PŘÍKLADY Z ALGEBRY

DAVID STANOVSKÝ
stanovsk@karlin.mff.cuni.cz

Motto:
Není jiné rozumné výchovy než příkladem; když to nejde jinak, tak aspoň odstrašujícím.
Albert Einstein

Toto je pracovní verze sbírky příkladů k základní přednášce z obecné algebry. Sbírka pokrývá základní témata, která se vyskytují ve všech variantách kurzu: základy strukturní teorie grup a okruhů, dělitelnost v obecných oborech integrity, úvod do teorie těles. Dále jsou zařazeny různé doplňující partie: především jde o první kapitolu věnovanou obecným algebrám (hlavně pologrupám) a uspořádaným množinám, a dále různé aplikace (teorie čísel, Burnsideova věta, konstrukce pravítkem a kružítkem atd.).

Jednotlivé kapitoly jsou na sobě nezávislé, lze je cvičit v libovolném pořadí. Některé sekce v rámci jednotlivých kapitol na sebe navazují. Pořadí úloh není ideální, například úlohy uvedené v sekcích „Příklady a základní vlastnosti“ je lepší řešit až po procvičení pojmů na konkrétních příkladech. V dalších verzích sbírky to snad napravím.

Každá sekce shrnuje teoretické poznatky z obecné algebry používané ve cvičeních. Většina úloh je víceméně elementárních, nicméně některé typy úloh (lineární grupy, maticové okruhy, rozšíření těles atd.) vyžadují znalosti z lineírní algebry na úrovni prvního ročníku.

Hvězdičky označují vyšší obtížnost úlohy. Jednohvězdičková cvičení zpravidla vyžadují nějaký nápad nebo větší množství výpočtů, dobrý student by je však měl v dostatečném čase zvládnout. Dvojhvězdičkové úlohy pak mohou být pro dobré studenty výzvou k otestování svých znalostí. Použití návodu zpravidla úlohu o hvězdičku zjednoduší.

Heslo `[Ř]` značí, že k úloze je na konci sbírky uvedeno řešení. Heslo `[N]` značí, že k úloze je na konci sbírky uveden návod. Heslo `[?]` značí, že jsem úlohu ještě neřešil, a tudíž je možná vadná.

Opakuji, že se jedná o pracovní verzi a řada sekcí není v ideálním stavu. Text s největší pravděpodobností obsahuje chyby, nepřesnosti, neřešitelné úlohy, nefungující návody a špatná řešení :-) Jakékoliv opravy, návody, řešení i zajímavá zadání úloh velice uvítám na uvedeném emailu.

Date: 4. ledna 2018.

Obsah

I. Uspořádání

Relaci $\leq$ na množině X nazýváme *částečné uspořádání*, pokud je

(1) *reflexivní*, tj. $x \leq x$ pro všechna x,
(2) *tranzitivní*, tj. $x \leq y$ a $y \leq z$ implikuje $x \leq z$,
(3) a *antisymetrická*, tj. $x \leq y$ a $y \leq x$ implikuje $x = y$.

Alternativně říkáme, že $(X, \leq)$ je *uspořádaná množina*. Uspořádání se nazývá *lineární*, pokud navíc pro každé x, y nastane $x \leq y$ nebo $y \leq x$. Pokud $x \leq y$ a $x \neq y$, píšeme $x < y$.

Řekneme, že prvek $a \in X$ je v $(X, \leq)$

- *největší*, pokud pro každé $b \in X$ platí $b \leq a$;
- *nejmenší*, pokud pro každé $b \in X$ platí $b \geq a$;
- *maximální*, pokud neexistuje žádné $b \in X$ takové, že $b > a$;
- *minimální*, pokud neexistuje žádné $b \in X$ takové, že $b < a$.

Nechť $Y \subseteq X$. Řekneme, že prvek $a \in X$ je

- *horní mez* množiny Y, pokud $a \geq y$ pro každý prvek $y \in Y$;
- *supremum* množiny Y, pokud to je nejmenší horní mez Y; značí se $a = \sup Y$.
- *dolní mez* množiny Y, pokud $a \leq y$ pro každý prvek $y \in Y$;
- *infimum* množiny Y, pokud to je největší dolní mez Y; značí se $a = \inf Y$.

Jinými slovy, supremum množiny Y je nejmenší prvek množiny X, který je větší než všechny prvky Y. Podobně, infimum množiny Y je největší prvek množiny X, který je menší než všechny prvky Y.

Uspořádaná množina se nazývá *svazově uspořádaná*, pokud v ní existují suprema a infima všech *dvouprvkových* podmnožin (pak také zřejmě existují suprema a infima všech *neprázdných konečných* podmnožin). Nazývá se *úplně svazově uspořádaná*, pokud v ní existují suprema a infima všech podmnožin. Často se používá značení

$$a \vee b = \sup\{a, b\} \quad \text{a} \quad a \wedge b = \inf\{a, b\}.$$

Příklad.
- Lineární uspořádání jsou svazová, $a \vee b = \max(a, b)$, $a \wedge b = \min(a, b)$.
- $(\mathbb{R}, \leq)$ je svazově uspořádaná, ale ne úplně, protože $\inf \mathbb{R}$ neexistuje.
- $(\mathbb{R} \cup \{\pm\infty\}, \leq)$ je úplné svazové uspořádání.

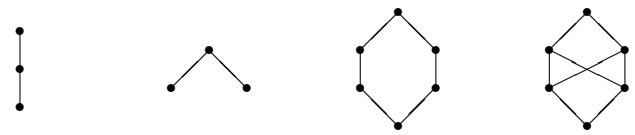
Malou uspořádanou množinu $(X, \leq)$ je možné zakreslit pomocí tzv. *Hasseova diagramu*. Jde o graf, jehož vrcholy tvoří množina X, přičemž porovnatelné prvky jsou nakreslené tak, že menší je níže, a hrana mezi dvěma vrcholy a, b je nakreslena právě tehdy, když $a < b$ a neexistuje žádné c splňující $a < c < b$.

1. Zjistěte, zda existuje a jaký nejmenší počet prvků může mít uspořádaná množina taková, že

(a) má alespoň dva maximální a alespoň jeden minimální prvek;
(b) má alespoň dva maximální a alespoň jeden nejmenší prvek;
(c) má alespoň dva největší, ale žádný nejmenší prvek;
(d) má alespoň jeden maximální, ale žádný nejmenší prvek;
(e) má alespoň jeden maximální, ale žádný minimální prvek;
(f) má právě jeden maximální, ale žádný největší prvek;
(g) každá podmnožina supremum, ale nejaká podmnožina nemá infimum;
(h) jako (f), ale navíc je svazově uspořádaná;
(k) každá její podmnožina má dolní i horní mez, ale přitom není svazově uspořádaná.

Uveďte příklady! [Ř]

2. Rozhodněte, zda jsou následující uspořádané množiny svazově uspořádané. [Ř]



3. Najděte nějaké lineární uspořádání na množině $\mathbb{N} \times \mathbb{N}$ a na množině $\mathbb{C}$.

Lemma. *Následující podmínky jsou ekvivalentní pro uspořádanou množinu* $(X, \leq)$.

(1) $(X, \leq)$ *je úplně svazově uspořádaná.*
(2) $V\,(X, \leq)$ *existují infima všech množin a obsahuje největší prvek.*
(3) $V\,(X, \leq)$ *existují suprema všech množin a obsahuje nejmenší prvek.*

4. * Dokažte předešlé lemma. [Ř]

5. Buď X neprázdná množina a označme $P(X)$ množinu všech podmnožin množiny X. Dokažte, že je $\mathbf{P}(X) = (P(X), \subseteq)$ úplně svazově uspořádaná množina. [N]

6. Buď X neprázdná množina a označme $Eq(X)$ množinu všech ekvivalencí na množině X. Dokažte, že je $\mathbf{Eq}(X) = (Eq(X), \subseteq)$ úplně svazově uspořádaná množina. [N]

7. Nakreslete Hasseův diagram svazů $\mathbf{P}(\{0, 1, 2\})$ a $\mathbf{Eq}(\{0, 1, 2\})$.

8. Označme $P_{fin}(\mathbb{N})$ množinu všech *konečných* podmnožin množiny $\mathbb{N}$. Rozhodněte, zda je uspořádaná množina $(P_{fin}(\mathbb{N}), \subseteq)$ a) svazově, b) úplně svazově uspořádaná. [Ř]

9. Rozhodněte, zda jsou uspořádané množiny $(\mathbb{N}, |)$ a $(\mathbb{N} \cup \{0\}, |)$ a) svazově, b) úplně svazově uspořádané. Relací $|$ rozumíme relaci dělitelnosti (tj. a „je menší než“ b, pokud a dělí b); uvědomte si, že 0 je dělitelná jakýmkoliv přirozeným číslem. Co jsou sup a inf, pokud existují? [Ř]

10. Označme F množinu všech funkcí $\mathbb{R} \to \mathbb{R}$. Pro $f, g \in F$ definujme $f \leq g$, pokud $f(x) \leq g(x)$ pro všechna $x \in \mathbb{R}$. Je uspořádaná množina $(F, \leq)$ a) svazově, b) úplně svazově uspořádaná? Jaká by byla odpověď, kdybychom uvažovali funkce $\langle 0, 1\rangle \to \langle 0, 1\rangle$? [Ř]

11. Definujme uspořádání na množině $\mathbb{R} \times \mathbb{R}$ předpisem $(a_1, a_2) \leq (b_1, b_2)$, pokud $a_0 = b_0$ a $a_1 \leq b_1$. Je $(\mathbb{R} \times \mathbb{R}, \leq)$ uspořádaná množina? Pro které dvojice párů existuje supremum a infimum? [Ř]

II. Dělitelnost v oborech integrity

1. Elementární teorie čísel

Matematická indukce je technika pro dokazování vlastností přirozených čísel. Dokážeme-li, že

(1) číslo 1 má vlastnost V,
(2) pro každé n, má-li číslo n vlastnost V, pak má tuto vlastnost i číslo $n+1$,

pak můžeme dedukovat, že každé přirozené číslo n má vlastnst V.

12. Dokažte, že $7 \mid n^7 - n$.

13. Dokažte, že $9 \mid 4^n + 6n - 1$.

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

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

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

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

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

Věta (Bézoutova rovnost). *Pro každou dvojici přirozených čísel a, b existují celá čísla u, v splňující*

$$\mathrm{NSD}(a, b) = u \cdot a + v \cdot b.$$

NSD i koeficienty u, v lze najít Eukleidovým algoritmem popsaným v následující sekci.

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

Zavedeme značení

$$a \equiv b \pmod{m}$$

(čteme *a je kongruentní s b modulo m*), pokud $m \mid a - b$, tj. pokud a a b dávají stejný zbytek po dělení m. Relace „býti kongruentní modulo m“ je ekvivalencí, znaménko kongruence je tedy možno používat podobně jako rovnítko. Je-li $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, pak

- $a \pm c \equiv b \pm d \pmod{m}$;
- $a \cdot c \equiv b \cdot d \pmod{m}$;
- $a^k \equiv b^k \pmod{m}$ pro libovolné $k \in \mathbb{N}$.

Pro krácení lze použít vlastnosti

- $a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{cm}$;
- jsou-li c, m nesoudělná, pak $a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{m}$.

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

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

22. 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]

Věta (Čínská věta o zbytcích). *Nechť $m_1, \ldots, m_n$ jsou po dvou nesoudělná přirozená čísla, označme $M = m_1 \cdot \ldots \cdot m_n$. Pak pro libovolná celá čísla $a_1, \ldots, a_n$ existuje právě jedno $x \in \{0, \ldots, M-1\}$, které řeší soustavu kongruencí*

$$x \equiv a_1 \pmod{m_1}, \quad \ldots, \quad x \equiv a_n \pmod{m_n}.$$

První dvě úlohy se údajně vyskytují v některé ze staročínských a staroindických matematických knih.

23. 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]

24. 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]

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

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

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

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

29. * 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 $d \mid b$.

Zavedeme *Eulerovu funkci* předpisem

$$\varphi(n) = \text{ počet prvků v intervalu } 1, \ldots, n-1 \text{ nesoudělných s } n.$$

Je-li $n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ prvočíselný rozklad čísla n, platí

$$\varphi(n) = p_1^{k_1-1} p_2^{k_2-1} \cdot \ldots \cdot p_m^{k_m-1}(p_1-1)(p_2-1) \cdot \ldots \cdot (p_m-1).$$

30. Najděte všechna čísla n taková, že $\varphi(n) = 18$.

31. * Najděte všechna čísla n taková, že $\varphi(n) \mid n$.

32. * Sečtěte $\sum_{k|n} \varphi(k)$.

Věta (Eulerova). *Jsou-li a, n nesoudělná, pak $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Věta (malá Fermatova). *Je-li p prvočíslo a $p \nmid a$, pak $a^{p-1} \equiv 1 \pmod{p}$.*

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

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

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

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

37. Spočtěte $2^{\ell} \bmod 13$, kde ℓ je současný letopočet.

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

39. Spočtěte $3^{3^{3^{3^3}}} \bmod 28$. [Ř]

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

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

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

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

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

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

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

47. ** 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.) [?]

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

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

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

[Wilsonovo kritérium] [N]

2. Základní vlastnosti oborů integrity

Oborem integrity rozumíme komutativní okruh s jednotkou, ve kterém pro každé $a, b \neq 0$ platí $a \cdot b \neq 0$. (Tj. neexistují vlastní dělitelé nuly.)

50. Dokažte, že tělesa jsou obory integrity. [Ř]

51. Dokažte, že je-li $\mathbf{R}$ obor integrity, pak a) $\mathbf{R}[x]$, b) * $\mathbf{R}[[x]]$ také obor integrity. [N]

52. Pro která n jsou $\mathbb{Z}_n$ obory integrity? [Ř]

53. a) Zjistěte, zda je okruh $\mathbb{Z} \times \mathbb{Z}$ oborem integrity. b) Nechť $\mathbf{R}_1, \ldots, \mathbf{R}_n$ jsou okruhy. Za jakých podmínek je direktní součin $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ oborem integrity? [Ř]

54. Dokažte, že v oborech integrity lze krátit, tj. pokud $ab = ac$ pro nějaké $a \neq 0$, pak $b = c$. [Ř]

55. Dokažte, že konečné obory integrity jsou tělesa. [N]

Řekneme, že a *dělí* b v oboru $\mathbf{R}$ (píšeme $a \mid b$), pokud existuje $c \in R$ takové, že $b = ac$. Alternativně, pokud $bR \subseteq aR$. Řekneme, že prvky a a b jsou *asociované* (píšeme $a \parallel b$), pokud $a \mid b$ a $b \mid a$. Alternativně, pokud $aR = bR$. Prvek a se nazývá *invertibilní*, pokud $a \parallel 1$. Množina invertibilních prvků tvoří grupu s operací násobení, značí se $\mathbf{R}^*$.

Není těžké nahlédnout, že dva prvky a, b jsou asociované právě tehdy, když existuje invertibilní prvek q takový, že $a = bq$.

Příklad.

- v tělesech je každý nenulový prvek invertibilní; tedy $a \parallel b$ pro každé $a, b \neq 0$;
- v okruhu $\mathbb{Z}$ jsou invertibilní pouze prvky ± 1; tedy $a \parallel b \Leftrightarrow a = \pm b$;
- v okruhu $\mathbb{Z}[i]$ jsou invertibilní pouze prvky ± 1 a $\pm i$.
- v okruhu $\mathbf{R}[x]$ jsou invertibilní právě polynomy stupně 0, jejichž člen je invertibilní v $\mathbf{R}$; tj. $\mathbf{R}[x]^* = \mathbf{R}^*$.

56. Rozhodněte, zda je prvek $x + 1$ invertibilní v oboru $\mathbb{Z}[[x]]$. [Ř]

57. * Buď $\mathbf{T}$ těleso. Dokažte, že mocninná řada $\sum a_i x^i$ je v $\mathbf{T}[[x]]$ invertibilní právě tehdy, když $a_0 \neq 0$.

Řekneme, že $c = \mathrm{NSD}(a, b)$ (*největší společný dělitel*), pokud $c \mid a$, $c \mid b$ a pro každé d s vlastností $d \mid a$, $d \mid b$ platí $d \mid c$. Řekneme, že $c = \mathrm{NSN}(a, b)$ (*nejmenší společný násobek*), pokud $c \cdot \mathrm{NSD}(a, b) = a \cdot b$. NSD a NSN nemusí existovat. Pokud existují, jsou určeny jednoznačně až na asociovanost.

Neinvertibilní prvek a se nazývá

- *ireducibilní*, pokud $a = bc$ implikuje $b \parallel 1$ nebo $c \parallel 1$;
- *prvočinitel*, pokud $a \mid bc$ implikuje $a \mid b$ nebo $a \mid c$.

Prvočinitelé jsou ireducibilní, opak nemusí být pravdou.

Příklad.

- v tělesech žádné ireducibilní prvky nejsou;
- v oboru $\mathbb{Z}$ jsou ireducibilní právě prvky $\pm p$, p prvočíslo;
- v oboru $\mathbb{C}[x]$ jsou ireducibilní právě polynomy stupně 1;
- v oboru $\mathbb{R}[x]$ jsou ireducibilní právě polynomy stupně 1 a ty polynomy stupně 2, které nemají reálný kořen;
- v oboru $\mathbb{Z}[x]$, resp. $\mathbb{Q}[x]$, existují ireducibilní polynomy libovolně vysokého stupně, např. polynomy $\frac{x^p-1}{x-1}$ pro libovolné prvočíslo p.
- v oborech $\mathbb{Z}_p[x]$ (p prvočíslo) existují ireducibilní polynomy libovolně vysokého stupně.
- v oboru $\mathbb{Z}[\sqrt{5}]$ je prvek 2 ireducibilní, ale není to prvočinitel.

[K procvičení NSD, NSN a ireducibility využijte úloh v následujících dvou sekcích.]

58. * Spočtěte $\mathrm{NSD}(\sum_{i=0}^{\infty}(-1)^i i^2(i-1)x^i, \sum_{i=0}^{\infty} 3\sin^2(\pi i/4)2^{i+1}x^i)$ a) v oboru $\mathbb{Q}[[x]]$, b) v oboru $\mathbb{Z}[[x]]$. [Ř]

Obor integrity se nazývá *Gaussovský*, pokud každý nenulový neinvertibilní prvek lze jednoznačně rozložit na součin ireducibilních prvků. To je právě tehdy když existují NSD všech dvojic prvků a neexistuje nekonečná posloupnost vlastních dělitelů. V Gaussovských oborech jsou všechny ireducibilní prvky jsou prvočinitelé.

Obor, v němž je každý ideál hlavní, nazýváme *oborem integrity hlavních ideálů* (zkráceně *OIHI*).

Obor integrity se nazývá *Eukleidovský*, pokud na něm existuje *Eukleidovská norma*, tj. zobrazení $\nu : R \to \mathbb{N} \cup \{0\}$ splňující

(0) $\nu(0) = 0$;
(1) pokud $a \mid b \neq 0$, pak $\nu(a) \leq \nu(b)$;
(2) pro každé $a, b \neq 0$ existuje q, r takové, že $a = bq + r$ a $\nu(r) < \nu(b)$.

(Neformálně řečeno, v Eukleidovských oborech existuje dělení se zbytkem, ovšem podíl a zbytek nemusejí být jednoznačně určené.)

Pro komutativní okruhy s jednotkou platí

$$\textit{Eukleidovský obor} \Longrightarrow \textit{OIHI} \Longrightarrow \textit{Gaussův obor} \Longrightarrow \textit{obor integrity.}$$

V Gaussovských oborech existují NSD, v OIHI pro ně platí Bézoutova rovnost a v Eukleidovských oborech můžeme NSD i Bézoutovy koeficienty počítat pomocí *Eukleidova algoritmu*:

- `VSTUP:` $a, b \in R$, $\nu(a) \geq \nu(b)$.
- `VÝSTUP:` $\mathrm{NSD}(a, b)$ a $u, v \in R$ splňující $\mathrm{NSD}(a, b) = ua + vb$.
- $a_0 = a$, $u_0 = 1$, $v_0 = 0$.
  $a_1 = b$, $u_1 = 0$, $v_1 = 1$.
  $a_{i+1} = r$, $u_{i+1} = u_{i-1} - u_i q$, $v_{i+1} = v_{i-1} - v_i q$, kde q, r zvolíme tak, že
  $$a_{i-1} = a_i q + r \quad \text{a} \quad \nu(r) \leq \nu(a_i).$$
  Pokud $a_{i+1} = 0$, odpověz a_i, u_i, v_i.

(*Bézoutova rovnost* říká pro každé $a, b \in R$ existují $u, v \in R$ (Bézoutovy koeficienty) splňující $\mathrm{NSD}(a, b) = u \cdot a + v \cdot b$.)

Příklad.

(1) *Eukleidovské obory:*
- libovolné těleso, s Eukleidovskou normou $\nu(0) = 0$ a $\nu(a) = 1$ pro každé $a \neq 0$;
- $\mathbf{T}[x]$ pro libovolné těleso $\mathbf{T}$, s Eukleidovskou normou $\nu(p) = 1 + \deg(p)$;
- $\mathbb{Z}$, s Eukleidovskou normou $\nu(a) = |a|$;
- $\mathbb{Z}[i]$ a některé další obory $\mathbb{Z}[\sqrt{s}]$ jsou Eukleidovské, např. pro $s = -1, \pm 2, 3$ (rozumí se $\sqrt{-1} = i$), s normou $\nu(a + b\sqrt{s}) = |a^2 - sb^2|$.

(2) *OIHI:*
- $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ je OIHI, ale není Eukleidovský.

(3) *Gaussovské obory:*
- (Gaussova věta) je-li $\mathbf{R}$ Gaussovský obor, pak $\mathbf{R}[x_1, \ldots, x_k]$ je také Gaussovský obor;
- $\mathbb{Z}[x]$ je Gaussovský obor a není OIHI;
- $\mathbf{R}[x_1, \ldots, x_k]$ není OIHI kdykoliv $k \geq 2$.

(4) *Obory integrity:*
- Je-li $\mathbf{R}$ obor integrity, pak $\mathbf{R}[x_1, \ldots, x_k]$ i $\mathbf{R}[[x_1, \ldots, x_k]]$ jsou také obory integrity;
- libovolný podokruh (s jednotkou) tělesa $\mathbb{C}$ je obor integrity;
- např. $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[i\sqrt{3}]$ jsou obory integrity, ale ne Gaussovské.

59. * Buď $\mathbf{T}$ těleso. Rozhodněte, zda je $\mathbf{T}[[x]]$ Gaussovský obor. Je Eukleidovský? [N] [Ř]

60. ** Najděte obor integrity, v kterém existují NSD všech prvků, ale přesto není Gaussovský. [N]

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

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

63. Buď $\mathbf{T}$ těleso. Dokažte, že $\mathbf{T}[x]$ je Eukleidovský obor.

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

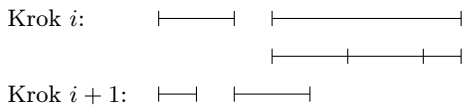
65. Buď $\mathbf{R}$ obor integrity a $\nu : R \to \mathbb{N} \cup \{0\}$ zobrazení splňující

(1) $\nu(a) = 0$ právě tehdy, když $a = 0$;
(2) pro každé $a, b \in R$, pokud $\nu(a) \leq \nu(b)$, pak buď $a \mid b$, nebo existují $u, v \in R$ taková, že $0 < \nu(au + bv) < \nu(a)$.

Dokažte, že $\mathbf{R}$ je OIHI.

66. ** Dokažte, že $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ je OIHI. Použijte předchozí cvičení. (Tento obor není eukleidovský, ale dokázat to je poměrně složité.)

Poznamenejme, že sám Eukleides uvažoval problém nalezení NSD v geometrické formě, jako následující úlohu: Jsou dány dvě úsečky. Najděte nejhrubší společnou „měrnou jednotku“ těchto úseček. Například, jsou-li dány úsečky délek 6 a 14, největší jednotkou je 2. Eukleidův algoritmus lze provést geometricky, bez jakéhokoliv použití čísel: kratší úsečku naneseme do delší tolikrát, kolikrát se tam vejde a v dalším kroku uvažujeme kratší úsečku a to co tam zbylo.



