Sbírka příkladů

z odborné soutěže pro předmět Algebra II konané v semestru Podzim 2014

Autorský kolektiv: Radan Kučera, Ondřej Klíma a Jaromír Kuben

Příklady jsou určeny těm studentům, kteří mají hlubší zájem o algebru. Jsou tedy zamýšleny nejen pro studenty Obecné matematiky nebo studenty Statistiky a analýzy dat, ale také pro všechny ostatní studenty matematiky, tedy bez ohledu na studijní obor – zkrátka pro všechny, kterým je blízký abstraktní styl myšlení a kteří budou, například při volbě tématu bakalářské práce, inklinovat ke studiu abstraktních matematických oborů.

První část sbírky obsahuje zadání 10 příkladů, jež byly v semestru Podzim 2014 pravidelně zadávány v rámci soutěže podpořené FRMU a jsou proto označeny jako kolo 1 až 10. Druhá část sestává ze vzorových řešení k jednotlivým kolům. U každého kola jsou v úvodu uvedeny doporučené znalosti, odkazy míří na přednášky o svazech a okruzích probírané v Algebře II v podzimním semestru 2014; tyto přednášky jsou k dispozici na stránce
https://is.muni.cz/el/1431/podzim2014/M3150/um/.

Část I – Zadání

1. kolo – Svaz všech relací na množině $\mathbb{N}$

Doporučené znalosti: svazy, podsvazy, homomorfismy svazů, úplné svazy – přednáška Svazy.pdf.

Zadání: Symbolem $\mathcal{R}$ označíme množinu všech binárních relací na množině všech přirozených čísel $\mathbb{N}$, tj. $\mathcal{R} = \mathcal{P}(\mathbb{N} \times \mathbb{N})$. Jakožto systém všech podmnožin množiny $\mathbb{N} \times \mathbb{N}$ je množina $\mathcal{R}$ uspořádána inkluzí a $(\mathcal{R}, \subseteq)$ je úplný svaz. Označme $\mathcal{E} \subseteq \mathcal{R}$ množinu všech relací ekvivalence na množině $\mathbb{N}$ a $\mathcal{U} \subseteq \mathcal{R}$ množinu všech uspořádání na stejné množině.

a) (1 bod) Rozhodněte, zda je $\mathcal{E}$ nebo $\mathcal{U}$ podsvazem svazu $(\mathcal{R}, \subseteq)$.

b) (1 bod) Dokažte, že $(\mathcal{E}, \subseteq)$ je svaz.

c) (1 bod) Rozhodněte, zda je $(\mathcal{E}, \subseteq)$ úplný svaz.

d) (1 bod) Rozhodněte, zda je $(\mathcal{U}, \subseteq)$ svaz a zda je úplný svaz.

e) (2 body) Uvažujme zobrazení $f : \mathcal{R} \to \mathcal{P}(\mathbb{N})$, které relaci ρ přiřadí množinu všech čísel, která jsou v relaci s číslem 1, tj. $f(\rho) = \{x \in \mathbb{N}; (x, 1) \in \rho\}$. Rozhodněte, zda je zobrazení f homomorfismus svazu $(\mathcal{R}, \cup, \cap)$ do svazu $(\mathcal{P}(\mathbb{N}), \cup, \cap)$. Je homomorfismus svazů některé ze zúžení zobrazení f na definiční obory $\mathcal{E}$ resp. $\mathcal{U}$?

f) (4 body) Dejte příklad injektivního homomorfismu svazu $\mathcal{R}$ do svazu $\mathcal{E}$.

Komentář: Pro zisk kladného počtu bodů není nezbytně nutné odevzdávat kompletní řešení všech jednotlivých úloh, nicméně pokud odpovídáte na některou z otázek *ano/ne*, pak se očekává, že odpověď zdůvodníte.

Připomeňme, že pro libovolnou množinu X značí $\mathcal{P}(X)$ systém všech podmnožin množiny X, přitom na množině $\mathcal{P}(X)$ uvažujeme uspořádání inkluzí $\subseteq$. V uvažované uspořádané množině $(\mathcal{P}(X), \subseteq)$ je potom libovolná podmnožina $Z \subseteq \mathcal{P}(X)$ systémem podmnožin množiny X, a tedy můžeme psát $Z = \{X_i \subseteq X; i \in I\}$, kde I je vhodná indexová množina. Supremum Z je potom sjednocení systému Z, tj. $\sup Z = \bigcup_{i \in I} X_i$. Podobně infimum neprázdné množiny Z je průnik systému Z, tj. $\inf Z = \bigcap_{i \in I} X_i$, přitom infimum prázdné množiny Z je největší prvek v $(\mathcal{P}(X), \subseteq)$, tj. $\inf \emptyset = X$. Výsledná uspořádaná množina $(\mathcal{P}(X), \subseteq)$ je proto úplný svaz, zejména lze tedy uvažovat svaz $(\mathcal{P}(X), \cup, \cap)$.

Řešení – str. 18.

2. kolo – Konečné distributivní svazy

Doporučené znalosti: distributivní svazy, nedosažitelné prvky – přednáška Distr.pdf.

Zadání: Pro dvouprvkový svaz $(\{0,1\}, \max, \min)$ budeme používat označení $\mathbf{2}$.

a) (1 bod) Buď $\mathbf{M} = (M, \vee, \wedge)$ konečný svaz a $\alpha : \mathbf{M} \to \mathbf{2}$ homomorfismus svazů takový, že $1 \in \operatorname{Im} \alpha$. Označme $F_\alpha = \{x \in M; \alpha(x) = 1\}$. Dokažte, že podmnožina F_α má nejmenší prvek, který označíme f_α. Dokažte dále, že prvek f_α je $\vee$-nedosažitelný.

b) (1 bod) Ukažte, že v předchozím tvrzení je předpoklad konečnosti svazu $\mathbf{M}$ nezbytný. Tj. dejte příklad svazu $\mathbf{M}$ a homomorfismus svazů $\alpha : \mathbf{M} \to \mathbf{2}$ takového, že podmnožina $F_\alpha \neq \emptyset$ nemá nejmenší prvek.

c) (3 body) Nechť $\mathbf{M} = (M, \vee, \wedge)$ je svaz. Pro $\vee$-nedosažitelný prvek m svazu $\mathbf{M}$ definujeme podmnožinu $X_m = \{x \in M; x \not\geq m\}$ a zobrazení $\alpha_m : M \to \{0,1\}$ předpisem

$$\alpha_m(x) = \begin{cases} 1 & \text{pro } x \geq m, \\ 0 & \text{pro } x \in X_m. \end{cases}$$

Dokažte, že pokud $\mathbf{M}$ je distributivní svaz, pak X_m je jeho ideál a α_m je homomorfismus svazu $\mathbf{M}$ do svazu $\mathbf{2}$.

d) (1 bod) Ukažte, že v předchozím tvrzení je předpoklad distributivity svazu $\mathbf{M}$ nezbytný. Tj. dejte příklad svazu $\mathbf{M}$ a v něm $\vee$-nedosažitelného prvku m takového, že X_m není ideál a α_m není homomorfismus svazů.

e) (1 bod) O konečném distributivním svazu $\mathbf{M}$ víme, že má právě n $\vee$-nedosažitelných prvků. Určete, kolik existuje homomorfismů ze svazu $\mathbf{M}$ do svazu $\mathbf{2}$.

f) (3 body) Buď $\mathbf{M} = (M, \vee, \wedge)$ konečný distributivní svaz a $P \subseteq M$ jeho podsvaz. Dále buď $\beta : P \to \mathbf{2}$ homomorfismus svazů. Dokažte, že existuje homomorfismus svazů $\alpha : \mathbf{M} \to \mathbf{2}$ takový, že pro všechny prvky $x \in P$ platí $\alpha(x) = \beta(x)$.

Komentář: Hlavním úkolem v tomto kole je tvrzení v části f). Zadání v ostatních částech lze chápat jako přípravné či doplňující. Tvrzení z f) lze také formulovat následujícím způsobem: *Pro konečný distributivní svaz* $\mathbf{M}$ *a jeho podsvaz* P *lze libovolný homomorfismus svazů* $\beta : P \to \mathbf{2}$ *rozšířit na homomorfismus svazů* $\alpha : \mathbf{M} \to \mathbf{2}$. Požadovaná podmínka totiž říká, že zúžení zobrazení α na definiční obor P je dané zobrazení β.

Pro důkaz tvrzení f) lze použít i poznatek, že libovolný prvek v konečném svazu lze zapsat jako supremum $\vee$-nedosažitelných prvků dle věty 7.7 z učebního textu ke svazům a také následujících vět o konečných distributivních svazech.

Pro zisk kladného počtu bodů není nezbytně nutné odevzdávat kompletní řešení jednotlivých úloh. Zejména se nebojte v řešení jedné části zadání použít tvrzení z jiné části, přestože jste potřebné tvrzení sami nedokázali.

Připomeňme ještě, že prvek $m \in M$ se nazývá $\vee$-nedosažitelný, jestliže pro libovolnou dvojici prvků $b, c \in M$ takových, že $m = b \vee c$, platí $m = b$ nebo $m = c$ (viz definice na str. 21 v učebním textu). Svaz $\mathbf{2}$ lze alternativně popsat jako uspořádanou množinu $(\{0,1\}, \leq)$, kde $0 < 1$. Výrokem $x \not\geq m$ samozřejmě máme na mysli negaci výroku $x \geq m$.

