grupou $\mathbb{R}^n$.

269. * Dokažte, že grupa $\mathbf{GO}_n(\mathbb{R})$ je izomorfní s grupou všech izometrií Eukleidovského prostoru $\mathbb{R}^n$, které zachovávají počátek.

270. * Dokažte, že grupa $\mathbf{SO}_n(\mathbb{R})$ je izomorfní s grupou všech otočení Eukleidovského prostoru $\mathbb{R}^n$ se středem v počátku.

Předchozí dvě úlohy dávají důležitou geometrickou představu ortogonálních grup. Nadále budeme uvažovat grupy $\mathbf{GO}_n(\mathbb{R})$ a $\mathbf{SO}_n(\mathbb{R})$ jako uvedené grupy izometrií.

Řekneme, že zobrazení f zachovává množinu X, pokud $f(x) = x$ pro každé $x \in X$. Otočení v $\mathbb{R}^n$ se nazývá *jednoduché*, pokud je rovinné, tj. zachovává $(n-2)$-dimenzionální podprostor.

271. Dokažte, že každý prvek $\mathbf{GO}_n(\mathbb{R})$, který zachovává nějaký k-dimenzionální podprostor $\mathbb{R}^n$, lze napsat jako složení $n-k$ osových symetrií. Tedy grupa $\mathbf{GO}_n(\mathbb{R})$ je generovaná osovými symetriemi. [N]

272. Dokažte, že složení dvou osových symetrií je jednoduché otočení. Dedukujte, že grupa $\mathbf{SO}_n(\mathbb{R})$ je generovaná jednoduchými otočeními.

Popis izometrií v prostoru $\mathbb{R}^2$ lze provést užitím komplexních čísel.

273. Dokažte, že každé otočení roviny se středem v počátku lze zapsat jako zobrazení $\mathbb{C} \to \mathbb{C}$, $z \mapsto uz$ pro nějaké $u \in \mathbb{C}$, $|u| = 1$. Tedy grupa $\mathbf{SO}_2(\mathbb{R})$ je izomorfní s podgrupou $\{z \in \mathbb{C} : |z| = 1\}$ grupy $\mathbb{C}^*$.

274. Dokažte, že grupa $\mathbf{GO}_2(\mathbb{R})$ je izomorfní s grupou všech zobrazení $\mathbb{C} \to \mathbb{C}$ tvaru $z \mapsto uz$ nebo $z \mapsto u\bar{z}$ pro nějaké $u \in \mathbb{C}$, $|u| = 1$.

275. Popište všechny konečné podgrupy $\mathbf{SO}_2(\mathbb{R})$. [Ř]

Popis izometrií v prostoru $\mathbb{R}^3$ lze provést užitím kvaternionů. Pro tyto účely kvaternion $a + bi + cj + dk \in \mathbb{H}$ identifikujeme s vektorem $(b, c, d) \in \mathbb{R}^3$. (Tj. reprezentace není jednoznačná, na reálné složce kvaternionu nezáleží.)

276. Dokažte, že zobrazení $\mathbb{R}^3 \to \mathbb{R}^3$, $v \mapsto zvz^{-1}$, kde $z \in \mathbb{H}$, je jednoduché otočení. Je-li $z = r(\cos\varphi + u\sin\varphi)$, kde u je jednodtkový vektor z $\mathbb{R}^3$, pak jde o otočení o úhel 2φ kolem osy dané u.

277. Dokažte, že každé otočení $\mathbb{R}^3$ je jednoduché otočení, a lze zapsat způsobem uvedeným v předchozím cvičení. Přitom dvě $z_1, z_2 \in \mathbb{H}$ určují stejné otočení právě tehdy, když $z_1 = rz_2$ pro nějaké $r \in \mathbb{R} \setminus \{0\}$. Tedy grupa $\mathbf{SO}_3(\mathbb{R})$ je izomorfní s grupou $\mathbf{Inn}(\mathbb{H}^*)$.

5. Působení grupy na množině

278. Vypište orbity působení grupy $\mathbf{S}_6$ a) na množině $\{1,\dots,6\}$, b) na množině $\{(i,j) : i,j = 1,\dots,6\}$. [Ř]

279. Vypište orbity působení grupy $\mathbf{D}_{10}$ všech symetrií pravidelného pětiúhelníka a) na množině jeho vrcholů, b) na množině jeho hran. [Ř]

280. Co jsou orbity působení dané grupy $\mathbf{G}$ konjugací na svoji nosnou množinu G? Vypište orbity pro grupy $\mathbf{S}_4$ a $\mathbf{A}_4$. [Ř]

281. Vypište orbity působení grupy $\mathbf{GL}_n(\mathbf{T})$ na vektorový prostor $\mathbf{T}^n$? Uvědomte si, že X_A jsou právě vlastní vektory matice A příslušné vlastnímu číslu 1 (pokud takové je). [Ř]

282. Uvažujme působení grupy $\mathbf{S}_6$ a) na množině $\{1,\dots,6\}$, b) na množině $\{(i,j) : i,j = 1,\dots,6\}$. Kolik prvků má stabilizátor bodu a) 2, b) $(2,5)$? [Ř]

283. Nechť grupa $\mathbf{D}_{10}$ všech symetrií pravidelného pětiúhelníka působí na množině jeho vrcholů. Kolik pevných bodů má a) otočení o $72°$, b) daná osová symetrie? [Ř]

284. Nechť grupa $\mathbf{D}_{10}$ všech symetrií pravidelného pětiúhelníka působí na množině jeho vrcholů. Kolik prvků má stabilizátor daného vrcholu? [Ř]

285. Nechť grupa $\mathbf{D}_{12}$ všech symetrií pravidelného šestiúhelníka působí na množině jeho vrcholů. Kolik pevných bodů má a) středová symetrie, b) daná osová symetrie? [Ř]

286. Nechť grupa $\mathbf{D}_{12}$ všech symetrií pravidelného pětiúhelníka působí na množině jeho vrcholů. Kolik prvků má stabilizátor daného vrcholu? [Ř]

287. Uvažujme působení grupy otočení čtverce na množinu všech obarvení šachovnice 3×3 dvěma barvami. Kolik prvků má stabilizátor obarvení, kde jsou a) jedno rohové políčko černé a ostatní bílá, b) dvě protilehlá rohová políčka černá a ostatní bílá, c) prostřední políčko černé a ostatní bílá? [Ř]

288. Uvažujme působení grupy $\mathbf{D}_8$ všech symetrií čtverce na množinu všech obarvení šachovnice 3×3 dvěma barvami. Kolik prvků má stabilizátor obarvení, kde jsou a) jedno rohové políčko černé a ostatní bílá, b) dvě protilehlá rohová políčka černá a ostatní bílá, c) prostřední políčko černé a ostatní bílá? [Ř]

289. Buď $\mathbf{G}$ grupa izometrií v rovině a $X = \mathbb{R}^2$ rovina (v přirozeném působení). Pro daný bod $x \in X$, co jsou prvky množin $[x]$ a G_x ? [Ř]

290. Buď $\mathbf{G}$ grupa izometrií v rovině a $X = \mathbb{R}^2$ rovina (v přirozeném působení). Co jsou prvky X_g v případě, kdy je g a) otočení, b) translace, c) osová symetrie? [Ř]

291. Buď $\mathbf{G} = \mathbb{R}$ a $X = \mathbb{R}^2$ rovina. Označme $\pi(n)$ permutaci $(a, b) \mapsto (a+n, b)$ (tj. horizontální posunutí o n). Je to působení? Pokud ano, co jsou prvky množin $[x]$, G_x a X_n pro dané $x \in X$ a $n \in G$? [Ř]

292. Buď $\mathbf{G} = \mathbb{R}$ a $X = \mathbb{R}^2$ rovina. Označme $\pi(n)$ otočení roviny o n stupňů se středem $(0, 0)$. Je to působení? Pokud ano, co jsou prvky množin $[x]$, G_x a X_n pro dané $x \in X$ a $n \in G$? [Ř]

293. Spočtěte kolika způsoby lze obarvit políčka šachovnice o rozměrech a) 3×3, b) 4×4, c) $n \times n$ černou a bílou barvou. Dvě obarvení považujeme za totožná, pokud lze jedno z druhého dostat otočením šachovnice. [Ř]

294. Řešte předchozí úlohu za předpokladu, že se obarvuje průhledná šachovnice. (Tj. zajímá nás počet obarvení až na otočení a převrácení šachovnice.) [Ř]

295. a) Dětská stavebnice obsahuje 3 červené, 3 zelené a 3 modré čtvercové destičky. Kolika způsoby je lze sestavit do velkého čtverce 3×3? Dvě sestavy považujeme za totožné, pokud jednu z druhé dostaneme otočením. b) Jak se výsledek změní, pokud je možné dílky pevně spojovat? Tedy pokud dvě sestavy považujeme za totožné, dostaneme-li jednu z druhé otočením a převrácením. [Ř]

296. Řešte předchozí úlohu pro stavebnici, která obsahuje devět čtvercových destiček, na kterých je nakreslena šipka směřující k středu jedné z hran. (Opět a) až na otočení, b) až na otočení a převrácení; předpokládejte, že šipka ukazuje z obou stran stejným směrem.) [N]

297. Řešte předchozí úlohu pro stavebnici, která obsahuje devět čtvercových destiček, na kterých je nakreslena šipka směřující k jednomu z vrcholů (Opět a) až na otočení, b) až na otočení a převrácení; předpokládejte, že šipka ukazuje z obou stran stejným směrem.)

298. a) Dětská stavebnice obsahuje 8 červených a 8 modrých trojúhelníkových destiček. Kolika způsoby je lze sestavit do velkého trojúhelníku s hranou 4? Dvě sestavy považujeme za totožné, dostaneme-li jednu z druhé otočením. b) Jak se výsledek změní, pokud je možné dílky pevně spojovat? Tedy pokud dvě sestavy považujeme za totožné, dostaneme-li jednu z druhé otočením a převrácením. [Ř]

299. Řešte předchozí úlohu pro stavebnici, která obsahuje šestnáct trojúhelníkových destiček, na kterých je nakreslena šipka směřující k jednomu z vrcholů.

300. Kolik náhrdelníků lze sestavit ze a) čtyř modrých a čtyř červených, b) k modrých a $8 - k$ červených kuliček? Nezáleží na poloze náhrdelníku, je možno jej převracet či otáčet. [Ř]

301. Kolika způsoby lze z šesti bílých a šesti modrých trojúhelníkových desticek sestavit pravidelnou šesticípou hvezdu? Dve sestavy považujeme za totožné, dostaneme-li jednu z druhé otočením a převrácením.

302. a) Spočtěte kolika způsoby lze rozesadit české poslance kolem kulatého stolu s 200 židlemi (tj. ke každé židli umisťujeme cedulku se jménem poslance). b) Kolika způsoby to lze udělat, pokud navzájem nerozlišujeme poslance jedné strany (tj. ke každé židli umisťujeme cedulku se jménem strany)? (Počty poslanců: ODS 81, ČSSD 74, KSČM 26, KDU-ČSL 13, SZ 6.) Dva zasedací pořádky považujeme za totožné, pokud lze jeden z druhého dostat otočením stolu.

303. Kolika způsoby lze obarvit stěny krychle a) dvěma, b) k barvami? Dvě obarvení považujeme za totožná, pokud lze jedno z druhého dostat otočením krychle. [Ř]

304. Kolika způsoby lze umístit na stěny krychle šipku, která ukazuje a) na střed jedné z hran, b) k jednomu z vrcholů? Dvě umístění považujeme za totožná, pokud lze jedno z druhého dostat otočením krychle.

305. Kolika způsoby lze umístit na stěny krychle čísla 1,...,6? Kolika způsoby to lze udělat tak, aby součet protilehlých čísel byl 7? Dvě umístění považujeme za totožná, pokud lze jedno z druhého dostat otočením krychle. [Ř]

306. Spočtěte kolika způsoby lze obarvit stěny pravidelného čtyřstěnu k barvami. Dvě obarvení považujeme za totožná, pokud lze jedno z druhého dostat otočením čtyřstěnu. [Ř]

307. Řešte předchozí úlohu za předpokladu, že uvažujeme všechny symetrie čtyřstěnu. [Ř]

308. Kolik existuje neizomorfních grafů na 3, 4, 5, * 6 prvcích? [?] [Ř]

309. * Kolik existuje neizomorfních dvou a tříprvkových algeber s jednou binární operací? [Ř]

310. Buď $\mathbf{T}$ těleso. Rozhodněte, zda je působení grupy a) $\mathbf{GL}_n(\mathbf{T})$, b) $\mathbf{SL}_n(\mathbf{T})$, c) $\mathbf{O}_n(\mathbf{T})$ na množinu $T^n \setminus \{0\}$ tranzitivní. [Ř]

311. Buď $\mathbf{H}$ je podgrupa grupy $\mathbf{G}$. Co jsou orbity působení $\mathbf{H}$ translacemi na G? [Ř]

312. Dokažte, že působení grupy $\mathbf{G}$ konjugací na G je skutečně působení. Co jsou jeho orbity? Může být toto působení tranzitivní? [Ř]

313. * Buď π působení tranzitivní grupy $\mathbf{G}$ na množině X. Pak svaz kongruencí unární algebry $(X, \pi(g) : g \in G)$ je izomorfní intervalu $[\mathbf{G}_a, \mathbf{G}]$ ve svazu podgrup grupy $\mathbf{G}$ (zde $\mathbf{G}_a$ značí stabilizátor bodu $a \in X$). [?]