67. Nechť jsou dány dvě úsečky. Dokažte, že se Eukleidův algoritmus pro tyto úsečky zastaví právě tehdy, když je poměr jejich délek racionální. V tom případě je výsledkem jejich nejdelší společná „měrná jednotka“.

3. Obory polynomů

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

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

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

71. * 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]

72. * 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]

Prvek a se nazývá *kořen* polynomu f, pokud $f(a) = 0$. Ekvivalentně, pokud $x - a \mid f$.

73. 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]

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

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

76. [VOID]

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

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

79. * 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]

Na zjišťování existence racionálního kořene celočíselného polynomu lze použít následující jednoduché kritérium.

Tvrzení. *Nechť $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$, $a_n \neq 0$. Má-li polynom f racionální kořen $\frac{r}{s}$ (kde r, s jsou nesoudělná celá čísla), pak $r \mid a_0$ a $s \mid a_n$.*

80. Dokažte kritérium existence racionálního kořene. [N]

81. 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]

V oboru polynomů nad tělesem

(1) polynomy stupně nula jsou invertibilní;
(2) polynomy stupně 1 jsou vždy ireducibilní;
(3) polynom stupně 2 nebo 3 je ireducibilní právě tehdy, když nemá kořen;
(4) mohou existovat ireducibilní polynomy stupně 4 a více, které nemají kořen.

Polynom $f = \sum a_i x^i$ nazýváme *primitivní*, pokud $\mathrm{NSD}(a_0, \ldots, a_n) = 1$. Je-li $f \in \mathbb{Z}[x]$ primitivní, pak je ireducibilní v $\mathbb{Z}[x]$ právě tehdy, když je ireducibilní v $\mathbb{Q}[x]$.

Věta (Eisensteinovo kritérium). *Buď $f = \sum_{i=0}^{n} a_i x^i$ primitivní polynom v $\mathbb{Z}[x]$. Pokud existuje prvočíslo p splňující $p \mid a_0$, $p \mid a_1$, …, $p \mid a_{n-1}$ a $p^2 \nmid a_0$, pak je polynom f ireducibilní v $\mathbb{Z}[x]$.*

82. 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]

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

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

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

86. * 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]

87. 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]

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

89. * Dokažte Eisensteinovo kritérium. [N]

90. 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]

91. 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]

92. 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]

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

94. 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]

95. 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]

96. * 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]

Připomeňme, že obory $\mathbf{T}[x]$, $\mathbf{T}$ těleso, jsou Eukleidovské, pro počítání NSD a koeficientů z Bézoutovy rovnosti tedy lze použít Eukleidův algoritmus. Druhá možnost je porovnat ireducibilní rozklady obou polynomů.

Máme-li neeukleidovský obor $\mathbf{R}[x]$ (jako např. $\mathbb{Z}[x]$), můžeme použít následující rovnost:

$$\mathrm{NSD}_{\mathbf{R}[x]}(f, g) = \mathrm{NSD}_{\mathbf{R}}(pc(f), pc(g)) \cdot \mathrm{NSD}_{\mathbf{Q}[x]}(pp(f), pp(g)).$$

Zde $\mathbf{Q}$ značí podílové těleso oboru $\mathbf{R}$ a pro $h = \sum_{i=0}^{n} a_i x^i$ se rozumí $pc(h) = \mathrm{NSD}(a_0, \ldots, a_n)$ a $pp(h) = \sum_{i=0}^{n} \frac{a_i}{pc(h)} x^i$.

97. 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]

98. 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]

99. 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]

100. 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]

101. Spočtěte 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]

Derivací polynomu $f = \sum_{i=0}^{n} a_i x^i$ rozumíme polynom

$$f' = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i.$$

Pro $k \geq 0$ definujeme *k-tou derivaci* indukcí jako $f^{(0)} = f$ a $f^{(k)} = (f^{(k-1)})'$.

102. Buď $\mathbf{R}$ komutativní okruh s jednotkou, $f, g \in R[x]$ a $n \in \mathbb{N}$. Dokažte

(1) $(f+g)' = f' + g'$;
(2) * $(f \cdot g)' = f'g + g'f$;
(3) $(f^n)' = n \cdot f^{n-1} \cdot f'$.

103. * Buď $\mathbf{R}$ komutativní okruh s jednotkou, $f, g \in R[x]$ a $n \in \mathbb{N}$. Dokažte $(f \cdot g)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} \cdot f^{(i)} \cdot g^{(n-i)}$ [Leibnitzova formule]. [N]

Prvek a se nazývá *n-násobný kořen* polynomu f, pokud

$$(x-a)^n \mid p \quad \text{a} \quad (x-a)^{n+1} \nmid p.$$

Věta. *Buď* $\mathbf{R}$ *obor integrity charakteristiky* n, $a \in R$, $0 \neq f \in R[x]$ *a předpokládejme* $\deg f < n$ *nebo* $n = 0$. *Pak* a *je* n*-násobným kořenem polynomu* f *právě tehdy, když* $f^{(k)}(a) = 0$ *pro všechna* $k = 0, \ldots, n-1$, *ale nikoliv pro* $k = n$.

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

105. 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]

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

107. 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]

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

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

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

111. 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. [?]

Pomocí série cvičení si odvodíme tzv. *Cardanovy vzorce* na výpočet kořenů polynomů druhého, třetího a čtvrtého stupně. Všechny úlohy řešte v oboru komplexních čísel.

112. Odvoďte vzorec pro kořeny polynomu $ax^2 + bx + c$. [N]

113. Buď $f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$. Navrhněte substituci tak, aby vznikl polynom s nulovým koeficientem u $(n-1)$-té mocniny. [Ř]

Tartagliův postup výpočtu kořenů polynomu $x^3 + px + q$.

114. Všimněte si, že libovolná u, v splňují

$$(u-v)^3 + 3uv(u-v) + (v^3 - u^3) = 0.$$

Dokažte, že řešením soustavy

$$3uv = p, \qquad v^3 - u^3 = q$$

je dvojice

$$u = \sqrt[3]{\frac{-q+\sqrt{D}}{2}}, \qquad v = \sqrt[3]{\frac{q+\sqrt{D}}{2}},$$

kde $D = q^2 + \frac{4}{27}p^3$, a dedukujte, že $x = u - v$ je kořenem daného polynomu.

115. Ověřte, že druhé řešení této soustavy, totiž dvojice $u = \sqrt[3]{\frac{-q-\sqrt{D}}{2}}$, $v = \sqrt[3]{\frac{q-\sqrt{D}}{2}}$, dává stejný kořen x.

116. Buď $\omega = e^{\frac{2\pi i}{3}} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ komplexní třetí odmocnina z jedné. Dokažte, že

$$x_0 = u - v, \qquad x_1 = \omega u - \omega^2 v, \qquad x_2 = \omega^2 u - \omega v$$

jsou právě všechny kořeny daného polynomu.

117. Najděte kořeny polynomu $x^3 - 6x - 9$. [Ř]

118. Najděte kořeny polynomu $x^3 - 15x - 4$. [Ř]

Ferrariho postup výpočtu kořenů polynomu $x^4 + px^2 + qx + r$.

119. Napište si rovnici ve tvaru

$$x^4 + 2ax^2 + a^2 = -px^2 - qx - r + 2ax^2 + a^2.$$

Levá strana je rovna $(x^2 + a)^2$. Najděte a takové, aby i pravá strana byla jako polynom druhou mocninou. Poté obě strany odmocněte a dedukujte vzorec.

120. Najděte všechny kořeny polynomu $x^4 + x^2 + 4x - 3$ v oboru komplexních čísel. [Ř]

121. Najděte všechny kořeny polynomu $x^4 + x^2 + x + 1$ v oboru komplexních čísel. Komplexní čísla ve výsledku nemusíte odmocňovat. [Ř]

4. Číselné obory

V této sekci bude s značit číslo, jež není dělitelné druhou mocninou prvočísla. Definujme zobrazení

$$\nu : \mathbb{Z}[\sqrt{s}] \to \mathbb{N} \cup \{0\}, \qquad a + b\sqrt{s} \mapsto |a^2 - sb^2|.$$

Pro každé $u, v \in \mathbb{Z}[\sqrt{s}]$ platí

(1) $\nu(u) = 1 \;\Leftrightarrow\; u$ je invertibilní;
(2) $\nu(u \cdot v) = \nu(u) \cdot \nu(v)$.

Tedy pokud $u \mid v$, pak $\nu(u) \mid \nu(v)$.

122. Dokažte obě předchozí tvrzení. [Ř]

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

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

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

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

127. * 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]

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

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

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

131. 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.

132. 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]

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

Pro některá s je uvedené zobrazení ν Eukleidovskou normou na oboru $\mathbb{Z}[\sqrt{s}]$. Např. v $\mathbb{Z}[i]$ lze nalézt prvky q, r z podmínky (2) takto: buď

$$z = \frac{a}{b} \in \mathbb{C}$$

přesný podíl v $\mathbb{C}$ a označme q nejbližší prvek $\mathbb{Z}[i]$ k prvku z (tj. takový, že $|z - q|$ je minimální; je-li jich více, pak libovolný z nich) a $r = a - bq$.

134. 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]

135. 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]

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

137. 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]

138. 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]

139. 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]

Některé diofantické rovnice (rovnice v oboru celých čísel) lze úspěšně řešit využitím teorie dělitelnosti v oborech $\mathbb{Z}[\sqrt{s}]$.

140. * Řešte v $\mathbb{Z}$ rovnici $x^2 + 1 = y^3$. Návrh postupu: rozložte $x^2 + 1 = (x + i)(x - i)$ a uvažujte ireducibilní rozklad tohoto čísla v oboru $\mathbb{Z}[i]$. [N] [Ř]

141. * Řešte v $\mathbb{Z}$ rovnici $x^2 + 2 = y^3$ (viz předchozí cvičení; ovšem rozložte $x^2 + 2 = (x + \sqrt{2}i)(x - \sqrt{2}i)$ a uvažujte ireducibilní rozklad tohoto čísla v oboru $\mathbb{Z}[i\sqrt{2}]$). [Ř]

142. ** Řešte v $\mathbb{Z}$ rovnici $x^2 + 4 = y^3$. [Ř]

143. ** Řešte v $\mathbb{Z}$ rovnici $x^2 + 49 = y^3$.

III. Grupy

1. Příklady a základní vlastnosti

Grupou nazýváme algebru $\mathbf{G} = (G, *, ', e)$ typu $(2, 1, 0)$ splňující pro každé $a, b, c \in G$

(1) $a * (b * c) = (a * b) * c$,
(2) $a * e = e * a = a$,
(3) $a * a' = a' * a = e$.

Grupa se nazývá *abelovská*, pokud je operace $*$ komutativní, tj. $a * b = b * a$ pro každé $a, b \in G$. Algebry $(A, *)$ splňující podmínku (1) se nazývají *pologrupy*, algebry $(A, *, e)$ splňující podmínky (1) a (2) se nazývají *monoidy*.

Zobrazení $L_a, R_a : G \to G$ definovaná $L_a(x) = a * x$, $R_a(x) = x * a$ se nazývají *levá* a *pravá* translace prvku a v grupě G. Jsou to permutace na G. Naopak, pokud algebra $(G, *, e)$ splňuje podmínky (1) a (2) a všechny její translace jsou permutace, pak existuje (jednoznačně určená) operace $'$ taková, že $\mathbf{G} = (G, *, ', e)$ je grupa.

Příklad.

(1) Abelovské grupy:
- (Aditivní) grupa celých čísel $\mathbb{Z} = (\mathbb{Z}, +, -, 0)$.
- *Cyklické grupy* $\mathbb{Z}_n = (\{0, 1, \dots, n-1\}, +_{\bmod n}, -_{\bmod n}, 0)$.
- Pro libovolné těleso $\mathbf{T}$ lze uvažovat
  - *aditivní grupu* $(T, +, -, 0)$ a
  - *multiplikativní grupu* $\mathbf{T}^* = (T \setminus \{0\}, \cdot, ^{-1}, 1)$.

  (Připomeňme tělesa $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a konečná tělesa $\mathbb{Z}_p$.)
- Obecněji, pro libovolný komutativní okruh $\mathbf{R}$ lze uvažovat *grupu invertibilních prvků* $\mathbf{R}^*$. Zvlášť zajímavým případem je grupa $\mathbb{Z}_n^*$ s nosnou množinou všech čísel $k \in \{1, \dots, n-1\}$ nesoudělných s n, operací násobení modulo n a s jednotkovým prvkem 1. Z Eulerovy věty plyne, že $a' = a^{\varphi(n)-1} \bmod n$.
- Grupa komplexních jednotek $(\{z \in \mathbb{C} : |z| = 1\}, \cdot, ^{-1}, 1)$ a její podgrupy. Mezi nimi jmenujme např. grupy $\mathbb{C}_n$ sestávající ze všech kořenů polynomu $x^n - 1$ a tzv. *Prüferovu p-grupu* $\mathbb{C}_{p^\infty} = \bigcup_{k=1}^{\infty} \mathbb{C}_{p^k}$ sestávající ze všech komplexních čísel z splňujících $z^{p^n} = 1$ pro nějaké n.

(2) Neabelovské grupy:
- *Symetrická grupa*

$$\mathbf{S}_X = (\{g : g \text{ je permutace na } X\}, \circ, ^{-1}, id),$$

  kde $\circ$ značí skládání permutací, $^{-1}$ invertování permutací a id identitu. Je-li $X = \{1, \dots, n\}$, pak místo $\mathbf{S}_X$ píšeme $\mathbf{S}_n$. Mezi jejími podgrupami zmiňme
  - *alternující grupu* $\mathbf{A}_n$ všech sudých permutací;
  - *dihedrální grupu* $\mathbf{D}_{2n}$ všech symetrií pravidelného n-úhelníka;
  - nejrůznější grupy symetrií geometrických těles, automorfismů grafů a dalších struktur, ...
- *Obecná lineární grupa*

$$\mathbf{GL}_n(\mathbf{T}) = (\{A : A \text{ je regulární matice } n \times n \text{ nad tělesem } \mathbf{T}\}, \cdot, ^{-1}, E),$$

  kde $\cdot$ značí maticové násobení, $^{-1}$ invertování (regulárních) matic a E jednotkovou matici. Mezi jejími podgrupami zmiňme např.
  - *speciální lineární grupu* $\mathbf{SL}_n(\mathbf{T})$ všech matic s determinantem 1;
  - *ortogonální grupu* $\mathbf{GO}_n(\mathbf{T})$ všech ortogonálních matic, tj. takových A co splňují $AA^T = E$. (Nad tělesem $\mathbb{R}$ to odpovídá maticím, jejichž řádky, resp. sloupce, jsou ortonormální vektory vzhledem k standardnímu skalárnímu součinu.)
- *Kvaternionová grupa* $\mathbf{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$ s násobením daným $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $ik = -ki = -j$, $jk = -kj = i$.

Symetrické a lineární grupy jsou v jistém smyslu charakteristické příklady, neboť každou grupu lze vnořit do nějaké symetrické grupy (*Cayleyova reprezentace*) a každou konečnou grupu lze vnořit do nějaké obecné lineární grupy nad libovolným tělesem (*lineární reprezentace*).

n	grupy s n prvky
1	$\mathbb{Z}_1$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ \mathbf{S}_3 = \mathbf{D}_6$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbf{D}_8,\ \mathbf{Q}$
	$\dots$
p	$\mathbb{Z}_p$
p^2	$\mathbb{Z}_{p^2},\ \mathbb{Z}_p \times \mathbb{Z}_p$
$2p$	$\mathbb{Z}_{2p},\ \mathbf{D}_{2p}$

Tabulka obsahuje seznam všech malých grup a několik obecných výsledků; zde p značí libovolné prvočíslo. Každá grupa s n prvky je izomorfní právě jedné z grup uvedených v pravém sloupci.

144. 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]

145. 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]

146. 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]

147. 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]

Řádem grupy $\mathbf{G}$ se rozumí velikost množiny G.

Řádem prvku a v grupě $\mathbf{G}$ se rozumí nejmenší $n > 0$ takové, že $a^n = e$, pokud takové n existuje; v opačném případě je řád ∞. Řád prvku se značí $|a|$. Je-li grupa $\mathbf{G}$ konečná, pak řád každého jejího prvku dělí $|G|$.

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

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

150. * 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]

151. 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 $|a * b| = |a| \cdot |b|$.

Podalgebry grupy $\mathbf{G} = (G, *, ', e)$ se nazývají *podgrupy*. Jinými slovy, je-li $H \subseteq G$ podmnožina obsahující prvek e a splňující pro každé $a, b \in H$ podmínky $a' \in H$ a $a * b \in H$, pak grupu $\mathbf{H} = (H, *, ', e)$ nazýváme podgrupou grupy $\mathbf{G}$ (operacemi se rozumí restrikce původních operací na množinu H); též říkáme, že množina H *tvoří podgrupu* grupy $\mathbf{G}$. Píšeme $\mathbf{H} \leq \mathbf{G}$. Podgrupy $\mathbf{G}$ a $\{e\}$ nazýváme *nevlastní*.

Věta (Lagrangeova). *Je-li* $\mathbf{H}$ *podgrupa konečné grupy* $\mathbf{G}$*, pak* $|H|$ *dělí* $|G|$.

152. 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]

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

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

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

156. 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 $AB = BA$.

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

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

Nejmenší podgrupa grupy $\mathbf{G} = (G, *, ', e)$ obsahující danou množinu $X \subseteq G$ se nazývá *podgrupa generovaná množinou* X a značí se $\langle X \rangle_{\mathbf{G}}$. Platí

$$\langle X \rangle_{\mathbf{G}} = \{x_1^{k_1} * x_2^{k_2} * \ldots * x_n^{k_n} : \ x_1, \ldots, x_n \in X, \ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Rozumí se $x^k = \underbrace{x * \ldots * x}_{k}$ pro $k > 0$, $x^k = \underbrace{x' * \ldots * x'}_{-k}$ pro $k < 0$ a $x^0 = e$.

159. Dokažte předchozí tvrzení.

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

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

Buď $\mathbf{G} = (G, *, ', e)$ a $\mathbf{H} = (H, \cdot, ^{-1}, 1)$ grupy. Zobrazení φ je homomorfismus $\mathbf{G} \to \mathbf{H}$, pokud pro každé $a, b \in G$ platí

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b).$$

Pojmy *monomorfismus* (neboli *vnoření*), *epimorfismus*, *izomorfismus*, *endomorfismus* a *automorfismus* se používají stejně jako pro obecné algebry. Definujeme

- *jádro* homomorfismu φ předpisem
$$\mathrm{Ker}(\varphi) = \{a \in G : \varphi(a) = 1\};$$
- *obraz* homomorfismu φ předpisem
$$\mathrm{Im}(\varphi) = \{b \in H : b = \varphi(a) \text{ pro nějaké } a \in G\}.$$

Jádro tvoří (normální) podgrupu grupy $\mathbf{G}$ a obraz tvoří (ne nutně normální) podgrupu grupy $\mathbf{H}$. Homomorfismus je prostý právě tehdy, když je jeho jádro triviální.

161. 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.

162. 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.

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

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

165. 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]

Izomorfismem rozumíme bijektivní homomorfismus. Řekneme, že grupy $\mathbf{G}$ a $\mathbf{H}$ jsou *izomorfní*, značíme $\mathbf{G} \simeq \mathbf{H}$, pokud existuje izomorfismus $\mathbf{G} \to \mathbf{H}$.

Tvrzení. *Buď* $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ *abelovská grupa,* $\mathbf{A}, \mathbf{B}$ *její podgrupy a předpokládejme, že* $A \cap B = \{e\}$ *a* $AB = G$. *Pak* $\mathbf{G} \simeq \mathbf{A} \times \mathbf{B}$.

166. Dokažte předchozí tvrzení.

167. 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 $\mathbf{G} \simeq \mathbf{G/A} \times \mathbf{G/B}$. 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.

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

Chceme-li dokázat, že dané dvě grupy *nejsou* izomorfní, hodí se nalézt tzv. *invariant* (vlastnost zachovávaná izomorfismem), který v jedné grupě platí a v druhé nikoliv — viz konec úvodní kapitoly sbírky. Jedním z nejužitečnějších invariantů je v případě grup existence a počet prvků daného řádu, viz následující cvičení.

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

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

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

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

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

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

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

Prvky a, b grupy $\mathbf{G} = (G, *, ', e)$ se nazývají *konjugované*, pokud existuje prvek $c \in G$ takový, že $a = c * b * c'$.

176. 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?

2. Cyklické a abelovské grupy

177. 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]

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

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

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

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

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

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

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

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

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

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

188. 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]

189. 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]

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

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

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

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

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

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

196. 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]

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

198. 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]

199. 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]

200. 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]

201. 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]

202. 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]

203. 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]

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

205. 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]

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

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

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

209. 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]

210. 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]

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

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

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

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

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

216. * 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]

Grupa $\mathbf{G}$ se nazývá *cyklická*, je-li generovaná jedním prvkem a, tj. $\mathbf{G} = \langle a \rangle$. Každá cyklická grupa je izomorfní buď grupě $\mathbb{Z}$ (v případě $|a| = \infty$), nebo grupě $\mathbb{Z}_n$ (pokud $n = |a| < \infty$).

217. Dokažte, že nekonečná cyklická grupa je izomorfní grupě $\mathbb{Z}$ a konečná n-prvková grupě $\mathbb{Z}_n$.

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

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

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

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

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

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

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

225. 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 $a = b$.

226. * 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.

227. 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 $\mathbf{G} = \langle k \times a \rangle$.

Věta. *Buď $\mathbf{G}$ alespoň dvouprvková konečná abelovská grupa. Existují prvočísla $p_1, \ldots, p_m$ a přirozená čísla $k_1, \ldots, k_m$ taková, že*

$$\mathbf{G} \simeq \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

Čísla $p_1, \ldots, p_m$ a $k_1, \ldots, k_m$ jsou určena jednoznačně až na pořadí.

228. Dokažte Základní větu aritmetiky jako důsledek Klasifikace konečných abelovských grup.

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

230. 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]

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

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

233. Existuje n takové, že $\mathbb{Z}_n^*$ je izomorfní a) $\mathbb{Z}_7$, b) $\mathbb{Z}_8$, c) $\mathbb{Z}_9$? [?]

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

235. ** Využijte vlastnost $\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$ a dokažte, že pro prvočíslo $p > 2$ platí $\mathbb{Z}_{p^k}^* \simeq \mathbb{Z}_{p^{k-1}} \times \mathbb{Z}_{p-1}$. [N] [?]

3. Permutační grupy

Permutací na množině X rozumíme bijekci (vzájemně jednoznačné zobrazení) $X \to X$. Pro permutace π, σ na X definujeme operace $\circ$, $^{-1}$, id předpisy

- $\pi \circ \sigma : x \mapsto \pi(\sigma(x))$,
- $\pi^{-1} : x \mapsto$ ten (jediný) prvek y splňující $\pi(y) = x$,
- $id : x \mapsto x$.

Označíme-li S_X množinu všech permutací na množině X, pak $\mathbf{S}_X = (S_X, \circ, ^{-1}, id)$ je tzv. *symetrická grupa* na X. Zápisem π^k rozumíme permutaci $\underbrace{\pi \circ \pi \circ \cdots \circ \pi}_{k\text{-krát}}$.

Cyklus v permutaci π je posloupnost $x_1, \ldots, x_k$ navzájem různých prvků množiny X splňující $\pi(x_1) = x_2$, $\pi(x_2) = x_3$, …, $\pi(x_k) = x_1$. *Rozkladem na cykly* se rozumí zápis

$$(x_{11}\ x_{12}\ \ldots\ x_{1k_1})(x_{21}\ x_{22}\ \ldots\ x_{2k_2}) \ldots (x_{m1}\ x_{m2}\ \ldots\ x_{mk_m}),$$

kde $x_{i1}, x_{i2}, \ldots, x_{ik_i}$ jsou navzájem různé cykly, $i = 1, \ldots, m$. Cykly délky 1 se ze zápisu zpravidla vynechávají. Permutace se zapisují také v maticovém tvaru

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \pi(x_1) & \pi(x_2) & \ldots & \pi(x_n) \end{pmatrix},$$

kde $X = \{x_1, \ldots, x_n\}$. Například permutaci na množině $\{1, 2, 3, 4, 5, 6\}$ definovanou předpisem $1 \mapsto 3$, $2 \mapsto 6$, $3 \mapsto 4$, $4 \mapsto 1$, $5 \mapsto 5$, $6 \mapsto 2$ lze zapsat $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$ nebo (1 3 4)(2 6).