Řešení – str. 19.

3. kolo – Konečně generované distributivní svazy

Doporučené znalosti: distributivní svazy, nedosažitelné prvky – přednáška Distr.pdf.

Zadání:

a) (2 body) Nechť $(G, \vee, \wedge)$ je libovolný distributivní svaz a A jeho podmnožina. Dokažte, že pro $\langle A \rangle$, podsvaz svazu $(G, \vee, \wedge)$ generovaný množinou A, platí:

$$\langle A \rangle = \{\ (a_{11} \wedge a_{12} \wedge \cdots \wedge a_{1k_1}) \vee (a_{21} \wedge a_{22} \wedge \cdots \wedge a_{2k_2}) \vee \ldots$$

$$\cdots \vee (a_{n1} \wedge a_{n2} \wedge \cdots \wedge a_{nk_n})\ ;\ n, k_1, \ldots k_n \in \mathbb{N}, a_{11}, \ldots a_{nk_n} \in A\ \}\ .$$

b) (1 bod) Nechť $(G, \vee, \wedge)$ je libovolný distributivní svaz, který je generovaný n-prvkovou množinou prvků A, tj. $\langle A \rangle = G$. O prvku $g \in G$ řekneme, že je infimem generátorů, jestliže lze psát ve tvaru $g = a_1 \wedge a_1 \wedge \cdots \wedge a_k$, kde $k \in \mathbb{N}$ a $a_1, a_2, \ldots, a_k \in A$. Množinu všech prvků, které jsou infimem generátorů, označíme $A^\wedge$. Dokažte, že $A^\wedge$ má nejvýše $2^n - 1$ prvků.

c) (1 bod) Dokažte, že libovolný distributivní svaz, který je generovaný konečnou množinou prvků, je konečný.

d) (2 body) Nechť $(G, \vee, \wedge)$ je libovolný distributivní svaz, který je generovaný 3-prvkovou množinou prvků $\{a, b, c\}$. Dokažte, že $|G| \leq 18$.

e) (1 bod) Pro libovolnou uspořádanou množinu $(M, \leq)$ uvažujeme $H(M)$, množinu všech dědičných podmnožin. Dokažte, že $(H(M), \subseteq)$ je úplný svaz, který je distributivním svazem. Jestliže má navíc uspořádaná množina $(M, \leq)$ nejmenší prvek, pak je distributivním svazem i množina $(D(M), \subseteq)$ všech neprázdných dědičných podmnožin uspořádané množiny $(M, \leq)$.

f) (3 body) Nalezněte největší distributivní svaz, který je generovaný trojicí svých prvků. Tedy, zvolte vhodnou uspořádanou množinu $(M, \leq)$ takovou, že $(D(M), \subseteq)$ má 18 prvků a přitom je svaz $(D(M), \cup, \cap)$ generovaný vhodnou trojicí svých prvků.

Komentář: Protože rozumíte podgrupám generovaným množinou, jistě jste si uvědomili, že existence podsvazu $\langle A \rangle$ je zaručena, neboť $\langle A \rangle$ je průnik všech podsvazů svazu G obsahujících podmnožinu A. Přitom množina všech podsvazů daného svazu uspořádaná inkluzí tvoří úplný svaz.

Připomeňme, že B je dědičná podmnožina uspořádané množiny $(M, \leq)$, jestliže pro každé $b \in B$ a $a \in M$ takové, že $a \leq b$, platí $a \in B$. Zejména si povšimněme, že $\emptyset$ je dědičná podmnožina $(M, \leq)$ a že platí $H(M) = D(M) \cup \{\emptyset\}$. Protože konečný svaz má vždy nejmenší prvek, bylo na str 22. textu o svazech výhodnější pracovat pouze s $D(M)$.

Poznamenejme, že tvrzení c) neplatí pro svazy. Existuje totiž svaz, který je nekonečný a přitom je generovaný svojí čtyřprvkovou podmnožinou. Tento svaz si však ukážeme až na semináři.

Řešení – str. 22.

4. kolo – Reprezentace Booleových algeber pomocí ultrafiltrů

Doporučené znalosti: Booleovy algebry – přednášky Distr.pdf a BooleovyOkruhy.pdf.

Zadání:

a) (1 bod) Nechť F je neprázdný filtr svazu S a x je prvek svazu S. Dokažte, že filtr generovaný sjednocením $F \cup \{x\}$ je roven množině všech prvků $s \in S$, pro které existuje $f \in F$ tak, že $s \geq f \wedge x$.

b) (3 body) Nechť $\boldsymbol{A}$ je netriviální Booleova algebra a F je její neprázdný vlastní filtr. Dokažte, že následující podmínky jsou ekvivalentní:

   (i) F je ultrafiltr $\boldsymbol{A}$,

   (ii) pro každé prvky $x, y \in \boldsymbol{A}$ takové, že $x \vee y \in F$, platí $x \in F$ nebo $y \in F$,

   (iii) pro každý prvek $x \in \boldsymbol{A}$ platí $x \in F$ nebo $x' \in F$.

c) (3 body) Nechť $\boldsymbol{A}$ je netriviální Booleova algebra, F její vlastní filtr a I její vlastní ideál takové, že $F \cap I = \emptyset$. Dokažte, že existuje ultrafiltr U Booleovy algebry $\boldsymbol{A}$ takový, že $F \subseteq U$ a $U \cap I = \emptyset$.

d) (3 body) Nechť $\boldsymbol{A}$ je netriviální Booleova algebra. Označme $\mathcal{U}(\boldsymbol{A})$ množinu všech ultrafiltrů Booleovy algebry $\boldsymbol{A}$. Nechť $i\colon \boldsymbol{A} \to \mathcal{P}(\mathcal{U}(\boldsymbol{A}))$ je zobrazení dané předpisem $i(x) = \{U \in \mathcal{U}(\boldsymbol{A}); x \in U\}$. Dokažte, že i je injektivní homomorfismus Booleových algeber (kde systém $\mathcal{P}(\mathcal{U}(\boldsymbol{A}))$ všech podmnožin množiny $\mathcal{U}(\boldsymbol{A})$ je uspořádán inkluzí).

   [Nápověda: v částech c) a d) lze využít charakterizaci ultrafiltrů v Booleových algebrách z podmínky ii) části b); dále v části c) použijte Zornovo lemma na vhodnou množinu filtrů $\boldsymbol{A}$; pro důkaz injektivity zobrazení v d) využijte tvrzení z c).]

Komentář: Booleova algebra se nazývá *triviální*, pokud má jediný prvek (který je zároveň nulou i jedničkou této algebry). Pokud má Booleova algebra naopak aspoň dva prvky, nazývá se *netriviální*. Snadno se uvidí, že Booleova algebra je netriviální právě tehdy, když v ní platí $0 \neq 1$.

Filtr nebo ideál v nějakém svazu se nazývá *vlastní*, pokud je vlastní podmnožinou daného svazu, tj. není roven celému svazu. V Booleově algebře je zřejmě filtr vlastní resp. neprázdný právě tehdy, když neobsahuje nulu resp. obsahuje jedničku (a analogicky pro ideály). Filtr v nějakém svazu se nazývá *ultrafiltr*, pokud je to maximální (vzhledem k inkluzi) vlastní filtr, tj. pokud v daném svazu neexistuje žádný ostře větší vlastní filtr.

Nakonec uvedeme tvrzení známé jako *Zornovo lemma* (též nazývané Kuratowski–Zornovo lemma nebo princip maximality), které má spoustu aplikací v nejrůznějších oblastech matematiky. Nechť $(S, \leq)$ je neprázdná uspořádaná množina taková, že každý neprázdný řetězec C v S má v S horní závoru (tj. pro každou podmnožinu $\emptyset \neq C \subseteq S$ takovou, že C je vzhledem k danému uspořádání řetězec, existuje prvek množiny S větší nebo roven než všechny prvky C). Potom platí, že pro každý prvek $a \in S$ existuje prvek $m \in S$ takový, že m je maximální prvek S a navíc $m \geq a$. Snadným důsledkem tohoto tvrzení (který se rovněž nazývá Zornovo lemma) je, že S má za daných předpokladů aspoň jeden maximální prvek (naopak z tohoto důsledku snadno plyne předchozí tvrzení, rozmyslete si proč). Zornovo lemma se dokazuje v teorii množin, k důkazu je potřeba tzv. axiom výběru (přesněji platí, že nad tzv. Zermelo–Fraenkelovou teorií množin je Zornovo lemma ekvivalentní axiomu výběru).

Řešení – str. 24.

5. kolo – Mocniny algebraických prvků a rozšíření těles

Doporučené znalosti: stupeň rozšíření, algebraický prvek, – přednáška RozsireniTeles.pdf.