314. * Použitím předchozího cvičení dokažte, že každý interval ve svazu podgrup nějaké grupy je izomorfní svazu kongruencí nějaké (unární) algebry. [?] [N]

6. Rozklady, normální podgrupy a faktorgrupy

315. Dokažte, že je-li $\mathbf{H} \leq \mathbf{G}$ a $[\mathbf{G} : \mathbf{H}] = 2$, pak $\mathbf{H} \trianglelefteq \mathbf{G}$. [Ř]

316. Najděte podgrupu $\mathbf{H}$ grupy $\mathbf{S}_3$ takovou, že existuje levá rozkladová třída $a * H$, která není pravou rozkladovou třídou. Tj. najděte $\mathbf{H} \leq \mathbf{S}_3$ a $a \in S_3$ takové, že $a * H \neq H * b$ pro libovolné $b \in S_3$. [Ř]

317. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $\mathbf{H}$ její podgrupa. Dokažte, že množina A je levou rozkladovou třídou $\mathbf{H}$ v $\mathbf{G}$ právě tehdy, když je množina $A' = \{a' : a \in A\}$ pravou rozkladovou třídou $\mathbf{H}$ v $\mathbf{G}$.

318. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $\mathbf{A}$,$\mathbf{B}$ její normální podgrupy. Dokažte, že $A \cap B$ a $AB = \{a * b : a \in A, b \in B\}$ tvoří normální podgrupu grupy $\mathbf{G}$.

319. Rozhodněte, zda je $\mathbf{A}_n$ normální podgrupou grupy $\mathbf{S}_n$. [Ř]

320. Rozhodněte, zda je $\mathbf{D}_{2n}$ normální podgrupou grupy $\mathbf{S}_n$. [Ř]

321. Nechť $\mathbf{H}$ je Kleinova podgrupa grupy $\mathbf{S}_4$, tj. podgrupa sestávající z identity a všech tří permutací typu $(i\ j)(k\ l)$. Rozhodněte, zda je $\mathbf{H}$ normální podgrupou grupy $\mathbf{S}_4$. [Ř]

322. Rozhodněte, zda množina $\{\pi \in S_4 : \pi^3 = id\}$ tvoří normální podgrupu grupy $\mathbf{S}_4$. [Ř]

323. Spočtěte nejmenší normální podgrupu grupy $\mathbf{S}_5$ obsahující a) permutaci (1 2 3), b) permutaci (1 2 3 4). [Ř]

324. Spočtěte nejmenší normální podgrupu grupy $\mathbf{D}_{10}$ obsahující a) permutaci (1 2 3 4 5), b) permutaci (1 2)(3 5) (uvažujte $\mathbf{D}_{10}$ jako grupu symetrií pětiúhelníka, jehož vrcholy jsou očíslovány $1, \ldots, 5$ po směru hodinových ručiček). [Ř]

325. Najděte všechny normální podgrupy grupy $\mathbf{S}_3$. [Ř]

326. Najděte všechny normální podgrupy grupy $\mathbf{S}_4$. [Ř]

327. ** Dokažte, že grupa $\mathbf{S}_n$, $n \neq 4$, má právě tři normální podgrupy. Návod: ??? [?]

328. ** Dokažte, že grupa $\mathbf{A}_n$, $n \neq 4$, nemá žádné vlastní normální podgrupy. Návod: ??? [?]

329. * Najděte všechny normální podgrupy a) dihedrální grupy $\mathbf{D}_8$, b) dihedrální grupy $\mathbf{D}_{10}$, c) kvaternionové grupy $\mathbf{Q}$. [Ř]

330. Dokažte, že $\mathbf{Inn}(\mathbf{G})$ tvoří normální podgrupu grupy $\mathbf{Aut}(\mathbf{G})$.

331. Dokažte, že následující tvrzení jsou ekvivalentní pro grupu $\mathbf{G}$:

(1) $\mathbf{Aut}(\mathbf{G})$ je normální podgrupou grupy $\mathbf{S}_G$;
(2) $|\mathbf{Aut}(\mathbf{G})| = 1$;
(3) $\mathbf{G} = \mathbb{Z}_2$.

332. Rozhodněte, zda je grupa všech regulárních horních trojúhelníkových matic $n \times n$ nad tělesem $\mathbb{Q}$ normální podgrupou grupy $\mathbf{GL}_n(\mathbb{Q})$. [Ř]

333. Rozhodněte, zda je grupa všech regulárních diagonálních matic $n \times n$ nad tělesem $\mathbb{Q}$ normální podgrupou a) grupy $\mathbf{GL}_n(\mathbb{Q})$, b) grupy všech regulárních horních trojúhelníkových matic. [Ř]

334. Rozhodněte, zda je grupa všech regulárních horních trojúhelníkových matic $n \times n$ nad tělesem $\mathbb{Q}$ *s jedničkami na diagonále* normální podgrupou a) grupy $\mathbf{GL}_n(\mathbb{Q})$, b) grupy všech regulárních horních trojúhelníkových matic. [Ř]

335. Rozhodněte, zda je grupa $\mathbf{SL}_n(\mathbb{Q})$ normální podgrupou grupy $\mathbf{GL}_n(\mathbb{Q})$. [Ř]

336. Rozhodněte, zda je grupa $\mathbf{GO}_n(\mathbb{Q})$ normální podgrupou grupy $\mathbf{GL}_n(\mathbb{Q})$. [Ř]

337. Rozhodněte, zda je grupa $\mathbf{SO}_n(\mathbb{Q})$ normální podgrupou grupy $\mathbf{SL}_n(\mathbb{Q})$. ($\mathbf{SO}_n(\mathbb{Q})$ značí grupu všech ortogonálních matic s determinantem 1.) [Ř]

338. * Najděte všechny normální podgrupy grupy $\mathbf{GO}_2(\mathbb{R})$.

339. Buď $A = \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a, b \in \mathbb{Q}, a \neq 0\}$, $B = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) : 0 \neq a, b \in \mathbb{Q}\}$, $C = \{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : 0 \neq a \in \mathbb{Q}\}$. Rozhodněte, které z těchto množin tvoří podgrupu a které normální podgrupu grupy $\mathbf{GL}_2(\mathbb{Q})$. [Ř]

340. * Předpokládejme, že každá podgrupa grupy $\mathbf{G}$ je normální. Musí být $\mathbf{G}$ abelovská? [Ř]

341. Předpokládejme, že je $\mathbf{G}$ a) abelovská, b) neabelovská grupa, a uvažujme nějakou její vlastní normální podgrupu $\mathbf{H}$. Rozhodněte, zda $\mathbf{H}$ a $\mathbf{G}/\mathbf{H}$ může, musí nebo nemůže být abelovská. [Ř]

342. * Buď $\mathbf{G}$ konečná abelovská grupa a $\mathbf{H}$ její podgrupa. Dokažte, že existuje podgrupa grupy $\mathbf{G}$ izomorfní s $\mathbf{G}/\mathbf{H}$. Uveďte příklad neabelovské grupy a její normální podgrupy, pro kterou tvrzení neplatí. Uveďte příklad nekonečné abelovské grupy a její podgrupy, pro kterou tvrzení neplatí.

343. S kterou známou grupou je izomorfní grupa $\mathbf{GL}_n(\mathbb{Q})/\mathbf{SL}_n(\mathbb{Q})$? [Ř]

344. S kterou známou grupou je izomorfní grupa $\mathbb{R}^*/\mathbb{R}^+$, kde $\mathbb{R}^+$ značí podgrupu kladných čísel? [Ř]

345. S kterou známou grupou je izomorfní grupa $\mathbb{R}^*/\{\pm 1\}$? [Ř]

346. Jak vypadá faktorgrupa a) $\mathbb{R}/\mathbb{Z}$, b) $\mathbb{Q}/\mathbb{Z}$? Uvažujte interval $\langle 0, 1)$ a operace „seříznuté“ do tohto intervalu (co to znamená přesně?). [Ř]

347. S kterou známou grupou je izomorfní grupa $\mathbb{C}/\mathbb{R}$? [Ř]

348. S kterou známou grupou je izomorfní grupa $\mathbb{C}^*/\mathbb{R}^+$? [Ř]

349. S kterou známou grupou je izomorfní grupa $\mathbb{C}^*/\{z \in \mathbb{C} : |z| = 1\}$? [Ř]

350. * S kterou známou grupou je izomorfní grupa $\mathbb{C}^*/\mathbb{C}_n$? [Ř]

351. * S kterou známou grupou je izomorfní grupa $\mathbb{C}_{p^\infty}/\mathbb{C}_{p^k}$? [Ř]

352. Buď $\mathbf{H}$ Kleinova podgrupa grupy $\mathbf{S}_4$, tj. podgrupa sestávající z identity a všech tří permutací typu $(i\ j)(k\ l)$. Dokažte, že $\mathbf{S}_4/\mathbf{H} \simeq \mathbf{S}_3$. [N]

353. Buď $\mathbf{Q}$ osmiprvková kvaternionová grupa. Vypište její podgrupy a ověřte, že jsou všechny normální. Rozhodněte, zda je $\mathbf{Q}/\mathbf{Z}(\mathbf{Q})$ izomorfní grupě $\mathbb{Z}_4$ nebo grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$.

354. Uvažujte grupu $\mathbf{D}_{2n}$ symetrií pravidelného n-úhelníka pro *sudé* $n \geq 4$.

a) Dokažte, že středová symetrie (tj. otočení o 180 stupňů) generuje normální podgrupu, označme ji $\mathbf{N}$.

b) V závisosti na n rozhodněte, zda je grupa $\mathbf{D}_{2n}/\mathbf{N}$ abelovská.

355. S kterou známou grupou je izomorfní grupa $\mathbf{GL}_2(\mathbb{C})/\mathbf{H}$, kde $H = \{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : 0 \neq a \in \mathbb{C}\}$? [?]

356. Uvažujme grupu $\mathbf{G}$ všech regulárních horních trojúhelníkových matic 2×2 nad $\mathbb{Q}$ a její podgrupu $\mathbf{H}$ matic s kladnými čísly na diagonále. Dokažte, že $\mathbf{H} \trianglelefteq \mathbf{G}$. S kterou známou grupou je izomorfní grupa $\mathbf{G}/\mathbf{H}$? [?]

357. * Uvažujme grupu $\mathbf{G}$ všech regulárních horních trojúhelníkových matic $n \times n$ nad $\mathbb{Q}$ a její podgrupu $\mathbf{H}$ matic s jedničkami na diagonále. Dokažte, že $\mathbf{H} \trianglelefteq \mathbf{G}$. S kterou známou grupou je izomorfní grupa $\mathbf{G}/\mathbf{H}$? [N] [Ř]

358. * Dokažte, že posunutí tvoří normální podgrupu grupy všech symetrií v rovině. Které známé grupě je izomorfní příslušná faktorgrupa?

359. Buď $\mathbf{A}$ a $\mathbf{B}$ normální podgrupy grupy $\mathbf{G}$. Dokažte, že $AB = \{ab : a \in A, b \in B\}$ tvoří normální podgrupu grupy $\mathbf{G}$.

360. * Buď $\mathbf{A}$ a $\mathbf{B}$ normální podgrupy grupy $\mathbf{G}$, předpokládejme, že $A \cap B = \{1\}$ a $AB = G$. Dokažte, že $\mathbf{G} \simeq \mathbf{G}/\mathbf{A} \times \mathbf{G}/\mathbf{B}$. [N]

III. Okruhy

1. Příklady a základní vlastnosti

361. Buď $\mathbf{A}$ abelovská grupa. Dokažte, že $(\mathrm{End}(\mathbf{A}), +, -, \circ, 0)$ je okruh. Zde $\mathrm{End}(\mathbf{A})$ značí množinu všech endomorfismů grupy $\mathbf{A}$, sčítání a odčítání endomorfismů je definováno po prvcích, tj. $(f \pm g)(x) = f(x) \pm g(x)$, 0 značí konstantní endomorfismus $x \mapsto 0$ a $\circ$ značí skládání zobrazení.

362. Buď X množina, označme $P(X)$ množinu všech podmnožin X a definujme na $P(X)$ operaci $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Dokažte, že je $(P(X), \triangle, id, \cap, \emptyset)$ komutativní okruh. Má jednotku?

363. Rozhodněte, zda je $(\mathbb{R} \times \mathbb{R} \times \mathbb{R}, +, -, \times, 0)$ okruh. Zde sčítání a odčítání je definováno po složkách a $\times$ značí vektorový součin. [Ř]

364. Rozhodněte, zda je $(\mathbb{Z} \times \mathbb{Z}, +, -, *, 0)$ okruh. Zde sčítání a odčítání je definováno po složkách a $(a, b) * (c, d) = (ac + bd, ad + bc)$. [Ř]

365. Definujme operace

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	a	a	a
d	a	b	c	d

Rozhodněte, zda je $(\{a, b, c, d\}, +, -, \cdot, a)$ okruh. [Ř]

366. Buď $\mathbf{R}$ okruh splňující $x^2 = 0$ pro všechna $x \in R$. Rozhodněte, zda pro všechna $x, y \in R$ platí a) $xy = -yx$, b) * $xy = yx$. [?] [Ř]

367. Buď $\mathbf{R}$ komutativní okruh. Rozhodněte, zda je okruhem také algebra $(R, +, -, *, 0)$, kde operace $*$ je definována předpisem $a * b = ab + ba$.