Transpozicí rozumíme permutaci tvaru $(x\ y)$, kde $x, y \in X$, $x \neq y$. Každá permutace na konečné množině je složením (konečně mnoha) transpozic. Permutace se nazývá *sudá*, pokud se skládá ze sudého počtu transpozic, *lichá* v opačném případě (dá se dokázat, že tato vlastnost nezáleží na zvoleném rozkladu). *Znaménko* sudé permutace je 1, liché permutace -1, značí se $\operatorname{sgn}(\pi)$. Platí

$$\operatorname{sgn}(\pi \circ \sigma) = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\sigma) \quad \text{a} \quad \operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi).$$

Znaménko permutace na n-prvkové množině X lze spočítat též takto:

$$\begin{aligned} \operatorname{sgn}(\pi) &= (-1)^{n - \text{počet cyklů v } \pi} \\ &= (-1)^{\text{počet inverzí v } \pi}, \end{aligned}$$

kde inverzí v π se rozumí dvojice (i, j) taková, že $i < j$ a $\pi(i) > \pi(j)$ (předpokládáme nějaké lineární uspořádání na X).

Označme $\mathbf{S}_n = (S_n, \circ, ^{-1}, id)$ grupu všech permutací na množině $\{1, \ldots, n\}$, $\mathbf{A}_n$ její podgrupu sudých permutací a $\mathbf{D}_{2n}$ její podgrupu permutací, které zachovávají pravidelný n-úhelník s vrcholy $1, \ldots, n$ (tj. $\mathbf{D}_{2n}$ sestává z n otočení a n osových symetrií).

236. 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) ∘ (1 2 5) ∘ (3 6 1 7). [Ř]

237. Řešte v S_5 rovnici (1 3 2) ∘ π ∘ (3 5 2)(1 4) = (2 4)(1 5). [Ř]

238. 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]

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

240. 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.

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

242. * 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 $i = 1, \ldots, m$.

243. * 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.]

244. 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]

245. 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]

246. 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]

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

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

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

250. * Dokažte oba vzorce na výpočet znaménka permutace.

251. 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]

252. 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]

253. 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]

254. 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 $(\sigma^3 \circ \tau^{-17})^{18} \circ \sigma^{10} \circ (\upsilon^9 \circ \tau)^{-2}$.

255. 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]

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

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

Permutace π, σ jsou konjugované v grupě $\mathbf{S}_n$ (tj. existuje permutace $\rho \in S_n$ taková, že $\pi = \rho \circ \sigma \circ \rho^{-1}$) právě tehdy, když mají stejný počet cyklů každé délky.

258. 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]

259. 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]

260. 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]

261. 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]

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

263. 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.

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

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

Tvrzení, že každá permutace lze napsat jako složení transpozic a každá sudá jako složení trojcyklů, lze přeložit do řeči algebry tak, že grupa $\mathbf{S}_n$ je generovaná množinou všech transpozic a grupa $\mathbf{A}_n$ množinou všech trojcyklů.

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

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

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

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

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

271. * 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.

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

273. 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.

274. 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]

275. * 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 $1 \leq m < n-1$. Dokažte, že $\mathbf{G} = \mathbf{S}_n$ pro m liché a $\mathbf{G} = \mathbf{A}_n$ pro m sudé.

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

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

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

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

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

281. 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.]

282. * 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] [?]

283. ** 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]

284. 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 $\mathbf{X} = (X, \leq)$ rozumíme permutaci $\varphi \in S_X$ takovou, že

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

285. 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.

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

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

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

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

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

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

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

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

294. 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]

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

296. 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 $\mathbf{Aut}(\mathbb{Z}_m \times \mathbb{Z}_n) \simeq \mathbf{Aut}(\mathbb{Z}_m) \times \mathbf{Aut}(\mathbb{Z}_n)$.)

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

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

299. 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 $\mathbf{Inn}(\mathbf{G})$.

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

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

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

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

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

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

4. Maticové a geometrické grupy

Připoměňme, že $\mathbf{GL}_n(\mathbf{T})$ značí multiplikativní grupu regulárních matic $n \times n$ nad tělesem $\mathbf{T}$ a

- $\mathbf{SL}_n(\mathbf{T})$ její podgrupu matic s determinantem 1;
- $\mathbf{GO}_n(\mathbf{T})$ její podgrupu ortogonálních matic;
- $\mathbf{SO}_n(\mathbf{T}) = \mathbf{SL}_n(\mathbf{T}) \cap \mathbf{GO}_n(\mathbf{T})$.

306. 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]

307. 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]

308. 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.

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

310. * 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.

311. 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]

312. 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.]

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

314. * 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]

315. 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 $(0, \ldots, 0)$. (Ostatní izometrie dostanem složením s vhodným posunutím.)

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

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

318. * 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.

319. 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]`

320. 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.

321. 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 $\mathbb{C}^*$.

322. 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 $u \in \mathbb{C}$, $|u| = 1$.

323. 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.)

324. 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.

325. 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

Působením grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ *na množině* X rozumíme homomorfismus $\pi : \mathbf{G} \to \mathbf{S}_X$. Hodnotu permutace $\pi(g)$ na prvku x budeme značit krátce $g(x)$. Protože jde o homomorfismus, jednotka působí jako identita, g^{-1} působí jako inverzní permutace k $\pi(g)$ a platí vztah $(g \cdot h)(x) = g(h(x))$.

Příklad.

- Je-li $\mathbf{G}$ podgrupa grupy $\mathbf{S}_X$, můžeme uvažovat přirozené působení na množinu X, přičemž $\pi = id$. Speciálně, je-li $\mathbf{X}$ nějaká struktura (např. algebra, graf, uspořádaná množina), pak grupa $\mathbf{Aut}(\mathbf{X})$ působí přirozeně na nosnou množinu X (resp. vrcholy grafu).
- Grupa $\mathbf{GL}_n(\mathbf{T})$ působí na vektorový prostor $\mathbf{T}^n$ jako násobení vektoru maticí; tj. $\pi(A)$ je permutace množiny T^n, která vektor v zobrazí na Av.
- Grupa $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ působí svoji na nosnou množinu G
  - *translacemi*, když za π vezmeme Cayleyovu reprezentaci, tj. $g(x) = g \cdot x$;
  - *konjugací*, když za π vezmeme homomorfismus, který prvku g přiřadí vnitřní automorfismus daný prvkem g; tj. $g(x) = g \cdot x \cdot g^{-1}$.

Definujeme ekvivalenci $\sim$ na množině X následujícím způsobem: řekneme, že $x \sim y$, pokud existuje $g \in G$ takové, že $g(x) = y$. Bloky této ekvivalence nazýváme *orbity*. Orbitu obsahující prvek x budeme značit $[x] = \{y \in X : x \sim y\}$.

Bod x se nazývá *pevným bodem* permutace π, pokud $\pi(x) = x$. Množinu všech pevných bodů permutace $\pi(g)$ budeme značit $X_g = \{x \in X : g(x) = x\}$ a *stabilizátorem prvku* $x \in X$ rozumíme podgrupu $G_x = \{g \in G : g(x) = x\}$ grupy $\mathbf{G}$. Platí $|G| = |G_x| \cdot |[x]|$.

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

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

328. 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]

329. 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]

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

331. 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]

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

333. 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]

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

335. 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]

336. 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]

337. 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]

338. 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]

339. 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]

340. 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]

Věta (Burnsideova). *Působí-li konečná grupa* $\mathbf{G}$ *na konečnou množinu* X*, pak*

$$\textit{počet orbit} = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

Vzorec lze interpretovat tak, že „počet orbit je roven průměrnému počtu pevných bodů permutací v $\mathbf{G}$“. Řešením většiny níže uvedených úloh je právě *počet orbit* při působení grupy symetrií daného objektu na množinu všech obarvení/konfigurací/apod.

341. Kolik náhrdelníků lze sestavit ze tří modrých a tří červených kuliček? Nezáleží na poloze náhrdelníku, je možno jej převracet či otáčet.

Řešení. Místo náhrdelníků budeme uvažovat barvení vrcholů pravidelného šestiúhelníka. Čili X bude množina všech obarvení vrcholů pravidelného šestiúhelníka třemi modrými a třemi červenými barvami a $\mathbf{G}$ bude grupa všech symetrií pravidelného šestiúhelníka (tj. $\mathbf{G} = \mathbf{D}_{12}$). Tedy $\mathbf{G}$ působí na X tak, že příslušná permutace otočí/převrátí šestiúhelník i s daným obarvením. Každé orbitě tohoto působení odpovídá právě jeden náhrdelník (jehož kuličky uspořádány podle vzoru daného tím obarvením). Vyrobíme tabulku, v jejímž prvním sloupci je seznam prvků grupy $\mathbf{G}$, v druhém počet prvků daného typu a ve třetím počet pevných bodů těchto prvků. Pevným bodem se rozumí takové obarvení, které po daném otočení/převrácení vypadá stejně.

g	#	$\lvert X_g\rvert$
id	1	20
$\circlearrowleft \pm 60°$	2	0
$\circlearrowleft \pm 120°$	2	2
$\circlearrowleft +180°$	1	0
osa přes vrcholy	3	4
osa středem hran	3	0

Podle Burnsideovy věty je počet obarvení $\frac{1}{12} \cdot (20 + 2 \cdot 0 + 2 \cdot 2 + 1 \cdot 0 + 3 \cdot 4 + 3 \cdot 0) = 3$.

342. 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]

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

344. 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]

345. 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]

346. 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.)

347. 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]

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

349. 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]

350. 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.

351. 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.

352. 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]

353. 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.

354. 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]

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

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

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

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

Působení grupy se nazývá *tranzitivní*, má-li jen jednu orbitu. Podgrupa $\mathbf{G}$ grupy $\mathbf{S}_n$ se nazývá tranzitivní, pokud je tranzitivní její přirozené působení na množinu $\{1, \ldots, n\}$.

359. * Dokažte, že tranzitivní grupa na množině s aspoň dvěma prvky obsahuje alespoň jednu permutaci bez pevného bodu. [Ř]

360. 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]

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

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

363. * 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 $a \in X$). [?]

364. * 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

Levým rozkladem grupy $\mathbf{G} = (G, *, ', e)$ podle podgrupy $\mathbf{H}$ se rozumí množina $\{a * H : a \in G\}$, pričemž množinám $a * H = \{a * h : h \in H\}$ se říká *levé rozkladové třídy. Pravým rozkladem* grupy $\mathbf{G}$ podle podgrupy $\mathbf{H}$ se rozumí množina $\{H * a : a \in G\}$, pričemž množinám $H * a = \{h * a : h \in H\}$ se říká *pravé rozkladové třídy.* Množina $T \subseteq G$ se nazývá *levou transverzálou*, pokud obsahuje z každé levé rozkladové třídy právě jeden prvek; resp. *pravou transverzálou*, pokud obsahuje z každé pravé rozkladové třídy právě jeden prvek. Dá se dokázat, že dvě levé (resp. pravé) rozkladové třídy jsou buď disjunktní nebo totožné, že velikost všech pravých a levých rozkladových tříd podle dané podgrupy je stejná a že stejný je i jejich počet (tj. všechny transverzály jsou stejně velké) — tento počet se nazývá *index podgrupy* $\mathbf{H}$ *v grupě* $\mathbf{G}$ a značí se $[\mathbf{G} : \mathbf{H}]$.

Je-li $a * H = H * a$ pro každé $a \in G$, pak se podgrupa $\mathbf{H}$ nazývá *normální*, píšeme $\mathbf{H} \trianglelefteq \mathbf{G}$.

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

366. 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]

367. 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 $\mathbf{G}$.

Podgrupa $\mathbf{H}$ je *normální* v $\mathbf{G}$ právě tehdy, když je uzavřena na konjugaci libovolným prvkem grupy $\mathbf{G}$, tj. pokud pro každé $g \in G$ a $h \in H$ platí $g * h * g' \in H$.

368. Dokažte předchozí tvrzení.

369. 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 $\mathbf{G}$.

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

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

372. 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]

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

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

375. 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]

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

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

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

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

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

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

382. 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) $\mathbf{G} = \mathbb{Z}_2$.

383. 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]

384. 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]

385. 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]

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

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

388. 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]

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

390. 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]

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

Buď $\mathbf{G} = (G, *, ', e)$ grupa a $\mathbf{H}$ její normální podgrupa. Definujeme ekvivalenci $a \sim b \Leftrightarrow a * b' \in H$. Její bloky jsou $[a] = a * H = H * a$. Na těchto blocích definujeme operace předpisy $[a] * [b] = [a * b]$ a $[a]' = [a']$. Grupa

$$\mathbf{G}/\mathbf{H} = (\{[a] : a \in G\}, *, ', [e])$$

se nazývá *faktorgrupa grupy* $\mathbf{G}$ *podle podgrupy* $\mathbf{H}$.

Věta (1. věta o izomorfismu)**.** *Je-li* $\varphi : \mathbf{G} \to \mathbf{H}$ *homomorfismus grup, pak*

$$\mathbf{G}/\mathbf{Ker}(\varphi) \simeq \mathbf{Im}(\varphi).$$

1. věta o izomorfismu je dobrý nástroj, pokud chceme vyšetřit, jak vypadá daná faktorgrupa. Chceme-li dokázat, že $\mathbf{G}/\mathbf{N} \simeq \mathbf{H}$, stačí najít homomorfismus $\mathbf{G}$ na $\mathbf{H}$, jehož jádro je $\mathbf{N}$.

Příklad. Zobrazení $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $x \mapsto x \bmod n$ je homomorfismus, jehož jádro je podgrupa $\{x : x \bmod n = 0\} = n\mathbb{Z}$ a obraz $\mathbb{Z}_n$. Tedy $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.

392. 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]

393. * 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.

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

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

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

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

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

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

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

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

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

403. 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]

404. 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 $\mathbb{Z}_2 \times \mathbb{Z}_2$.

405. 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.

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

407. 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 $\mathbf{G}/\mathbf{H}$? [?]

408. * 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]

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

410. * Najděte vnoření Prüferovy grupy $\mathbb{C}_{p^\infty}$ do grupy $\mathbb{Q}/\mathbb{Z}$.

411. ** Buď $\mathbf{T}$ těleso a označme $\mathbf{PSL}_n(\mathbf{T}) = \mathbf{SL}_n(\mathbf{T})/\mathbf{D}$, kde $\mathbf{D}$ značí normální podgrupu diagonálních matic s determinantem 1. Dokažte, že je-li $p > 3$ prvočíslo, pak $\mathbf{PSL}_n(\mathbb{Z}_p)$ nemá žádné vlastní normální podgrupy. [?]

412. Dokažte, že $\mathbf{PSL}_2(\mathbb{Z}_2) \simeq \mathbf{S}_3$ a $\mathbf{PSL}_2(\mathbb{Z}_3) \simeq \mathbf{A}_4$.

413. 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 $\mathbf{G}$.

414. * 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]

IV. Okruhy

1. Příklady a základní vlastnosti

Okruhem nazýváme algebru $\mathbf{R} = (R, +, -, \cdot, 0)$ typu $(2, 1, 2, 0)$ splňující následující podmínky:

(1) $(R, +, -, 0)$ je abelovská grupa;
(2) operace $\cdot$ je asociativní;
(3) pro všechna $x, y, z \in R$ platí tzv. *distributivita*:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \quad \text{a} \quad (y + z) \cdot x = (y \cdot x) + (z \cdot x).$$

Okruh se nazývá *komutativní*, pokud platí $x \cdot y = y \cdot x$ pro všechna $x, y \in R$. Říkáme, že okruh má *jednotku*, pokud existuje prvek $1 \in R$ splňující $1 \cdot x = x \cdot 1 = x$ pro všechna $x \in R$. *Tělesa* jsou komutativní okruhy s jednotkou, kde pro každé $x \neq 0$ existuje y splňující $x \cdot y = 1$.

Příklad. Mezi základní příklady patří následující okruhy:

- všechna tělesa, tedy zejména $\mathbb{Z}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
- okruh celých čísel $\mathbb{Z} = (\mathbb{Z}, +, -, \cdot, 0)$;
- okruhy $\mathbb{Z}_n = (\mathbb{Z}_n, +_{\bmod n}, -_{\bmod n}, \cdot_{\bmod n}, 0)$ s operacemi modulo n;
- okruh *kvaternionů*

  $$\mathbb{H} = (\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}, +, -, \cdot, 0),$$

  kde, podobně jako v komplexních číslech, se sčítá po složkách a násobí tak, že výraz roznásobíme a upravíme podle pravidel

  $$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ik = -ki = -j, \quad jk = -kj = i.$$

Příklad. Existuje řada konstrukcí, jak z daného okruhu $\mathbf{R}$ sestrojit další okruhy.

- *Podokruhy* a *direktní součiny*. Mezi důležité typy okruhů patří tzv. *rozšíření* $\mathbf{R}[a_1, \ldots, a_n] \leq \mathbf{S}$, viz níže. Uveďme např. okruh *Gaussovských celých čísel*

  $$\mathbb{Z}[i] = (\{a + bi : a, b \in \mathbb{Z}\}, +, -, \cdot, 0) \leq \mathbb{C}.$$

- Okruh *matic* $n \times n$ nad $\mathbf{R}$

  $$\mathbf{M}_n(\mathbf{R}) = (\{A : A \text{ je matice } n \times n \text{ nad } \mathbf{R}\}, +, -, \cdot, 0),$$

  kde $+, -, \cdot$ je maticové sčítání, odčítání a násobení a 0 je nulová matice.
- Okruhy *polynomů* jedné proměnné nad $\mathbf{R}$

  $$\mathbf{R}[x] = (\{\sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}, a_0, \ldots, a_n \in R\}, +, -, \cdot, 0),$$

  resp. více proměnných

  $$\mathbf{R}[x_1, \ldots, x_n] = (\{\sum_{k_1, \ldots, k_n = 0}^{N} a_{k_1, \ldots, k_n} x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} : a_{k_1, \ldots, k_n} \in R\}, +, -, \cdot, 0).$$

- Okruh *formálních mocninných řad* jedné proměnné nad $\mathbf{R}$

  $$\mathbf{R}[[x]] = (\{\sum_{i=0}^{\infty} a_i x^i : a_0, a_1, \cdots \in R\}, +, -, \cdot, 0),$$

  resp. více proměnných

  $$\mathbf{R}[[x_1, \ldots, x_n]] = (\{\sum_{k_1, \ldots, k_n = 0}^{\infty} a_{k_1, \ldots, k_n} x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} : a_{k_1, \ldots, k_n} \in R\}, +, -, \cdot, 0).$$

415. Buď $\mathbf{R}$ komutativní okruh. Dokažte, že jsou $\mathbf{R}[x]$ a $\mathbf{R}[[x]]$ skutečně komutativní okruhy s jednotkou.

416. Buď $\mathbf{R}$ okruh. Dokažte, že je $\mathbf{M}_n(\mathbf{R})$ skutečně okruh s jednotkou.

417. Dokažte, že kvaterniony skutečně tvoří okruh.

418. 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.

419. 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?

420. 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]

421. 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]

422. 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]

423. * Na každé abelovské grupě lze definovat násobení tak, že výsledkem je okruh: např. triviálně $x \cdot y = 0$ pro všechna x, y. Platí i opačné tvrzení, tj. lze na každé pologrupě $(A, \cdot)$ s nulou definovat sčítání a odčítání tak, že výsledkem je okruh? [?]

424. Buď $\mathbf{R}$ okruh splňující $x^2 = x$ pro všechna $x \in R$. Definujme operace $x \wedge y = xy$ a $x \vee y = x + y + xy$. Dokažte, že $(R, \wedge, \vee)$ je distributivní svaz.

425. 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]

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

427. [VOID]

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

Buď $\mathbf{R}$ okruh s jednotkou a označme R^* množinu všech *invertibilních prvků*, tj. $R^* = \{a \in R : \text{existuje } b \in R \text{ takové, že } a \cdot b = 1\}$.

429. Dokažte, že R^* s operací násobení tvoří grupu.

430. Spočtěte grupy $\mathbb{Z}^*$ a $\mathbb{Z}[i]^*$. Co je $\mathbf{M}_n(\mathbf{T})^*$? [Ř]

431. Buď $\mathbf{R}$ komutativní okruh s jednotkou. Dokažte, že $\mathbf{R}[x]^* = \mathbf{R}^*$.

432. Spočtěte $\mathbb{H}^*$, kde $\mathbb{H}$ značí okruh kvaternionů. [Ř]

Prvek a okruhu $\mathbf{R}$ se nazývá *nilpotentní*, pokud $a^n = 0$ pro nějaké přirozené n. Nazývá se *dělitel nuly*, pokud existuje prvek $b \neq 0$ takový, že $ab = 0$. Nazývá se *invertibilní*, pokud existuje prvek b takový, že $ab = 1$ (v okruzích s jednotkou).

433. Buď $\mathbf{R}$ okruh s jednotkou. Dokažte, že pokud je a nilpotentní prvek, pak je $1+a$ invertibilní.

434. Najděte všechny nilpotentní prvky, dělitele nuly a invertibilní prvky v oborech $\mathbb{Z}$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$ a obecně $\mathbb{Z}_{p^k}$ (p prvočíslo). [Ř]

435. Dokažte, že v oboru $\mathbf{M}_2(\mathbb{R})$ jsou invertibilní právě regulární matice a dělitelé nuly právě singulární matice. * Popište nilpotentní matice.

436. Buď $\mathbf{R}$ okruh s jednotkou. Dokažte, že polynom $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ je a) nilpotentní právě tehdy, když $a_0, \ldots, a_n$ jsou nilpotentní v $\mathbf{R}$; b) invertibilní právě tehdy, když

a_0 je invertibilní a $a_1, \dots, a_n$ nilpotentní v $\mathbf{R}$; c) dělitel nuly právě tehdy, když existuje $b \in R$ takový, že $bf = 0$.

437. Buď $\mathbf{R}, \mathbf{S}$ okruhy. Popište nilpotentní prvky, dělitele nuly a invertibilní prvky v oboru $\mathbf{R} \times \mathbf{S}$ pomocí odpovídajících prvků oborů $\mathbf{R}$, $\mathbf{S}$. [Ř]

2. Podokruhy a ideály

Podalgebry okruhu $\mathbf{R} = (R, +, -, \cdot, 0)$ se nazývají *podokruhy*. Jinými slovy, je-li $S \subseteq R$ podmnožina obsahující prvek 0 a splňující pro každé $a, b \in S$ podmínky $a + b \in S$, $-a \in S$ a $a \cdot b \in S$, pak okruh $\mathbf{S} = (S, +, -, \cdot, 0)$ nazýváme podokruh okruhu $\mathbf{R}$ (operacemi se rozumí restrikce původních operací na množinu S); též říkáme, že množina S *tvoří podokruh* okruhu $\mathbf{R}$. Píšeme $\mathbf{S} \leq \mathbf{R}$. Podokruhy $\{0\}$ a $\mathbf{R}$ nazýváme *nevlastní*.

438. Dokažte, že podokruhy daného okruhu tvoří úplný svaz. * Musí být distributivní? Musí být modulární? Pokud ano, dokažte, pokud ne, uveďte protipříklad. [Ř]

439. 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]

440. 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]

441. 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]

442. 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.

Je-li $\mathbf{S}$ podokruh okruhu $\mathbf{R}$ a $a_1, \dots, a_n \in R$, definujeme

$$\mathbf{S}[a_1, \dots, a_n] = \langle S \cup \{a_1, \dots, a_n\} \rangle_{\mathbf{R}}.$$

Pokud $|S| > 1$, pak

$$\mathbf{S}[a_1, \dots, a_n] = \{f(a_1, \dots, a_n) : f \in S[x_1, \dots, x_n]\}.$$

Příklad. $\mathbb{R}[i] = \mathbb{C}$, $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Z}\}$.