Zadání:

a) (1 bod) Nechť $K \subseteq T$ je algebraické rozšíření těles, nechť P je podokruh tělesa T obsahující těleso K. Dokažte, že pak P je podtěleso tělesa T.

b) (1 bod) Nechť $K \subseteq T$ je rozšíření těles, prvek $\alpha \in T$ je algebraický nad tělesem K. Dokažte, že je-li stupeň rozšíření $[K(\alpha) : K]$ liché číslo, pak platí $K(\alpha) = K(\alpha^2)$.

c) (1 bod) Ukažte na vhodně zvoleném příkladu rozšíření těles $K \subseteq T$ a algebraického prvku $\alpha \in T$, že přestože stupeň rozšíření $[K(\alpha) : K]$ není dělitelný třemi, nemusí platit $K(\alpha) = K(\alpha^3)$.

d) (1 bod) Nechť n je přirozené číslo, nechť $K \subseteq T$ je rozšíření těles a prvek $\alpha \in T$ je algebraický nad tělesem K. Dokažte, že pokud stupeň rozšíření $[K(\alpha) : K]$ není dělitelný žádným prvočísem $p \leq n$, pak platí $K(\alpha) = K(\alpha^n)$.

e) (2 body) Nechť K je podtěleso tělesa komplexních čísel $\mathbb{C}$, nechť $\mu, \nu \in \mathbb{C}$ jsou taková, že platí $\mu^2, \nu^2 \in K$ a současně $\mu + \nu \neq 0$. Dokažte, že pak platí $K(\mu + \nu) = K(\mu, \nu)$.

f) (4 body) Nechť K je podtěleso tělesa komplexních čísel $\mathbb{C}$. Nechť jsou dána čísla $a, b \in K$ taková, že b není druhou mocninou v tělese K. Dokažte, že následující výroky jsou ekvivalentní:

  (i) $a^2 - b$ je druhou mocninou v K.

  (ii) Existuje $\beta \in \mathbb{C}$ takové, že $\beta^2 = b$, a existují $\mu, \nu \in \mathbb{C}$ tak, že platí $\mu^2, \nu^2 \in K$ a současně $a + \beta = (\mu + \nu)^2$.

  (iii) Pro každé $\beta \in \mathbb{C}$ takové, že $\beta^2 = b$, existují $\mu, \nu \in \mathbb{C}$ tak, že platí $\mu^2, \nu^2 \in K$ a současně $a + \beta = (\mu + \nu)^2$.

Komentář: Rozšíření těles $K \subseteq T$ nazýváme algebraické, jestliže každý prvek $\alpha \in T$ je algebraický nad tělesem K. O prvku $b \in K$ říkáme, že je druhou mocninou v tělese K, právě když existuje $r \in K$ tak, že $r^2 = b$.

Poznamenejme, že podmínku z poslední úlohy f) lze také formulovat takto: existují $m, n \in K$ taková, že $\sqrt{a + \sqrt{b}} = \sqrt{m} + \sqrt{n}$ (při vhodné volbě znamének u odmocnin). Všimněte si, že pokud je tato rovnost splněna a b není druhou mocninou v tělese K, pak užitím úlohy e) dostaneme $K(\sqrt{a + \sqrt{b}}) = K(\sqrt{m} + \sqrt{n}) = K(\sqrt{m}, \sqrt{n})$.

Řešení – str. 26.

6. kolo – Uspořádaná a formálně reálná tělesa

Doporučené znalosti: uspořádaní, Algebra I.

Zadání:

a) (1 bod) Nechť F je formálně reálné těleso. Dokažte, že $\operatorname{char} F = 0$.

b) (2 body)

(i) Nechť F je uspořádané těleso. Označme $P = \{a \in F : a \geq 0\}$ množinu všech prvků F, které jsou v daném uspořádání nezáporné. Dokažte, že platí $P + P \subseteq P$, $P \cdot P \subseteq P$, $-1 \notin P$ a $P \cup (-P) = F$.

(ii) Nechť F je těleso a P je jeho podmnožina taková, že platí $P + P \subseteq P$, $P \cdot P \subseteq P$, $-1 \notin P$ a $P \cup (-P) = F$. Definujme na F binární relaci $\leq$ tak, že pro každé $a, b \in F$ je $a \leq b$ právě tehdy, když $b - a \in P$. Dokažte, že tato relace je lineární uspořádání na F, vzhledem ke kterému je to uspořádané těleso.

c) (2 body)

(i) Nechť $\preceq$ je lineární uspořádání tělesa $\mathbb{R}$, vzhledem ke kterému je to uspořádané těleso. Dokažte, že $\preceq = \leq$, kde $\leq$ je standardní uspořádání $\mathbb{R}$.

(ii) Nechť $\trianglelefteq$ je lineární uspořádání tělesa $\mathbb{Q}$, vzhledem ke kterému je to uspořádané těleso. Dokažte, že $\trianglelefteq = \leq$, kde $\leq$ je standardní uspořádání $\mathbb{R}$ zúžené na $\mathbb{Q}$.

d) (2 body) Dokažte, že existují právě dvě lineární uspořádání tělesa $\mathbb{Q}(\sqrt{2})$, vzhledem ke kterým je to uspořádané těleso, a popište, jak vypadají nezáporné prvky v těchto uspořádáních.

[Nápověda: Využijte toho, že existuje automorfismus tělesa $\mathbb{Q}(\sqrt{2})$ zadaný vztahem $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ pro $a, b \in \mathbb{Q}$.]

e) (1 bod) Dokažte, že každé uspořádatelné těleso F je formálně reálné.

f) (2 body) Nechť F je formálně reálné těleso.

(i) Uvažme množinu $\mathcal{S}$ všech podmnožin M tělesa F takových, že $M + M \subseteq M$, $M \cdot M \subseteq M$, $F^2 \subseteq M$ a $-1 \notin M$. Dokažte, že existuje množina $P \in \mathcal{S}$, která je maximální prvek $\mathcal{S}$ vzhledem k inkluzi.

[Nápověda: Použijte Zornovo lemma na uspořádanou množinu $(\mathcal{S}, \subseteq)$ (nezapomeňte také dokázat, že $\mathcal{S}$ je neprázdná).]

(ii) Nechť P je libovolný maximální prvek $\mathcal{S}$ vzhledem k inkluzi. Dokažte, že platí $P \cup (-P) = F$, a odvoďte, že F je uspořádatelné těleso.

[Nápověda: Předpokládejte sporem, že existuje $a \in F$ takové, že $a, -a \notin P$, a uvažte množinu $P + a \cdot P$.]

Komentář: Těleso F se nazývá *formálně reálné*, pokud v něm nejde -1 napsat jako součet čtverců, tj. neexistuje $n \in \mathbb{N}$ a prvky $a_1, \ldots, a_n \in F$ takové, že $-1 = \sum_{i=1}^{n} a_i^2$. Snadno se uvidí, že F je formálně reálné právě tehdy, když v něm nejde 0 napsat jako součet čtverců, z nichž aspoň jeden je nenulový, tj. pokud $0 = \sum_{i=1}^{n} a_i^2$ pro nějaké $n \in \mathbb{N}$ a $a_1, \ldots, a_n \in F$, pak $a_1 = \ldots = a_n = 0$.

Skutečně, pokud by existovaly takové prvky, že $0 = \sum_{i=1}^n a_i^2$ a bez újmy na obecnosti $a_1 \neq 0$, pak by platilo $-1 = \sum_{i=2}^n (a_i/a_1)^2$; naopak ze vztahu $-1 = \sum_{i=1}^n a_i^2$ plyne $0 = 1^2 + \sum_{i=1}^n a_i^2$. Příkladem formálně reálného tělesa je těleso $\mathbb{R}$ nebo jeho libovolné podtěleso.

Uspořádané těleso je struktura $(F, +, \cdot, \leq)$, kde $(F, +, \cdot)$ je těleso a relace $\leq$ je lineární uspořádání (tj. řetězec) na F takové, že:

- pro každé prvky $a, b, c \in F$ platí, že pokud $a \leq b$, pak $a + c \leq b + c$,
- pro každé prvky $a, b \in F$ platí, že pokud $a \geq 0$, $b \geq 0$, pak $ab \geq 0$.

  (Zápis $a \geq b$ znamená totéž, co $b \leq a$, stejně tak můžeme používat symboly $<$ a $>$ obvyklým způsobem.)

Z podmínky z prvního puntíku je snadno vidět, že platí $a \leq b$ právě tehdy, když $b - a \geq 0$. Takováto uspořádání se tedy dají jednoznačně popsat pouze pomocí množiny prvků, které jsou vzhledem k nim nezáporné (tj. větší nebo rovny než 0). Tvrzení z příkladu b) navíc ukazují vlastnosti, které taková množina musí mít. Příkladem uspořádaného tělesa je těleso $\mathbb{R}$ se „standardním“ uspořádáním nebo jeho libovolné podtěleso s příslušným zúženým uspořádáním.

Ne pro každé těleso existuje lineární uspořádání, vzhledem ke kterému je to uspořádané těleso, nebo naopak takových uspořádání může existovat více než jedno. Řekneme, že F je *uspořádatelné těleso*, pokud pro něj aspoň jedno takové uspořádání existuje (nicméně narozdíl od uspořádaného tělesa nemáme vybráno jedno konkrétní). Z tvrzení z příkladů e) a f) plyne, že těleso je uspořádatelné právě tehdy, když je formálně reálné. Příkladem tělesa, které uspořádatelné není, je tedy např. těleso $\mathbb{C}$. Z tvrzení z a) rovněž plyne, že žádné těleso s kladnou charakteristikou není uspořádatelné.