368. Dokažte, že pro okruhy s jednotkou plyne komutativita sčítání z ostatních axiomů.

2. Podokruhy a ideály

369. Rozhodněte, zda a) $\{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$, b) $\{a + b\sqrt[3]{5} : a, b \in \mathbb{Z}\}$ tvoří podokruh okruhu $\mathbb{R}$. [Ř]

370. Rozhodněte, zda a) polynomy s nulovým absolutním členem, b) polynomy stupně nevýše 1, c) polynomy stupně alespoň 1 tvoří podokruh okruhu $\mathbb{Z}[x]$. [Ř]

371. Zjistěte, zda množina všech a) symetrických matic, b) regulárních matic, c) ortogonálních matic, d) horních trojúhelníkových matic, e) matic s posledním sloupcem nulovým, tvoří podokruh okruhu $\mathbf{M}_n(\mathbb{R})$. [Ř]

372. Buď $\mathbf{R}$ okruh a $M = \{a \in R : ar = ra \text{ pro všechna } r \in R\}$. Dokažte, že M tvoří podokruh okruhu $\mathbf{R}$. * Uveďte příklad okruhu, v němž je tento podokruh vlastní.

373. Dokažte, že okruh $\mathbb{Q}$ je generován množinou $\{\frac{1}{p} : p \text{ je prvočíslo}\}$ a že není generován žádnou její podmnožinou. * Dokažte, že okruh $\mathbb{Q}$ není generován vůbec žádnou konečnou množinou.

374. Spočtěte prvky podokruhů $\langle 28, 63\rangle_{\mathbb{Z}}$ a $\langle 15, 18, 40\rangle_{\mathbb{Z}}$. [Ř]

375. Spočtěte prvky podokruhů $\langle 18, 33, 69\rangle_{\mathbb{Q}}$, $\langle \frac{3}{4}\rangle_{\mathbb{Q}}$, $\langle \frac{3}{4}, \frac{2}{7}\rangle_{\mathbb{Q}}$ a $\langle \frac{2}{3}, \frac{2}{5}\rangle_{\mathbb{Q}}$. [Ř]

376. * Spočtěte prvky podokruhu $\langle \frac{a}{b}, \frac{c}{d}\rangle_{\mathbb{Q}}$ pro obecná $c, d \in \mathbb{Z}$.

377. Spočtěte prvky podokruhů $\langle 2, 3\rangle_{\mathbb{R}}$, $\langle \sqrt{2}\rangle_{\mathbb{R}}$ a $\langle \sqrt{2}, \sqrt{3}\rangle_{\mathbb{R}}$. [Ř]

378. Spočtěte prvky okruhů $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ a $\mathbb{Z}[\sqrt[3]{2}, i]$. [Ř]

379. Spočtěte prvky okruhu $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$. [Ř]

380. Spočtěte prvky podokruhů $\langle x^2, x^3\rangle_{\mathbb{Z}[x]}$, $\langle x^2+2, -x\rangle_{\mathbb{Z}[x]}$ a $\langle 2, x^2\rangle_{\mathbb{Z}[x]}$. [Ř]

381. Spočtěte prvky podokruhů $\langle \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)\rangle_{\mathbf{M}_2(\mathbb{Z})}$, $\langle \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)\rangle_{\mathbf{M}_2(\mathbb{Z})}$ a podokruhu $\langle \left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\rangle_{\mathbf{M}_2(\mathbb{Z})}$. [Ř]

382. Najděte všechny podokruhy okruhů $\mathbb{Z}$, $\mathbb{Z}_5$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$, obecně $\mathbb{Z}_n$ a $\mathbb{Z}_3 \times \mathbb{Z}_3$. [Ř]

383. Rozhodněte, zda existuje okruh, který je sjednocením svých dvou vlastních podokruhů. [Ř]

384. Najděte všechny ideály okruhů $\mathbb{Z}$, $\mathbb{Z}_5$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$, obecně $\mathbb{Z}_n$ a $\mathbb{Z}_3 \times \mathbb{Z}_3$. [Ř]

385. Spočtěte prvky nejmenšího ideálu okruhu $\mathbb{Z}$ obsahujícího a) $28, 63$, b) $15, 18, 40$. [Ř]

386. Spočtěte prvky nejmenšího ideálu okruhu $\mathbb{Q}$ obsahujícího $\frac{3}{4}, \frac{2}{7}$. [Ř]

387. Spočtěte prvky nejmenšího ideálu okruhu $\mathbb{Z}[x]$ obsahujícího a) x^2, x^3, b) $x^2+2, -x$, c) $2, x^2$. [Ř]

388. Rozhodněte, zda množina $\{\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x] : a_0 + a_1 + \ldots + a_n = 0\}$ tvoří ideál okruhu $\mathbb{Z}[x]$. Je to hlavní ideál? Pokud ano, najděte generátor. [Ř]

389. Rozhodněte, zda množina $\{f \in \mathbb{Z}[x] : f(1) = 0 \text{ a } x^2+1 \mid f\}$ tvoří ideál okruhu $\mathbb{Z}[x]$. Je to hlavní ideál? Pokud ano, najděte generátor. [Ř]

390. Rozhodněte, zda množina $\{x \cdot f + 3g : f, g \in \mathbb{Z}[x]\}$ tvoří ideál okruhu a) $\mathbb{Z}[x]$, b) $\mathbb{Q}[x]$. Je to hlavní ideál? Pokud ano, najděte generátor. [Ř]

391. Najděte generátor hlavního ideálu a) $(x^3-1)\mathbb{Q}[x] \cap (x^2+3)\mathbb{Q}[x]$, b) $(x^3-1)\mathbb{Q}[x] + (x^2+3)\mathbb{Q}[x]$ v oboru $\mathbb{Q}[x]$. [Ř]

392. Najděte generátor hlavního ideálu a) $(x^3-1)\mathbb{Q}[x] \cap (x^2-1)\mathbb{Q}[x]$, b) $(x^3-1)\mathbb{Q}[x] + (x^2-1)\mathbb{Q}[x]$ v oboru $\mathbb{Q}[x]$. [Ř]

393. Najděte nejmenší podtěleso tělesa $\mathbb{C}$ obsahující prvky a) $2, -4$, b) $\sqrt[3]{2}$, c) i, d) $\{z \in \mathbb{C} : |z| = 1\}$. [Ř]

3. Homomorfismy

394. Buď $\mathbf{R}$ komutativní okruh a $a \in R$. Dokažte, že zobrazení $\mathbf{R}[x] \to \mathbf{R}$, $f \mapsto f(a)$ je okruhový homomorfismus. Spočtěte jádro a obraz. [Ř]

395. Dokažte, že zobrazení $\mathbb{Z}[x] \to \mathbb{C}$, $f \mapsto f(i)$ je okruhový homomorfismus. Spočtěte jádro a obraz. [Ř]

396. Dokažte, že zobrazení $\mathbb{Z}[x] \to \mathbb{R}$, $f \mapsto f(\sqrt{2})$ je okruhový homomorfismus. Spočtěte jádro a obraz. [Ř]

397. Pro která s, u je zobrazení

$$\varphi : \mathbb{Z}[\sqrt{s}] \to \mathbb{Z}_n, \qquad a + b\sqrt{s} \mapsto a + bu \bmod n$$

homomorfismem? [Ř]

398. Rozhodněte, zda je zobrazení $\mathbb{Z}_n \to \mathbb{C}$, $k \mapsto e^{2k\pi i/n}$ okruhovým homomorfismem. Pokud ano, spočtěte jádro a obraz. [Ř]

399. Dokažte, že pro každý homomorfismus $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{C}$ platí $\varphi(a) = a$ pro každé $a \in \mathbb{Q}$. [?]

400. Buď $\mathbf{R} = (R, +, -, \cdot, 0)$ okruh a definujme operace $a \oplus b = a + b - 1$ a $a \odot b = a + b - ab$. Dokažte, že existují operace $\ominus$ a konstanta o takové, že $\mathbf{R}' = (R, \oplus, \ominus, \odot, o)$ je okruh. Dokažte, že $\mathbf{R} \simeq \mathbf{R}'$.

401. Buď X n-prvková množina, označme $P(X)$ množinu všech podmnožin X a definujme na $P(X)$ operaci $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Dokažte, že je okruh $(P(X), \triangle, id, \cap, \emptyset)$ izomorfní s okruhem $(\mathbb{Z}_2)^n$. [Ř]

402. Dokažte, že a) podokruh $\{\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) : a, b \in \mathbb{R}\} \leq \mathbf{M}_2(\mathbb{R})$ je izomorfní okruhu $\mathbb{C}$; b) podokruh $\{\left(\begin{smallmatrix} a & b \\ -\bar{b} & \bar{a} \end{smallmatrix}\right) : a, b \in \mathbb{C}\} \leq \mathbf{M}_2(\mathbb{C})$ je izomorfní okruhu kvaternionů (zde $\bar{a}$ značí číslo komplexně sdružené).

403. Zjistěte, pro která $s \in \mathbb{Z}$ platí

$$\mathbb{Z}[\sqrt{s}] \simeq (\{\left(\begin{smallmatrix} a & b\sqrt{s} \\ b\sqrt{s} & a \end{smallmatrix}\right) : a, b \in \mathbb{Z}\}, +, -, \cdot, 0).$$

[Ř]

404. Nechť $\mathbf{R} = \mathbb{Z}[\pi] \leq \mathbb{R}$ (π značí číslo $3.1415\ldots$). Dokažte, že $\mathbf{R} \simeq \mathbb{Z}[x]$. [Ř]

405. Rozhodněte, které z následujících okruhů jsou izomorfní: $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$. [Ř]

406. Buď $\mathbf{R}$ komutativní okruh. Najděte nekonečně mnoho podokruhů $\mathbf{R}[x]$, každý z nich izomorfní s $\mathbf{R}[x]$. [Ř]

407. Dokažte, že je-li $n = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$, pak je okruh $\mathbb{Z}_n$ izomorfní direktnímu součinu $\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$.

408. Dokažte, že okruh všech endomorfismů vektorového prostoru $\mathbf{T}^n$ nad tělesem $\mathbf{T}$ je izomorfní s okruhem $\mathbf{M}_n(\mathbf{T})$. [Ř]

409. Dokažte, že podílové těleso oboru $\mathbb{Z}[\sqrt{s}]$ je izomorfní s tělesem $\mathbb{Q}[\sqrt{s}]$.

410. Dokažte, že podokruh $\{\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) : a, b \in \mathbb{R}\}$ okruhu $\mathbf{M}_2(\mathbb{R})$ je izomorfní tělesu $\mathbb{C}$. [N]

411. Dokažte, že podokruh $\{\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) : a, b \in \mathbb{Z}_3\}$ okruhu $\mathbf{M}_2(\mathbb{Z}_3)$ je izomorfní tělesu $\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2 + 1$. [N]

412. * Najděte reprezentaci tělesa $\mathbb{F}_4 = \mathbb{Z}_2[x]/x^2 + x + 1$ v okruhu $\mathbf{M}_2(\mathbb{Z}_2)$. [?]

413. * Najděte všechny dvou a tříprvkové okruhy.

Endomorfismem okruhu $\mathbf{R}$ se rozumí homomorfismus $\mathbf{R} \to \mathbf{R}$, *automorfismem* se rozumí izomorfismus $\mathbf{R} \to \mathbf{R}$. Množina všech automorfismů daného okruhu $\mathbf{R}$ tvoří podgrupu grupy $\mathbf{S}_R$, značí se $\mathbf{Aut}(\mathbf{R})$.

414. Spočtěte všechny endomorfismy oboru $\mathbb{Z}$ a tělesa $\mathbb{Q}$. Najděte všechny spojité endomorfismy tělesa $\mathbb{R}$. Které z nich jsou automorfismy? [Ř]

415. Spočtěte všechny endomorfismy okruhu $\mathbb{Z}_n$. Které z nich jsou automorfismy? [Ř]

4. Faktorokruhy

416. Dokažte, že $\mathbb{Z}[x]/3 \simeq \mathbb{Z}_3[x]$. [Ř]

417. Buď $I = \{f \in \mathbb{Z}[x] : 3 \mid f(0)\}$. Dokažte, že $\mathbb{Z}[x]/\mathbf{I} \simeq \mathbb{Z}_3$. [Ř]

418. Dokažte, že $\mathbf{R}[x]/(x - a) \simeq \mathbf{R}$ pro libovolný komutativní okruh $\mathbf{R}$ a $a \in R$. [Ř]

419. Dokažte, že

(1) $\mathbb{Z}[x]/(x^2 + 1) \simeq \mathbb{Z}[i]$.
(2) $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$.
(3) $\mathbb{C}[x]/(x^2 + 1) \simeq \mathbb{C} \times \mathbb{C}$.

[Ř]

420. Dokažte, že

(1) $\mathbb{Z}[x]/(x^2 - 1) \simeq \{(a, b) : a \equiv b \pmod 2\} \leq \mathbb{Z} \times \mathbb{Z}$.
(2) $\mathbb{Q}[x]/(x^2 - 1) \simeq \mathbb{Q} \times \mathbb{Q}$.