443. 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.

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

445. 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]

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

447. 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]

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

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

450. 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]

451. 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]

452. 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]

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

Centrem okruhu $\mathbf{R}$ se rozumí $\{a \in R : ar = ra \text{ pro všechna } r \in R\}$.

454. Dokažte, že centrum skutečně tvoří podokruh.

455. Spočtěte centrum okruhu $\mathbf{M}_n(\mathbf{R})$. Dokažte, že je izomorfní s okruhem $\mathbf{R}$. [Ř]

Podokruh $\mathbf{I}$ okruhu $\mathbf{R}$ se nazývá *ideál*, pokud navíc splňuje $ri \in I$ a $ir \in I$ pro každé $i \in I$ a každé $r \in R$. Ideály $\{0\}$ a $\mathbf{R}$ se nazývají *nevlastní*. Průnik dvou ideálů $I_1 \cap I_2$ a součet dvou ideálů $I_1 + I_2 = \{a_1 + a_2 : a_1 \in I_1, a_2 \in I_2\}$ také tvoří ideál okruhu $\mathbf{R}$.

Není těžké nahlédnout, že v komutativním okruhu tvoří množina $aR = \{au : u \in R\}$ ideál, a to nejmenší ideál obsahující prvek a. Takový ideál se nazývá *hlavní*. Nejmenší ideál komutativního okruhu $\mathbf{R}$ obsahující prvky $a_1, \ldots, a_n$, tzv. *ideál generovaný* $a_1, \ldots, a_n$, je ideál $a_1R + \cdots + a_nR$.

456. Dokažte, že ideály daného okruhu tvoří úplný svaz. Musí být distributivní? Musí být modulární? Pokud ano, dokažte, pokud ne, uveďte protipříklad. [Ř]

457. 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]

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

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

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

461. 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]

462. 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]

463. 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]

464. 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]

465. 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]

Jsou-li A, B, C, D množiny, pak se rozumí

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a \in A, b \in B, c \in C, d \in D\}$$

(apod. pro větší matice).

466. Rozhodněte, zda následující množiny tvoří ideál okruhu $\mathbf{M}_2(\mathbf{R})$:
$\left(\begin{smallmatrix} \mathbf{R} & \mathbf{R} \\ 0 & \mathbf{R} \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} \mathbf{R} & \mathbf{R} \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} \mathbf{R} & 0 \\ 0 & \mathbf{R} \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & \mathbf{R} \\ 0 & 0 \end{smallmatrix}\right)$. [Ř]

467. Rozhodněte, zda následující množiny tvoří ideál okruhu $\left(\begin{smallmatrix} \mathbf{R} & \mathbf{R} \\ 0 & \mathbf{R} \end{smallmatrix}\right)$:
$\left(\begin{smallmatrix} \mathbf{R} & \mathbf{R} \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} \mathbf{R} & 0 \\ 0 & \mathbf{R} \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & \mathbf{R} \\ 0 & 0 \end{smallmatrix}\right)$. [Ř]

468. Spočtěte prvky nejmenšího ideálu okruhu $\mathbf{M}_2(\mathbb{Z})$ obsahujícího matici $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. [Ř]

469. a) Dokažte, že těleso neobsahuje vlastní ideály. b) Dokažte, že komutativní okruh s jednotkou, který neobsahuje vlastní ideály, je těleso.

470. Buď $\mathbf{T}$ těleso. Dokažte, že okruh $\mathbf{M}_n(\mathbf{T})$ neobsahuje vlastní ideály.

471. * Najděte všechny ideály okruhu $\mathbf{M}_n(\mathbb{Z})$. [N] [Ř]

472. * Buď $\mathbf{R}$ okruh a $\mathcal{I}$ množina jeho ideálů. Jak vypadají ideály okruhu $\mathbf{M}_n(\mathbf{R})$? [N] [Ř]

473. Buď $\mathbf{T}$ těleso. Najděte všechny ideály okruhu $\left(\begin{smallmatrix} \mathbf{T} & \mathbf{T} \\ 0 & \mathbf{T} \end{smallmatrix}\right)$. [Ř]

474. * Najděte všechny ideály okruhu $\left(\begin{smallmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{smallmatrix}\right)$. [?] [N]

475. Najděte všechny ideály okruhu kvaternionů. [Ř]

476. Buď $\mathbf{R}$ okruh a $M = \{a \in R : ar = ra = 0 \text{ pro všechna } r \in R\}$. Dokažte, že M tvoří ideál okruhu $\mathbf{R}$. (Nazývá se *anihilátor*.) * Uveďte příklad okruhu, v němž je tento ideál vlastní.

477. Buď $\mathbf{R}$ okruh a M množina jeho nilpotentních prvků. Dokažte, že M tvoří ideál okruhu $\mathbf{R}$. (Nazývá se *nilradikál*.) * Uveďte příklad okruhu, v němž a) nilradikál je roven anihilátoru a je vlastní; b) nilradikál není roven anihilátoru.

478. Buď $\mathbf{R}$ okruh, v němž průnik všech ideálů je různý od $\{0\}$, a buď M množina dělitelů nuly v $\mathbf{R}$. Dokažte, že M tvoří ideál okruhu $\mathbf{R}$.

3. Homomorfismy

Zobrazení $\varphi : R \to S$ je homomorfismem okruhů $\mathbf{R}, \mathbf{S}$ právě tehdy, když

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{a} \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

pro každé $a, b \in R$. Definujeme *jádro* homomorfismu φ předpisem

$$\mathrm{Ker}(\varphi) = \{a \in R : \varphi(a) = 0\}$$

a *obraz* homomorfismu φ předpisem

$$\mathrm{Im}(\varphi) = \{b \in S : b = \varphi(a) \text{ pro nějaké } a \in R\}.$$

Jádro tvoří ideál okruhu $\mathbf{R}$ a obraz podokruh okruhu $\mathbf{S}$. Homomorfismus je prostý právě tehdy, když je jeho jádro triviální.

479. 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]

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

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

482. 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]

483. 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]

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

Izomorfismem rozumíme bijektivní homomorfismus. Řekneme, že okruhy $\mathbf{R}$ a $\mathbf{S}$ jsou *izomorfní*, značíme $\mathbf{R} \simeq \mathbf{S}$, pokud existuje izomorfismus $\mathbf{R} \to \mathbf{S}$.

485. 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 $\mathbf{R} \simeq \mathbf{R}'$.

486. 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]

487. 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).

488. 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]

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

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

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

492. 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 $\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$.

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

494. * 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 $\mathbf{Aut}(\mathbf{R})$.

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

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

497. Spočtěte grupu automorfismů okruhu $\mathbb{Z}[x]$ a $\mathbb{Q}[x]$. [?]

4. Faktorokruhy

Buď $\mathbf{R}$ okruh a $\mathbf{I}$ jeho ideál. Definujeme ekvivalenci $a \sim b \Leftrightarrow a - b \in I$. Její bloky jsou $[a] = a + I$. Na těchto blocích definujeme operace předpisy $[a] + [b] = [a + b]$, $-[a] = [-a]$ a $[a] \cdot [b] = [a \cdot b]$. Okruh

$$\mathbf{R}/\mathbf{I} = (\{[a] : a \in R\}, +, -, \cdot, [0])$$

se nazývá *faktorokruh okruhu* $\mathbf{R}$ *podle ideálu* $\mathbf{I}$.

Je-li $\mathbf{I} = m\mathbf{R}$ hlavní ideál, píšeme místo $\mathbf{R}/m\mathbf{R}$ zjednodušeně $\mathbf{R}/m$. Pokud je v $\mathbf{R}$ definováno dělení se zbytkem, pak můžeme prvky okruhu $\mathbf{R}/m$ reprezentovat pomocí zbytků po dělení m a operace v $\mathbf{R}/m$ fungují jako operace v původním okruhu modulo m.

Věta (1. věta o izomorfismu)**.** *Je-li $\varphi : \mathbf{R} \to \mathbf{S}$ homomorfismus okruhů, pak*

$$\mathbf{R}/\mathbf{Ker}(\varphi) \simeq \mathbf{Im}(\varphi).$$

1. věta o izomorfismu je dobrý nástroj, pokud chceme vyšetřit, jak vypadá daný faktorokruh. Chceme-li dokázat, že $\mathbf{R}/\mathbf{I} \simeq \mathbf{S}$, stačí najít homomorfismus $\mathbf{R}$ na $\mathbf{S}$, jehož jádro je $\mathbf{I}$.

Příklad. Zobrazení $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $x \mapsto x \bmod n$ je homomorfismus, jehož jádro je ideál $\{x : x \bmod n = 0\} = n\mathbb{Z}$ a obraz $\mathbb{Z}_n$. Tedy $\mathbb{Z}/n \simeq \mathbb{Z}_n$.

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

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

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

501. 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]

502. 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]

503. 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]

504. 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]

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

506. 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]

507. 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]

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

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

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

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

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

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

514. 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]

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

516. 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]

517. 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]

518. 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.

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

520. 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]

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

522. 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]

523. * 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]

V. Další třídy algeber

1. Obecné algebry

n-ární operací na množině A rozumíme zobrazení z $A^n = A\times\ldots\times A$ do A. Speciálně, 0-ární operace je zobrazení z jednoprvkové množiny do A, tedy *konstanta*. Místo 1-ární říkáme *unární*, místo 2-ární říkáme *binární*.

Typem algebry rozumíme zobrazení $\tau : \Omega \to \mathbb{N}\cup\{0\}$, kde Ω je nějaká množina (nazývá se *množina symbolů*). *Algebra typu* τ je dvojice $\mathbf{A} = (A, F)$, kde A je neprázdná množina (*nosná množina*) a F je zobrazení z množiny Ω do množiny všech operací na A přiřazující symbolu ω nějakou $\tau(\omega)$-ární operaci F_ω na A. Výsledek operace F_ω na prvcích $a_1,\ldots,a_{\tau(\omega)}$ zapisujeme jako $F_\omega(a_1,\ldots,a_{\tau(\omega)})$. Často se typ zapisuje zkráceně jako $(n_1,\ldots,n_k)$ a algebry tohoto typu jako $(A, f_1,\ldots,f_k)$, kde f_i je n_i-ární operace odpovídající i-tému symbolu. Binání operace se zpravidla značí symboly $+,\cdot,*,\circ$ apod., pro unární operace se používá $',-$ či $^{-1}$ (jako horní index, čti „inverz“).

Tučným písmem budeme vždy značit *algebry*, zatímco normálním písmem *množiny*. Není-li výslovně uvedeno jinak, označíme-li algebru $\mathbf{A}$, předpokládáme, že její nosná množina je A, a naopak. Výjimkou budou zavedená značení typu $\mathbb{Z},\mathbb{Q},\mathbb{R}$, která nám vnucují stejné značení pro nosnou množinu i algebru (v těchto případech je třeba vždy uvést, které oprace máme na mysli).

Vzhledem k tomu, že všechny třídy algeber studované v základním kurzu mají pouze konstanty, unární a binární operace, zavedeme následující pojmy pouze pro algebry s operacemi arity ≤ 2.

Řekneme, že podmnožina $B \subseteq A$ je *uzavřena* na

- binární operaci $*$, pokud pro každé $a, b \in B$ platí $a * b \in B$;
- unární operaci $'$, pokud pro každé $b \in B$ platí $b' \in B$;
- nulární operaci (konstantu) c, pokud $c \in B$.

Algebra $\mathbf{B}$ se nazývá *podalgebrou* algebry $\mathbf{A}$, pokud je množina $B \subseteq A$ je uzavřena na všechny operace algebry $\mathbf{A}$ a operace algebry $\mathbf{B}$ jsou restrikcemi operací algebry $\mathbf{A}$ na množinu B. Značíme $\mathbf{B} \le \mathbf{A}$.

Příklad. Uvažujeme-li množiny $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ s operacemi $+,\cdot$, pak $\mathbb{Z}\le\mathbb{Q}\le\mathbb{R}\le\mathbb{C}$.

Označme $M_n(X)$ množinu všech matic $n\times n$ s prvky z množiny X.

524. Pro která $u\in\mathbb{R}$ tvoří množina $A_u = \{z\in\mathbb{C} : |z| = u\}$ podalgebru algebry a) $(\mathbb{C},+)$, b) $(\mathbb{C},\cdot)$ c) $(\mathbb{C}\setminus\{0\},:)$? [Ř]

525. Rozhodněte, zda množina $B = \mathbb{R}\setminus\mathbb{Q}$ tvoří podalgebru algebry a) $(\mathbb{R},+)$, b) $(\mathbb{R},\cdot)$. [Ř]

526. Rozhodněte, zda regulární matice tvoří podalgebru algebry a) $(M_n(\mathbb{R}),+)$, b) $(M_n(\mathbb{R}),\cdot)$. [Ř]

527. Rozhodněte, pro která $u\in\mathbb{Z}$ tvoří množina $\{\left(\begin{smallmatrix} a & b \\ ub & a\end{smallmatrix}\right) : a,b\in\mathbb{Z}\}$ podalgebru algebry $(M_2(\mathbb{Z}),+,\cdot)$. [Ř]

528. Najděte nekonečné množství podalgeber algebry $(\mathbb{N},+,\cdot)$. [Ř]

529. Najděte všechny podalgebry algebry $\mathbf{A} = (\{a,b,c,d\}, f)$ typu (1), kde $f(a) = f(b) = c$ a $f(c) = f(d) = d$. [Ř]

530. Najděte všechny podalgebry algebry $\mathbf{A} = (\{1,2,3,a,b,c\}, f)$ typu (1), kde $f(a) = f(1) = 2$, $f(b) = f(2) = 3$, $f(c) = f(3) = 1$.

531. Najděte všechny podalgebry algebry $\mathbf{A} = (\mathbb{Z}, f)$ typu (1), kde $f(k) = k+1$. [Ř]

532. * Najděte všechny podalgebry algebry $\mathbf{A}_n = (\{0,\ldots,n-1\},*)$ typu (2), kde $a * b = a + b \bmod n$. [N] [Ř]

533. Buď $\mathbf{A} = (A, a, b, c)$, kde $a\ne b\ne c\ne a$, n-prvková algebra typu $(0,0,0)$. Kolik má tato algebra podalgeber? [Ř]

534. Buď $\mathbf{A} = (A,*)$ algebra typu (2). Ověřte, že množina $\{a\in A : (x*a)*y = x*(a*y)$ pro všechna $x,y\in A\}$ je buď prázdná, nebo tvoří podalgebru algebry $\mathbf{A}$. Uveďte příklad algebry, kdy je tato množina prázdná.

535. Buď $\mathbf{V}$ vektorový prostor nad tělesem $\mathbb{R}$ a uvažujme na množině V binární operace $*_r$ definované pro každé $r \in \mathbb{R}$ předpisem

$$u *_r v = ru + (1-r)v.$$

Dokažte, že

(a) algebra $(V, *_r : r \in (0,1))$ typu $(2,2,2,\ldots)$ má za podalgebry právě všechny konvexní podmnožiny prostoru $\mathbf{V}$;

(b) * algebra $(V, *_r : r \in \mathbb{R})$ typu $(2,2,2,\ldots)$ má za podalgebry právě všechny afinní podprostory prostoru $\mathbf{V}$.

Nejmenší podalgebra algebry $\mathbf{A}$ obsahující danou podmnožinu $X \subset A$ se nazývá *podalgebra generovaná množinou* X a značí se $\langle X \rangle_{\mathbf{A}}$. Řekneme, že algebra $\mathbf{A}$ je generovaná množinou X, pokud $\langle X \rangle_{\mathbf{A}} = \mathbf{A}$.

Prvky podalgebry $\langle X \rangle_{\mathbf{A}}$ můžeme najít tak, že začneme s prvky množiny X a aplikováním operací algebry $\mathbf{A}$ získáváme postupně další prvky. Ve chvíli, kdy už žádnou operací algebry $\mathbf{A}$ nedostaneme nic nového (tj. když už je zkonstruovaná množina *uzavřená* na operace algebry $\mathbf{A}$), máme celou $\langle X \rangle_{\mathbf{A}}$.

536. Ověřte, že $(\mathbb{N}, +) = \langle 1 \rangle$. Jaké prvky obsahuje $\langle 1 \rangle_{(\mathbb{N},\cdot)}$, $\langle 1 \rangle_{(\mathbb{Z},+)}$ a které prvky generují celé $(\mathbb{Z}, +)$? [Ř]

537. Dokažte, že $(\mathbb{N}, \cdot) = \langle 1, p : p \text{ je prvočíslo} \rangle$ a že tato algebra není konečně generovaná (tj. není generována žádnou konečnou množinou). [Ř]

538. Spočtěte prvky algeber $\langle 2,3,4 \rangle_{(\mathbb{N},+)}$, $\langle 2,3,4 \rangle_{(\mathbb{N},\cdot)}$ a $\langle 3,-10 \rangle_{(\mathbb{Z},+,\cdot)}$. [Ř]

539. Spočtěte prvky algeber $\langle 2 \rangle_{(\mathbb{Z},-)}$ a $\langle 2 \rangle_{(\mathbb{R},\sqrt[3]{\ })}$. Uvažujte $-$ jako unární operaci. [Ř]

540. Spočtěte prvky algeber $\langle 2 \rangle_{(\mathbb{Z},-)}$ a $\langle 2 \rangle_{(\mathbb{Q}\setminus\{0\},:)}$. Uvažujte $-$ jako binární operaci. [Ř]

541. Spočtěte prvky algeber $\langle \frac{1}{2}, \frac{2}{3} \rangle_{(\mathbb{Q},+,-)}$, $\langle \frac{1}{2}, \frac{2}{3} \rangle_{(\mathbb{Q},+,-,\cdot)}$ a $\langle \frac{2}{5}, \frac{2}{3} \rangle_{(\mathbb{Q},+,-)}$. [Ř]

542. Spočtěte prvky algeber $\langle -1, 2i \rangle_{(\mathbb{C},+)}$, $\langle \mathbb{R} \cup \{2i\} \rangle_{(\mathbb{C},+)}$ a $\langle 2i \rangle_{(\mathbb{C},+,-,\cdot)}$. [Ř]

543. Kolik prvků má algebra $\langle A \rangle_{(M_8(\mathbb{Z}),\cdot)}$? Zde

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 0 & 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

544. Ověřte, že $(M_2(\mathbb{Z}), +, -, \cdot) = \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \rangle$.

545. Buď $\mathbf{T}_3 = (T_3, \circ)$ algebra všech zobrazení na množině $\{1,2,3\}$ s operací skládání zobrazení. Ověřte, že $\mathbf{T}_3 = \langle \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \end{smallmatrix}\right) \rangle$, a dokažte, že tato algebra není generována žádnou dvouprvkovou množinou.

546. * Dokažte, že každá podalgebra algebry $(\mathbb{N}, +)$ je konečně generovaná.

547. * Buď $\mathbf{A}$ konečně generovaná algebra. Dokažte, že je-li $\mathbf{A} = \langle X \rangle$, pak existuje $Y \subseteq X$ konečná taková, že $\mathbf{A} = \langle Y \rangle$.

Direktním součinem algeber $\mathbf{A}_i$, $i = 1, \ldots, n$, stejného typu rozumíme algebru

$$\mathbf{A}_1 \times \cdots \times \mathbf{A}_n = (A_1 \times \cdots \times A_n, F),$$

přičemž její operace jsou definovány následovně:

- jsou-li $*_1, \ldots, *_n$ navzájem si odpovídající binární operace algeber $\mathbf{A}_1, \ldots, \mathbf{A}_n$, pak odpovídající operaci $*$ v algebře $\mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ definujeme předpisem

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 *_1 b_1, \ldots, a_n *_n b_n)$$

pro každé $a_1, b_1 \in A_1, \ldots, a_n, b_n \in A_n$.

- jsou-li $'^1, \ldots, '^n$ navzájem si odpovídající unární operace algeber $\mathbf{A}_1, \ldots, \mathbf{A}_n$, pak odpovídající operaci $'$ v algebře $\mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ definujeme předpisem

$$(a_1, \ldots, a_n)' = ((a_1)'^1, \ldots, (a_n)'^n)$$

  pro každé $a_1 \in A_1, \ldots, a_n \in A_n$.
- jsou-li $c_1, \ldots, c_n$ navzájem si odpovídající konstanty algeber $\mathbf{A}_1, \ldots, \mathbf{A}_n$, pak odpovídající konstantu c v algebře $\mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ definujeme předpisem

$$c = (c_1, \ldots, c_n).$$

Tedy operace provádíme po složkách, podobně jako s vektory. Pod pojmem *navzájem si odpovídající operace* rozumíme operace přiřazené témuž symbolu $\omega \in \Omega$.

548. Označme $\mathbf{N}_0 = (\mathbb{N} \cup \{0\}, +)$ a $\mathbf{N}_1 = (\mathbb{N}, +)$. Najděte minimální množinu generátorů (minimální vzhledem k inkluzi) algebry a) $\mathbf{N}_0 \times \mathbf{N}_0$, b) $\mathbf{N}_0 \times (\mathbb{N}, \cdot)$ c) $\mathbf{N}_1 \times \mathbf{N}_1$. Dokažte, že posledně jmenovaná algebra není konečně generovaná. [Ř]

549. Najděte tříprvkovou množinu generátorů algebry $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$. * Dokažte, že dvouprvková množina generátorů neexistuje.

550. Napište, jak vypadají operace algebry $\mathbf{A} = (\mathbb{Z}, +, \cdot) \times (\mathbb{Z}, \cdot, +)$. Spočtěte $\langle (1,0), (0,1) \rangle_{\mathbf{A}}$.

551. Buď $\mathbf{A}, \mathbf{B}$ algebry stejného typu a $\mathbf{C}, \mathbf{D}$ jejich podalgebry. Dokažte, že algebra $\mathbf{C} \times \mathbf{D}$ je podalgebrou algebry $\mathbf{A} \times \mathbf{B}$. Je každá podalgebra algebry $\mathbf{A} \times \mathbf{B}$ tohoto tvaru? [Ř]

552. Buď $\mathbf{A}, \mathbf{B}$ algebry stejného typu a $\mathbf{U}$ podalgebra algebry $\mathbf{A} \times \mathbf{B}$. Tvoří množina $\{a : (a, b) \in U$ pro nějaké $b \in B\}$ podalgebru algebry $\mathbf{A}$? [Ř]

Nechť $\mathbf{A}$ a $\mathbf{B}$ jsou algebry stejného typu. Zobrazení $\varphi : A \to B$ se nazývá *homomorfismus* algeber $\mathbf{A}$, $\mathbf{B}$, píšeme $\varphi : \mathbf{A} \to \mathbf{B}$, pokud

- pro každou binární operaci $*$ algebry $\mathbf{A}$ a odpovídající operaci $\circ$ algebry $\mathbf{B}$ platí pro každé $a, b \in A$

$$\varphi(a * b) = \varphi(a) \circ \varphi(b);$$

- pro každou unární operaci $'$ algebry $\mathbf{A}$ a odpovídající operaci $''$ algebry $\mathbf{B}$ platí pro každé $a \in A$

$$\varphi(a') = \varphi(a)'';$$

- pro každou konstantu c algebry $\mathbf{A}$ a odpovídající konstantu d algebry $\mathbf{B}$ platí

$$\varphi(c) = d.$$

Používá se následující terminologie:

- *monomorfismus*, neboli *vnoření*, je prostý homomorfismus (někdy se značí šipkou $\hookrightarrow$),
- *epimorfismus* je homomorfismus na (někdy se značí šipkou $\twoheadrightarrow$),
- *izomorfismus* je homomorfismus, který je bijekcí (užívá se symbol $\simeq$),

a dále

- *endomorfismem* algebry $\mathbf{A}$ rozumíme homomorfismus z $\mathbf{A}$ do $\mathbf{A}$,
- *automorfismem* nazýváme takový endomorfismus algebry $\mathbf{A}$, který je zároveň permutací.