Vysvětlíme ještě použitou notaci. Pro libovolné podmnožiny $A, B \subseteq F$ tělesa F a prvek $c \in F$ značíme $A + B = \{a + b \colon a \in A, b \in B\}$, $A \cdot B = \{ab \colon a \in A, b \in B\}$, $A^2 = \{a^2 \colon a \in A\}$, $-A = \{-a \colon a \in A\}$, $c \cdot A = \{ca \colon a \in A\}$.

Zornovo lemma je vysvětleno v komentáři ke 4. kolu soutěže.

Řešení – str. 27.

7. kolo – Věty o izomorfismech pro okruhy

Doporučené znalosti: ideál okruhu a jím určený faktorokruh – přednášky IdealyOkruhu.pdf a FaktorizaceOkruhu.pdf.

Zadání:

a) (2 body) Nechť R je podokruh okruhu S a I je ideál okruhu S. Dokažte, že $R+I$ je podokruh S, I je ideál $R+I$, $R \cap I$ je ideál R, a okruhy $R/(R \cap I)$ a $(R+I)/I$ jsou izomorfní.

[Nápověda k poslednímu úkolu: Dokažte, že složení inkluze $R \to R+I$ a projekce $R+I \to (R+I)/I$ je surjektivní homomorfismus okruhů, jehož jádro je $R \cap I$.]

b) (2 body) Nechť R je okruh a I, J jsou jeho ideály. Označme p projekci z R do R/I.

(i) Dokažte, že $(J+I)/I$ je ideál okruhu R/I a platí $p(J) = (J+I)/I$.

(ii) Pokud navíc platí $I \subseteq J$, dokažte, že J/I je ideál okruhu R/I a okruhy R/J a $(R/I)/(J/I)$ jsou izomorfní.
[Nápověda: Ukažte, že existuje surjektivní homomorfismus okruhů $R/I \to R/J$, jehož jádro je J/I.]

c) (2 body) Nechť R je okruh, I jeho ideál a p je projekce z R do R/I. Označme $\mathcal{L}(R)$, resp. $\mathcal{L}(R/I)$ svazy ideálů R, resp. R/I uspořádané inkluzí. Dále označme $\mathcal{L}_I(R)$ filtr svazu $\mathcal{L}(R)$ generovaný prvkem I (tj. svaz všech ideálů R, které obsahují I). Konečně označme $\alpha\colon \mathcal{L}_I(R) \to \mathcal{L}(R/I)$ zobrazení definované pro každé $J \in \mathcal{L}_I(R)$ vztahem $\alpha(J) = p(J)$ a $\beta\colon \mathcal{L}(R/I) \to \mathcal{L}_I(R)$ zobrazení dané pro každé $K \in \mathcal{L}(R/I)$ vztahem $\beta(K) = p^{-1}(K)$.

(i) Dokažte, že zobrazení α a β jsou korektně definovaná izotonní zobrazení, která jsou vzájemně inverzní, a odvoďte, že svazy $\mathcal{L}_I(R)$ a $\mathcal{L}(R/I)$ jsou izomorfní.

(ii) Dokažte, že v tomto izomorfismu odpovídají maximální ideály, resp. prvoideály okruhu R obsahující I maximálním ideálům, resp. prvoideálům okruhu R/I.

d) (4 body)

(i) Najděte příklad netriviálních komutativních okruhů R a S, surjektivního homomorfismu okruhů $f\colon R \to S$ a maximálního ideálu M okruhu R takových, že $f(M)$ není maximální ideál S.

(ii) Najděte příklad netriviálních komutativních okruhů R a S, surjektivního homomorfismu okruhů $f\colon R \to S$ a nenulového prvoideálu P okruhu R takových, že $f(P)$ je vlastní ideál okruhu S, který není prvoideál.

Komentář: Poznamenejme, že tvzení z a) se nazývá *druhá věta o izomorfismu*, tvrzení z b) *třetí věta o izomorfismu* a tvrzení z c) *čtvrtá věta o izomorfismu* (nebo také věta o korespondenci, anglicky rovněž lattice theorem). Hlavní věta o faktorokruzích (dokazovaná na přednášce) se často také nazývá *první věta o izomorfismu*. Přesněji řečeno v tomto případě hovoříme o větách o izomorfismech pro okruhy, analogická tvrzení platí pro grupy, vektorové prostory, atd.

Na závěr ještě zmiňme, že součet podokruhu a ideálu je definován podobně jako součet ideálů, tedy $R + I = \{r + a;\, r \in R,\, a \in I\}$.

Řešení – str. 28.

8. kolo – Jacobsonův radikál, nilradikál okruhu a radikál ideálu

Doporučené znalosti: ideál okruhu a jím určený faktorokruh – přednášky IdealyOkruhu.pdf a FaktorizaceOkruhu.pdf.

Zadání:

a) (1 bod) Nechť R je okruh. Dokažte, že pro každý vlastní ideál I tohoto okruhu existuje maximální ideál M okruhu R takový, že $I \subseteq M$.

[Nápověda: Použijte Zornovo lemma na množinu všech vlastních ideálů okruhu R uspořádanou inkluzí.]

b) (2 body) Nechť R je netriviální komutativní okruh a $x \in R$. Dokažte, že $x \in J(R)$ právě tehdy, když pro všechna $r \in R$ platí $1 + rx \in R^{\times}$.

[Nápověda: k důkazu implikace zleva doprava využijte tvrzení z a).]

c) (2 body) Nechť R je komutativní okruh.

(i) Dokažte, že $N(R)$ je ideál okruhu R.

(ii) Nechť I je ideál okruhu R a p je kanonická projekce $R \to R/I$. Dokažte, že $\sqrt{I} = p^{-1}(N(R/I))$, a odvoďte, že $\sqrt{I}$ je ideál okruhu R.

d) (3 body) Nechť R je komutativní okruh a $x \in R$ jeho prvek takový, že $x \notin N(R)$. Označme $S = \{x^n : n \in \mathbb{N}\}$. Dále označme $\mathcal{T}$ množinu všech ideálů okruhu R, které jsou disjunktní s S.

(i) Dokažte, že existuje ideál P okruhu R, který je maximální prvek $\mathcal{T}$ vzhledem k inkluzi. [Nápověda: Použijte Zornovo lemma na uspořádanou množinu $(\mathcal{T}, \subseteq)$ (nezapomeňte dokázat, že $\mathcal{T} \neq \emptyset$).]

(ii) Nechť P je libovolný ideál okruhu R, který je maximální prvek $\mathcal{T}$ vzhledem k inkluzi. Dokažte, že P je prvoideál.

[Nápověda: Předpokládejte sporem, že existují $y, z \in R$ takové, že $y, z \notin P$ a $yz \in P$, a ukažte, že potom platí $P + (y) \in \mathcal{T}$ nebo $P + (z) \in \mathcal{T}$.]

e) (2 body) Nechť R je netriviální komutativní okruh.

(i) Dokažte, že $N(R)$ je roven průniku všech prvoideálů okruhu R.

[Nápověda: k důkazu inkluze „$\supseteq$“ použijte tvrzení z d).]

(ii) Nechť I je vlastní ideál okruhu R. Dokažte, že $\sqrt{I}$ je roven průniku všech prvoideálů okruhu R, které obsahují I.

[Nápověda: Použijte c)ii), e)i) a tvrzení z c)ii) ze 7. kola soutěže.]

Komentář: Nechť R je netriviální komutativní okruh. Pak podle a)i) existuje aspoň jeden maximální ideál tohoto okruhu, neboť $\{0\}$ je jeho vlastní ideál (připomeňme, že vlastním ideálem okruhu R rozumíme každý jeho ideál I splňující $I \neq R$), takže můžeme uvážit průnik všech maximálních ideálů okruhu R. To je zřejmě ideál okruhu R, který se nazývá *Jacobsonův radikál* okruhu R a značí se $J(R)$.

Nechť nyní R je libovolný komutativní okruh a I je jeho ideál. Potom značíme $\sqrt{I}$ množinu všech prvků okruhu R takových, že nějaká jejich mocnina patří do ideálu I, tedy $\sqrt{I} = \{r \in R\colon (\exists n \in \mathbb{N}\colon r^n \in I)\}$. Množina $\sqrt{I}$ se nazývá *radikál ideálu* I. Podle c)ii) je $\sqrt{I}$ ideál okruhu R. Zřejmě platí $I \subseteq \sqrt{I}$, nicméně tato inkluze může být ostrá, například pro ideál $4\mathbb{Z}$ okruhu $\mathbb{Z}$ platí $\sqrt{4\mathbb{Z}} = 2\mathbb{Z}$. Pokud $\sqrt{I} = I$, pak se I nazývá *radikálový ideál*. Snadno se uvidí, že platí $\sqrt{\sqrt{I}} = \sqrt{I}$, takže $\sqrt{I}$ je vždy radikálový ideál. Konečně *nilradikál* okruhu R definujeme jako radikál nulového ideálu a značíme $N(R)$, tj. $N(R) = \sqrt{\{0\}}$. Jinými slovy $N(R)$ je množina všech prvků $x \in R$, pro které existuje $n \in \mathbb{N}$ tak, že $x^n = 0$ (prvek x s touto vlastností se nazývá *nilpotentní*).