[Ř]

421. S jakými známými okruhy jsou izomorfní $\mathbb{Z}[x]/(x^2 - 3)$, $\mathbb{Q}[x]/(x^2 - 3)$ a $\mathbb{R}[x]/(x^2 - 3)$? [Ř]

422. S jakými známými okruhy jsou izomorfní $\mathbb{Q}[x]/(x^4 - 4)$, $\mathbb{R}[x]/(x^4 - 4)$ a $\mathbb{C}[x]/(x^4 - 4)$? [Ř]

423. * S jakým známým okruhem je izomorfní $\mathbb{Q}[x]/(x^3 - 2)$? [N] [Ř]

424. Zjistěte, které okruhy (až na izomorfismus) lze získat jako $\mathbf{T}[x]/f$ volbou různých polynomů $f \in T[x]$ stupně 2. Zde $\mathbf{T}$ značí těleso a) $\mathbb{C}$, b) $\mathbb{R}$, c) * $\mathbb{Q}$. [Ř]

425. Zjistěte, které okruhy (až na izomorfismus) lze získat jako $\mathbf{T}[x]/f$ volbou různých polynomů $f \in T[x]$ stupně 3. Zde $\mathbf{T}$ značí těleso a) $\mathbb{C}$, b) $\mathbb{R}$. [Ř]

426. Kolik prvků má okruh $\mathbb{Z}_2[x]/(x^2+1)$? Napište tabulky sčítání a násobení v tomto okruhu. Je to těleso?

427. Kolik prvků má okruh $\mathbb{Z}_2[x]/(x^2+x+1)$? Napište tabulky sčítání a násobení v tomto okruhu. Je to těleso?

428. Kolik prvků má okruh $\mathbb{Z}_2[x]/(x^3+x+1)$? Napište tabulky sčítání a násobení v tomto okruhu. Je to těleso?

429. Kolik prvků má okruh $\mathbb{Z}_3[x]/(x^2+1)$? Napište tabulky sčítání a násobení v tomto okruhu. Je to těleso?

430. Dokažte, že $\mathbf{R}[x,y]/y \simeq \mathbf{R}[x]$ pro libovolný komutativní okruh $\mathbf{R}$. [Ř]

431. * Najděte nějaký známý okruh, s nímž je izomorfní $\mathbf{R}[x,y]/(x+y)$. (Zde $\mathbf{R}$ je libovolný komutativní okruh.) [Ř]

432. Buď X spočetná množina a $x \in X$. Dokažte, že $\mathbf{R}[X]/x \simeq \mathbf{R}[X]$ pro libovolný komutativní okruh $\mathbf{R}$. [Ř]

433. Dokažte, že matice, jejichž prvky jsou sudá čísla, tvoří ideál v okruhu $\mathbf{M}_n(\mathbb{Z})$. Dokažte, že příslušný faktorokruh je izomorfní okruhu $\mathbf{M}_n(\mathbb{Z}_2)$.

434. Dokažte, že $\begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} / \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & 0 \end{pmatrix} \simeq \mathbb{Q}$. [Ř]

435. Dokažte, že $\begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} / \begin{pmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{pmatrix} \simeq \mathbb{Q} \times \mathbb{Q}$. [Ř]

436. Buď $\mathbf{I}$ prvoideál komutativního okruhu s jednotkou $\mathbf{R}$ (*prvoideál* znamená, že kdykoliv $a \cdot b \in I$, pak $a \in I$ nebo $b \in I$). Dokažte, že $\mathbf{R}/\mathbf{I}$ je obor integrity.

437. Dokažte, že faktorokruh $\mathbb{Z}[i]/2$ není obor integrity.

438. Buď $\mathbf{I}$ maximální ideál okruhu $\mathbf{R}$ (*maximální* znamená, že v $\mathbf{R}$ neexistuje větší *vlastní* ideál). Dokažte, že okruh $\mathbf{R}/\mathbf{I}$ nemá žádné vlastní ideály. [Tedy je-li $\mathbf{R}$ komutativní s jednotkou, pak je $\mathbf{R}/\mathbf{I}$ těleso.] [N]

439. Nechť $\mathbf{I}$ není maximální ideál okruhu $\mathbf{R}$ (viz předchozí cvičení). Dokažte, že okruh $\mathbf{R}/\mathbf{I}$ má nějaký vlastní ideál. [N]

440. Buď $\mathbf{T}$ těleso. Dokažte, že ideál $\mathbf{I}$ je maximální v okruhu $\mathbf{T}[x]$ právě tehdy, když $I = fT[x]$ pro nějaký ireducibilní polynom f. [N]

441. * Buď $\mathbf{R}$ okruh a $\mathbf{I}$ jeho ideál. Dokažte, že svaz ideálů okruhu $\mathbf{R}/\mathbf{I}$ je izomorfní intervalu $[\mathbf{I}, \mathbf{R}]$ ve svazu ideálů okruhu $\mathbf{R}$. [Ř]

IV. Tělesová rozšíření

1. Rozšíření konečného stupně

442. Spočtěte minimální polynom prvků -2, i, $\sqrt[3]{2}$, $1+\sqrt{5}$ a $e^{2\pi i/3}$ nad tělesem $\mathbb{Q}$. [Ř]

443. Spočtěte minimální polynom prvků $\sqrt{3}$ a $\sqrt[4]{2}$ nad tělesem $\mathbb{Q}(\sqrt{2})$. [Ř]

444. Spočtěte minimální polynom prvku $\sqrt{3}+\sqrt{5}$ nad tělesem $\mathbb{Q}$.

445. Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a \in S$. Vyjádřete polynom $m_{a^{-1},\mathbf{T}}$ pomocí koeficientů polynomu $m_{a,\mathbf{T}}$. [Ř]

446. Spočtěte $[\mathbb{Q}(i-4):\mathbb{Q}]$, $[\mathbb{Q}(\sqrt{3},\sqrt[3]{3}):\mathbb{Q}]$, $[\mathbb{Q}(\sqrt{2},\sqrt[4]{2}):\mathbb{Q}]$. [Ř]

447. Spočtěte $[\mathbb{Q}(e^{2\pi i/p}):\mathbb{Q}]$ pro p prvočíslo. [Ř]

448. * Spočtěte $[\mathbb{Q}(\sqrt{3}+\sqrt{7}):\mathbb{Q}]$. [N] [Ř]

449. * Dokažte, že $[\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n}):\mathbb{Q}] = 2^n$, pokud $p_1,\ldots,p_n$ jsou po dvou různá prvočísla.

450. Spočtěte $[\mathbb{Q}(\sqrt[q]{p}):\mathbb{Q}]$ pro p prvočíslo. [Ř]

451. Buď $\mathbf{T} < \mathbf{S} \leq \mathbb{C}$. Je-li $[\mathbf{S}:\mathbf{T}] = 2$, pak $\mathbf{S} = \mathbf{T}(\sqrt{r})$ pro nějaké $r \in T$. [N]

452. Buď $\mathbf{T} < \mathbf{S} \leq \mathbb{C}$. Je-li $[\mathbf{S}:\mathbf{T}] = 3$, musí být nutně $\mathbf{S} = \mathbf{T}(\sqrt[3]{r})$ pro nějaké $r \in T$? [Ř]

453. Jsou prvky $1+\sqrt{2}+\sqrt[3]{3}$ a $\sqrt[4]{2}/(\sqrt{2}+\sqrt{3})$ algebraické nad tělesem $\mathbb{Q}$? [Ř]

454. Předpokládejme, že je číslo $a \in \mathbb{R}$ transcendentní nad $\mathbb{Q}$. Dokažte, že a) číslo $\sqrt{a}$, b) číslo $f(a)$, kde f je libovolný polynom z $\mathbb{Q}[x]$, je také transcendentní nad $\mathbb{Q}$.

455. Buď $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$ rozšíření těles, $\mathbf{U}$ algebraické nad $\mathbf{S}$ a $\mathbf{S}$ algebraické nad $\mathbf{T}$. Je $\mathbf{U}$ algebraické nad $\mathbf{T}$? [N]

456. Buď p, q různá prvočísla. Dokažte, že jsou čísla $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$ lineárně nezávislá nad tělesem $\mathbb{Q}$. [Ř]

457. Buď $\mathbf{T}$ těleso a a algebraický prvek nad $\mathbf{T}$ takový, že $[\mathbf{T}(a):\mathbf{T}]$ je lichý. Dokažte, že $\mathbf{T}(a) = \mathbf{T}(a^2)$. [Ř]

458. Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a, b \in S$ algebraické nad $\mathbf{T}$. Předpokládejme, že stupně polynomů $m_{a,\mathbf{T}}$, $m_{b,\mathbf{T}}$ jsou nesoudělné. Pak $[\mathbf{T}(a,b):\mathbf{T}] = [\mathbf{T}(a):\mathbf{T}] \cdot [\mathbf{T}(b):\mathbf{T}]$. Uveďte protipříklad na tuto rovnost, pokud stupně nesoudělné nejsou.

459. Buď $\mathbf{T}$ těleso, a transcendentní prvek nad $\mathbf{T}$ a uvažujme těleso $\mathbf{S}$ splňující $\mathbf{T} < \mathbf{S} < \mathbf{T}(a)$. Rozhodněte, které z následujících tvrzení je pravdivé: a) $\mathbf{T} \leq \mathbf{S}$ je algebraické rozšíření, b) $\mathbf{S} \leq \mathbf{T}(a)$ je algebraické rozšíření. [?]

460. Buď $\mathbf{T}$ těleso a a, b algebraické prvky nad $\mathbf{T}$ takové, že jejich minimální polynomy f, g jsou nesoudělné v $\mathbf{T}[x]$. Dokažte, že polynom g je ireducibilní v $\mathbf{T}(a)[x]$. [?]

461. * Buď $\mathbf{T} \leq \mathbf{U}, \mathbf{V} \leq \mathbf{S}$ rozšíření těles takové, že $[\mathbf{U}:\mathbf{T}]$ i $[\mathbf{V}:\mathbf{T}]$ jsou konečné. Dokažte, že nejmenší podtěleso $\mathbf{S}$ obsahující $U \cup V$ je tvořené množinou $\{\sum_{i=0}^{n} a_i b_i : n \in \mathbb{N}, a_i \in U, b_i \in V\}$.

462. * Buď $\mathbf{T}$ je těleso a $\mathbf{R}$ obor integrity takový, že $\mathbf{T} \leq \mathbf{R}$. Obor $\mathbf{R}$ můžeme považovat za vektorový prostor nad $\mathbf{T}$. Dokažte, že je-li konečné dimenze, pak je $\mathbf{R}$ těleso.

463. * Buď $\mathbf{R}, \mathbf{S}$ obory integrity, $\mathbf{R} \leq \mathbf{S}$ a předpokládejme, že každý prvek $\mathbf{R}$ je kořenem nějakého monického polynomu z $\mathbf{S}[x]$. Dokažte, že $\mathbf{R}$ je těleso právě tehdy, když $\mathbf{S}$ je těleso.

464. * Uvažujme rozšíření $\mathbf{T} \leq \mathbf{S}$ stupně n. Najděte prostý homomorfismus $\mathbf{S} \to \mathbf{M}_n(\mathbf{T})$. [N]

465. * Na základě předchozího cvičení navrhněte algoritmus na výpočet minimálního polynomu. [?]

466. Jsou dány tři různé body A, B, C. Dokažte, že lze pravítkem a kružítkem sestrojit přímku, která je kolmá na přímku AB a prochází bodem C. (Nezapomeňte rozlišit případ, kdy C leží/neleží na AB!)

467. Jsou dány tři body A, B, C neležící na přímce. Dokažte, že lze pravítkem a kružítkem sestrojit bod D takový, že úhel BAD je stejný, jako úhel CAD.

468. Dokažte, že žádné transcendentní číslo není konstruovatelné.
Tedy pravítkem a kružítkem nelze řešit ani *rektifikaci kružnice* (k dané kružnici nalézt úsečku, která je stejně dlouhá jako obvod této kružnice), ani *kvadraturu kruhu* (k danému kruhu nalézt úsečku takovou, že čtverec nad ní sestrojený má plochu stejnou jako tento kruh). [Ř]

469. Dokažte, že algebraické číslo, jehož minimální polynom má stupeň, který není mocnina dvou, není konstruovatelné.
Tedy pravítkem a kružítkem nelze řešit *zdvojení krychle* (k dané úsečce u sestrojit úsečku v takovou, že krychle s hranou dlouhou jako v má dvakrát větší objem, než krychle s hranou dlouhou jako u). [Ř]

470. Dokažte, že pravítkem a kružítkem nelze zkonstruovat číslo $\cos 20°$. [N]
Tedy pravítkem a kružítkem nelze řešit *trisekci úhlu* (k danému úhlu sestrojit třetinový úhel): nelze roztřetit úhel 60°. Zároveň je vidět, že nelze zkonstruovat pravidelný k-úhelník pro žádné k dělitelné devíti.

471. Dokažte, že pravítkem a kružítkem lze sestrojit pravidelný n-úhelník právě tehdy, když je konstruovatelné číslo $\cos(2\pi/n)$.

472. Buď p prvočíslo. Dokažte, že pokud lze sestrojit pravítkem a kružítkem pravidelný p-úhelník, pak $p-1$ je mocnina dvou.

473. * Buď p prvočíslo. Dokažte, že pokud lze sestrojit pravítkem a kružítkem pravidelný p-úhelník, pak $p = 2^{2^k}+1$ pro nějaké k. [N]

474. Dokažte, že pokud lze sestrojit pravítkem a kružítkem pravidelný n-úhelník, pak lze sestrojit i pravidelný $2n$-úhelník.

475. Které pravidelné n-úhelníky pro $n < 17$ lze sestrojit pravítkem a kružítkem? [Ř]

476. ** Které pravidelné n-úhelníky lze sestrojit pravítkem a kružítkem?