Nechť $\mathbf{A}, \mathbf{B}, \mathbf{C}$ jsou algebry stejného typu a $\varphi : \mathbf{A} \to \mathbf{B}$ a $\psi : \mathbf{B} \to \mathbf{C}$ homomorfismy. Pak

(1) složené zobrazení $\psi \circ \varphi$ je homomorfismus $\mathbf{A} \to \mathbf{C}$;
(2) je-li φ izomorfismus, pak inverzní zobrazení φ^{-1} je izomorfismus $\mathbf{B} \to \mathbf{A}$.

553. Dokažte výše uvedené tvrzení o složení homomorfismů a inverzním izomorfismu.

554. Rozhodněte, které z následujících zobrazení jsou homomorfismy:

$$\alpha : (\mathbb{C}, \cdot) \to (\mathbb{R}, \cdot), \qquad z \mapsto |z|$$
$$\beta : (\mathbb{C}, +) \to (\mathbb{R}, +), \qquad z \mapsto |z|$$
$$\gamma : (\mathbb{R}, +) \to (\mathbb{R}, \cdot), \qquad x \mapsto 2^x$$
$$\delta : (\mathbb{C}, +, \cdot) \to (M_2(\mathbb{R}), +, \cdot), \qquad a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$
$$\varepsilon : (\mathbb{Z}, +, \cdot) \to (\{0, \ldots, n-1\}, +_{\bmod n}, \cdot_{\bmod n}), \qquad x \mapsto x \bmod n$$
$$\zeta : (\{0, \ldots, n-1\}, +_{\bmod n}, \cdot_{\bmod n}) \to (\mathbb{Z}, +, \cdot), \qquad x \mapsto x$$
$$\eta : (\{0, \ldots, n-1\}, +_{\bmod n}) \to (\mathbb{C}, \cdot), \qquad k \mapsto e^{2\pi i \cdot \frac{k}{n}}$$

Které z nich jsou vnoření a epimorfismy? [Ř]

555. Zjistěte, zda je zobrazení $x \mapsto x - [x]$, kde $[x]$ značí dolní celou část, homomorfismem $(\mathbb{R}, +) \to (\langle 0, 1), \oplus)$, přičemž $\oplus$ je sčítání „modulo 1“, tj. $x \oplus y = x + y - [x + y]$. [Ř]

556. Najděte všechny homomorfismy a) $(\mathbb{N}, +) \to (\mathbb{N}, +)$, b) $(\mathbb{N}, +, \cdot) \to (\mathbb{N}, +, \cdot)$, c) $(\mathbb{N}, +, 2) \to (\mathbb{N}, +, 10)$, d) $(\mathbb{N}, +) \to (\mathbb{N}, \cdot)$. [Ř]

557. Najděte všechny homomorfismy a) $(\mathbb{Z}, \cdot) \to (\mathbb{Z}, +)$, b) $(\mathbb{Z}, +) \to (\mathbb{N}, +)$, c) $(\mathbb{Z}, +) \to (\mathbb{N} \cup \{0\}, +)$, d)* $(\mathbb{Z}, +, \cdot) \to (\mathbb{Z}, +, \cdot)$. [Ř]

558. Označme $\mathbf{N}_0 = (\mathbb{N} \cup \{0\}, +)$ a $\mathbf{N}_1 = (\mathbb{N}, +)$. Najděte všechny homomorfismy a) $\mathbf{N}_0 \times \mathbf{N}_0 \to (\{1, -1\}, \cdot)$, b)* $\mathbf{N}_1 \times \mathbf{N}_1 \to (\{1, -1\}, \cdot)$. [Ř]

559. Buď $\mathbf{T}_n = (T_n, \circ)$ algebra všech zobrazení na množině $\{1, \ldots, n\}$ s operací skládání zobrazení. Rozhodněte, zda existuje homomorfismus a) $\mathbf{T}_n \to (\mathbb{N}, +)$, b) $\mathbf{T}_n \to (\{0, 1\}, \cdot)$. [Ř]

560. Najděte všechny homomorfismy $\mathbf{A} \to \mathbf{B}$, kde $\mathbf{A} = (\{a, b, c, d\}, f)$, $f(a) = f(b) = c$, $f(c) = f(d) = d$ a $\mathbf{B} = (\{0, 1\}, g)$, $g(0) = g(1) = 1$.

561. * Buď $\mathbf{A}_n = (\{0, \ldots, n-1\}, f_n)$ algebra s jednou unární operací definovanou předpisem $f_n(x) = (x + 1) \bmod n$. Pro dané m, n, nalezněte všechny homomorfismy $\mathbf{A}_n \to \mathbf{A}_m$.

562. * Najděte nějaké vnoření $(M_n(\mathbb{Z}), +) \to (M_{2n}(\mathbb{Z}), \cdot)$. [Ř]

563. Buď $f : \mathbf{A} \to \mathbf{B}$ homomorfismus algeber a $X \subseteq A$. Označme $\mathbf{C} = \langle X \rangle_{\mathbf{A}}$ a $\mathbf{D} = \langle f(X) \rangle_{\mathbf{B}}$. Dokažte, že $D = f(C)$.

564. Buď $f : \mathbf{A} \to \mathbf{B}$ homomorfismus algeber a $X \subseteq A$ takové, že $\mathbf{A} = \langle X \rangle$. Pomocí předchozího cvičení dokažte, že f je epimorfismus právě tehdy, když $\mathbf{B} = \langle f(X) \rangle$.

565. Nechť $\mathbf{A}, \mathbf{A}_1, \ldots, \mathbf{A}_n$ jsou algebry stejného typu a $f_i : \mathbf{A} \to \mathbf{A}_i$, $i = 1, \ldots, n$, homomorfismy. Dokažte, že zobrazení $f : \mathbf{A} \to \mathbf{A}_1 \times \ldots \times \mathbf{A}_n$, $a \mapsto (f_1(a), \ldots, f_n(a))$, je také homomorfismus.

Řekneme, že algebry $\mathbf{A}$ a $\mathbf{B}$ jsou *izomorfní*, značíme $\mathbf{A} \simeq \mathbf{B}$, pokud existuje izomorfismus $\mathbf{A} \to \mathbf{B}$. Neformálně řečeno, jak provádíme operace na prvcích algebry $\mathbf{A}$, tak provádíme odpovídající operace na obrazech těchto prvků v $\mathbf{B}$. Tedy izomorfní algebry mají stejné algebraické vlastnosti, jinými slovy, jsou „stejné až na přejmenování prvků“. Relace $\simeq$ je ekvivalencí na třídě všech algeber daného typu.

566. Dokažte, že algebry $(\{0, 1\}, +_{\bmod 2})$ a $(\{1, -1\}, \cdot)$ jsou izomorfní. [Ř]

567. Dokažte, že algebry $(\mathbb{R}^3, +, \times)$ a $\mathbf{SO}_3 = (SO_3, +, [.,.])$ jsou izomorfní. Operace $\times$ je vektorové násobení v $\mathbb{R}^3$. Algebra $\mathbf{SO}_3$ má nosnou množinu všech antisymetrických matic 3×3 nad reálnými čísly (antisymetrická matice znamená, že $a_{ij} = -a_{ji}$; spec. $a_{ii} = 0$), na které bereme operaci sčítání a tzv. *komutátor*, definovaný $[A, B] = AB - BA$. [?] [Ř]

Chceme-li dokázat, že dané dvě algebry *nejsou* izomorfní, obvykle se hledá tzv. *invariant*, tj. vlastnost V taková, že kdykoliv jsou nějaké algebry $\mathbf{A}, \mathbf{B}$ izomorfní a $\mathbf{A}$ má vlastnost V, pak $\mathbf{B}$ má vlastnost V. Obecně lze říci, že invariantem je jakákoliv vlastnost, kterou lze vyjádřit pomocí kvantifikátorů, logických spojek, proměnných, rovnítka a operací daných algeber. Eventuálně lze využívat dalších pojmů, které jsou podobným způsobem definovány. Např.

- počet prvků algebry je invariantem (mezi různě velkými množinami neexistuje vůbec žádná bijekce);

- minimální počet generátorů je invariantem;
- rovnosti (komutativita, asociativita, apod.);
- existence význačných prvků (např. vlastnosti typu „$\exists x \forall y\ x * y = x$“, což v lidském jazyce říká, že existuje něco jako nula vzhledem k násobení);
- pro grupy jsou velmi účinným invariantem řády prvků.

Příklad. Algebry $(\mathbb{N}, +)$ a $(\mathbb{R}, +)$ nejsou izomorfní hned z několika důvodů. Předně, nejsou stejně velké. Navíc $(\mathbb{N}, +) = \langle 1 \rangle$, kdežto algebru $(\mathbb{R}, +)$ nelze nagenerovat jedním prvkem. Kromě toho v $(\mathbb{R}, +)$ existuje nula (invariant „$\exists x \forall y\ y + x = y$“), v $\mathbb{N}$ nikoliv.

568. Dokažte, že vlastnosti uvedené v předchozím příkladě jsou invarianty.

569. Dokažte, že vlastnost $|\{a \in A |\ a \circ a = a\}| = n$ je invariantem pro každou algebru $(A, \circ)$ s binární operací $\circ$ a pro každé přirozené n.

570. Dokažte, že algebry $(\mathbb{C}, +)$ a $(\mathbb{R}, +) \times (\mathbb{R}, +)$ jsou izomorfní, avšak algebry $(\mathbb{C}, \cdot)$ a $(\mathbb{R}, \cdot) \times (\mathbb{R}, \cdot)$ nikoliv. [Ř]

571. Dokažte, že $(\mathbb{Z}, +) \not\simeq (\mathbb{N}, \cdot)$, $(\mathbb{Q}, +) \not\simeq (\mathbb{Q}^+, \cdot)$, zatímco $(\mathbb{R}, +) \simeq (\mathbb{R}^+, \cdot)$. [Ř]

572. Dokažte, že $(\mathbb{R}^2, \cdot) \not\simeq (\mathbb{R}^3, \cdot)$, zatímco $(\mathbb{R}^2, +) \simeq (\mathbb{R}^3, +)$.

573. Rozhodněte, které z následujících algeber jsou izomorfní: $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{R}^+, +)$, $(\mathbb{R}^+, \cdot)$. [Ř]

574. * Dokažte, že žádné dvě z následujících algeber nejsou izomorfní: $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}^+, +)$, $(\mathbb{Q}^+, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$.

575. Rozhodněte, zda jsou algebry $(\mathbb{Q}, \cdot)$ a $(\mathbb{Z}, \cdot) \times (\mathbb{N}, \cdot)$ izomorfní. [?]

V následujících úlohách značí $n\mathbb{N} = \{na : a \in \mathbb{N}\} = \{a \in \mathbb{N} : n \mid a\}$.

576. * Rozhodněte, které z následujících algeber jsou izomorfní: $(\mathbb{N}, \cdot)$, $(2\mathbb{N}, \cdot)$ $(3\mathbb{N}, \cdot)$, $(\mathbb{N} \setminus 2\mathbb{N}, \cdot)$. [Ř]

577. * Rozhodněte, pro která m, n je $(m\mathbb{N}, \cdot) \simeq (n\mathbb{N}, \cdot)$.

Relaci $\sim$ na množině X nazýváme *ekvivalence*, pokud je

(1) *reflexivní*, tj. $x \sim x$ pro všechna x,
(2) *tranzitivní*, tj. $x \sim y$ a $y \sim z$ implikuje $x \sim z$,
(3) a *symetrická*, tj. $x \sim y$ právě tehdy, když $y \sim x$.

Blokem (nebo *třídou*) ekvivalence $\sim$ příslušnou prvku $x \in X$ rozumíme množinu

$$[x]_\sim = \{y \in X : x \sim y\}.$$

Pro daná x, y jsou příslušné bloky buď stejné (pokud $x \sim y$), nebo disjunktní; tvoří tedy *rozklad* množiny X.

Naopak, každému disjunktnímu rozkladu $X = \bigcup_{B \in \mathcal{B}} B$ přísluší ekvivalence definovaná předpisem $x \sim y$, pokud x, y leží ve stejném bloku.

578. Spočtěte počet ekvivalencí na tří, čtyř a pětiprvkové množině.

579. Rozhodněte, zda následující relace jsou ekvivalence:

(1) Na množině $\mathbb{N}$ definujeme $a \sim b \ \Leftrightarrow\ a + b$ je sudé.
(2) Na množině $P(\mathbb{N})$ všech podmnožin definujeme $A \sim B \ \Leftrightarrow\ A = B$ nebo $A \cap B = \emptyset$.
(3) Na množině $\mathbb{C}$ definujeme $a \sim b \ \Leftrightarrow\ |a| = |b|$.

Pokud ano, kolik mají bloků? [Ř]

580. Buď $\mathbf{G} = (V, E)$ graf, definujme na množině V relaci $a \sim b \ \Leftrightarrow$ existuje cesta mezi vrcholy a, b. Jde o ekvivalenci? Co jsou její bloky? Jaká by byla odpověď, kdybychom uvažovali orientované cesty v orientovaném grafu? [Ř]

Buď $\mathbf{A}$ algebra. Ekvivalence $\sim$ na nosné množině A se nazývá *kongruence* algebry $\mathbf{A}$, pokud

- pro každou binární operaci $*$ algebry $\mathbf{A}$

$$a \sim c,\ b \sim d \quad \text{implikuje} \quad a * b \sim c * d;$$

- pro každou unární operaci $'$ algebry $\mathbf{A}$

$$a \sim b \quad \text{implikuje} \quad a' \sim b'.$$

Každá algebra $\mathbf{A}$ má alespoň dvě kongruence, říká se jim *nevlastní*: je to nejmenší kongruence $id = \{(a,a) : a \in A\}$ a největší kongruence $A \times A = \{(a,b) : a,b \in A\}$. Algebra, která jiné kongruence nemá, se nazývá *jednoduchá*.

581. Dokažte, že podmínka pro binární operaci $*$ je ekvivalentní následující podmínce:

Pro každé $a \sim b$ a každé c platí $a * c \sim b * c$ a $c * a \sim c * b$.

Na blocích ekvivalence $\sim$ definujeme operace předpisy

- $[a] * [b] := [a * b]$ pro každou binární operaci $*$ algebry $\mathbf{A}$;
- $[a]' := [a']$ pro každou unární operaci $'$ algebry $\mathbf{A}$;
- $C := [c]$ pro každou konstantu c algebry $\mathbf{A}$.

Algebra

$$\mathbf{A}/\!\sim = (\{[a] : a \in A\}, G)$$

stejného typu jako $\mathbf{A}$ s výše uvedenými operacemi se nazývá *faktoralgebra algebry* $\mathbf{A}$ *podle kongruence* $\sim$.

582. Definujme relaci $x \sim y \Leftrightarrow |x| = |y|$ na množině komplexních čísel. Rozhodněte, zda jde o kongruenci algebry a) $(\mathbb{C}, +)$, b) $(\mathbb{C}, \cdot)$. [Ř]

583. Definujme relaci $A \sim B \Leftrightarrow \det A = \det B$ na množině reálných matic $n \times n$. Rozhodněte, zda jde o kongruenci algebry a) $(\mathbf{M}_n(\mathbb{R}), +)$, b) $(\mathbf{M}_n(\mathbb{R}), \cdot)$. [Ř]

584. Definujme relaci $x \sim y \Leftrightarrow x - [x] = y - [y]$ na množině reálných čísel. Rozhodněte, zda jde o kongruenci algebry a) $(\mathbb{R}, +)$, b) $(\mathbb{R}, -)$, c) $(\mathbb{R}, \cdot)$. [Ř]

585. Najděte všechny kongruence algebry $\mathbf{A} = (\{a,b,c,d\}, f)$ typu (1), kde $f(a) = f(b) = c$ a $f(c) = f(d) = d$.

586. Najděte všechny kongruence algebry $\mathbf{A} = (\{0, \ldots, n-1\}, f)$ typu (1), kde $f(k) = k + 1 \pmod n$.

587. * Popište všechny algebry typu (1), které mají jen dvě kongruence.

588. * Buď $\mathbf{G} = (G, *, ', e)$ grupa a $\mathbf{N}$ její normální podgrupa. Definujme relaci na G předpisem $a \sim b$ právě tehdy, když $a * b' \in N$. Dokažte, že $\sim$ je kongruencí grupy $\mathbf{G}$.

589. * Buď $\mathbf{G} = (G, *, ', e)$ grupa a $\sim$ její kongruence. Dokažte, že blok $[e]$ tvoří normální podgrupu této grupy.

590. * Buď $\mathbf{R} = (R, +, -, \cdot, 0)$ okruh a $\mathbf{I}$ jeho ideál. Definujme relaci na R předpisem $a \sim b$ právě tehdy, když $a - b \in I$. Dokažte, že $\sim$ je kongruencí okruhu $\mathbf{R}$.

591. * Buď $\mathbf{R} = (R, +, -, \cdot, 0)$ okruh a $\sim$ jeho kongruence. Dokažte, že blok $[0]$ tvoří ideál tohoto okruhu.

Binární operace se často zapisují pomocí tzv. *Cayleyovy tabulky*. Hodnotu $a * b$ nalezneme na řádku popsaném hodnotou a v sloupci popsaném hodnotou b. Např.

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

jsou Cayleovy tabulky logických operací $\wedge$ a $\vee$ na hodnotách 0,1.

592. Definujme algebry $\mathbf{A} = (\{a,b,c\}, *)$ a $\mathbf{B} = (\{a,b,c,d,e\}, \circ)$ typu (2), kde operace $*, \circ$ jsou dány tabulkami

$*$	a	b	c
a	a	c	b
b	a	c	c
c	a	b	c

$\circ$	a	b	c	d	e
a	a	e	c	a	a
b	e	d	e	b	b
c	a	e	c	a	c
d	c	b	a	e	e
e	a	e	a	d	b

Najděte všechny podalgebry a kongruence těchto algeber.

593. Definujme algebry $\mathbf{A} = (\{0,1\}, *)$ a $\mathbf{B} = (\{0,1,2,3\}, \circ)$ typu (2), kde operace $*, \circ$ jsou dány tabulkami

$*$	0	1
0	0	1
1	0	0

$\circ$	0	1	2	3
0	0	1	2	3
1	0	2	0	2
2	0	3	0	3
3	0	0	0	0

Rozhodněte, zda jsou následující zobrazení homomorfismy těchto algeber:

(1) $\varphi : A \to A$, $\varphi(0) = \varphi(1) = 0$.
(2) $\varphi : A \to A$, $\varphi(0) = \varphi(1) = 1$.
(3) $\varphi : A \to B$, $\varphi(0) = 0$, $\varphi(1) = 2$.
(4) $\varphi : B \to A$, $\varphi(0) = \varphi(2) = 0$, $\varphi(1) = \varphi(3) = 1$.
(5) $\varphi : B \to B$, $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(2) = \varphi(3) = 2$.

[Ř]

594. Najděte všechny podalgebry a kongruence algebry $(\mathbb{N}, *)$ typu (2), kde $a*b = \max(a,b)+1$.

2. Svazy

Svazem nazýváme algebru $\mathbf{L} = (L, \wedge, \vee)$ typu $(2,2)$ splňující pro každé $x, y, z \in L$ podmínky

(1) $x \vee (y \vee z) = (x \vee y) \vee z$ a $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ *(asociativita)*;
(2) $x \vee y = y \vee x$ a $x \wedge y = y \wedge x$ *(komutativita)*;
(3) $x \vee x = x$ a $x \wedge x = x$ *(idempotence)*;
(4) $x \vee (x \wedge y) = x$ a $x \wedge (x \vee y) = x$ *(absorpce)*.

Jak je vidět z následujících čtyřech cvičení, svazy a svazově uspořádané množiny jsou de facto totéž, jde jen o formu zápisu (jednou jde o uspořádání, podruhé o algebru). Tyto pojmy budeme volně zaměňovat.

595. * Buď $(L, \wedge, \vee)$ svaz a definujme relaci $\leq$ na L podmínkou

$$a \leq b \iff a \wedge b = a.$$

Dokažte, že $(L, \leq)$ je svazově uspořádaná množina.

596. Buď $(L, \leq)$ svazově uspořádaná množina a označme $a \wedge b = \inf(a,b)$ a $a \vee b = \sup(a,b)$. Dokažte, že algebra $(L, \wedge, \vee)$ je svaz.

597. Buď $(L, \wedge, \vee)$ svaz, vytvořme z něj výše uvedenými způsoby nejprve svazově uspořádanou množinu, a poté zpátky svaz. Dokažte, že obdržíme zpět původní svaz.

598. Buď $(L, \leq)$ svazově uspořádaná množina, vytvořme z ní výše uvedenými způsoby nejprve svaz, a poté zpátky svazově uspořádanou množinu. Dokažte, že obdržíme zpět původní uspořádání.

599. Co jsou operace $\wedge, \vee$ ve svazu $\mathbf{P}(X)$? [Ř]

600. Co jsou operace $\wedge, \vee$ ve svazu $\mathbf{Eq}(X)$? Dokažte, že $\wedge$ je průnik a že spojením ekvivalencí $\sim$ a $\approx$ je ekvivalence

$$\{(a,b) \in X \times X : \exists u_0, \ldots, u_n \in X \; a = u_0 \sim u_1 \approx u_2 \sim u_3 \approx u_4 \cdots u_n = b\}.$$

601. Dokažte, že ve svazu $\mathbf{Sub}(\mathbf{A})$ je $B \wedge C = B \cap C$ a $B \vee C$ je nosná množina podalgebry $\langle B \cup C \rangle_{\mathbf{A}}$.

602. * Co jsou operace $\wedge, \vee$ ve svazu $\mathbf{Sub}(\mathbf{A})$? [Ř]

603. * Co jsou operace $\wedge, \vee$ ve svazu $\mathbf{Con}(\mathbf{A})$? [Ř]

604. Nakreslete všechny (až na izomorfismus) svazy s nejvýše pěti prvky.

Dále se budeme věnovat algebraickým vlastnostem svazů.

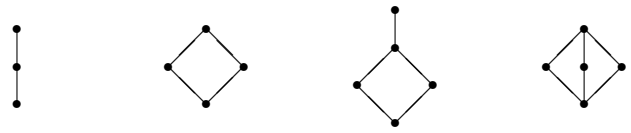
605. Rozhodněte, zda následující množiny tvoří podsvaz svazu $\mathcal{P}(\mathbb{N})$: a) konečné podmnožiny $\mathbb{N}$, b) podmnožiny množiny sudých čísel, c) podmnožiny $\mathbb{N}$ uzavřené na operaci sčítání, d) podmnožiny $\mathbb{N}$ obsahující prvek 1. [Ř]

606. Buď $\mathbf{A}$ algebra. Rozhodněte, a) zda $\mathbf{Sub}(\mathbf{A})$ tvoří podsvaz svazu $\mathbf{P}(A)$, b) zda $\mathbf{Con}(\mathbf{A})$ tvoří podsvaz svazu $\mathbf{Eq}(A)$. [Ř]

607. ** Buď X konečná množina. Najděte nejmenší množinu generátorů svazu $\mathbf{Eq}(X)$. [Ř]

608. Buď $\mathbf{L}_1, \mathbf{L}_2$ svazy a $\varphi : L_1 \to L_2$ bijekce splňující $x \leq y$ právě tehdy, když $\varphi(x) \leq \varphi(y)$. Dokažte, že je φ izomorfismus $\mathbf{L}_1 \simeq \mathbf{L}_2$.

609. a) Zjistěte, zda jsou následující svazy *jednoduché*, tj. zda mají jen 2 kongruence. b) Spočtěte svazy kongruencí těchto svazů. [Ř]



610. * Buď $\mathbf{V}$ vektorový prostor nad tělesem $\mathbf{T}$ *konečné* dimenze alespoň 2. Dokažte, že svaz $\mathbf{Sub}(\mathbf{V})$ jeho podprostorů je jednoduchý. [N]

611. ** Buď $\mathbf{V}$ vektorový prostor nad tělesem $\mathbf{T}$ *nekonečné* dimenze. Dokažte, že svaz $\mathbf{Sub}(\mathbf{V})$ jeho podprostorů *není* jednoduchý. [Ř]

Svaz se nazývá *modulární*, pokud pro každé $a \leq b$ a každé c platí rovnost

$$(c \vee a) \wedge b = (c \wedge b) \vee a.$$

Svaz se nazývá *distributivní*, pokud pro každé a, b, c platí rovnosti

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad \text{a} \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Označme následující svazy

Svaz je modulární právě tehdy, když neobsahuje podsvaz izomorfní svazu $\mathbf{N}_5$. Svaz je distributivní právě tehdy, když neobsahuje podsvaz izomorfní svazu $\mathbf{M}_3$ ani $\mathbf{N}_5$.