Víme, že množina $\mathcal{L}(R)$ všech ideálů okruhu R uspořádaná inkluzí je úplný svaz. Infimum libovolné neprázdné podmnožiny tohoto svazu je rovno průniku všech ideálů patřících do této podmnožiny, zatímco infimum prázdné množiny je rovno nevlastnímu ideálu R. Tvrzení z e)i) a e)ii) jsme tedy ekvivalentně mohli formulovat tak, že $N(R)$, resp. $\sqrt{I}$ jsou rovny infimu množiny všech prvoideálů okruhu R, resp. množiny všech prvoideálů okruhu R obsahujících I ve svazu $\mathcal{L}(R)$. Výhoda této formulace je v tom, že potom tato tvrzení budou platit i pokud je R triviální okruh, resp. I je nevlastní ideál okruhu R. Stejně tak $J(R)$ můžeme ekvivalentně definovat jako infimum množiny všech maximálních ideálů okruhu R v $\mathcal{L}(R)$. Tato definice potom dává smysl i pokud je R triviální okruh, v tom případě bude $J(R) = R$. Rovněž tvrzení z b) bude po tomto rozšíření definice platit i pro triviální R.

Není těžké nahlédnout, že v komutativním okruhu R je každý prvoideál rovněž radikálový ideál (opačná implikace ale neplatí, neboť např. $6\mathbb{Z}$ je radikálový ideál okruhu $\mathbb{Z}$, který není prvoideál). Stejně tak se snadno uvidí, že průnik libovolné neprázdné množiny radikálových ideálů je opět radikálový ideál. Odtud a z úlohy e)ii) dostáváme, že vlastní radikálové ideály okruhu R jsou právě průniky prvoideálů tohoto okruhu. Pokud analogicky jako v předchozím odstavci nahradíme tento průnik infimem ve svazu $\mathcal{L}(R)$, tak bude tato charakterizace platit i pro nevlastní ideál okruhu R (který je zjevně radikálový).

Zornovo lemma je vysvětleno v komentáři ke 4. kolu soutěže.

Řešení – str. 31.

9. kolo – Čínská zbytková věta pro komutativní okruhy

Doporučené znalosti: ideál okruhu a jím určený faktorokruh – přednášky IdealyOkruhu.pdf a FaktorizaceOkruhu.pdf.

Zadání:

a) (1 bod) Nechť R je okruh, I a J ideály okruhu R. Dokažte, že součin $I \cdot J$ ideálů I a J je množina všech konečných součtů prvků tvaru $r \cdot s$, kde $r \in I$ a $s \in J$, tedy

$$I \cdot J = \Big\{ \sum_{i=1}^{n} r_i \cdot s_i;\ n \in \mathbb{N},\, r_1, \dots, r_n \in I,\, s_1, \dots, s_n \in J \Big\}.$$

Dokažte dále inkluzi $I \cdot J \subseteq I \cap J$.

b) (1 bod) Nechť R je okruh, I, J, K ideály okruhu R. Dokažte, že platí rovnost

$$(I \cdot J) \cdot K = I \cdot (J \cdot K).$$

c) (1 bod) Nechť R je komutativní okruh. Dokažte, že je-li $I = (a_1, \dots, a_n)$ ideál generovaný množinou $\{a_1, \dots, a_n\} \subseteq R$ a $J = (b_1, \dots, b_m)$ ideál generovaný množinou $\{b_1, \dots, b_m\} \subseteq R$, pak jejich součin $I \cdot J$ je ideál generovaný množinou všech součinů $a_i \cdot b_j$ těchto generátorů, tj.

$$I \cdot J = \big(\{a_i \cdot b_j;\ i = 1, \dots, n,\ j = 1, \dots, m\}\big).$$

d) (1 bod) Nechť R je okruh, I, J, K ideály okruhu R. Dokažte, že pokud je ideál I nesoudělný s oběma ideály J a K, pak je ideál I nesoudělný s jejich součinem $J \cdot K$.

e) (1 bod) Nechť R je komutativní okruh a I, J nesoudělné ideály okruhu R. Dokažte, že pak $I \cdot J = I \cap J$.

f) (5 bodů) Nechť R je komutativní okruh a $I_1, I_2, \dots, I_n$, kde $n \geq 2$, ideály okruhu R. Definujme zobrazení $\varphi\colon R \to R/I_1 \times \cdots \times R/I_n$ předpisem

$$\varphi(x) = (x + I_1,\ x + I_2,\ \dots,\ x + I_n)$$

pro libovolné $x \in R$.

(i) Dokažte, že φ je homomorfismus okruhů s jádrem $I_1 \cap I_2 \cap \cdots \cap I_n$.

(ii) Dokažte, že φ je surjektivní, právě když ideály $I_1, I_2, \dots, I_n$ jsou po dvou nesoudělné.

(iii) Dokažte, že jsou-li ideály $I_1, \dots, I_n$ jsou po dvou nesoudělné, pak $I_1 \cdot I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$, a tedy homomorfismus φ dává izomorfismus $R/(I_1 \cdot I_2 \cdots I_n) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n$.

[Nápověda: Pro ii) a iii) použijte indukci vzhledem k n. V ii) v případě $n = 2$ využijte prvky $r \in I_1$ a $s \in I_2$ splňující $r + s = 1$ k tomu, abyste pro dané $a, b \in R$ sestrojili prvek $c = r \cdot b + s \cdot a$ a ukázali, že $c \in (a + I_1) \cap (b + I_2)$. Užitečné jsou i úlohy d) a e).]

Komentář: Součin ideálů I a J okruhu R je definován jako ideál generovaný množinou $\{r \cdot s;\ r \in I,\ s \in J\}$ všech součinů prvků ideálu I s prvky ideálu J, úloha a) popisuje, jaké má tento ideál prvky. Uvědomte si, že rovnost dokázaná v úloze b) znamená, že množina všech ideálů okruhu R tvoří s operací násobení pologrupu, máme tedy definován součin libovolného konečného počtu ideálů.

Ideály I a J okruhu R se nazývají nesoudělné, jestliže $I + J = R$, což je podmínka ekvivalentní s tím, že existují $r \in I$ a $s \in J$ tak, že $r + s = 1$. Ideály $I_1, \dots, I_n$ okruhu R se nazývají po dvou nesoudělné, jestliže pro každé $1 \leq j < k \leq n$ jsou ideály I_j a I_k nesoudělné.

Tvrzení f) se nazývá Čínská zbytková věta pro komutativní okruhy. Z Algebry I známe její speciální případ pro okruh celých čísel $\mathbb{Z}$ a dvě nesoudělná přirozená čísla m, n. Pak jsou hlavní ideály (m), (n) nesoudělné (vzpomeňte si na Bezoutovu identitu) a podle c) platí $(m) \cdot (n) = (mn)$. Proto $\mathbb{Z}/(m) \times \mathbb{Z}/(n) \cong \mathbb{Z}/(mn)$, neboli $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Řešení – str. 32.

10. kolo – Okruhy polynomů a formálních mocninných řad nad komutativním okruhem

Doporučené znalosti: polynomy, 8. a 9. kolo soutěže.

Zadání:

a) (2 body) Nechť R je komutativní okruh a $f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ je formální mocninná řada nad R, kde $a_i \in R$ pro všechna $i \in \mathbb{N}_0$. Dokažte, že $f(x) \in R[[x]]^\times$ právě tehdy, když $a_0 \in R^\times$.

   [Nápověda: V důkazu implikace zprava doleva rekurzivně zkonstruujte posloupnost koeficientů inverze prvku $f(x)$.]

b) (4 body) Nechť R je komutativní okruh a $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ je polynom nad R, kde $n \in \mathbb{N}_0$ a $a_i \in R$ pro všechna $0 \le i \le n$. Dokažte, že $f(x) \in R[x]^\times$ právě tehdy, když $a_0 \in R^\times$ a $a_i \in N(R)$ pro všechna $1 \le i \le n$.

   [Nápověda: Pro implikaci zleva doprava použijte tvrzení z e)i) z 8. kola soutěže, pro implikaci zprava doleva použijte tvrzení z a) a ukažte, že inverzní prvek prvku $f(x)$ v $R[[x]]$ je polynom.]

c) (4 body) Nechť R je komutativní okruh a $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ je nenulový polynom nad R stupně n, kde $n \in \mathbb{N}_0$, $a_i \in R$ pro všechna $0 \le i \le n$ a $a_n \ne 0$. Dokažte, že $f(x)$ je dělitel nuly v okruhu $R[x]$ právě tehdy, když existuje nenulové $c \in R$takové, že $cf(x) = 0$.