477. Dokažte, že konstruovatelná čísla tvoří podtěleso $\mathbf{K}$ tělesa $\mathbb{R}$ takové, že $\sqrt{a} \in K$ pro každé $a \in K$.

478. Dokažte, že každé číslo, jehož minimální polynom má stupeň 2, je konstruovatelné.

479. ** Uveďte číslo, jehož minimální polynom má stupeň 4, ale není konstruovatelné.

2. Kořenová a rozkladová nadtělesa

480. Najděte všechna kořenová nadtělesa polynomů x^2-1, x^2+1 a x^2-2. [Ř]

481. Najděte všechna kořenová nadtělesa polynomů x^3-1, x^3+1 a x^3-2. [Ř]

482. Najděte všechna kořenová nadtělesa polynomů x^p-1, x^p+1 a x^p-2, kde p je prvočíslo.

483. Najděte všechna kořenová nadtělesa polynomů x^4-1 a x^4+1. [Ř]

484. Najděte všechna kořenová nadtělesa polynomů x^6-1 a x^6+1.

485. Najděte rozkladová nadtělesa polynomů x^n-1 a x^n+1 nad $\mathbb{Q}$. [Ř]

486. Najděte všechna kořenová nadtělesa a rozkladové nadtěleso polynomu x^3-6x-9 nad $\mathbb{Q}$. [Ř]

487. Najděte všechna kořenová nadtělesa a rozkladové nadtěleso polynomu x^4-5x^2+6 nad $\mathbb{Q}$. [Ř]

488. Dokažte, že $\mathbb{Q}(\sqrt[5]{2}, e^{2\pi i/5})$ je rozkladové nadtěleso polynomu x^5-2 nad $\mathbb{Q}$. Spočtěte jeho stupeň nad $\mathbb{Q}$.

489. Určete počet prvků rozkladového nadtělesa následujících polynomů: a) $x^3 + x^2 + 1$ nad $\mathbb{Z}_5$, b) $2x^4 + 1$ nad $\mathbb{Z}_3$, c) $x^4 + 2x^2 + 1$ nad $\mathbb{Z}_3$, d) $x^{16} + x$ nad $\mathbb{Z}_2$. [Ř]

490. Existuje polynom $f \in \mathbb{Q}[x]$ takový, že má n různých komplexních kořenů, ale stupeň rozkladového nadtělesa je menší než n? [Ř]

491. Buď $\mathbf{S}$ rozkladové nadtěleso polynomu $f \in T[x]$ stupně n. Dokažte, že $[\mathbf{S} : \mathbf{T}]$ dělí $n!$. [N]

492. Dokažte, že tělesa $\mathbb{Q}(\sqrt{7})$ a $\mathbb{Q}(\sqrt{11})$ nejsou $\mathbb{Q}$-izomorfní.

493. * Zjistěte, pro jaká $r, s \in \mathbb{Z}$ jsou tělesa $\mathbb{Q}(\sqrt{r})$ a $\mathbb{Q}(\sqrt{s})$ izomorfní. [?] [Ř]

Konečné těleso $\mathbb{F}_{p^n}$ lze uvažovat také jako rozkladové nadtěleso polynomu $x^{p^m-1} - 1$.

494. Buď p prvočíslo. a) Dokažte, že v oboru $\mathbb{Z}$ platí $p^n - 1 \mid p^m - 1$ právě tehdy, když $n \mid m$. b) Dokažte, že v oboru $\mathbb{Z}_p[x]$ platí $x^n - 1 \mid x^m - 1$ právě tehdy, když $n \mid m$.

495. * Užitím předchozího cvičení dokažte, že existuje vnoření $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ právě tehdy, když $n \mid m$. [N]

3. Galoisova teorie

496. Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles, $\varphi : \mathbf{S} \to \mathbf{S}$ buď $\mathbf{T}$-homomorfismus a $0 \neq f \in \mathbf{T}[x]$. Dokažte, že φ permutuje kořeny polynomu f, které leží v $\mathbf{S}$.

497. Buď $\mathbf{S}_1$ a $\mathbf{S}_2$ rozšíření tělesa $\mathbf{T}$ a $\varphi : \mathbf{S}_1 \to \mathbf{S}_2$ $\mathbf{T}$-izomorfismus. Dokažte, že je-li $f \in T[x]$ a $a \in S_1$, pak a je kořen f v $\mathbf{S}_1$ právě tehdy, když $f(a)$ je kořen f v $\mathbf{S}_2$.

498. Spočtěte $\mathbf{Gal}(\mathbb{C}/\mathbb{R})$.

499. Spočtěte $\mathbf{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$, kde p je prvočíslo.

500. Spočtěte $\mathbf{Gal}(\mathbb{Q}(\sqrt[n]{p})/\mathbb{Q})$, kde p je prvočíslo a $n \in \mathbb{N}$.

501. Spočtěte $\mathbf{Gal}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, kde p je prvočíslo a $n \in \mathbb{N}$.

502. Spočtěte $\mathbf{Gal}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$, kde p je prvočíslo a $n \in \mathbb{N}$.

503. Spočtěte $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$, kde $\mathbf{S}$ je rozkladové nadtěleso polynomu a) $x^3 - 1$, b) $x^3 + 1$, c) $x^3 - 2$, d) $x^3 + 2$.

504. Spočtěte $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$, kde $\mathbf{S}$ je rozkladové nadtěleso polynomu a) $x^5 - 1$, b) $x^6 - 1$.

505. Spočtěte $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$, kde $\mathbf{S}$ je rozkladové nadtěleso polynomu $x^5 - x^4 - x^3 - x - 2$.

506. Spočtěte $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$, kde $\mathbf{S}$ je rozkladové nadtěleso polynomu $x^5 + x^3 - 2x^2 - 2$.

507. Spočtěte $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$, kde $\mathbf{S}$ je rozkladové nadtěleso polynomu a) $x^4 + 7x^2 + 4$, b) $x^4 + 4x^2 + 2$, a) $x^4 + 6x^2 + 6$.

508. * Buď $\mathbf{S}$ je rozkladové nadtěleso polynomu $x^4 + ax^2 + b$ nad $\mathbb{Q}$. Dokažte, že $\mathbf{Gal}(\mathbf{S}/\mathbb{Q})$ je izomorfní

- $\mathbb{Z}_2 \times \mathbb{Z}_2$, pokud b je druhá mocnina racionálního čísla;
- $\mathbb{Z}_4$, pokud b není druhá mocnina, ale $b(a^2 - 4b)$ je druhá mocnina;
- $\mathbf{D}_8$ v ostatních případech.

509. * Buď $\mathbf{S}$ je rozkladové nadtěleso polynomu $x^n - 1$. Dokažte, že $\mathbf{Gal}(\mathbf{S}/\mathbb{Q}) \simeq \mathbb{Z}_n^*$.

510. * Spočtěte $|\mathbf{Gal}(\mathbf{S}/\mathbb{Q})|$, kde $\mathbf{S}$ je rozkladové nadtěleso polynomu $x^n - a$, $a \in \mathbb{Q}$.

511. * Spočtěte $|\mathbf{Gal}(\mathbf{S}/\mathbb{Q})|$, kde $\mathbf{S}$ je rozkladové nadtěleso polynomu $x^6 + 14x^3 - 7$.

512. Dokažte, že $|\mathbf{Gal}(\mathbb{R}/\mathbb{Q})| = 1$. Návod: $\mathbb{Q}$-automorfismy zachovávají uspořádání.

513. * Dokažte, že $\mathbf{Gal}(\mathbb{C}/\mathbb{Q})$ je nekonečná.

NÁVODY

5. Buď z předchozího cvičení odvoďte součet sudých čísel a výsledky sečtěte. Nebo dosazením několika hodnot odhadněte výsledek jako polynom an^3+bn^2+cn+d a dokaľte, ľe je váa odhad správný. **6.** Dosazením několika hodnot odhadněte výsledek jako polynom čtvrtého stupně a dokaľte, ľe je váa odhad správný. **30.** Dokaľte, ľe je dělitelné 7. **35.** ($\Rightarrow$) Pomocí malé Fermatovy věty zpárujte prvky $2,\ldots,p-2$ do dvojic, jejichľ součin je 1; díky předchozímu cvičení jsou to skutečně dvojice. Levá strana je tedy rovna součinu spousty jedniček a $p-1$. ($\Leftarrow$) Na levé straně se vyskytuje nějaký dělitel p. **42.** Nech» $f=\sum_0^k a_i x^{ni}$. Platí $f(x^n)=(x-1)g(x)$ pro nějaký polynom g, spočtěte koeficienty toho g. Ukáľe se, ľe $1+x+\cdots+x^{n-1}\mid g$. **49.** Protoľe ztotoľnění $u_i=u_j$ způsobí, ľe je determinant nulový, musí být determinant dělitelný členy u_i-u_j pro kaľdé $i\neq j$. Nyní uvaľujte stupeň výsledného polynomu. **55.** Dokaľte, ľe je-li u kořen tohoto polynomu, pak je $u+1$ také kořen. **57.** Pouľijte cvičení, které říkalo, ľe p je ireducibilní právě tehdy, kdyľ $p(x+a)$ je ireducibilní, a Eisensteinovo kritérium. **76.** Je-li a kořenem f i f', pak je také kořenem $\mathrm{NSD}(f,f')$. (Protoľe $x-a$ dělí oba dva, tedy i NSD.) **80.** Převeďte na řeaení diofantické rovnice $a^2-2b^2=1$. Není cyklická, protoľe $1+\sqrt{2}$ a -1 jsou „nezávislé“ generátory. **82.** Těľká je pouze implikace ($\Rightarrow$). Dokaľte nejprve, ľe $a+bi$ je ireducibilní právě tehdy, kdyľ $a-bi$ je ireducibilní. Poté pouľijte vlastnost jednoznačného ireducibilního rozkladu v oboru $\mathbb{Z}[i]$. **84.** Dokaľte a) $p\mid(((p-1)/2)!)^2+1$, b) není moľné, aby v $\mathbb{Z}[i]$ ireducibilní prvek dělil a^2+b^2 pro nesoudělná $a,b\in\mathbb{Z}$. **91.** Volba q,r podobně jako pro $\mathbb{Z}[i]$, ale důkaz správnosti je těľaí, protoľe $\nu(r)\neq|r|^2$. **94.** $4\mid\nu(a)$ právě tehdy, kdyľ $2\mid a$. **105.** Pouľijte Eulerovu větu nebo Eukleidův algoritmus. **108.** Uľijte Bézoutovu rovnost. **122.** Definujte $\varphi(x)=\psi(x')$. **124.** Stačí ji umět rozloľit na direktní součin. **125.** Protoľe $\varphi(a)^k=e$ právě tehdy, kdyľ $a^k=e$. **129.** Vyplňujte tabulku. **130.** Hodně dlouho vyplňujte tabulku, nebo buďte chytřejaí :–). **138.** Pouľijte předchozí cvičení a Lagrangeovu větu. **146.** Uľijte Bézoutovu nerovnost. **152.** Uľijte Bézoutovu nerovnost. **163.** a) Dokaľte, ľe $\varphi(x)=kx$ pro kaľdé $x\in\mathbb{Z}$ a potom ověřte, ľe tento vztah platí i pro zlomky. b) Spojitá funkce je dána hodnotami v racionálních bodech. c) Podívejte se na endomorfismy vektorového prostoru $\mathbb{R}$ nad tělesem $\mathbb{Q}$. **167.** V soudělném případě v $\mathbb{Z}_m\times\mathbb{Z}_n$ nenajdete prvek řádu mn. V nesoudělném pouľijte Čínskou větu o zbytcích. **171.** Kaľdé kladné racionální číslo lze napsat ve tvaru $p_1^{k_1}\cdot\ldots\ldots 22\ldots\cdot p_n^{k_n}$ pro nějaká prvočísla p_i a nějaká $k_i\in\mathbb{Z}$. **172.** Vezměte je nejmenaí kladný prvek grupy $\mathbf{H}$. **176.** Pouľijte Čínskou větu o zbytcích. **177.** Postupujte podobně jako charakterizaci podgrup grupy $\mathbb{Z}$. **187.** Uvaľujte podgrupy generované $-1,5$. **200.** K řeaení části c) si prostudujte kapitolu o cyklických grupách. **234.** a) Označme a,b generátory grupy $\mathbf{D}_n$, kde a je přísluaná rotace a b jedna z osových symterií. Analogicky označme c,d a e,f generátory $\mathbf{D}_{2^k}$ a $\mathbf{D}_m$. Pak zobrazení $a^ib^j\mapsto(c^ud^j,e^vf^j)$, kde $u=i \bmod 2^k$ a $v=i \operatorname{div} 2^k$, je vnoření. b),c) analogicky. **235.** Vnořte $\mathbf{G}$ do $\mathbf{S}_{G\cup G'}$, kde G' je disjunktní kopie mnoľiny G. Zdvojenou permutaci jiľ snadno odmocníme. **236.** Spočítejte, ľe má 8 prvků, ľe není abelovská, a dokaľte, ľe není izomorfní $\mathbf{D}_8$. **242.** Uvědomte si, ľe spojitá reálná funkce je jednoznačně určena svými hodnotami v racionálních bodech. **257.** Pouľijte-li předchozí cvičení, zbývá vyaetřit pouze případ abelovských grup. **266.** $1\mapsto E$, $i\mapsto\left(\begin{smallmatrix}i&0\\0&-i\end{smallmatrix}\right)$, $j\mapsto\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$, $k\mapsto\left(\begin{smallmatrix}0&i\\i&0\end{smallmatrix}\right)$. Z komplexních matic na reálné pak přejdeme nahrazením komplexních čísel za matice 2×2 jako v minulém cvičení. **271.** Indukcí podle $n-k$. **296.** Při počítání symetrií nezapomeňte, ľe i kdyľ při otočení zůstane destička na místě, aipka můľe ukazovat jinam. **314.** Označme ten interval $[\mathbf{H},\mathbf{G}]$. Uvaľujte působení grupy $\mathbf{G}$ na rozkladových třídách $\mathbf{G}/\mathbf{H}$. **352.** $\mathbf{S}_4/\mathbf{H}$ má $24/4=6$ prvků. Není-li abelovská, je izomorfní $\mathbf{S}_3$. **357.** $\simeq\mathbb{Q}^*\times\cdots\times\mathbb{Q}^*$. **360.** Uvaľujte homomorfismus $x\mapsto(xA,xB)$. Obtíľné je dokázat, ľe je toto zobrazení na. K tomu se hodí pozorování, ľe pro kaľdé $x\in G$ existuje $b\in B$ takové, ľe $xA=bA$ a analogicky pro xB. **410.** $a+bi\mapsto\left(\begin{smallmatrix}a&b\\-b&a\end{smallmatrix}\right)$ je izomorfismus. **411.** $[ax+b]\mapsto\left(\begin{smallmatrix}b&a\\-a&b\end{smallmatrix}\right)$ je izomorfismus. **423.** Pouľijte minimální polynom prvku $\sqrt[3]{2}$. **438.** Kdyby existoval vlastní ideál $\mathbf{K}$ v $\mathbf{R}/\mathbf{I}$, pak by byl $\mathbf{J}=\{a:[a]\in K\}$ ideál v $\mathbf{R}$ ve sporu s maximalitou $\mathbf{I}$. **439.** Uvaľujte $\{[a]:a\in I\}$. **440.**