612. Dokažte, že svaz $\mathbf{M}_3$ je modulární, ale není distributivní. Dokažte, že $\mathbf{N}_5$ není modulární.

613. * Dokažte, že pokud svaz není modulární, obsahuje podsvaz izomorfní $\mathbf{N}_5$.

614. Dokažte, že svaz splňuje pro každé a, b, c rovnost $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ právě tehdy, když splňuje pro každé a, b, c rovnost $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

615. Dokažte, že distributivní svazy jsou modulární.

616. Rozhodněte, zda je svaz $\mathbf{P}(X)$ a) modulární, b) distributivní. [Ř]

617. Rozhodněte, pro která n je svaz $\mathbf{Eq}(n)$ a) modulární, b) distributivní. [Ř]

618. Rozhodněte, zda je svaz $(\mathbb{N}, |)$ a) modulární, b) distributivní. [N] [Ř]

619. Označme D_n množinu všech dělitelů čísla n. Dokažte, že existuje množina X taková, že $(D_n, |) \simeq \mathbf{P}(X)$ právě tehdy, když n není dělitelné žádnou druhou mocninou prvočísla. [Ř]

620. Buď C množina všech konvexních podmnožin roviny $\mathbb{R}^2$. Dokažte, že je $(C, \subseteq)$ svaz (co jsou operace $\vee, \wedge$?) a rozhodněte, zda je a) modulární, b) distributivní.

621. Buď $\mathbf{V}$ vektorový prostor nad tělesem $\mathbf{T}$ dimenze alespoň 2. Rozhodněte, zda je svaz $\mathbf{Sub}(\mathbf{V})$ jeho podprostorů a) modulární, b) distributivní. [Ř]

622. Uvažujme svazy $(Sub(\mathbf{G}), \subseteq)$, kde $\mathbf{G}$ je grupa.

a) Najděte příklad grupy $\mathbf{G}$, kde $(Sub(\mathbf{G}), \subseteq)$ není modulární.
b) Dokažte, že pro abelovskou grupu $\mathbf{G}$ je svaz $(Sub(\mathbf{G}), \subseteq)$ vždy modulární. Můžete využít faktu, že $A \vee B = A + B = \{a + b : a \in A, b \in B\}$ (což v neabelovských grupách neplatí).
c) Najděte příklad abelovské grupy $\mathbf{G}$, kde $(Sub(\mathbf{G}), \subseteq)$ není distributivní.

623. Je svaz $\mathbf{Sub}(\mathbf{A})$ pro každou algebru $\mathbf{A}$ distributivní? Je modulární? Pokud ano, dokažte, pokud ne, uveďte protipříklad.

624. Je svaz $\mathbf{Con}(\mathbf{A})$ pro každou algebru $\mathbf{A}$ distributivní? Je modulární? Pokud ano, dokažte, pokud ne, uveďte protipříklad.

625. Je svaz $\mathbf{Sub}(\mathbf{L})$ pro každý svaz $\mathbf{L}$ distributivní? Je modulární? Pokud ano, dokažte, pokud ne, uveďte protipříklad.

626. * Je svaz $\mathbf{Con}(\mathbf{L})$ pro každý svaz $\mathbf{L}$ distributivní? Je modulární? Pokud ano, dokažte, pokud ne, uveďte protipříklad. `[Ř]`

627. Buď C množina všech konvexních podmnožin roviny. Dokažte, že je $(C, \subseteq)$ svaz (co jsou operace $\vee, \wedge$?) a rozhodněte, zda je a) modulární, b) distributivní. `[Ř]`

628. * Buď X neprázdná množina a uvažujme algebru $\mathbf{B}(X) = (P(X), \cap, \cup, ', \emptyset, X)$ (zde $'$ značí doplněk množiny). Dokažte, že $\mathbf{Sub}(\mathbf{B}(X)) \simeq \mathbf{Eq}(X)^\delta$, kde $\mathbf{L}^\delta$ značí duální svaz k $\mathbf{L}$, tedy $(L, \wedge, \vee)^\delta = (L, \vee, \wedge)$. `[N]`

629. Dokažte, že svaz $\mathbf{L}$ je distributivní právě tehdy, když každý interval $[a, b]$ v $\mathbf{L}$ má vlastnost, že každý prvek má nejvýše jeden komplement. Intervalem $[a, b]$ rozumíme podsvaz $\{x \in L : a \leq x \leq b\}$. (Svaz $\mathbf{L}$ nemusí být omezený, ale interval vždy omezený je, proto má smysl mluvit o komplementech.)

630. Podmožina A svazu $\mathbf{L}$ se nazývá ideál, pokud je uzavřená na spojení a pro každé $a < b \in A$ platí $a \in A$. Dokažte, že ideály svazu $\mathbf{L}$ tvoří úplný svaz vzhledem k inkluzi. Je to podsvaz svazu $\mathbf{P}(L)$? Najděte prostý homomorfismus z $\mathbf{L}$ do tohoto svazu.

Booleovy algebry.

631. Dokažte, že Booleova algebra $\mathbf{P}(X)$ je izomorfní direktní mocnině $\mathbf{2}^{|X|}$. Zde $\mathbf{P}(X)$ značí algebru všech podmnožin množiny X a $\mathbf{2}$ dvouprvkovou Booleovu algebru.

632. Uveďte příklad distributivního svazu, který není Booleovou algebrou. Uveďte příklad komplementárního svazu, který není Booleovou algebrou.

633. Dokažte, že kongruence Booleových algeber si vzájemně jednoznačně odpovídají s filtry.

634. Buď $\mathbf{R}$ okruh splňující $x^2 = x$ pro všechna $x \in R$. Definujme operace $x \wedge y = xy$ a $x \vee y = x + y + xy$. Dokažte, že pro jistou operaci $'$ je $(R, \wedge, \vee, ', 0, 1)$ Booleova algebra.

635. Buď $\mathbf{B}$ Booleova algebra. Definujme operace $x + y = (x \vee y) \wedge (x \wedge y)'$ a $xy = x \wedge y$. Dokažte, že pro jistou operaci $-$ je $(B, +, -, \cdot, 0)$ okruh splňující $x^2 = x$ pro všechna $x \in B$.

VI. Teorie těles

1. Příklady a základní vlastnosti

Tělesem rozumíme komutativní okruh s jednotkou, jehož každý nenulový prvek je invertibilní. (Někteří autoři definují tělesa tak, že nemusejí být nutně komutativní; je-li to nutné, pak výslovně uvádějí „komutativní těleso“.) Nejdůležitějšími příklady jsou

- těleso *komplexních čísel* $\mathbb{C}$ a jeho podtělesa ($\mathbb{Q}$, $\mathbb{R}$ a další, viz následující sekce);
- a dále *konečná tělesa* ($\mathbb{Z}_p$ a další, viz níže).

Dále připomeňme

- konstrukci *podílového tělesa* daného oboru integrity;
- a konstrukci těles jako faktorokruhů podle maximálních ideálů.

Charakteristikou tělesa rozumíme nejmenší $n \in \mathbb{N}$ takové, že $\underbrace{1+\ldots+1}_{n} = 0$, pokud takové n existuje, resp. 0 v opačném případě. Charakteristika tělesa je zaručeně 0 nebo prvočíslo. Nejmenší podtěleso (musí obsahovat prvek 1) se nazývá *prvotěleso*; je izomorfní buď $\mathbb{Q}$ (v charakteristice 0) nebo $\mathbb{Z}_p$ (v charakteristice p).

636. Dokažte, že $\mathbb{Z}_n$ je těleso právě tehdy, když n je prvočíslo. [Ř]

637. Buď $\mathbf{R}_1, \ldots, \mathbf{R}_n$ okruhy. Za jakých podmínek je direktní součin $\mathbf{R}_1 \times \cdots \times \mathbf{R}_n$ tělesem? [Ř]

638. 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]

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

640. * Řešte následující rovnice v podílovém tělese oboru $\mathbb{R}[x]$: a) $f^4 = 1$, b) $f^2 - f = x$. [?]

641. Dokažte, že v tělese charakteristiky p platí $(x+y)^{p^m} = x^{p^m} + y^{p^m}$ pro libovolné $m \in \mathbb{N}$. [Ř]

642. Uveďte příklad nekonečného tělesa charakteristiky > 0. [Ř]

Každé konečné těleso $\mathbf{T}$ má p^k prvků, kde p je prvočíslo rovné charakteristice $\mathbf{T}$ a k je přirozené číslo; p^k-prvkové těleso existuje právě jedno až na izomorfismus a značí se $\mathbb{F}_{p^k}$.

- $\mathbb{F}_p = \mathbb{Z}_p$;
- $\mathbb{F}_{p^k}$ pro $k > 1$ lze reprezentovat jako faktorokruh $\mathbb{Z}_p[x]/f$, kde f je (libovolný) ireducibilní polynom stupně k v $\mathbb{Z}_p[x]$. (Uvědomte si, že $\mathbb{F}_{p^k}$ není ani $\mathbb{Z}_{p^k}$ ani $(\mathbb{Z}_p)^k$!)

Multiplikativní grupa konečného tělesa je cyklická. Její generátory se nazývají *primitivní prvky*.

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

644. 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]

645. 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]

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

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

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

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

650. Dokažte, že v konečném tělese charakteristiky p je zobrazení $x \mapsto x^p$ automorfismus. [Ř]

651. Dokažte, že v $\mathbb{F}_q$ platí $a^{p^k} = a$ pro každé a. [Ř]

652. Dokažte, že v $\mathbb{F}_q[x]$ platí $x^q - x = \prod_{a \in \mathbb{F}_q} x - a$. [Ř]

653. 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]

654. 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]

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

Označme $N_p(k)$ počet ireducibilních polynomů stupně k v $\mathbb{Z}_p[x]$.

656. * Dokažte, že $\sum_{d|k} N_p(d)d = p^k$.

657. * Dokažte, že $N_p(k) = \frac{1}{k} \cdot (\sum_{d|k} \mu(k/d)p^d)$. [N]

658. Dokažte, že $N_p(k) \neq 0$ pro každé prvočíslo p a $k \in \mathbb{N}$.
(Tedy existuje konečné těleso velikosti p^k pro každé prvočíslo p a $k \in \mathbb{N}$.)

2. Rozšíření konečného stupně

Rozšířením těles $\mathbf{T} \leq \mathbf{S}$ rozumíme situaci, kdy $\mathbf{T}$ je podtěleso $\mathbf{S}$.
Minimálním polynomem prvku $a \in S$ nad tělesem $\mathbf{T}$ rozumíme monický polynom $m_{a,\mathbf{T}} \in T[x]$ splňující

(1) $m_{a,\mathbf{T}}(a) = 0$;
(2) každý polynom $f \in T[x]$ splňující $f(a) = 0$ je dělitelný polynomem $m_{a,\mathbf{T}}$.

Minimální polynom je v $\mathbf{T}[x]$ ireducibilní a platí i opačné tvrzení: je-li a kořen monického ireducibilního polynomu $f \in T[x]$, pak $f = m_{a,\mathbf{T}}$.

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

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

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

662. 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]

Prvek $a \in S$ nazýváme *algebraický* nad $\mathbf{T}$, pokud je kořenem nějakého nenulového polynomu z $\mathbf{T}[x]$; v opačném případě jej nazýváme *transcendentní*. Je-li každý prvek tělesa $\mathbf{S}$ algebraický nad $\mathbf{T}$, hovoříme o *algebraickém rozšíření*. Ke každému algebraickému prvku existuje právě jeden minimální polynom.

Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a_1, \ldots, a_n \in S$. Pak $\mathbf{T}(a_1, \ldots, a_n)$ značí nejmenší podtěleso $\mathbf{S}$ obsahující $\mathbf{T}$ i $a_1, \ldots, a_n$. Jsou-li prvky $a_1, \ldots, a_n$ algebraické nad $\mathbf{T}$, pak $\mathbf{T}(a_1, \ldots, a_n) = \mathbf{T}[a_1, \ldots, a_n]$.

Nadtěleso $\mathbf{S} \geq \mathbf{T}$ lze považovat za vektorový prostor nad tělesem $\mathbf{T}$. Jeho dimenze se nazývá *stupeň rozšíření* $\mathbf{T} \leq \mathbf{S}$ a značí se $[\mathbf{S} : \mathbf{T}]$. Je-li stupeň $[\mathbf{S} : \mathbf{T}]$ konečný, říkáme, že jde o rozšíření *konečného stupně*. Platí následující tvrzení:

- Jsou-li $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$ rozšíření těles, platí
$$[\mathbf{U} : \mathbf{T}] = [\mathbf{U} : \mathbf{S}] \cdot [\mathbf{S} : \mathbf{T}].$$
- Je-li a algebraický nad $\mathbf{T}$, pak
$$[\mathbf{T}(a) : \mathbf{T}] = \deg m_{a,\mathbf{T}}.$$
- Rozšíření konečného stupně jsou algebraická.
- Rozšíření $\mathbf{T} \leq \mathbf{S}$ je konečného stupně právě tehdy, když $\mathbf{S} = \mathbf{T}(a_1, \ldots, a_n)$ pro nějaké prvky $a_1, \ldots, a_n \in S$ algebraické nad $\mathbf{T}$.

663. 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]

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

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

666. * 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.

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

668. 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]

669. 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]

670. Dokažte, že množina všech algebraických prvků nad tělesem $\mathbb{Q}$ je spočetná. [N]

671. Buď $a \in \mathbb{C}$ transcendentní nad $\mathbb{Q}$. Spočtěte $[\mathbb{Q}(a) : \mathbb{Q}]$. [Ř]

672. Spočtěte $[\mathbb{R} : \mathbb{Q}]$. [Ř]

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

674. 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 $\mathbb{Q}$.

675. 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]

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

677. 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]

678. 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.

679. 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. [?]

680. 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 $\mathbf{T}(a)[x]$. [?]

681. * 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 $\{\sum_{i=0}^{n} a_i b_i : n \in \mathbb{N}, a_i \in U, b_i \in V\}$.

682. * 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.

683. * 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.

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

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

Mezi klasické starořecké úlohy patřily konstrukce pomocí pravítka a kružítka. Teorie rozšíření konečného stupně umožňuje dokázát, že některé konstrukce nejsou proveditelné.

Konstrukcí pravítkem a kružítkem rozumíme posloupnost $\mathcal{M}_0 \subseteq \mathcal{M}_1 \subseteq \ldots \subseteq \mathcal{M}_n$ konečných množin bodů v rovině takových, že $\mathcal{M}_{i+1} = \mathcal{M}_i \cup \{X\}$, kde X vznikne jako

(1) průsečík přímky AB a přímky CD;
(2) průsečík přímky AB a kružnice se středem C a poloměrem $|DE|$;
(3) průsečík kružnice se středem A a poloměrem $|BC|$ a kružnice se středem D a poloměrem $|EF|$

pro nějaké body $A, B, C, D, E, F \in \mathcal{M}_i$.

686. 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!)

687. 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.

Zvolme v rovině souřadnice a uvažujme nejmenší těleso $\mathbf{T}_i$, které obsahuje x-ové i y-ové souřadnice všech bodů z $\mathcal{M}_i$. Dostáváme řetězec rozšíření těles $\mathbf{T}_0 \leq \mathbf{T}_1 \leq \mathbf{T}_2 \leq \ldots \leq \mathbf{T}_n$. Stěžejním krokem pro řešení uvedených úloh je následující tvrzení.

Tvrzení. $[\mathbf{T}_n : \mathbf{T}_0]$ *je mocnina čísla 2.*

688. * Dokažte, že $[\mathbf{T}_{i+1} : \mathbf{T}_i]$ je 1 nebo 2. [N]

689. Pomocí předchozího cvičení dokažte Tvrzení. [Ř]

Reálné číslo a nazveme *konstruovatelné*, pokud lze z úsečky délky 1 sestrojit úsečku délky a.

690. 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]

691. 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]

692. 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.

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

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

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

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

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

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

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

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

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

3. Kořenová a rozkladová nadtělesa, algebraický uzávěr

Kořenová a rozkladová nadtělesa - DOPLNIT

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

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

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

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

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

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

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

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

710. 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 $\mathbb{Q}$.

711. 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]

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

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

714. Buď $\mathbf{T}$ těleso obsahující primitivní m-tou odmocninu z jedné pro nějaké $m > 1$. Buď $a, b \in T$ takové, že polynomy $f = x^m - a$, $g = x^m - b$ jsou ireducibilní. Dokažte, že mají

polynomy f, g stejná rozkladová nadtělesa právě tehdy, když $b = c^m a^r$ pro nějaké $c \in T$ a $r \in \mathbb{N}$ splňující $\mathrm{NSD}(r, m) = 1$. [?]

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

716. * 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 $x^{p^m-1} - 1$.

717. 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 $n \mid m$.

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

Algebraický uzávěr - DOPLNIT

719. Dokažte, že konečná tělesa nejsou algebraicky uzavřená. [Ř]

720. * Buď $\mathbf{T}$ těleso. Dokažte, že podílové těleso oboru $\mathbf{T}[x]$ není algebraicky uzavřené. [?]

721. * Dokažte, že algebraický uzávěr nekonečného tělesa $\mathbf{T}$ má stejnou velikost jako $\mathbf{T}$. [N]

722. Buď $\mathbf{T}_1$, $\mathbf{T}_2$ dvě algebraicky uzavřená tělesa stejné charakteristiky. Dokažte, že se dá vnořit $\mathbf{T}_1$ do $\mathbf{T}_2$ nebo naopak. [?]

4. Galoisova teorie

Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles. $\mathbf{T}$-*homomorfismem* tělesa $\mathbf{S}$ rozumíme homomorfismus φ tělesa $\mathbf{S}$ splňující $\varphi(x) = x$ pro každé $x \in T$.

723. 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 $\mathbf{S}$.

724. 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 $\mathbf{S}_2$.

Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles. *Galoisova grupa* $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$ je grupa všech $\mathbf{T}$-automorfismů tělesa $\mathbf{S}$. Je-li $\mathbf{S}$ rozkladové nadtěleso polynomu $f \in T[x]$, pak

(1) $\mathbf{Gal}(\mathbf{S}/\mathbf{T})$ se vnořuje do symetrické grupy $\mathbf{S}_n$, kde n je počet různých kořenů polynomu f;
(2) je-li f ireducibilní, pak pro každé dva kořeny a, b existuje $\varphi \in \mathbf{Gal}(\mathbf{S}/\mathbf{T})$ takový, že $\varphi(a) = b$.

Je-li $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$ rozšíření těles a obě tělesa $\mathbf{S}, \mathbf{U}$ jsou rozkladová pro nějaké polynomy z $\mathbf{T}[x]$, pak platí

(3) $\mathbf{Gal}(\mathbf{U}/\mathbf{T})/\mathbf{Gal}(\mathbf{U}/\mathbf{S}) \simeq \mathbf{Gal}(\mathbf{S}/\mathbf{T})$.

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

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

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

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

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

730. 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) $x^3 + 2$.

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

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

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

734. 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) $x^4 + 6x^2 + 6$.

735. * 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.

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

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

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

739. ** Buď $f \in \mathbb{Q}[x]$ ireducibilní polynom prvočíselného stupně p, který má 2 imaginární a $p-2$ reálných kořenů. Buď $\mathbf{T}$ je rozkladové nadtěleso polynomu f nad $\mathbb{Q}$. Dokažte, že $\mathbf{Gal}(\mathbf{T}/\mathbb{Q}) \simeq \mathbf{S}_p$.

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

741. * Dokažte, že $\mathbf{Gal}(\mathbb{C}/\mathbb{Q})$ je nekonečná. (Je potřeba axiom výběru.)