   [Nápověda: Pro důkaz implikace ve směru zleva doprava uvažte nenulový polynom $g(x) = \sum_{i=0}^{m} b_i x^i$ nad R nejmenšího možného stupně takový, že platí $f(x)g(x) = 0$, a předpokládejte sporem, že $\mathrm{st}(g(x)) > 0$. Dokažte, že existuje $\ell \in \{0, \dots, n\}$, pro které je $a_\ell g(x) \ne 0$, a že pro největší takové ℓ platí $\mathrm{st}(a_\ell g(x)) < \mathrm{st}(g(x))$.]

Komentář: Nechť R je komutativní okruh. *Formální mocninná řada* nad R je formální výraz $\sum_{i=0}^{\infty} a_i x^i$, kde $a_i \in R$ pro $i \in \mathbb{N}_0$. Narozdíl od reálných nebo komplexních mocninných řad používaných v matematické analýze zde x nechápeme jako (reálnou nebo komplexní) proměnnou, ale pouze jako abstraktní symbol, stejně tak nekonečná suma v tomto výrazu je pouze formální. Formální mocninnou řadu tedy můžeme chápat jako posloupnost $\{a_i\}_{i=0}^{\infty}$ prvků R, nicméně výše uvedený zápis je více intuitivní pro počítání s těmito řadami. Množinu všech formálních mocninných řad nad okruhem R značíme $R[[x]]$ (popřípadě s jiným písmenem místo x).

Na množině $R[[x]]$ můžeme definovat operace sčítaní a násobení takové, že je vzhledem k nim komutativní okruh. Sčítaní definujeme „po složkách“, tj. pro formální mocninné řady $\sum_{i=0}^{\infty} a_i x^i$, $\sum_{i=0}^{\infty} b_i x^i \in R[[x]]$, kde $a_i, b_i \in R$ pro všechna $i \in \mathbb{N}_0$, máme

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) + \left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} (a_i + b_i) x^i.$$

Násobení definujeme tak, že vynásobíme členy „každý s každým“ a dáme dohromady členy se stejnými mocninami, tj.

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) x^i,$$

kde vnitřní suma je konečný součet v okruhu R a vnější suma je formální (takto definovaný součin mocninných řad se nazývá *Cauchyho součin*).

Není těžké (byť trochu pracné) ověřit, že $R[[x]]$ s takto definovanými operacemi je skutečně komutativní okruh. Stejně tak se snadno uvidí, že okruh polynomů $R[x]$ můžeme považovat za podokruh okruhu $R[[x]]$ (pokud každý polynom ztotožníme s příslušnou formální mocninnou řadou, která má jenom konečně mnoho nenulových koeficientů).

Hlavní výhodou formálních mocninných řad oproti mocninným řadám chápaným jako funkce proměnné x je v tom, že zde nemusíme řešit, jestli a kde daná řada konverguje. Například přímo z výše uvedených definic se snadno spočítá, že pro libovolný komutativní okruh R platí v $R[[x]]$ rovnost $\left(\sum_{i=0}^{\infty} x^i\right) \cdot (1-x) = 1$ (kde používáme výše popsanou konvenci, tj. např. $1-x$ chápeme jako formální mocninnou řadu $\sum_{i=0}^{\infty} a_i x^i$, kde $a_0 = 1$, $a_1 = -1$ a $a_i = 0$ pro $i \geq 2$, stejně tak $\sum_{i=0}^{\infty} x^i$ samozřejmě znamená $\sum_{i=0}^{\infty} 1 \cdot x^i$). Pokud ovšem tuto rovnost chápeme jako rovnost funkcí reálné nebo komplexní proměnné, tak platí pouze pro $|x| < 1$.

Připomeňme, že nenulový prvek $a \in R$ komutativního okruhu R se nazývá dělitel nuly, pokud existuje nenulové $b \in R$ takové, že $ab = 0$ (obecněji pokud daný okruh není komutativní, tak je třeba rozlišovat levé a pravé dělitele nuly). Dále připomeňme, že $N(R)$ značí nilradikál komutativního okruhu R, tj. množinu všech nilpotentních prvků tohoto okruhu, viz komentář k 8. kolu soutěže.

Řešení – str. 34.

Část II – Řešení

1. kolo — řešení

Označme Δ nejmenší prvek v uspořádané množině $\mathcal{E}$, tj. $\Delta = \{(n,n); n \in \mathbb{N}\}$.

a) Ve svazu $\mathcal{R}$ platí $\inf\{\rho,\sigma\} = \rho \cap \sigma$ a $\sup\{\rho,\sigma\} = \rho \cup \sigma$. Aby podmnožina $\mathcal{E}$ byla podsvazem svazu $\mathcal{R}$, musí být průnik i sjednocení dvou relací ekvivalence ρ, σ také relace ekvivalence. To pro průnik platí, ovšem pro sjednocení nikoliv, jak lze ukázat například následujícím protipříkladem. Buď $\rho = \Delta \cup \{(1,2),(2,1)\}$ a $\sigma = \Delta \cup \{(2,3),(3,2)\}$. Relace $\tau = \rho \cup \sigma$, která je supremem relací ρ a σ ve svazu $\mathcal{R}$, není relace ekvivalence, protože $(1,2) \in \tau$, $(2,3) \in \tau$ a $(1,3) \notin \tau$.

Podobně lze pro $\mathcal{U}$ uvážit uspořádání $\rho = \Delta \cup \{(1,2)\}$ a $\sigma = \Delta \cup \{(2,1)\}$, pro něž relace $\tau = \rho \cup \sigma = \Delta \cup \{(1,2),(2,1)\}$ není antisymetrická, a není tedy ani uspořádání.

Ani $\mathcal{E}$ ani $\mathcal{U}$ není podsvazem svazu $(\mathcal{R}, \cup, \cap)$.

b), c) Dokážeme, že $\mathcal{E}$ je úplný svaz, čímž jednak dokážeme úlohu b) a zároveň pozitivně zodpovíme otázku v úloze c).

Nejmenším prvkem $\mathcal{E}$ je Δ a největším prvkem je relace $\mathbb{N} \times \mathbb{N}$, což je infimum prázné podmnožiny. Podle věty o úplných svazech tak stačí dokázat, že libovolný systém prvků $Z = \{\rho_i \in \mathcal{E}; i \in I\}$, kde I je neprázná indexová množina, má infimum. Ukážeme, že $\inf Z = \bigcap_{i\in I} \rho_i$. Označme uvažovanou relaci $\tau = \bigcap_{i\in I} \rho_i$ a dokažme nejdříve, že τ je relace ekvivalence.

Protože pro všechna $i \in I$ platí $\Delta \subseteq \rho_i$, vidíme, že $\Delta \subseteq \bigcap_{i\in I} \rho_i = \tau$, a tudíž τ je reflexivní relace. Snadno se také dokáže, že symetrie relace τ plyne ze symetrie všech relací ρ_i: pro libovolná $a, b \in \mathbb{N}$ platí

$$(a,b) \in \tau \implies (\forall i \in I \ : \ (a,b) \in \rho_i) \implies (\forall i \in I \ : \ (b,a) \in \rho_i) \implies (b,a) \in \tau.$$

Podobně se dokáže tranzitivita: pro libovolná $a, b, c \in \mathbb{N}$ platí

$$(a,b),(b,c) \in \tau \implies (\forall i \in I \ : \ (a,b),(b,c) \in \rho_i) \implies (\forall i \in I \ : \ (a,c) \in \rho_i) \implies (a,c) \in \tau.$$

Zbývá dokázat, že τ je infimem množiny $Z = \{\rho_i \in \mathcal{E}; i \in I\}$. Protože pro všechna $i \in I$ máme $\tau \subseteq \rho_i$, je τ dolní závorou množiny Z. Buď dále α libovolná dolní závora Z, tj. $\alpha \subseteq \rho_i$ pro všechna $i \in I$. Potom $\alpha \subseteq \bigcap_{i\in I} \rho_i = \tau$ a τ je tudíž největší dolní závora Z, tj. $\tau = \inf Z$.

d) Ukážeme, že uspořádaná množina $\mathcal{U}$ není svaz, a tudíž ani úplný svaz. Stačí uvažovat například dvě uspořádání z části a): $\rho = \Delta \cup \{(1,2)\} \in \mathcal{U}$ a $\sigma = \Delta \cup \{(2,1)\} \in \mathcal{U}$. Pro tyto prvky neexistuje prvek $\alpha \in \mathcal{U}$, který by byl horní závorou dvouprvkové množiny $\{\rho,\sigma\}$, protože předpoklady $(1,2) \in \rho \subseteq \alpha$, $(2,1) \in \sigma \subseteq \alpha$ jsou ve sporu s předpokladem, že α je antisymetrická relace.

e) Aby zobrazení bylo homomorfismem svazů, musí zachovávat obě operace, tj. infima i suprema. Ukážeme, že i) f je homomorfismus a ii) zúžení f na $\mathcal{E}$ homomorfismus není. V případě $\mathcal{U}$ pak není třeba nad otázkou přemýšlet, protože $\mathcal{U}$ není svaz, a tudíž zúžení f na $\mathcal{U}$ nemůže být homomorfismus svazů.

Ad i): Pro zobrazení f a libovolnou dvojici relací $\rho, \sigma \in \mathcal{R}$ ověříme, že platí $f(\rho \cup \sigma) = f(\rho) \cup f(\sigma)$ i $f(\rho \cap \sigma) = f(\rho) \cap f(\sigma)$.