$\mathbf{T}[x]$ je OIHI, tedy $\mathbf{I}$ je hlavní ideál. Dále pouľijte fakt, ľe $aR \subseteq bR \Leftrightarrow b \mid a$. **448.** Uvaľujte mezitěleso $\mathbb{Q}[\sqrt{21}]$. **451.** Uvaľujte $a \in S \setminus T$. Pak $\mathbf{S} = \mathbf{T}(a)$, a je kořen kvadratického polynomu a pouľijte známý vzorec na výpočet kořenů. **455.** Je-li a kořen polynomu $\sum a_i x^i \in S[x]$, pak je to prvek $\mathbf{T}(a, a_1, \ldots, a_n)$, coľ je roaíření konečného stupně. **464.** Prvku a přiřaďte matici, která odpovídá endomorfismu $L_a : x \mapsto ax$ vektorového prostoru $\mathbf{S}$ nad $\mathbf{T}$. **470.** Pouľijte vzorec $\cos 3x = 4(\cos x)^3 - 3\cos x$. **473.** Podle předchozího cvičení je $p = 2^m + 1$. Pokud liché n dělí m, pak $2^{m/n} + 1$ dělí p. **491.** Postupujte indukcí stejně jako v důkazu existence rozkladového nadtělesa. **495.** Vnoření se zkonstruuje pomocí následujícího pozorování: pokud $f \mid g$, pak rozkladové nadtěleso polynomu f je podtělesem rozkladového nadtělesa polynomu g. Opačná implikace: uvaľujte grupy $\mathbb{F}_{p^n}^*$ a $\mathbb{F}_{q^n}^*$ a uľijte Lagrangeovu větu.

ŘEŠENÍ

8. $3, -3, 32.\ 12, -7, 3$. **9.** 1. **11.** a) $x = 5{+}7k$, $k \in \mathbb{Z}$, b) $x = 11{+}21k$, $k \in \mathbb{Z}$, c) $x = 5{+}11k$, $k \in \mathbb{Z}$. **12.** 363. **13.** 231. **14.** $x = 1320k{+}14$, $k \in \mathbb{Z}$. **15.** $x = 120k{+}34$, $k \in \mathbb{Z}$. **16.** Nemá řeaení. **17.** $x = 15k{+}8$, $k \in \mathbb{Z}$. **19.** Počítejte mod 11. Vyjde 0. **20.** Počítejte mod 13. Vyjde 0. **21.** 13, 1. **24.** 8. **25.** -1. **26.** 33. **27.** 2. **28.** 07. **29.** a pro $5 \nmid a$, 0 v opačném případě. **31.** Pokud $5 \mid n$, je to zřejmé. V opačném případě, podle malé Fermatovy věty $n^9 \equiv n^5 \equiv n \pmod 5$ a $n^7 \equiv n^3 \pmod 5$ a pak uľ je to také jasné. **32.** $\{(x, y) : 7 \nmid x, y \equiv -1 \pmod 7\}$. **36.** Např. ideál vaech polynomů, jejichľ absolutní člen je sudý. **37.** Např. ideál vaech polynomů, jejichľ absolutní člen je nula. **38.** Zvolte v podmínce (2) $a = 3x, b = 2x$. Zkuste vyjádřit $1 = \mathrm{NSD}(x, 2) = xu + 2v$. **39.** Právě tehdy, kdyľ $m \mid n$. **40.** $x^{n \bmod m} - 1$. **41.** $x^{\mathrm{NSD}(m,n)} - 1$. **42.** Ano. **43.** Dosaďte několik hodnot a pouľijte větu, ľe polynom má jen konečně mnoho kořenů. **44.** 10. **45.** Např. $(2x-1)(x-i)(x+i)(x-(2-i))(x-(2+i))$. **46.** $x^3 - 9x^2 + 26x - 18$. **47.** Např. $x^2 + x \in \mathbb{Z}_6[x]$. **48.** $x^2 + 1$ má kořeny $\pm i, \pm j, \pm k$. **49.** Pokračování návodu: tedy determinant je dělitelný součinem $\prod_{i \neq j}(u_i - u_j)$, ale přitom má stupeň nejvýae $n(n-1)/2$, takľe je roven tomuto výrazu aľ na konstantu. Není těľké nahlédnout, ľe konstanta je 1. **50.** a) -1, b) $-3, -1/2, 1/3, 1, 2$, c) $-1/2, 2$. **51.** Ne, ne, ano, ne, ne. **52.** Ano (nemá kořen), ne $((2x-1)(2x+1))$, ano (Eisenstein). **53.** a) vaechny polynomy stupně 1, b) vaechny polynomy stupně 1 a ty polynomy stupně 2 které nemají reálný kořen. **56.** Ano. Je-li $f(x{+}a) = g(x)h(x)$, pak $f(x) = g(x{-}a)h(x{-}a)$, spor. **58.** $(x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i)$, $(x-\sqrt{2})(x+\sqrt{2})(x^2+1)$, $(x^2-2)(x^2+1)$, $(x^2+3)(x+2)(x+3)$, $(x^2+1)^2$. **59.** Ireducibilní, $(x^2+x+1)(x^2-x+1)$, ireducibilní, $(x+2)(2x+5)$. **60.** První: $2 \cdot (x^3 + 2x^2 - x + 2)$, ireducibilní. Druhý: $(2x+3)(x^2+1)$. **61.** $(x+2)(x^2+x+1)(x^2+2x+4)$. **62.** Ireducibilní, $(x^2{+}1)(x^3{+}2x{+}2)$, $(x^2{+}1)^3$. **63.** $(2x{+}1)(x^2{+}1)(x^2{-}2)$, $(2x{+}1)(x{+}2)(x{+}3)(x^2{+}3)$. **64.** a) $(x{+}1)(x^2{+}x{+}1)(x^4{+}x^3{+}x^2{+}x{+}1)(x^4{+}x^3{+}1)(x^4{+}x{+}1)$, b) $(x{-}1)(x{+}1)(x^2{+}1)(x^4{+}1)$. **65.** $x^3{+}2x^2{+}x{+}2$, $-2x$, 1. **66.** a) $x{+}1$, b) 1, c) $x{-}1$. **67.** 1, $x{+}1$. Zde je výhodné uľít výpočet pomocí rozkladů. **68.** a) 1, b) $x^2{+}2$. **69.** $x^3{+}x^2{+}x{+}1$ v obou. **70.** $a \neq -5$ jednonásobný, $a = -5$ dvojnásobný. **71.** $a = -n$, $b = n + 1$. **72.** $a = -5/3c^2$, $b \in \{-7/3c^2, 2/3c^2\}$, pro libovolné $c \in \mathbb{N}$. **73.** 2, 4, 3. V c) nelze pouľít Větu kvůli charakteristice!!! **74.** -2. **75.** Nejsou. **78.** $\pm 1, \pm i, \simeq \mathbb{Z}_4$; $\pm 1, \simeq \mathbb{Z}_2$. **79.** $1{+}\sqrt{2}$ je takový. **81.** $(1{+}i)^2(2{+}i)$, $(2{+}i)(1{+}2i)$, $(1{+}i)(-2{-}3i)$, $3(1{+}i)(1{-}i)$, 11. **82.** Pokračování návodu: $(a{+}bi)(a{-}bi) = a^2 + b^2$. Kdyby měla pravá strana netriviální ireducibilní rozklad v $\mathbb{Z}$, pak by ovaem ten ireducibilní rozklad musel mít dva prvky, jeden asociovaný s $a + bi$, druhý s $a - bi$. Ale ľádné celé číslo nemůľe být asociované s $a + bi$ pro $a, b \neq 0$. Opačná implikace plyne z multiplikativnosti normy. **83.** Pokud se rozkládá, pak na součin dvou prvků normy p. Takové ale neexistují: jedna sloľka musí být lichá, druhá sudá, součet čtverců tedy bude $\equiv 1 \pmod 4$. **85.** ireducibilní, ireducibilní,