NÁVODY

5. Infima jsou průniky, suprema jsou sjednocení. **6.** Infima jsou průniky, stačí tedy popsat největaí prvek. (Suprema nejsou sjednocení!!) **16.** 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. **17.** Dosazením několika hodnot odhadněte výsledek jako polynom čtvrtého stupně a dokaľte, ľe je váa odhad správný. **44.** Dokaľte, ľe je dělitelné 7. **49.** ($\Rightarrow$) 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. **51.** b) Uvaľujte $\sum a_i x^i$ a $\sum b_i x^i$ a vezměte m, n nejmenaí takové, ľe $a_m \neq 0$, $b_n \neq 0$. Podívejte se v součinu na koeficient u x^{m+n}. **55.** Díky krácení jsou levé translace (vzhledem k násobení) prosté, tedy (na konečné mnoľině) jsou i na. **59.** Vyuľijte cvičení, které říká, ľe mocninná řada je invertibilní právě tehdy, kdyľ $a_0 \neq 0$. **60.** NSD dávají jednoznačnost rozkladů, hledáme tedy obor, kde nějaký prvek nejde rozloľit vůbec. Jinými slovy, chceme, aby nějaký prvek a ael dělit do nekonečna. Uvaľujte faktorokruh $\mathbf{T}[x_1, x_2, \ldots\ldots 22\ldots]$ podle ideálu generovaného polynomy $x_1 - x_2^2, x_2 - x_3^2, \ldots\ldots 22\ldots$ Dokaľte, ľe to je obor integrity (stačí, ľe uvedený ideál je prvoideál), ľe v něm existují NSD a a je prvek $[x_1]$. **71.** 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 $1 + x + \cdots + x^{n-1} \mid g$. **79.** 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. **80.** Dosaďte $\frac{r}{s}$ do polynomu a zkoumejte dělitelnost jednotlivých členů čísly r, s. **86.** Dokaľte, ľe je-li u kořen tohoto polynomu, pak je $u+1$ také kořen. **88.** Pouľijte cvičení, které říkalo, ľe p je ireducibilní právě tehdy, kdyľ $p(x+a)$ je ireducibilní, a Eisensteinovo kritérium. **89.** Uvaľujte f jako součin dvou polynomů a diskutujte dělitelnost koeficientů provčíslem p. **103.** Dokaľte indukcí podle n za pomoci předchozího cvičení. V indukčním kroku uľijte vzorec pro součet kombinačních čísel $\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}$. **110.** Je-li a kořenem f i f', pak je také kořenem $\mathrm{NSD}(f, f')$. (Protoľe $x - a$ dělí oba dva, tedy i NSD.) **112.** Substituujte $x = y - \frac{b}{2a}$. **125.** Převeďte na řeaení diofantické rovnice $a^2 - 2b^2 = 1$. Není cyklická, protoľe $1 + \sqrt{2}$ a -1 jsou „nezávislé“ generátory. **127.** 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 $\mathbb{Z}[i]$. **129.** 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 $a, b \in \mathbb{Z}$. **136.** Volba q, r podobně jako pro $\mathbb{Z}[i]$, ale důkaz správnosti je těľaí, protoľe $\nu(r) \neq |r|^2$. **139.** $4 \mid \nu(a)$ právě tehdy, kdyľ $2 \mid a$. **140.** Spočtěte, ľe čísla $x + i$ a $x - i$ musí být nesoudělná, a tudíľ kaľdé z nich musí být třetí mocninou. Třetích mocnin s imaginární sloľkou 1 je málo. Nesoudělnost se dá dokázat z toho, ľe $\mathrm{NSD}(x+i, x-i) = \mathrm{NSD}(x+i, 2i) = \mathrm{NSD}(x-i, 2i)$. **147.** Pouľijte Eulerovu větu nebo Eukleidův algoritmus. **150.** Uľijte Bézoutovu rovnost. **165.** Definujte $\varphi(x) = \psi(x')$. **168.** Stačí ji umět rozloľit na direktní součin. **169.** Protoľe $\varphi(a)^k = e$ právě tehdy, kdyľ $a^k = e$. **173.** Vyplňujte tabulku. **174.** Hodně dlouho vyplňujte tabulku, nebo buďte chytřejaí :–). **182.** Pouľijte předchozí cvičení a Lagrangeovu větu. **190.** Uľijte Bézoutovu nerovnost. **196.** Uľijte Bézoutovu nerovnost. **207.** 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 $\mathbb{Q}$. **211.** V soudělném případě v $\mathbb{Z}_m \times \mathbb{Z}_n$ nenajdete prvek řádu mn. V nesoudělném pouľijte Čínskou větu o zbytcích. **215.** Kaľdé kladné racionální číslo lze napsat ve tvaru $p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ pro nějaká prvočísla p_i a nějaká $k_i \in \mathbb{Z}$. **216.** Vezměte je nejmenaí kladný prvek grupy $\mathbf{H}$. **221.** Pouľijte Čínskou větu o zbytcích. **222.** Postupujte podobně jako charakterizaci podgrup grupy $\mathbb{Z}$. **234.** Uvaľujte podgrupy generované $-1, 5$. **235.** Uvaľujte podgrupu generovanou jistou mocninou nějakého generátoru grupy $\mathbb{Z}_p^*$ a podgrupu $\{a : a \equiv 1 \pmod p\}$. **248.** K řeaení části c) si prostudujte kapitolu o cyklických grupách. **282.** 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 $a^i b^j \mapsto (c^u d^j, e^v f^j)$, kde $u = i \bmod 2^k$ a $v = i \operatorname{div} 2^k$, je vnoření. b),c) analogicky. **283.** Vnořte $\mathbf{G}$ do $\mathbf{S}_{G \cup G'}$, kde G' je disjunktní kopie mnoľiny G. Zdvojenou permutaci jiľ snadno odmocníme. **284.** Spočítejte, ľe má 8 prvků, ľe není abelovská, a dokaľte, ľe není izomorfní $\mathbf{D}_8$. **290.** Uvědomte si, ľe spojitá reálná funkce je jednoznačně určena svými hodnotami v racionálních bodech. **305.** Pouľijte-li předchozí cvičení, zbývá vyaetřit pouze případ abelovských grup. **314.** $1 \mapsto E$, $i \mapsto \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $j \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $k \mapsto \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$. Z komplexních matic na reálné pak přejdeme nahrazením komplexních čísel za matice 2×2 jako v minulém cvičení. **319.** Indukcí podle $n - k$. **345.** Při počítání symetrií nezapomeňte, ľe i kdyľ při otočení zůstane destička na místě, aipka můľe ukazovat jinam. **364.** Označme ten interval $[\mathbf{H}, \mathbf{G}]$. Uvaľujte působení grupy $\mathbf{G}$ na rozkladových třídách $\mathbf{G}/\mathbf{H}$. **403.** $\mathbf{S}_4/\mathbf{H}$ má $24/4 = 6$ prvků. Není-li abelovská, je izomorfní $\mathbf{S}_3$. **408.** $\simeq \mathbb{Q}^* \times \cdots \times \mathbb{Q}^*$. **414.** 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. **471.** Nejprve najděte vaechny ideály okruhu $\mathbb{Z}$, a pak postupujte jako v předchozím cvičení. **472.** Vyřeate předchozí cvičení a postup zobecněte. **474.** Nejprve najděte vaechny ideály okruhu $\mathbb{Z}$, a pak postupujte jako v předchozím cvičení. **505.** Pouľijte minimální polynom prvku $\sqrt[3]{2}$. **520.** 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 $\mathbf{I}$. **521.** Uvaľujte $\{[a] : a \in I\}$. **522.** $\mathbf{T}[x]$ je OIHI, tedy $\mathbf{I}$ je hlavní ideál. Dále pouľijte fakt, ľe $aR \subseteq bR \Leftrightarrow b \mid a$. **532.** Nejprve si vaimněte, ľe pro kaľdé $k \mid n$ tvoří podalgebru mnoľina vaech čísel dělitelných k; tato podalgebra je generovaná prvkem k. Dále dokaľte, ľe $\langle a \rangle = \langle \mathrm{NSD}(a, n) \rangle$ a ľe $\langle a_1, \ldots, a_n \rangle = \langle \mathrm{NSD}(a_1, \ldots, a_n) \rangle$. Jinými slovy, kaľdá podalgebra je generovaná nějakým dělitelem n. K důkazu těchto faktů pouľijte vlastnost, ľe $\mathrm{NSD}(u, v) = ru + sv$ pro nějaká r, s. **610.** Krok 1: uvaľujte $0 \sim \langle e \rangle$ a dokaľte, ľe pak je $U \sim V$ pro vaechna U, V. Krok 2: uvaľujte $U \sim V$ pro $U \subseteq V$ a převeďte to na krok 1. Krok 3: převeďte obecný případ na krok 2. **618.** Uvaľujte eventuální podsvaz izomorfní $\mathbf{N}_5$ nebo $\mathbf{M}_3$, rozloľte čísla na součin prvočísel a zjistěte, ľe suprema nefungují. Alternativní řeaení: tento svaz je izomorfní direktnímu součinu nekonečně mnoha kopií svazu $(\mathbb{N}, \leq)$ a platí, ľe součin distributivních svazů je distributivní. **628.** Přiřaďte ekvivalenci $\sim$ mnoľinu vaech podmnoľin X, které jsou sjednocením jejích bloků, tj. mnoľinu $\{M \subseteq X :$ pokud $x \sim y$, pak $x \in M \Leftrightarrow y \in M\}$. **653.** $a + bi \mapsto \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ je izomorfismus. **654.** $[ax + b] \mapsto \left(\begin{smallmatrix} b & a \\ -a & b \end{smallmatrix}\right)$ je izomorfismus. **657.** Uľijte Möbiovu inverzní formuli na výsledek předchozího cvičení. **665.** Uvaľujte mezitěleso $\mathbb{Q}[\sqrt{21}]$. **668.** Uvaľujte $a \in S \setminus T$. Pak $\mathbf{S} = \mathbf{T}(a)$, a je kořen kvadratického polynomu a pouľijte známý vzorec na výpočet kořenů. **670.** Mnoľina vaech polynomů je spočetná (protoľe jde o konečné posloupnosti racionálních čísel) a kaľdý polynom má konečně mnoho kořenů. **675.** 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. **684.** Prvku a přiřaďte matici, která odpovídá endomorfismu $L_a : x \mapsto ax$ vektorového prostoru $\mathbf{S}$ nad $\mathbf{T}$. **688.** Rozeberte vaechny tři moľnosti, jak vzniká nový bod. Zjistíte, ľe buď $\mathbf{T}_{i+1} = \mathbf{T}_i$, nebo $\mathbf{T}_{i+1} = \mathbf{T}_i(\sqrt{r})$ pro nějaké r. **692.** Pouľijte vzorec $\cos 3x = 4(\cos x)^3 - 3 \cos x$. **695.** Podle předchozího cvičení je $p = 2^m + 1$. Pokud liché n dělí m, pak $2^{m/n} + 1$ dělí p. **713.** Postupujte indukcí stejně jako v důkazu existence rozkladového nadtělesa. **718.** 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. **721.** $|T[x]| = |T|$, protoľe jde o konečné posloupnosti prvků T. Kaľdý polynom má konečně mnoho kořenů, tedy mnoľina algebraických prvků nad T je stejně velká jako T. A algebraický uzávěr sestává z algebraických prvků.

ŘEŠENÍ

1. 2, 3, neexistuje, 2, nekonečno, nekonečno, 3, neexistuje, 6. **2.** Ano, ne, ano, ne. **4.** Supremum lze definovat jako infimum množiny vaech horních mezí. (Tato je neprázdná, nebo» exituje největaí prvek.) **8.** Ano, ne. **9.** Obě jsou svazy, ale jen $(\mathbb{N} \cup \{0\}, |)$ je úplný. Suprema jsou nejmenaí společné násobky (resp. 0 v případě nekonečné množiny). Infima jsou největaí společní dělitelé. **10.** $(F, \leq)$ je svaz, ale ne úplný. Na uzavřeném intervalu by to byl úplný svaz. **11.** Je to uspořádaná množina, $\sup\{(a_1, a_2), (b_1, b_2)\}$ existuje právě tehdy, když $a_1 = b_1$, inf taky tak. **19.** $3, -3, 32.$ $12, -7, 3.$ **20.** 1. **22.** a) $x = 5 + 7k$, $k \in \mathbb{Z}$, b) $x = 11 + 21k$, $k \in \mathbb{Z}$, c) $x = 5 + 11k$, $k \in \mathbb{Z}$. **23.** 363. **24.** 231. **25.** $x = 1320k + 14$, $k \in \mathbb{Z}$. **26.** $x = 120k + 34$, $k \in \mathbb{Z}$. **27.** Nemá řeaení. **28.** $x = 15k + 8$, $k \in \mathbb{Z}$. **33.** Počítejte mod 11. Vyjde 0. **34.** Počítejte mod 13. Vyjde 0. **35.** 13, 1. **38.** 8. **39.** -1. **40.** 33. **41.** 2. **42.** 07. **43.** a pro $5 \nmid a$, 0 v opačném případě. **45.** 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. **46.** $\{(x, y) : 7 \nmid x, y \equiv -1 \pmod 7\}$. **50.** Kdyby $ab = 0$ pro nějaká $a, b \neq 0$, pak $0 = aba^{-1} = aa^{-1}b = b$, spor. **52.** Jen pro prvočísla. **53.** a) Není: $(1, 0) \cdot (0, 1) = (0, 0)$. b) Jen pokud $n = 1$ a $\mathbf{R}_1$ je obor integrity. **54.** Pak $a(b - c) = 0$, a tedy $b - c = 0$. **56.** Ano, $(x + 1) \cdot \sum(-1)^i x^i = 1$. **58.** x^2, $2x^2$. **59.** Ano, ano — kaľdá mocninná řada je asociovaná s nějakým polynomem x^k, normou tedy je 1+stupeň. **61.** Např. ideál vaech polynomů, jejichľ absolutní člen je sudý. **62.** Např. ideál vaech polynomů, jejichľ absolutní člen je nula. **64.** Zvolte v podmínce (2) $a = 3x, b = 2x$. Zkuste vyjádřit $1 = \mathrm{NSD}(x, 2) = xu + 2v$. **68.** Právě tehdy, když $m \mid n$. **69.** $x^{n \bmod m} - 1$. **70.** $x^{\mathrm{NSD}(m,n)} - 1$. **71.** Ano. **72.** Dosaďte několik hodnot a použijte větu, že polynom má jen konečně mnoho kořenů. **73.** 10. **74.** Např. $(2x-1)(x-i)(x+i)(x-(2-i))(x-(2+i))$. **75.** $x^3 - 9x^2 + 26x - 18$. **77.** Např. $x^2 + x \in \mathbb{Z}_6[x]$. **78.** $x^2 + 1$ má kořeny $\pm i, \pm j, \pm k$. **79.** Pokračování návodu: tedy determinant je dělitelný součinem $\prod_{i \neq j}(u_i - u_j)$, ale přitom má stupeň nejvýae $n(n-1)/2$, takže je roven tomuto výrazu aľ na konstantu. Není těžké nahlédnout, že konstanta je 1. **81.** a) -1, b) $-3, -1/2, 1/3, 1, 2$, c) $-1/2, 2$. **82.** Ne, ne, ano, ne, ne. **83.** Ano (nemá kořen), ne $((2x - 1)(2x + 1))$, ano (Eisenstein). **84.** a) vaechny polynomy stupně 1, b) vaechny polynomy stupně 1 a ty polynomy stupně 2 které nemají reálný kořen. **87.** Ano. Je-li $f(x+a) = g(x)h(x)$, pak $f(x) = g(x-a)h(x-a)$, spor. **90.** $(x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i)$, $(x - \sqrt{2})(x + \sqrt{2})(x^2 + 1)$, $(x^2 - 2)(x^2 + 1)$, $(x^2 + 3)(x + 2)(x + 3)$, $(x^2 + 1)^2$. **91.** Ireducibilní, $(x^2 + x + 1)(x^2 - x + 1)$, ireducibilní, $(x + 2)(2x + 5)$. **92.** První: $2 \cdot (x^3 + 2x^2 - x + 2)$, ireducibilní. Druhý: $(2x + 3)(x^2 + 1)$. **93.** $(x + 2)(x^2 + x + 1)(x^2 + 2x + 4)$. **94.** Ireducibilní, $(x^2+1)(x^3+2x+2)$, $(x^2+1)^3$. **95.** $(2x+1)(x^2+1)(x^2-2)$, $(2x+1)(x+2)(x+3)(x^2+3)$. **96.** 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) $(x-1)(x+1)(x^2+1)(x^4+1)$. **97.** $x^3 + 2x^2 + x + 2$, $-2x$, 1. **98.** a) $x + 1$, b) 1, c) $x - 1$. **99.** 1, $x + 1$. Zde je výhodné uľít výpočet pomocí rozkladů. **100.** a) 1, b) $x^2 + 2$. **101.** $x^3 + x^2 + x + 1$ v obou. **104.** $a \neq -5$ jednonásobný, $a = -5$ dvojnásobný. **105.** $a = -n$, $b = n + 1$. **106.** $a = -5/3c^2$, $b \in \{-7/3c^2, 2/3c^2\}$, pro libovolné $c \in \mathbb{N}$. **107.** 2, 4, 3. V c) nelze použít Větu kvůli charakteristice!!! **108.** -2. **109.** Nejsou. **113.** $x = y - \frac{a_{n-1}}{na_n}$. **117.** 3, $(-3 \pm \sqrt{3}i)/2$. **118.** 4, $-2 \pm \sqrt{3}$. **120.** $(\pm 1 \pm \sqrt{11}i)/2$. **121.** $(\pm i \pm \sqrt{-1 + 4i})/2$. **122.** (1) Rozepiate $u = a + b\sqrt{s}$ a rozloľte $1 = a^2 - rb^2 = (a + b\sqrt{s})(a - b\sqrt{s})$. (2) Rozepiate $u = a + b\sqrt{s}$ a $v = c + d\sqrt{s}$ a roznásobte. **123.** $\pm 1, \pm i, \simeq \mathbb{Z}_4$; $\pm 1, \simeq \mathbb{Z}_2$. **124.** $1 + \sqrt{2}$ je takový. **126.** $(1 + i)^2(2 + i)$, $(2 + i)(1 + 2i)$, $(1 + i)(-2 - 3i)$, $3(1 + i)(1 - i)$, 11. **127.** 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 nemůže být asociované s $a + bi$ pro $a, b \neq 0$. Opačná implikace plyne z multiplikativnosti normy. **128.** Pokud se rozkládá, pak na součin dvou prvků normy p. Takové ale neexistují: jedna složka musí být lichá, druhá sudá, součet čtverců tedy bude $\equiv 1 \pmod 4$. **130.** ireducibilní, ireducibilní, $(i\sqrt{2})^2 \cdot (1 + i\sqrt{2})$. **132.** Například a) 2, b) $a = 4$, $b = 2 + 2\sqrt{5}$. **133.** $4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$. **134.** $|z - q| < 1$, tedy $\nu(r) = |a - bq|^2 = |b|^2 \cdot |a/b - q|^2 = |b|^2 \cdot |z - q| < |b|^2 = \nu(b)$. **135.** Analogicky jako v případě $\mathbb{Z}[i]$, protože $\nu(r) = |r|^2$. **137.** a) $(1+i)$, $(1+i)^2(2+i)(2-i)$, b) 3, $18+21i$, c) $1+4i$, $31+5i$, d)

$7+6i$, $85+85i$. **138.** Je to hlavní ideál s generátorem $\mathrm{NSN}(3+6i, 12-3i) = 18+21i$. **139.** Je to hlavní ideál s generátorem $\mathrm{NSN}(2, 7-3i) = 10+4i$. **140.** $(0,1)$. **141.** $(\pm 5, 3)$. **142.** $(\pm 2, 2), (\pm 11, 5)$. **144.** 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. **145.** $u = a'$, $x'' = a' * x' * a'$. **146.** $x = a^{-2} * c^{-2} * b^3$. **147.** a) 33, b) 34. **150.** $1 = um + vn$, $b = a^{vn}$, $c = a^{um}$. **152.** ($\Rightarrow$) 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 $a * b = a * b'' \in H$. **154.** Ne. Např. v $\mathbf{S}_{\mathbb{Z}}$, permutace $a = \ldots (i\ i+1)\ldots$ a $b = \ldots (i-1\ i)\ldots$ jsou konečného řádu, ale jejich sloľení ne. **155.** Ano, v abelovských grupách $|a * b|$ dělí $\mathrm{NSN}(|a|, |b|)$, viz cvičení výae. **158.** Buď a nějaký prvek. Podle Lagrangeovy věty je $|a| = p^i$, a je vidět, ľe $|a^{p^{i-1}}| = p$. **170.** Např. $\mathbb{Z}$ a $\mathbb{Z} \times \mathbb{Z}$. **177.** 16, 37, 4, 16. **180.** Uvaľujte komplexní kořeny polynomu $x^n - 1$. Pro nekonečno uvaľujte číslo $e^{2\pi i a}$ pro iracionální a. **182.** n. **183.** a) ne, b) ano. **184.** a) ne, b) ne. **185.** 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. uvaľujte podgrupy $\mathbb{Z}$ a $\sqrt{2}\mathbb{Z}$. **186.** Ne. **187.** $7\mathbb{Z}$, $\mathbb{Z}$. **188.** $3\mathbb{Z}$, $\{3a/4 : a \in \mathbb{Z}\}$, $\{a/28 : a \in \mathbb{Z}\}$, $\{2a/15 : a \in \mathbb{Z}\}$. **189.** $\{\pm 1, \pm i\}$, $\{1, -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i\}$, $\{\pm 2^n, \pm 2^n i : n \in \mathbb{Z}\}$. **192.** Uvaľujte grupu $\mathbb{Z}_n$ a počet prvků daného řádu v ní. Výsledek je n. **198.** Ano, ne, ne, ne, ano. **199.** Ne, ne, ano, ano, ano. **200.** Ano, ne, ano. **201.** Ne, ano. **202.** Endomorfismus pro vaechna n, prostý pro lichá, na je jen pro $n = \pm 1$. **203.** Ano, jádro je $\{(x, y, z) : 2x + y = z\}$, obraz je $\{2^x 3^y : x, y \in \mathbb{Z}\}$. **204.** a) $x \mapsto ax$ pro libovolné $a \in \mathbb{Z}$; b) $x \mapsto ax \mod n$ pro libovolné $a = 0, \ldots, n-1$; c) $x \mapsto 0$. **205.** 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 $k = 0, \ldots, \mathrm{NSD}(m, n) - 1$. **207.** 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 roľaiřte jej do homomorfismu $\mathbb{R} \to \mathbb{R}$. **208.** Ano, $x \mapsto (x \bmod 2, x \bmod 3, \ldots)$. **209.** Grupa $\mathbb{C}_n$. **210.** $a + bi \mapsto (a, b)$, $re^{i\varphi} \mapsto (r, e^{i\varphi})$. **212.** Ⓡádné dvě nejsou izomorfní — různé počty generátorů. **213.** Ⓡádné dvě nejsou izomorfní: $\mathbb{Q}^*$ obsahuje prvek řádu 2, pro zbytek uľijte invariant $\forall x \exists y\ y * y = x$. **214.** $exp : \mathbb{R}^+ \to \mathbb{R}$, $x \mapsto e^x$ je izomorfismus. Naopak $\mathbb{R}^*$ s nimi izomorfní není, protoľe obsahuje prvek -1 řádu 2. **215.** Nech» $p_1 < p_2 < p_3 < \ldots$ je seznam vaech prvočísel. Mějme $a \in \mathbb{Q}$. Pak existuje n takové, ľe $a = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, kde $k_i \in \mathbb{Z}$ jsou nějaké celé exponenty. Poloľme $\varphi(a) = \sum_i k_i x^i$. Není těľké dokázat, ľe φ je izomorfismus. **216.** Nech» a je nejmenaí 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 menaí. **220.** Ano, jsou to právě podgrupy $\langle e^{2\pi i/n} \rangle$ pro kaľdé n. **223.** Ne: např. $\mathbb{Z}_2 \times \mathbb{Z}_2$ nebo $\mathbb{C}_{p^\infty}$. **230.** $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, ??, $\mathbb{Z}_4 \times \mathbb{Z}_5$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$. **232.** Nejmenaí taková dvojice je 3,6. **236.** (1 4 7 5)(2 3), (1 7 4 2 5)(3 6). **237.** $\pi = (1\ 3\ 2)^{-1} \circ (2\ 4)(1\ 5) \circ (3\ 5\ 2)(1\ 4)^{-1} = (1\ 3\ 4\ 5)$. **238.** 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. **239.** Jsou to právě ty permutace, které obsahují sudý počet cyklů sudé délky. **244.** $\pi^r = id$ pro r liché, $\pi^r = \pi$ pro r sudé. U σ záleľí na zbytku po dělení aesti. **245.** Nejmenaí společný násobek délek cyklů v π. **246.** (1 2 3 4 5)(6 7 8), ne, ne, (1 2 3)(4 5)(6 7)(8). **247.** 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). **248.** 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 níľ je $\varphi(k)$ prvků řádu k pro kaľdé $k \mid n$. **251.** $a = 2$, $b = 3$. **252.** $\pi = (1\ 3 \ldots\ n{-}1)(2\ 4 \ldots\ n)$ pro n sudé a $(1\ 3 \ldots\ n\ 2\ 4 \ldots n{-}1)$ pro n liché. Tedy je sudá. **253.** a) 1 b) $(-1)^{n(n+1)/2}$. **255.** Ne, levá strana je nutně sudá permutace, pravá strana je lichá. **258.** (4 3 2 5 1)(7 6). **259.** (8 2 1)(7 9 5 3)(4 6). **260.** Ano, např. (3 4). Ne, nebo» ľádná permutace, která konjuguje ty dvě uvedené, není sudá. **261.** Ano, např. $(1\ 7\ 4\ 5\ 6\ 8\ 2) \in A_8$ řeaí obě otázky. **262.** (1 3)(1 5)(1 2)(3 6)(3 7). **264.** Každý cyklus lze nezávisle rozloľit jako $(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k) \ldots (a_1\ a_3)(a_1\ a_2)$. **265.** 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). **274.** 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. **276.** Ano, ne. **277.** a) ne, b) ano. **278.** 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. **288.** Nejmenaí existuje na aesti prvcích a jsou dva. Jeden je prasátko bez noľiček a druhý trojúhelník s různě dlouhými rohy. **289.** a) Jednoprvková grupa. b) Obsahuje právě vaechny funkce $x \mapsto x+k$, $k \in \mathbb{Z}$. **290.** Grupa obsahuje právě restrikce striktně rostoucích spojitých reálných funkcí na mnoľinu $\mathbb{Q}$. **294.** 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 $\mathbf{Aut}(\mathbf{S}_3) \simeq \mathbf{S}_3$. **295.** Automorfismy jsou právě $x \mapsto kx \bmod n$ pro $k \in \mathbb{Z}_n^*$. Přiřadíme-li tomuto zobrazení prvek k, dostaneme izomorfismus na $\mathbb{Z}_n^*$. **301.** Jen vnitřní, $\simeq \mathbf{S}_4$. **306.** Ano, ano, ne (mají determinant ± 1). **307.** Není, např. proto, ľe není abelovská. **311.** Ano. **313.** $a+bi \mapsto \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$. **314.** $a+bi+cj+dk \mapsto \left(\begin{smallmatrix} a+bi & c+di \\ -c+di & a-bi \end{smallmatrix}\right)$, $a+bi+cj+dk \mapsto \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & c & b & a \end{pmatrix}$. **323.** Jsou to právě podgrupy $\langle$ otočení o $2\pi/n\rangle$, $n \in \mathbb{N}$. **326.** V obou případech jen jedna orbita. **327.** V obou případech jen jedna orbita. **328.** 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 $\{id\}$, $\{(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$, $\{(1\,2\,3),(2\,1\,4),(3\,4\,1),(4\,3\,2)\}$, $\{(1\,3\,2),(2\,4\,1),(3\,1\,4),(4\,2\,3)\}$. **329.** Dvě orbity: $\{(0,\ldots,0)\}$ a $T^n \setminus \{(0,\ldots,0)\}$. **330.** a) 5!, b) 4!. **331.** a) 0, b) 1. **332.** 2. **333.** a) 0, b) 2 nebo 0, podle toho, zda prochází vrcholy nebo středy hran. **334.** 2. **335.** a) 1, b) 2, c) 4. **336.** a) 2, b) 4, c) 8. **337.** $[x] = X$, G_x obsahuje vaechna otočení se středem v x a osové symetrie s osou procházející x. **338.** X_g obsahuje a) střed otočení, b) nic, c) osu symetrie. **339.** Ano, $[x]$ je horizontální přímka procházející bodem x, $G_x = \{0\}$ a $X_n = \emptyset$. **340.** 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. **342.** Pro n sudé $\frac{1}{4}(2^{n^2} + 2\cdot 2^{\frac{n^2}{4}} + 2^{\frac{n^2}{2}})$. Pro n liché $\frac{1}{4}(2^{n^2} + 2\cdot 2^{\frac{n^2+3}{4}} + 2^{\frac{n^2+1}{2}})$. **343.** 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 $\frac{1}{8}(2^{n^2} + 2\cdot 2^{\frac{n^2+3}{4}} + 2^{\frac{n^2+1}{2}} + 4\cdot 2^{\frac{n(n+1)}{2}})$. **344.** a) 420, b) 228. **347.** a) $\frac{1}{3}\cdot\frac{16!}{8!8!}$. b) $\frac{1}{6}\cdot(\frac{16!}{8!8!} + 3\cdot 150)$. **349.** a) 8. **352.** a) 10. b) $k^6 + 3k^4 + 12k^3 + 8k^2$ **354.** 30, resp. 2. **355.** $(k^4 + 11k^2)/12$. **356.** $(k^4 + 6k^3 + 11k^2 + 6k)/24$. **357.** 4, 11, dál nevím. **358.** 10, 3405. **359.** Průměrný počet pevných bodů je 1, identita má více neľ 1, musí tedy existovat nějaká permutace, která má méně neľ 1. **360.** Ano, ano, ne. **361.** Rozkladové třídy $\mathbf{G}$ podle $\mathbf{H}$. **362.** Třídy konjugace. Jen pro jednoprvkovou grupu. **365.** 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. **366.** $H = \{id, (1\,2)\}$, $a = (1\,2\,3)$. **370.** Ano. **371.** Není uzavřena na kojugaci. **372.** Ano. **373.** Není uzavřená na násobení! **374.** a) Je to podgrupa $\mathbf{A}_5$, nebo» konjugováním získám vaechny trojcykly a ty generují $\mathbf{A}_5$. b) Je to celá $\mathbf{S}_5$. **375.** a) Je to podgrupa sestávající ze vaech otočení. b) Je to celá $\mathbf{D}_{10}$. **376.** $\{id\}$, $\mathbf{A}_3$, $\mathbf{S}_3$. **377.** $\{id\}$, Kleinova, $\mathbf{A}_4$, $\mathbf{S}_4$. **380.** 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. **383.** 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. **384.** 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. **385.** Ne, ano. **386.** Ano. **387.** 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. **388.** 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. **390.** Podgrupu vaechny, normální jen C. **391.** Ne, kvaternionová grupa je protipříklad. **392.** a) Musí, b) můľe ale nemusí. **394.** $\mathbb{R}^*$, homomorfismus $A \mapsto \det A$. **395.** $\mathbb{Z}_2 \simeq (\{\pm 1\}, \cdot, ^{-1}, 1)$, homomorfismus $x \mapsto \mathrm{sgn} x$. **396.** $\mathbb{R}^+$, homomorfismus $x \mapsto |x|$. **397.** Operace jsou $a \oplus b = a + b - [a+b]$ a $\ominus a = n - a$. Homomorfismus $a \mapsto a - [a]$. Pro racionální čísla uvaľujeme jen racionální prvky toho intervalu. **398.** $\mathbb{R}$, homomorfismus $a + bi \mapsto b$. **399.** $\{z \in \mathbb{C} : |z| = 1\}$, homomorfismus $z \mapsto z/|z|$. **400.** $\mathbb{R}^+$, homomorfismus $z \mapsto |z|$.