Pro libovolný prvek $a \in \mathbb{N}$ platí násedující ekvivalence:

$$a \in f(\rho \cup \sigma) \iff (a,1) \in \rho \cup \sigma \iff ((a,1) \in \rho \text{ nebo } (a,1) \in \sigma) \iff$$

$$\iff (a \in f(\rho) \text{ nebo } a \in f(\sigma)) \iff a \in f(\rho) \cup f(\sigma).$$

A také platí podobné ekvivalence:

$$a \in f(\rho \cap \sigma) \iff (a,1) \in \rho \cap \sigma \iff ((a,1) \in \rho \text{ a současně } (a,1) \in \sigma) \iff$$

$$\iff (a \in f(\rho) \text{ a současně } a \in f(\sigma)) \iff a \in f(\rho) \cap f(\sigma).$$

Ad ii): v případě svazu $\mathcal{E}$ zobrazení $f|_{\mathcal{E}}$ nezachovává suprema, jak lze vidět z následujícího příkladu. Buď $\rho = \Delta \cup \{(1,2),(2,1)\}$ a $\sigma = \Delta \cup \{(2,3),(3,2)\}$. Označme $\tau = \rho \vee \sigma = \Delta \cup \{(1,2),(2,1),(2,3),(3,2),(1,3),(3,1)\}$. Potom $f(\rho) = \{1,2\}$, $f(\sigma) = \{1\}$, $f(\tau) = \{1,2,3\}$ a tedy $f(\rho \vee \sigma) = f(\tau) = \{1,2,3\}$ a $f(\rho) \cup f(\sigma) = \{1,2\} \cup \{1\} = \{1,2\}$. Proto $f(\rho \vee \sigma) \neq f(\rho) \cup f(\sigma)$.

f) Protože množina $\mathbb{N} \times \mathbb{N}$ je spočetná, existuje bijekce mezi množinami $\mathbb{N} \times \mathbb{N}$ a $\mathbb{N} \setminus \{1\}$. Označme $\alpha : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \setminus \{1\}$ nějakou takovou bijekci. Intuitivně lze tedy říci, že jsme prvky množiny $\mathbb{N} \times \mathbb{N}$ očíslovali přirozenými čísly („labely“) většími než 1.

Dále pro libovolnou relaci $\rho \in \mathcal{R}$ označíme $\beta(\rho) = \{\alpha(x); x \in \rho\} \cup \{1\}$. Relace ρ je podmnožina množiny $\mathbb{N} \times \mathbb{N}$ a $\beta(\rho)$ je množina „labelů“ prvků ρ obohacená číslem 1. Zejména platí $\beta(\rho) \subseteq \mathbb{N}$ a definovali jsme tedy zobrazení $\beta : \mathcal{R} \to \mathcal{P}(\mathbb{N})$. Přitom je vidět, že zobrazení β je injektivní a navíc není obtížné dokázat, že se jedná i o homomorfismus svazu $(\mathcal{R}, \cup, \cap)$ do svazu $(\mathcal{P}(\mathbb{N}), \cup, \cap)$. (Dokonce bychom mohli říci, že se jedná o izomorfismus svazu $\mathcal{R}$ a podsvazu $\mathcal{P}(\mathbb{N})$ sestávajícího z podmnožin obsahujících prvek 1.)

Konečně pro relaci $\rho \in \mathcal{R}$ označíme $g(\rho) = (\beta(\rho) \times \beta(\rho)) \cup \Delta \subseteq \mathbb{N} \times \mathbb{N}$. Snadno se ověří, že pro libovolnou množinu $A \subseteq \mathbb{N}$ je relace $(A \times A) \cup \Delta$ relací ekvivalence na $\mathbb{N}$ – tuto relaci budeme značit τ_A. Proto je g korektně definované zobrazení z množiny $\mathcal{R}$ do množiny $\mathcal{E}$ a můžeme psát $g(\rho) = \tau_{\beta(\rho)}$. Vzhledem k tomu, že z rovnosti $\tau_A = \tau_B$ plyne $A = B$ a že β je injektivní zobrazení, dostaneme navíc, že g je injektivní zobrazení.

Uvažme nyní dvě podmnožiny $A, B \subseteq \mathbb{N}$ obsahující číslo 1 a k nim příslušné relace ekvivalence τ_A a τ_B. Potom ve svazu $\mathcal{E}$ platí:

$$\tau_A \wedge \tau_B = \tau_A \cap \tau_B = \tau_{A \cap B}, \quad \tau_A \vee \tau_B = \tau_{A \cup B}\,. \quad (*)$$

První rovnost plyne z jednoduché množinové rovnosti

$$(A \times A) \cap (B \times B) = (A \cap B) \times (A \cap B)$$

a druhá plyne ze skutečnosti, že supremum se ve svazu $\mathcal{E}$ počítá jako tranzitivní obal sjednocení příslušných relací. (Poznamenejme, že pro platnost druhé rovnosti je nezbytné, aby množiny A a B měly neprázdný průnik, což nám zajišťují předpoklady $1 \in A$, $1 \in B$.)

Zbývá nám dokázat, že zobrazení g zachovává operace infima a suprema. Buďte $\rho, \sigma \in \mathcal{R}$ libovolné relace. Pak

$$g(\rho \cup \sigma) = \tau_{\beta(\rho \cup \sigma)} = \tau_{\beta(\rho) \cup \beta(\sigma)} = \tau_{\beta(\rho)} \vee \tau_{\beta(\sigma)} = g(\rho) \vee g(\sigma)\ ,$$

kde první a čtvrtá rovnost platí dle definice zobrazení g, druhá rovnost platí, neboť β je homomorfismus svazů, a třetí rovnost plyne z vlastnosti $(*)$. Podobně dostaneme

$$g(\rho \cap \sigma) = \tau_{\beta(\rho \cap \sigma)} = \tau_{\beta(\rho) \cap \beta(\sigma)} = \tau_{\beta}(\rho) \wedge \tau_{\beta(\sigma)} = g(\rho) \wedge g(\sigma)\ .$$

Dokázali jsme, že g je injektivní homomorfismus svazu $\mathcal{R}$ do svazu $\mathcal{E}$.

2. kolo — řešení

a) Z předpokladu $1 \in \operatorname{Im} \alpha$ plyne $M \neq \emptyset$ i $F_\alpha \neq \emptyset$. Ukážeme, že neprázdná podmnožina F_α je uzavřená na operaci $\wedge$. Pokud $x, y \in F_\alpha$, pak $\alpha(x) = \alpha(y) = 1$, a protože α je homomorfismus svazů, dostáváme $\alpha(x \wedge y) = \alpha(x) \wedge \alpha(y) = 1 \wedge 1 = 1$, tzn. $x \wedge y \in F_\alpha$. Protože M je konečný svaz, je i množina F_α konečná a existuje tudíž $n \in \mathbb{N}$, a prvky $f_1, \ldots, f_n \in M$ takové, že $F_\alpha = \{f_1, \ldots, f_n\}$. Můžeme proto uvažovat prvek $f_1 \wedge \cdots \wedge f_n$, tj. infimum všech prvků množiny F_α. Protože je F_α uzavřená na operaci $\wedge$, vidíme, že prvek $f_\alpha = f_1 \wedge \cdots \wedge f_n$ je prvkem F_α. (Formálně se indukcí vzhledem ke k dokáže fakt $f_1 \wedge \cdots \wedge f_k \in F_\alpha$.) Navíc zřejmě platí $f_\alpha \leq f$ pro libovolný prvek $f \in F_\alpha$, a proto f_α je nejmenší prvek podmnožiny F_α.

Předpokládejme nyní, že máme dva prvky $b, c \in M$ takové, že $f_\alpha = b \vee c$. Zejména tedy platí $b, c \leq f_\alpha$. Protože $1 = \alpha(f_\alpha) = \alpha(b \vee c) = \alpha(b) \vee \alpha(c)$, nemůže být zároveň $\alpha(b) = 0$ a $\alpha(c) = 0$. Ovšem z předpokladu $\alpha(b) = 1$ dostáváme $b \in F_\alpha$ a tedy $f_\alpha \leq b$. To společně s $b \leq f_\alpha$ dává $b = f_\alpha$. Stejným způsobem z předpokladu $\alpha(c) = 1$ plyne $c = f_\alpha$. Dokázali jsme tedy, že f_α je $\vee$-nedosažitelný prvek v M.