$(i\sqrt{2})^2\cdot(1+i\sqrt{2})$. **87.** Například a) 2, b) $a=4$, $b=2+2\sqrt{5}$. **88.** $4=2\cdot 2=(1+i\sqrt{3})(1-i\sqrt{3})$. **89.** $|z-q|<1$, tedy $\nu(r)=|a-bq|^2=|b|^2\cdot|a/b-q|^2=|b|^2\cdot|z-q|<|b|^2=\nu(b)$. **90.** Analogicky jako v případě $\mathbb{Z}[i]$, protože $\nu(r)=|r|^2$. **92.** a) $(1+i)$, $(1+i)^2(2+i)(2-i)$, b) 3, $18+21i$, c) $1+4i$, $31+5i$, d) $7+6i$, $85+85i$. **93.** Je to hlavní ideál s generátorem $\mathrm{NSN}(3+6i,12-3i)=18+21i$. **94.** Je to hlavní ideál s generátorem $\mathrm{NSN}(2,7-3i)=10+4i$. **96.** $[4x]$, $[3x^2+2x+1]$, $[4x^2+4]$. **97.** $[x^3+x^2+1]$, $[2x^3+2x^2+2]$, $[x^3+2x^2+2x+2]$. **98.** $\mathbb{F}_8^*\simeq\mathbb{Z}_7$, a tedy vaechny prvky různé od 0,1 jsou primitivní. **99.** $\mathbb{F}_9^*\simeq\mathbb{Z}_8$, tedy existují 4 primitivní. Jsou to $x+1, x+2, 2x+1, 2x+2$. **101.** Dvě: sebe sama a podtěleso generované 1. **102.** Ne (nula nemá inverz), ne (není jednotka), ne (není jednotka), ano neab., ne (neasociativní), ano ab., ne (existují neregulární matice), ne (inverz může být racionální), ne (neexistují inverzy), ne (neexistují inverzy), ano ab. **103.** $u=a'$, $x''=a'*x'*a'$. **104.** $x=a^{-2}*c^{-2}*b^3$. **105.** a) 33, b) 34. **108.** $1=um+vn$, $b=a^{vn}$, $c=a^{um}$. **110.** ($\Rightarrow$) Je-li $a,b\in H$, pak $b'\in H$ a tedy i součin $a*b'\in H$. ($\Leftarrow$) Je-li $a,b\in H$, pak $e=a*a'\in H$, $a'=e*a'\in H$, $b'=e*b'\in H$ a tedy i $a*b=a*b''\in H$. **112.** Ne. Např. v $\mathbf{S}_{\mathbb{Z}}$, permutace $a=\ldots\ldots 22\ldots(i\ i+1)\ldots\ldots 22\ldots$ a $b=\ldots\ldots 22\ldots(i-1\ i)\ldots\ldots 22\ldots$ jsou konečného řádu, ale jejich složení ne. **113.** Ano, v abelovských grupách $|a*b|$ dělí $\mathrm{NSN}(|a|,|b|)$, viz cvičení výae. **116.** Buď a nějaký prvek. Podle Lagrangeovy věty je $|a|=p^i$, a je vidět, že $|a^{p^{i-1}}|=p$. **126.** Např. $\mathbb{Z}$ a $\mathbb{Z}\times\mathbb{Z}$. **133.** 16, 37, 4, 16. **136.** Uvažujte komplexní kořeny polynomu x^n-1. Pro nekonečno uvažujte číslo $e^{2\pi ia}$ pro iracionální a. **138.** n. **139.** a) ne, b) ano. **140.** a) ne, b) ne. **141.** Každá podgrupa $\mathbb{Q}$ jistě obsahuje nějaké celé číslo. Vezmeme-li takové a z jedné a b z druhé, jejich NSN padne do obou podgrup. V $\mathbb{R}$ to nefunguje, např. uvažujte podgrupy $\mathbb{Z}$ a $\sqrt{2}\mathbb{Z}$. **142.** Ne. **143.** $7\mathbb{Z}$, $\mathbb{Z}$. **144.** $3\mathbb{Z}$, $\{3a/4 : a\in\mathbb{Z}\}$, $\{a/28 : a\in\mathbb{Z}\}$, $\{2a/15 : a\in\mathbb{Z}\}$. **145.** $\{\pm1,\pm i\}$, $\{1,-\frac{1}{2}\pm\frac{\sqrt{3}}{2}i\}$, $\{\pm2^n,\pm2^n i : n\in\mathbb{Z}\}$. **148.** Uvažujte grupu $\mathbb{Z}_n$ a počet prvků daného řádu v ní. Výsledek je n. **154.** Ano, ne, ne, ne, ano. **155.** Ne, ne, ano, ano, ano. **156.** Ano, ne, ano. **157.** Ne, ano. **158.** Endomorfismus pro vaechna n, prostý pro lichá, na je jen pro $n=\pm1$. **159.** Ano, jádro je $\{(x,y,z) : 2x+y=z\}$, obraz je $\{2^x3^y : x,y\in\mathbb{Z}\}$. **160.** a) $x\mapsto ax$ pro libovolné $a\in\mathbb{Z}$; b) $x\mapsto ax \mod n$ pro libovolné $a=0,\ldots\ldots 22\ldots,n-1$; c) $x\mapsto 0$. **161.** a) $x\mapsto ax \bmod 6$ pro $a=0,2,4$, b) $x\mapsto ax \bmod 15$ pro $a=0,5,10$, c) $x\mapsto ax \bmod n$, kde $a=k\cdot\frac{n}{\mathrm{NSD}(m,n)}$ pro $k=0,\ldots\ldots 22\ldots,\mathrm{NSD}(m,n)-1$. **163.** a) $x\mapsto kx$, $k\in\mathbb{Q}$, b) $x\mapsto kx$, $k\in\mathbb{R}$, c) vezměte nějakou bázi B vektorového prostoru $\mathbb{R}$ nad tělesem $\mathbb{Q}$, nějaké (vhodné) zobrazení $B\to B$ a rozšiřte jej do homomorfismu $\mathbb{R}\to\mathbb{R}$. **164.** Ano, $x\mapsto(x \bmod 2, x \bmod 3,\ldots\ldots 22\ldots)$. **165.** Grupa $\mathbb{C}_n$. **166.** $a+bi\mapsto(a,b)$, $re^{i\varphi}\mapsto(r,e^{i\varphi})$. **168.** Řádné dvě nejsou izomorfní — různé počty generátorů. **169.** Řádné dvě nejsou izomorfní: $\mathbb{Q}^*$ obsahuje prvek řádu 2, pro zbytek užijte invariant $\forall x\exists y\ y*y=x$. **170.** $exp:\mathbb{R}^+\to\mathbb{R}$, $x\mapsto e^x$ je izomorfismus. Naopak $\mathbb{R}^*$ s nimi izomorfní není, protože obsahuje prvek -1 řádu 2. **171.** Nechť $p_1<p_2<p_3<\ldots$ je seznam vaech prvočísel. Mějme $a\in\mathbb{Q}$. Pak existuje n takové, že $a=p_1^{k_1}\cdot\ldots\ldots 22\ldots\cdot p_n^{k_n}$, kde $k_i\in\mathbb{Z}$ jsou nějaké celé exponenty. Položme $\varphi(a)=\sum_i k_i x^i$. Není těžké dokázat, že φ je izomorfismus. **172.** Nechť a je nejmenší kladný prvek grupy $\mathbf{H}$. Není-li $\mathbf{H}$ jednoprvková, pak takový určitě existuje díky té podmínce na intervaly. Kdyby a negeneroval celou $\mathbf{H}$, podaří se vám nějak nalézt menší. **175.** Ano, jsou to právě podgrupy $\langle e^{2\pi i/n}\rangle$ pro každé n. **178.** Ne: např. $\mathbb{Z}_2\times\mathbb{Z}_2$ nebo $\mathbb{C}_{p^\infty}$. **184.** $\mathbb{Z}_4$, $\mathbb{Z}_2\times\mathbb{Z}_2$, ??, $\mathbb{Z}_4\times\mathbb{Z}_5$, $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3$, $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_5$. **186.** Nejmenší taková dvojice je 3,6. **188.** (1 4 7 5)(2 3), (1 7 4 2 5)(3 6). **189.** $\pi=(1\ 3\ 2)^{-1}\circ(2\ 4)(1\ 5)\circ(3\ 5\ 2)(1\ 4)^{-1}=(1\ 3\ 4\ 5)$. **190.** a) (1 3 2)(4 6 5), (1 4 2 5 3 6), (1 5 2 6 3 4), (1 6 2 4 3 5) b) (1 3 5 7 2 4 6), c) neexistuje. **191.** Jsou to právě ty permutace, které obsahují sudý počet cyklů sudé délky. **196.** $\pi^r=id$ pro r liché, $\pi^r=\pi$ pro r sudé. U σ záleží na zbytku po dělení aesti. **197.** Nejmenší společný násobek délek cyklů v π. **198.** (1 2 3 4 5)(6 7 8), ne, ne, (1 2 3)(4 5)(6 7)(8). **199.** a) 4, (1 2 3 4). b) 12, (1 2 3 4)(5 6 7). c) 30, (1 2 3 4 5)(6 7 8)(9 10). **200.** a) $\mathbf{D}_{12}$ obsahuje dva řádu 6, dva řádu 3, sedm řádu 2 a jeden řádu 1; b) $\mathbf{A}_4$ obsahuje 8 řádu 3, tři řádu 2 jeden řádu 1; c) $\mathbf{D}_{2n}$ obsahuje n transpozic a n-prvkovou cyklickou podgrupu, v níž je $\varphi(k)$ prvků řádu k pro každé $k\mid n$. **203.** $a=2$, $b=3$. **204.** $\pi=(1\ 3\ \ldots\ldots 22\ldots\ n-1)(2\ 4\ \ldots\ldots 22\ldots\ n)$ pro n sudé a $(1\ 3\ \ldots\ldots 22\ldots\ n\ 2\ 4\ \ldots\ldots 22\ldots n-1)$ pro n liché. Tedy je sudá. **205.** a) 1

b) $(-1)^{n(n+1)/2}$. **207.** Ne, levá strana je nutně sudá permutace, pravá strana je lichá. **210.** $(4\ 3\ 2\ 5\ 1)(7\ 6)$. **211.** $(8\ 2\ 1)(7\ 9\ 5\ 3)(4\ 6)$. **212.** Ano, např. $(3\ 4)$. Ne, nebo» ľádná permutace, která konjuguje ty dvě uvedené, není sudá. **213.** Ano, např. $(1\ 7\ 4\ 5\ 6\ 8\ 2) \in A_8$ řeaí obě otázky. **214.** $(1\ 3)(1\ 5)(1\ 2)(3\ 6)(3\ 7)$. **216.** Kaľdý cyklus lze nezávisle rozloľit jako $(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k)\ldots(a_1\ a_3)(a_1\ a_2)$. **217.** Plyne z faktu, ľe $(i\ j)(j\ k) = (i\ j\ k)$ a $(i\ j)(k\ l) = (k\ i\ l) \circ (i\ j\ k)$ (předpokládáme i, j, k, l navzájem různé prvky). **226.** Stačí nahlédnout, ľe n-cyklus generuje n-prvkovou podgrupu neobsahující ľádnou osovou symetrii. Z Lagrangeovy věty, má li podgrupa $2n$-prvkové grupy alespoň $n+1$ prvků, pak je rovna celé grupě. **228.** Ano, ne. **229.** a) ne, b) ano. **230.** Pro kontrolu: $\mathbf{S}_3$ jich má 6, $\mathbf{A}_4$ jich má 10, $\mathbf{D}_8$ jich má 10, $\mathbf{Q}$ jich má 6. **240.** Nejmenaí existuje na aesti prvcích a jsou dva. Jeden je prasátko bez noľiček a druhý trojúhelník s různě dlouhými rohy. **241.** a) Jednoprvková grupa. b) Obsahuje právě vaechny funkce $x \mapsto x + k$, $k \in \mathbb{Z}$. **242.** Grupa obsahuje právě restrikce striktně rostoucích spojitých reálných funkcí na mnoľinu $\mathbb{Q}$. **246.** a) $x \mapsto ax$ pro $a = \pm 1$, tedy $\simeq \mathbb{Z}_2$. b) $x \mapsto ax$ pro $a \in \mathbb{Q} \setminus \{0\}$, je $\simeq \mathbb{Q}^*$. c) Libovolné prohození nenulových prvků; tedy $\simeq \mathbf{S}_3$. d) ???. e) Jde o automorfismy indukované přejmenováním prvků mnoľiny $\{1, 2, 3\}$; přitom víc neľ aest automorfismů být nemůľe, nebo» celá $\mathbf{S}_3$ je generovaná dvojicí transpozic, které se mohou zobrazit jedině na transpozice; tedy $\mathbf{Aut}(\mathbf{S}_3) \simeq \mathbf{S}_3$. **247.** Automorfismy jsou právě $x \mapsto kx \bmod n$ pro $k \in \mathbb{Z}_n^*$. Přiřadíme-li tomuto zobrazení prvek k, dostaneme izomorfismus na $\mathbb{Z}_n^*$. **253.** Jen vnitřní, $\simeq \mathbf{S}_4$. **258.** Ano, ano, ne (mají determinant ± 1). **259.** Není, např. proto, ľe není abelovská. **263.** Ano. **265.** $a+bi \mapsto \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$. **266.** $a+bi+cj+dk \mapsto \left(\begin{smallmatrix} a+bi & c+di \\ -c+di & a-bi \end{smallmatrix}\right)$, $a+bi+cj+dk \mapsto \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & c & b & a \end{pmatrix}$. **275.** Jsou to právě podgrupy $\langle$ otočení o $2\pi/n\rangle$, $n \in \mathbb{N}$. **278.** V obou případech jen jedna orbita. **279.** V obou případech jen jedna orbita. **280.** Mnoľiny navzájem konjugovaných prvků. Pro $\mathbf{S}_4$ to jsou právě mnoľiny permutací daného typu (tj. celkem 5 orbit), pro $\mathbf{A}_4$ to jsou $\{id\}$, $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, $\{(1\ 2\ 3), (2\ 1\ 4), (3\ 4\ 1), (4\ 3\ 2)\}$, $\{(1\ 3\ 2), (2\ 4\ 1), (3\ 1\ 4), (4\ 2\ 3)\}$. **281.** Dvě orbity: $\{(0, \ldots, 0)\}$ a $T^n \setminus \{(0, \ldots, 0)\}$. **282.** a) 5!, b) 4!. **283.** a) 0, b) 1. **284.** 2. **285.** a) 0, b) 2 nebo 0, podle toho, zda prochází vrcholy nebo středy hran. **286.** 2. **287.** a) 1, b) 2, c) 4. **288.** a) 2, b) 4, c) 8. **289.** $[x] = X$, G_x obsahuje vaechna otočení se středem v x a osové symetrie s osou procházející x. **290.** X_g obsahuje a) střed otočení, b) nic, c) osu symetrie. **291.** Ano, $[x]$ je horizontální přímka procházející bodem x, $G_x = \{0\}$ a $X_n = \emptyset$. **292.** Ano, $[x]$ je kruľnice se středem $(0,0)$ procházející bodem x, $G_x = 360\mathbb{Z}$ pro $x \neq (0,0)$, resp. $G_{(0,0)} = \mathbb{R}$, a $X_n = \{(0,0)\}$ pro $n \notin 360\mathbb{Z}$, resp. $X_n = X$ v opačném případě. **293.** Pro n sudé $\frac{1}{4}(2^{n^2} + 2 \cdot 2^{\frac{n^2}{4}} + 2^{\frac{n^2}{2}})$. Pro n liché $\frac{1}{4}(2^{n^2} + 2 \cdot 2^{\frac{n^2+3}{4}} + 2^{\frac{n^2+1}{2}})$. **294.** Pro n sudé $\frac{1}{8}(2^{n^2} + 2 \cdot 2^{\frac{n^2}{4}} + 3 \cdot 2^{\frac{n^2}{2}} + 2 \cdot 2^{\frac{n(n+1)}{2}})$. Pro n liché $\frac{1}{8}(2^{n^2} + 2 \cdot 2^{\frac{n^2+3}{4}} + 2^{\frac{n^2+1}{2}} + 4 \cdot 2^{\frac{n(n+1)}{2}})$. **295.** a) 420, b) 228. **298.** a) $\frac{1}{3} \cdot \frac{16!}{8!8!}$. b) $\frac{1}{6} \cdot (\frac{16!}{8!8!} + 3 \cdot 150)$. **300.** a) 8. **303.** a) 10. b) $k^6 + 3k^4 + 12k^3 + 8k^2$ **305.** 30, resp. 2. **306.** $(k^4 + 11k^2)/12$. **307.** $(k^4 + 6k^3 + 11k^2 + 6k)/24$. **308.** 4, 11, dál nevím. **309.** 10, 3405. **310.** Ano, ano, ne. **311.** Rozkladové třídy $\mathbf{G}$ podle $\mathbf{H}$. **312.** Třídy konjugace. Jen pro jednoprvkovou grupu. **315.** Jsou-li jen dvě rozkladové třídy, pak jedna je $H = e * H = H * e$ a druhá tudíľ musí být $a * H = H * a$ pro nějaké a. **316.** $H = \{id, (1\ 2)\}$, $a = (1\ 2\ 3)$. **319.** Ano. **320.** Není uzavřena na kojugaci. **321.** Ano. **322.** Není uzavřená na násobení! **323.** a) Je to podgrupa $\mathbf{A}_5$, nebo» konjugováním získám vaechny trojcykly a ty generují $\mathbf{A}_5$. b) Je to celá $\mathbf{S}_5$. **324.** a) Je to podgrupa sestávající ze vaech otočení. b) Je to celá $\mathbf{D}_{10}$. **325.** $\{id\}$, $\mathbf{A}_3$, $\mathbf{S}_3$. **326.** $\{id\}$, Kleinova, $\mathbf{A}_4$, $\mathbf{S}_4$. **329.** a) Je jich aest: vaechny tři čtyřprvkové podgrupy jsou normální a jejich průnik, podgrupa generovaná středovou symetrií, je normální. (???) b) Pouze otočení tvoří vlastní normální podgrupu. c) Vaech aest podgrup je normálních. **332.** Ne. Pro $n = 2$ konjugujte matici $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ maticí $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, pro n obecné doplňte diagonálu jedničkami. **333.** Ne, ne. Pro $n = 2$ konjugujte matici $\left(\begin{smallmatrix} u & 0 \\ 0 & v \end{smallmatrix}\right)$, $u \neq v$, maticí $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, pro n obecné doplňte diagonálu jedničkami. **334.** Ne, ano. **335.** Ano. **336.** Ne. Pro $n = 2$ konjugujte matici $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ maticí $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, pro n obecné doplňte diagonálu jedničkami. **337.** Ne. Pro $n = 2$ konjugujte matici $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ maticí $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, pro n obecné doplňte diagonálu jedničkami. **339.** Podgrupu vaechny,