401. $\mathbb{C}^*$, homomorfismus $z \mapsto z^n$. **402.** $\mathbb{C}_{p^\infty}$. **408.** Homomorfismus funguje tak, že se matici přiřadí vektor z prvků, které leží na diagonále. **420.** Ne, $\times$ není asociativní. **421.** Ano. **422.** Ano. **425.** ??? Ano, ne. ??? **430.** $\{\pm 1\}$, $\{\pm 1, \pm i\}$, $\mathbf{GL}_n(\mathbf{T})$. **432.** Vae kromě nuly. **434.** $\mathbb{Z}$: 0; 0; ± 1; $\mathbb{Z}_8$: 0,2,4,6; 0,2,4,6; 1,3,5,7; $\mathbb{Z}_{12}$: 0,6; čísla soudělná s 12; čísla nesoudělná s 12; $\mathbb{Z}_{p^k}$: čísla dělitelná p; čísla dělitelná p; čísla nedělitelná p. **437.** Prvek (a, b) je nilpotentní právě tehdy, když a i b jsou nilpotentní, dělitel nuly právě tehdy, když a *nebo* b je dělitel nuly, invertibilní právě tehdy, když a i b jsou invertibilní. **438.** Inf je průnik, sup je podokruh generovaný sjednocením. Nemusí být ani modulární: ????. **439.** Ano, ne. **440.** Ano, ne, ne. **441.** Ne, ne, ne, ano, ano. **444.** $7\mathbb{Z}$, $\mathbb{Z}$. **445.** $3\mathbb{Z}$, $\{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{N}\}$, $\{\frac{a}{2^n 7^m} : a \in \mathbb{Z}, m, n \in \mathbb{N}\}$, $\{\frac{2a}{3^n 5^m} : a \in \mathbb{Z}, m, n \in \mathbb{N}\}$. **447.** $\mathbb{Z}$, $\{2a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Z}\}$. **448.** $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Z}\}$, $\{a+b2^{\frac{1}{3}}+c2^{\frac{2}{3}}+di+ei2^{\frac{1}{3}}+fi2^{\frac{2}{3}} : a, b, c, d, e, f \in \mathbb{Z}\}$. **449.** $\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$. **450.** $\{\sum_{i=0}^n a_i x^i : a_0 = a_1 = 0\}$, $\{\sum_{i=0}^n a_i x^i : 2 \mid a_0\}$, $\{\sum_{i=0}^n a_i x^i : 2 \mid a_0, a_i = 0 \text{ pro } i \text{ liché}\}$. **451.** $\{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) : a, b \in \mathbb{Z}, a + b \text{ sudé}\}$, $\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) : a, b \in \mathbb{Z}\}$, $\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) : a, b \in \mathbb{Z}\}$. **452.** $\{0\}$ 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 $\mathbb{Z}_3 \times \{0\}$, $\{0\} \times \mathbb{Z}_3$. **453.** Ne. **455.** Diagonální matice, které navíc mají na diagonále vaechny prvky stejné. Přiřadíme-li matici ten prvek, který se vyskytuje na diagonále, dostaneme izomorfismus s $\mathbf{R}$. **456.** Inf je průnik, sup je nejmenaí ideál obsahující sjednocením. Musí být modulární, ale nemusí být distributivní: $\mathbb{Z}_2 \times \mathbb{Z}_2$. **457.** $a\mathbb{Z}$, $a \in \mathbb{N} \cup \{0\}$; 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 $\mathbb{Z}_3 \times \{0\}$, $\{0\} \times \mathbb{Z}_3$. **458.** $7\mathbb{Z}$, $\mathbb{Z}$. **459.** $\mathbb{Q}$. **460.** $\{\sum_{i=0}^n a_i x^i : a_0 = a_1 = 0\}$, $\{\sum_{i=0}^n a_i x^i : 2 \mid a_0\}$, $\{\sum_{i=0}^n a_i x^i : 2 \mid a_0, a_1\}$. **461.** Ano, je to $(x - 1)\mathbb{Z}[x]$. **462.** Ano, je to $(x^2 + 1)(x - 1)\mathbb{Z}[x]$. **463.** a) Ideál ano, hlavní ne, protože prvky 3 a x v něm jsou, ale jejich jediný společný dělitel nikoliv. b) Ano, je to $\mathbb{Q}[x]$. **464.** $(x^3 - 1)(x^2 + 3)$, 1. **465.** $x^4 - 1$, $x - 1$. **466.** Ne, ne, ne, ne. **467.** Ano, ne, ano. **468.** $\mathbf{M}_2(\mathbb{Z})$. **471.** $\mathbf{M}_n(a\mathbb{Z})$, $a \in \mathbb{Z}$. **472.** $\mathbf{M}_n(\mathbf{I})$, $\mathbf{I} \in \mathcal{I}$. **473.** Vlastní ideály jsou právě $\left(\begin{smallmatrix} \mathbf{T} & \mathbf{T} \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \mathbf{T} \\ 0 & \mathbf{T} \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \mathbf{T} \\ 0 & 0 \end{smallmatrix}\right)$. **475.** Jen nevlastní. **479.** Obraz je $\mathbf{R}$, jádro je $(x - a)\mathbf{R}[x]$. **480.** Obraz je $\mathbb{C}$, jádro je $(x^2 + 1)\mathbb{Z}[x]$. **481.** Obraz je $\mathbb{R}$, jádro je $(x^2 - 2)\mathbb{Z}[x]$. **482.** $u^2 \equiv s \pmod{n}$. **483.** Ne. **486.** Označme $X = \{x_1, \ldots, x_n\}$. Hledaný izomorfismus je $A \mapsto (a_1, \ldots, a_n)$, kde $a_i = 1$ právě tehdy, když $x_i \in A$. **488.** 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. **489.** $\mathbb{Z}[x] \to \mathbb{Z}[\pi]$, $p \mapsto p(\pi)$ je izomorfismus. Prostost plyne z toho, že π je transcendentní. **490.** Ⓡádné dva. **491.** Např. ideály $\mathbf{R}[x]$, $\mathbf{R}[x^2]$, $\mathbf{R}[x^3]$, atd. **493.** Matici odpovídá lineární zobrazení (endomorfismus) s touto maticí vzhledem k nějaké předem pevně zvolené bázi (např. kanonické). **495.** Ve vaech případech jen identita a konstantní zobrazení na 0. Automorfismus je tedy jen identita. **496.** $x \mapsto ax \bmod n$ pro $a = 0, \ldots, n-1$ splňující $a^2 \equiv a \pmod{n}$. Automorfismus je tedy jen identita. **498.** Hledaný homomorfismus je $f \mapsto f \bmod 3$. **499.** Hledaný homomorfismus je $f \mapsto f(0) \bmod 3$. **500.** Hledaný homomorfismus je $f \mapsto f(a)$. **501.** Hledané homomorfismy jsou $f \mapsto f(i)$, $f \mapsto f(i)$, $f \mapsto (f(i), f(-i))$. **502.** Hledané homomorfismy jsou $f \mapsto (f(1), f(-1))$. **503.** $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{R} \times \mathbb{R}$. **504.** Je to $\mathbb{Q}[i] \times \mathbb{Q}[\sqrt{2}i]$, $\mathbb{R} \times \mathbb{R} \times \mathbb{C}$, $\mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$. **505.** Je to $\mathbb{Q}[\sqrt[3]{2}]$, hledaný homomorfismus je $f \mapsto f(\sqrt[3]{2})$. **506.** 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. **507.** a) $\mathbb{C} \times \mathbb{C} \times \mathbb{C}$, b) $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ a $\mathbb{C} \times \mathbb{R}$. **512.** Hledaný homomorfismus je $f \mapsto f(x, 0)$. **513.** Je to $\mathbf{R}[x]$, homomorfismus je $f \mapsto f(x, -x)$. **514.** 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 $\varphi(y)$. **516.** Hledaný homomorfismus je $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mapsto c$. **517.** Hledaný homomorfismus je $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mapsto (a, c)$. **523.** $\mathbf{K} \mapsto \{a : [a] \in K\}$. **524.** $u = 0$, $u \in \{0, 1\}$, $u = 1$. **525.** Ne, ne. **526.** Ne, ano. **527.** Pro vaechna. **528.** Např. $\{n : k \mid n\}$ pro libovolné $k \in \mathbb{N}$, nebo $\{n : n \geq k\}$ pro libovolné $k \in \mathbb{N}$. **529.** Tvoří je podmnožiny d, cd, acd, bcd, $abcd$. **531.** Pro každé $k \in \mathbb{Z}$ tvoří podalgebru množina $\{k, k + 1, k + 2, \ldots\}$. A jeatě

celé $\mathbb{Z}$. Jiné nejsou. **532.** Pro každé $k \mid n$ tvoří podalgebru množina vaech čísel dělitelných k. Jiné nejsou. **533.** Pokud $a = b = c$, pak 2^{n-1}. Pokud jsou dve stejné a třetí různá, pak 2^{n-2}. A pokud jsou po dvou různé, pak 2^{n-3}. **536.** 1) Každý prvek dostaneme jako $1 + 1 + \ldots + 1$. 2) $\{1\}$, protože $1 \cdot 1 = 1$. 3) $\mathbb{N}$, stejně jako první část. 4) Abychom získali i záporná čísla, potřebujeme -1, tedy např. $\langle 1, -1\rangle$. **537.** Konečná množina $X \subseteq \mathbb{N}$ obsahuje jen konečně mnoho prvočíselných dělitelů. Prvočíslo, které mezi nimi není, nikdy nemůžeme získat násobením prvků X. **538.** $\{2, 3, 4, \ldots\}$, $\{2^k \cdot 3^l, 2^k, 3^l : k, l \in \mathbb{N}\}$, $\mathbb{Z}$. **539.** $\{2, -2\}$, $\{\sqrt[3^k]{2} : k \in \mathbb{N} \cup \{0\}\}$. **540.** $2\mathbb{Z}$, $\{2^k : k \in \mathbb{Z}\}$. **541.** $\{\frac{a}{6} : a \in \mathbb{Z}\}$, $\{\frac{a}{6^k} : a \in \mathbb{Z}, k \in \mathbb{N}\}$, $\{\frac{2a}{15} : a \in \mathbb{Z}\}$. **542.** $\{-a + 2bi : a, b \in \mathbb{N}\}$, $\{a + 2bi : a \in \mathbb{R}, b \in \mathbb{N}\}$, $\{4a + 2bi : a, b \in \mathbb{Z}\}$. **548.** a) $\langle (0,0), (1,0), (0,1)\rangle$, b) $\langle (1,1), (0,1), (0,p) : p$ prvočíslo $\rangle$, c) $\{(1,k), (k,1) : k \in \mathbb{N}\}$. Žádný prvek obsahující v některé složce jedničku nelze napsat jako součet jiných prvků, tedy vaechny musí být mezi generátory. **551.** Ne, v libovolné algebře $\mathbf{A} \times \mathbf{A}$ vezměte např. podalgebru $\mathbf{U} = \{(a, a) : a \in A\}$. **552.** Ano. **554.** Homomorfismy: vae kromě β, ζ. Epimorfismus: jen ε. Prostý: γ, δ, η. **555.** Ano. **556.** a) $x \mapsto kx$, $k \in \mathbb{N}$, b) $x \mapsto x$, c) $x \mapsto 5x$, d) $x \mapsto k^x$, $k \in \mathbb{N}$. **557.** a) $x \mapsto 0$, b) neexistuje, c) $x \mapsto 0$, d) $x \mapsto x$ a $x \mapsto 0$. **558.** a),b) $(a, b) \mapsto u^a v^b$, kde $a, b \in \{1, -1\}$. **559.** Ne, ano. **562.** Např. $A \mapsto$ matice, kde nad diagonále jsou jedničky, v pravé horní čtvrtině je matice A a jinde nuly. **566.** Izomorfismem je zobrazení $0 \mapsto 1$, $1 \mapsto -1$. **567.** Izomorfismem je zobrazení $(x, y, z) \mapsto \begin{pmatrix} 0 & z & -y \\ -z & 0 & x \\ y & -x & 0 \end{pmatrix}$. **570.** a) $a + bi \mapsto (a, b)$, b) invariantem je např. vlastnost „$\forall x \exists y\ y \cdot y = x$“. **571.** $\mathbb{Z}$: různý počet generátorů, $\mathbb{Q}$: problém s dělením 2, resp. odmocninami, $\mathbb{R}$: exponenciála je izomorfismus. **573.** $exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$, $x \mapsto e^x$ je izomorfismus. Ostatní izomorfní nejsou, použijte např. invarianty „$\exists x \forall y\ x * y = y$“ a „$\forall x \exists y\ y * y = x$“. **576.** První a poslední jsou izomorfní. Prostřední dvě jsou izomorfní. **579.** Ano – 2, ne, ano – nekonečně mnoho (každé nezáporné reálné číslo leží v právě jedné). **580.** Ano, komponenty souvislosti. Ne, není symetrie. **582.** Ne, ano. **583.** Ne, ano. **584.** Ano, ano, ne. **593.** Ano, ne, ano, ano, ne. **599.** Průnik, sjednocení. **602.** Průnik, podalgebra generovaná sjednocením. **603.** Stejné jako v $\mathbf{Eq}(A)$. **605.** Ano, ano, ne, ano. **606.** a) Ne, operace jsou jiné! (U podmnožin, jednou to je sjednocení, podruhé nosná množina podalgebry generované oběma algebrami.) b) Ano. **607.** Stačí 4 ekvivalence, bez ohledu na velikost X. **609.** a) ne, ne, ne, ano. **611.** $U \sim V$ právě tehdy když dimenze faktorprostoru $(U \cup V)/(U \cap V)$ je konečná (tj. právě když se liaí pouze o prostor konečné dimenze). **616.** Ano, ano. **617.** Pro $n \leq 2$ distributivní, pro $n = 3$ modulární, ale ne distributivní, pro $n > 3$ ani modulární. **618.** Ano, ano. **619.** Pokud není dělitelné, pak je izomorfní $\mathbf{P}(X)$, kde $|X|$ je rovno počtu prvočísel v rozkladu n. V opačném případě chybí komplementy např. pro prvočísla p taková, že $p^2 \mid n$. **621.** Ano, ne. **626.** Je distributivní. **627.** $\wedge = \cap$, $\vee =$ konvexní obal sjednocení. Není modulární ani distributivní. **636.** Jinak $ab = 0$ pro nějaká $a, b \neq 0$, a kdyby měl a inverz, pak $0 = aba^{-1} = aa^{-1}b = b$, spor. **637.** Jen pokud $n = 1$ a $\mathbf{R}_1$ je těleso. **638.** $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(i)$, $\mathbb{C}$. **641.** Indukcí podle m. Pro $m = 1$ užijte binomickou větu a pozorování, že p dělí každý binomický koeficient kromě těch dvou krajních. **642.** Např. podílové těleso oboru $\mathbb{Z}_p[x]$. **644.** $[4x]$, $[3x^2 + 2x + 1]$, $[4x^2 + 4]$. **645.** $[x^3 + x^2 + 1]$, $[2x^3 + 2x^2 + 2]$, $[x^3 + 2x^2 + 2x + 2]$. **646.** $\mathbb{F}_8^* \simeq \mathbb{Z}_7$, a tedy vaechny prvky různé od 0,1 jsou primitivní. **647.** $\mathbb{F}_9^* \simeq \mathbb{Z}_8$, tedy existují 4 primitivní. Jsou to $x+1, x+2, 2x+1, 2x+2$. **649.** Dvě: sebe sama a podtěleso generované 1. **650.** Idea důkazu: $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$ a přitom $p \mid \binom{p}{i}$ pro každé provočíslo p a $i \neq 0, p$. V tělese je každý nekonstantní homomorfismus bijektivní, protože jeho jádro je ideál a těleso neobsahuje vlastní ideály. **651.** Lagrangeova věta pro grupu $\mathbb{F}_q^*$. **652.** Každý prvek $\mathbb{F}_q$ je kořenem polynomu $x^q - x$, takže se rozkládá na uvedený součin monočlenů. **659.** $x + 2$, $x^2 + 1$, $x^3 - 2$, $x^2 - 2x - 4$, $x^2 - x + 1$. **660.** $x^2 - 3$, $x^2 - \sqrt{2}$. **662.** Je-li $m_{a,\mathbf{T}} = \sum_{i=0}^{n} a_i x^i$, pak $m_{a^{-1},\mathbf{T}} = \sum_{i=0}^{n} a_{n-i} x^i$. **663.** 2, 6, 4. **664.** $p - 1$, protože polynom $x^p - 1$ není ireducibilní! **665.** 4. **667.** n, protože polynom $x^n - p$ je podle Eisensteinova kritéria ireducibilní. **669.** Ne, viz Cardanův vzorec pro kořeny polynomu třetího stupně. **671.** Nekonečný spočetný. **672.** Nekonečný nespočetný ($2^{\aleph_0}$). **673.** Ano: jsou obsaženy v rozaíření konečného stupně $\mathbb{Q}(...)$, kde přidáváme vaechny uvedené odmocniny. **676.** Platí

$\sqrt{pq} \in \mathbb{Q}[\sqrt{p}, \sqrt{q}]$. Z teorie plyne, ľe stupeň tohoto rozaíření je 2 nebo 4. První případ vyloučíme tím, ľe dokáľeme (elementárním způsobem), ľe lineárně nezávislé jsou $1, \sqrt{p}, \sqrt{q}$. Tedy stupeň je 4 a lineárně nezávislé musí být vaechny čtyři uvedené prvky. **677.** Určitě $a^2 \in T(a)$. Je $a \in T(a^2)$? Kdyby ne, tak $[\mathbf{T}(a) : \mathbf{T}(a^2)] = 2$, takľe $[\mathbf{T}(a) : \mathbf{T}]$ je sudé, spor. **689.** Podle jedné z vlastností $[\mathbf{T}_n : \mathbf{T}_0] = [\mathbf{T}_n : \mathbf{T}_{n-1}] \cdot \ldots \cdot [\mathbf{T}_1 : \mathbf{T}_0]$. **690.** Stupeň transendentního rozaíření je nekonečný. **691.** Stupeň takového rozaíření není mocnina dvojky. Zdvojení krychle vede na $\sqrt[3]{2}$. **697.** 3,4,5,6,8,10,12,15,16. **702.** $\mathbb{Q}$. $\mathbb{Q}(i)$. $\mathbb{Q}(\sqrt{2})$. **703.** $\mathbb{Q}, \mathbb{Q}(e^{2\pi i/3})$. $\mathbb{Q}, \mathbb{Q}(e^{2\pi i/6})$. $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}e^{2\pi i/6})$. **705.** $\mathbb{Q}, \mathbb{Q}(i)$. $\mathbb{Q}(e^{2\pi i/8})$. **707.** $\mathbb{Q}(e^{2\pi i/n})$, $\mathbb{Q}(e^{\pi i/n})$. **708.** Kořenové: $\mathbb{Q}$ a $\mathbb{Q}(\sqrt{3}i)$. Rozkladové: $\mathbb{Q}(\sqrt{3}i)$. **709.** Kořenové: $\mathbb{Q}(\sqrt{2})$ a $\mathbb{Q}(\sqrt{3})$. Rozkladové: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. **711.** 5^3, 3^2, 3^2, ???. **712.** Např. pro $f = x^n - 1$ je stupeň $\geq n - 1$. **716.** Právě tehdy, kdyľ je $\frac{r}{s}$ druhá mocnina racionálního čísla. **719.** Označíme-li $a_1, \ldots, a_n$ prvky toho tělesa, pak polynom $(x - a_1) \cdot \ldots \cdot (x - a_n) + 1$ nemá v tomto tělese kořen.

K sestavení sbírky byly použity zejména tyto prameny:

[Ur] *Сборник задач по общей алгебре и дискретной математике,* Уральский государственный университет, 2003.

[SP] З. Стојаковић, Ђ. Паунић, *Задаци из алгебре: Групе, прстени, поља,* Универзитет у Новом Саду, 2001.

- zápisy ze cvičení a doporučené příklady ke zkoušce mých kolegů, zejména Jana Žemličky, Pavla Růžičky, Aleše Drápala, Jeronýma Zvánovce, Víti Kaly, Ondřeje Klímy a dalších.