normální jen C. **340.** Ne, kvaternionová grupa je protipříklad. **341.** a) Musí, b) může ale nemusí. **343.** $\mathbb{R}^*$, homomorfismus $A \mapsto \det A$. **344.** $\mathbb{Z}_2 \simeq (\{\pm 1\}, \cdot, ^{-1}, 1)$, homomorfismus $x \mapsto \mathrm{sgn} x$. **345.** $\mathbb{R}^+$, homomorfismus $x \mapsto |x|$. **346.** Operace jsou $a \oplus b = a + b - [a + b]$ a $\ominus a = n - a$. Homomorfismus $a \mapsto a - [a]$. Pro racionální čísla uvažujeme jen racionální prvky toho intervalu. **347.** $\mathbb{R}$, homomorfismus $a + bi \mapsto b$. **348.** $\{z \in \mathbb{C} : |z| = 1\}$, homomorfismus $z \mapsto z/|z|$. **349.** $\mathbb{R}^+$, homomorfismus $z \mapsto |z|$. **350.** $\mathbb{C}^*$, homomorfismus $z \mapsto z^n$. **351.** $\mathbb{C}_{p^\infty}$. **357.** Homomorfismus funguje tak, že se matici přiřadí vektor z prvků, které leží na diagonále. **363.** Ne, $\times$ není asociativní. **364.** Ano. **365.** Ano. **366.** ??? Ano, ne. ??? **369.** Ano, ne. **370.** Ano, ne, ne. **371.** Ne, ne, ne, ano, ano. **374.** $7\mathbb{Z}$, $\mathbb{Z}$. **375.** $3\mathbb{Z}$, $\{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{N}\}$, $\{\frac{a}{2^n 7^m} : a \in \mathbb{Z}, m, n \in \mathbb{N}\}$, $\{\frac{2a}{3^n 5^m} : a \in \mathbb{Z}, m, n \in \mathbb{N}\}$. **377.** $\mathbb{Z}$, $\{2a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Z}\}$. **378.** $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Z}\}$, $\{a+b2^{\frac{1}{3}}+c2^{\frac{2}{3}}+di+ei2^{\frac{1}{3}}+fi2^{\frac{2}{3}} : a, b, c, d, e, f \in \mathbb{Z}\}$. **379.** $\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$. **380.** $\{\sum_{i=0}^n a_i x^i : a_0 = a_1 = 0\}$, $\{\sum_{i=0}^n a_i x^i : 2 \mid a_0\}$, $\{\sum_{i=0}^n a_i x^i : 2 \mid a_0, a_i = 0 \text{ pro } i \text{ liché }\}$. **381.** $\{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) : a, b \in \mathbb{Z}, a+b \text{ sudé}\}$, $\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) : a, b \in \mathbb{Z}\}$, $\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) : a, b \in \mathbb{Z}\}$. **382.** $\{0\}$ a $a\mathbb{Z}$, $a \in \mathbb{N}$; jen nevlastní; nevlastní a $\{0, 2, 4, 6\}$, $\{0, 4\}$; nevlastní a $\{0, 2, 4, 6, 8, 10\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$; $\{0\}$ a $a\mathbb{Z}_n$, $a \mid n$; nevlastní a $\mathbb{Z}_3 \times \{0\}$, $\{0\} \times \mathbb{Z}_3$. **383.** Ne. **384.** $a\mathbb{Z}$, $a \in \mathbb{N} \cup \{0\}$; jen nevlastní; nevlastní a $\{0, 2, 4, 6\}$, $\{0, 4\}$; nevlastní a $\{0, 2, 4, 6, 8, 10\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$; $\{0\}$ a $a\mathbb{Z}_n$, $a \mid n$; nevlastní a $\mathbb{Z}_3 \times \{0\}$, $\{0\} \times \mathbb{Z}_3$. **385.** $7\mathbb{Z}$, $\mathbb{Z}$. **386.** $\mathbb{Q}$. **387.** $\{\sum_{i=0}^n a_i x^i : a_0 = a_1 = 0\}$, $\{\sum_{i=0}^n a_i x^i : 2 \mid a_0\}$, $\{\sum_{i=0}^n a_i x^i : 2 \mid a_0, a_1\}$. **388.** Ano, je to $(x - 1)\mathbb{Z}[x]$. **389.** Ano, je to $(x^2 + 1)(x - 1)\mathbb{Z}[x]$. **390.** a) Ideál ano, hlavní ne, protože prvky 3 a x v něm jsou, ale jejich jediný společný dělitel nikoliv. b) Ano, je to $\mathbb{Q}[x]$. **391.** $(x^3 - 1)(x^2 + 3)$, 1. **392.** $x^4 - 1$, $x - 1$. **393.** $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(i)$, $\mathbb{C}$. **394.** Obraz je $\mathbf{R}$, jádro je $(x - a)\mathbf{R}[x]$. **395.** Obraz je $\mathbb{C}$, jádro je $(x^2 + 1)\mathbb{Z}[x]$. **396.** Obraz je $\mathbb{R}$, jádro je $(x^2 - 2)\mathbb{Z}[x]$. **397.** $u^2 \equiv s \pmod n$. **398.** Ne. **401.** Označme $X = \{x_1, \ldots, x_n\}$. Hledaný izomorfismus je $A \mapsto (a_1, \ldots, a_n)$, kde $a_i = 1$ právě tehdy, když $x_i \in A$. **403.** Není-li s druhou mocninou přirozeného čísla, pak je $a + b\sqrt{s} \mapsto \left(\begin{smallmatrix} a & b\sqrt{s} \\ b\sqrt{s} & a \end{smallmatrix}\right)$ izomorfismus (pro $s = 0$ to funguje taky). V opačném případě je $\mathbb{Z}[\sqrt{s}] = \mathbb{Z}$ a okruhy izomorfní nejsou. **404.** $\mathbb{Z}[x] \to \mathbb{Z}[\pi]$, $p \mapsto p(\pi)$ je izomorfismus. Prostost plyne z toho, že π je transcendentní. **405.** Žádné dva. **406.** Např. ideály $\mathbf{R}[x]$, $\mathbf{R}[x^2]$, $\mathbf{R}[x^3]$, atd. **408.** Matici odpovídá lineární zobrazení (endomorfismus) s touto maticí vzhledem k nějaké předem pevně zvolené bázi (např. kanonické). **414.** Ve vaech případech jen identita a konstantní zobrazení na 0. Automorfismus je tedy jen identita. **415.** $x \mapsto ax \bmod n$ pro $a = 0, \ldots, n - 1$ splňující $a^2 \equiv a \pmod n$. Automorfismus je tedy jen identita. **416.** Hledaný homomorfismus je $f \mapsto f \bmod 3$. **417.** Hledaný homomorfismus je $f \mapsto f(0) \bmod 3$. **418.** Hledaný homomorfismus je $f \mapsto f(a)$. **419.** Hledané homomorfismy jsou $f \mapsto f(i)$, $f \mapsto f(i)$, $f \mapsto (f(i), f(-i))$. **420.** Hledané homomorfismy jsou $f \mapsto (f(1), f(-1))$. **421.** $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{R} \times \mathbb{R}$. **422.** Je to $\mathbb{Q}[i] \times \mathbb{Q}[\sqrt{2}i]$, $\mathbb{R} \times \mathbb{R} \times \mathbb{C}$, $\mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$. **423.** Je to $\mathbb{Q}[\sqrt[3]{2}]$, hledaný homomorfismus je $f \mapsto f(\sqrt[3]{2})$. **424.** a) $\mathbb{C} \times \mathbb{C}$, b) $\mathbb{R} \times \mathbb{R}$ pro f rozložitelný a $\mathbb{C}$ pro f ireducibilní. c) $\mathbb{Q} \times \mathbb{Q}$ pro f rozložitelný a $\mathbb{Q}[\sqrt{r}]$ pro různá $r \in \mathbb{Z}$ pro f ireducibilní. **425.** a) $\mathbb{C} \times \mathbb{C} \times \mathbb{C}$, b) $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ a $\mathbb{C} \times \mathbb{R}$. **430.** Hledaný homomorfismus je $f \mapsto f(x, 0)$. **431.** Je to $\mathbf{R}[x]$, homomorfismus je $f \mapsto f(x, -x)$. **432.** Vezměte nějakou bijekci $\varphi : X \to X \setminus \{x\}$ a uvažujte homomorfismus, který vezme polynom f a za proměnnou x dosadí 0 a za každou proměnnou $y \neq x$ dosadí $\varphi(y)$. **434.** Hledaný homomorfismus je $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mapsto c$. **435.** Hledaný homomorfismus je $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mapsto (a, c)$. **441.** $\mathbf{K} \mapsto \{a : [a] \in K\}$. **442.** $x+2$, x^2+1, x^3-2, x^2-2x-4, $x^2 - x + 1$. **443.** $x^2 - 3$, $x^2 - \sqrt{2}$. **445.** Je-li $m_{a,\mathbf{T}} = \sum_{i=0}^n a_i x^i$, pak $m_{a^{-1},\mathbf{T}} = \sum_{i=0}^n a_{n-i} x^i$. **446.** 2, 6, 4. **447.** $p-1$, protože polynom $x^p - 1$ není ireducibilní! **448.** 4. **450.** n, protože polynom $x^n - p$ je podle Eisensteinova kritéria ireducibilní. **452.** Ne, viz Cardanův vzorec pro kořeny polynomu třetího stupně. **453.** Ano: jsou obsaženy v rozaíření konečného stupně $\mathbb{Q}(...)$, kde přidáváme vaechny uvedené odmocniny. **456.** Platí $\sqrt{pq} \in \mathbb{Q}[\sqrt{p}, \sqrt{q}]$. Z teorie plyne, že stupeň tohoto rozaíření je 2 nebo 4. První případ vyloučíme tím, že dokážeme (elementárním způsobem), že lineárně nezávislé jsou $1, \sqrt{p}, \sqrt{q}$. Tedy stupeň je 4 a lineárně nezávislé musí být vaechny čtyři uvedené prvky. **457.** Určitě $a^2 \in T(a)$. Je $a \in T(a^2)$? Kdyby ne, tak

$[\mathbf{T}(a) : \mathbf{T}(a^2)] = 2$, takže $[\mathbf{T}(a) : \mathbf{T}]$ je sudé, spor. **468.** Stupeň transendentního rozaíření je nekonečný. **469.** Stupeň takového rozaíření není mocnina dvojky. Zdvojení krychle vede na $\sqrt[3]{2}$. **475.** 3,4,5,6,8,10,12,15,16. **480.** $\mathbb{Q}$. $\mathbb{Q}(i)$. $\mathbb{Q}(\sqrt{2})$. **481.** $\mathbb{Q}, \mathbb{Q}(e^{2\pi i/3})$. $\mathbb{Q}, \mathbb{Q}(e^{2\pi i/6})$. $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}e^{2\pi i/6})$. **483.** $\mathbb{Q}, \mathbb{Q}(i)$. $\mathbb{Q}(e^{2\pi i/8})$. **485.** $\mathbb{Q}(e^{2\pi i/n})$, $\mathbb{Q}(e^{\pi i/n})$. **486.** Kořenové: $\mathbb{Q}$ a $\mathbb{Q}(\sqrt{3}i)$. Rozkladové: $\mathbb{Q}(\sqrt{3}i)$. **487.** Kořenové: $\mathbb{Q}(\sqrt{2})$ a $\mathbb{Q}(\sqrt{3})$. Rozkladové: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. **489.** 5^3, 3^2, 3^2, ???. **490.** Např. pro $f = x^n - 1$ je stupeň $\geq n - 1$. **493.** Právě tehdy, když je $\frac{r}{s}$ druhá mocnina racionálního čísla.