Poznamenejme ještě, že F_α je filtr, protože pro libovolné prvky $x, y \in M$, splňující $x \in F_\alpha$ a $y \geq x$, dostáváme $\alpha(y) = \alpha(x \vee y) = \alpha(x) \vee \alpha(y) = 1 \vee \alpha(y) = 1$. (Tzn. fakt, že F_α je nahoru uzavřená podmnožina, plyne ze skutečnosti, že každý homomorfismus svazů je zároveň izotonní zobrazení.) Lze tedy F_α vyjádřit jako $F_\alpha = \{x \in M; x \geq f_\alpha\}$, což se nám bude hodit později.

b) Důkaz v předchozí části fungoval, protože pro konečnou množinu F_α bylo možné uvažovat infimum všech jejich prvků. V protipříkladu tedy stačí, aby F_α obsahovala nekonečný klesající řetězec bez infima. Například lze uvažovat množinu všech celých čísel $\mathbb{Z}$ uspořádanou dle velikosti. Pokud α bude konstantní zobrazení do 1, pak zřejmě množina $F_\alpha = \mathbb{Z}$ nemá nejmenší prvek. Jiným příkladem je třeba svaz $(\mathbb{Q}, \leq)$, taktéž uspořádaný dle velikosti, spolu se zobrazením α, které kladným číslům přiřadí 1 a nekladným 0. Zde F_α je podmnožina kladných racionálních čísel, která nemá nejmenší prvek.

c) Zjevně je množina $X_m = \{x \in M; x \ngeq m\}$ dolů uzavřená: pro $x \in X_m$, $x \geq y$ by $y \notin X_m$ totiž znamenalo $x \geq y \geq m$, což je spor s $x \in X_m$. Uzavřenost množiny X_m na operaci supremum dokážeme sporem. Předpokládejme existenci prvků $x, y \in X_m$ takových, že $x \vee y \notin X_m$. Potom platí $x \vee y \geq m$. Proto $m \wedge (x \vee y) = m$. Nyní použijeme distributivitu svazu M: $m = m \wedge (x \vee y) = (m \wedge x) \vee (m \wedge y)$. Protože m je $\vee$-nedosažitelný prvek v M, dostaneme buď $m \wedge x = m$ nebo $m \wedge y = m$. První možnost znamená $m \leq x$ a druhá $m \leq y$. Oba případy jsou ve sporu s předpokladem $x, y \in X_m$, a proto je předpoklad $x \vee y \notin X_m$ nesplnitelný. Dokázali jsme, že podmnožina X_m je uzavřená na operaci supremum, a je tedy ideál.

Uvažme nyní zobrazení $\alpha_m : M \to \{0, 1\}$ a libovolné prvky $x, y \in M$. Potřebujeme ověřit, že platí následující rovnosti

$$\alpha_m(x \wedge y) = \alpha_m(x) \wedge \alpha_m(y), \qquad (*)$$

$$\alpha_m(x \vee y) = \alpha_m(x) \vee \alpha_m(y) . \qquad (**)$$

Dokažme nejdříve rovnost $(*)$. Pokud $x \in X_m$ nebo $y \in X_m$, pak $x \wedge y \in X_m$, protože X_m je ideál. Obě strany rovnosti $(*)$ jsou tedy rovny 0. Pokud $x \notin X_m$ a zároveň $y \notin X_m$, pak $x \geq m$ a $y \geq m$, z čehož plyne $x \wedge y \geq m$. Dle definice α_m máme v tomto případě $\alpha_m(x) = \alpha_m(y) = \alpha_m(x \wedge y) = 1$ a rovnost $(*)$ opět platí.

Nyní ověříme rovnost $(**)$. Pokud x i y náleží do ideálu X_m, pak máme i $x \vee y \in X_m$, a proto rovnost $(**)$ v tomto případě platí, neboť $\alpha_m(x) = \alpha_m(y) = \alpha_m(x \vee y) = 0$. Pokud $x \notin X_m$ nebo $y \notin X_m$, tj. $x \geq m$ nebo $y \geq m$, pak $x \vee y \geq m$ a obě strany rovnosti $(**)$ jsou rovny 1. Tím jsme dokončili ověření obou požadovaných rovností $(*)$, $(**)$, a α_m je homomorfismus svazů.

d) Uvažme svaz M_5, tj. svaz obsahující nejmenší prvek 0, největší prvek 1 a trojici nesrovnatelných prvků x, y, z, pro něž platí $0 < x, y, z < 1$. Potom pro $m = x$ máme $X_m = \{0, y, z\}$, což není ideál, neboť $y \vee z \notin X_m$. (Povšimněme si, že X_m je dolů uzavřená podmnožina, protože v části c) jsme pro důkaz této vlastnosti distributivitu nepotřebovali.)

Dále $\alpha_m(y \vee z) = \alpha_m(1) = 1$, přitom $\alpha_m(y) = \alpha_m(z) = 0$. Tedy α_m není homomorfismus.

e) Je-li $\mathbf{M}$ prázdný svaz, pak existuje právě jeden homomorfismus svazu $\mathbf{M}$ do svazu $\mathbf{2}$. Předpokládejme dále, že $M \neq \emptyset$. Označme A množinu všech $\vee$-nedosažitelných prvků svazu $\mathbf{M}$ a B množinu všech homomorfismů svazu $\mathbf{M}$ do svazu $\mathbf{2}$, které zobrazují některý prvek na prvek 1. Z konečnosti množiny M plyne i konečnost množin A a B. Zřejmě existuje jediný homomorfismus svazu $\mathbf{M}$ do svazu $\mathbf{2}$, který není prvkem B, a tím je konstantní zobrazení na prvek 0. Proto je počet všech homomorfismů svazu $\mathbf{M}$ do svazu $\mathbf{2}$ roven $|B|+1$.

V části c) jsme pro libovolný prvek $m \in A$ zkonstruovali homomorfismus $\alpha_m \in B$. Můžeme tedy definovat zobrzení $\varphi : A \to B$, které prvku m přiřadí $\varphi(m) = \alpha_m$. Přitom pokud pro dva prvky $m, n \in A$ platí $\alpha_m = \alpha_n$, potom z rovnosti $1 = \alpha_m(m) = \alpha_n(m)$ plyne $m \geq n$, a naopak z rovnosti $1 = \alpha_n(n) = \alpha_m(n)$ plyne $n \geq m$. Tedy předpoklad $\alpha_m = \alpha_n$ implikuje $m = n$. Zobrazení φ je tedy injektivní a proto $|A| \leq |B|$.

V části a) jsme pro libovolný homomorfismus $\alpha \in B$ definovali F_α jako množinu všech prvků x splňujících $\alpha(x) = 1$, ukázali jsme, že má nejmenší prvek $f_\alpha \in F_\alpha$, a odvodili jsme rovnost $F_\alpha = \{x \in M; x \geq f_\alpha\}$. Můžeme tedy definovat zobrazení ψ, které homomorfismu $\alpha \in B$ přiřadí prvek f_α. Protože jsme dokázali, že prvek f_α je $\vee$-nedosažitelný, je ψ zobrazení množiny B do množiny A. Přitom pokud pro dva homomorfismy $\alpha, \beta \in B$ platí $f_\alpha = f_\beta$, potom $F_\alpha = \{x \in M; x \geq f_\alpha\} = \{x \in M; x \geq f_\beta\} = F_\beta$. Pro libovolné $x \in M$ tedy máme $\alpha(x) = 1 \iff x \in F_\alpha = F_\beta \iff \beta(x) = 1$. Předpoklad $f_\alpha = f_\beta$ proto implikuje $\alpha = \beta$. Zobrazení ψ je injektivní a tudíž $|B| \leq |A|$.

Dokázali jsme, že $|A| = |B|$. Počet všech homomorfismů svazu $\mathbf{M}$ do $\mathbf{2}$ je proto roven $|B|+1 = |A|+1 = n+1$.

f) Pokud $P = \emptyset$ nebo β je konstantní zobrazení, pak lze za α vzít také konstantní zobrazení. (V případě $M = \emptyset$ míníme konstatním zobrazením prázdné zobrazení.) Předpokládejme tedy, že $P \neq \emptyset$ a $\operatorname{Im}\beta = \{0, 1\}$.

Protože P je podsvaz $\mathbf{M}$, je také konečným distributivním svazem a můžeme na něj a na homomorfismus β aplikovat předchozí poznatky. Zejména dle části a) je podmnožina $F_\beta \subseteq P$ filtr v P s nejmenším prvkem $m = f_\beta$. Tento prvek m je $\vee$-nedosažitelný v P a proto $X_m = \{x \in P; x \ngeq m\}$ je ideál v P, dle části c). Přitom $X_m \neq \emptyset$, neboť $X_m = \emptyset$ by znamenalo, že m je nejmenší prvek P a β je konstantní zobrazení do 1, což jsme vyloučili předpokladem $\operatorname{Im}\beta = \{0, 1\}$. Protože svaz P je konečný, má neprázdný ideál X_m největší prvek (je to supremum všech jeho prvků) i. Pro libovolný prvek $x \in P$ tedy platí $\beta(x) = 1 \iff x \geq m$ a $\beta(x) = 0 \iff x \leq i$. Také vidíme, že z $i \in X_m$ plyne $i \ngeq m$. Dodejme ještě, že množiny X_m a $F_\beta = \{x \in P; x \geq m\}$ jsou tedy dvě disjunktní podmnožiny množiny P, jejichž sjednocení je celá množina P. (Tvoří tedy rozklad množiny P.)

Prvek m nemusí být $\vee$-nedosažitelný v M, ale z konečnosti M plyne, že m lze psát jako supremum $\vee$-nedosažitelných prvků v M, tj. $m = m_1 \vee m_2 \vee \cdots \vee m_k$, kde $m_1, \dots, m_k$ jsou vhodné $\vee$-nedosažitelné prvky v M. Snadno se vidí, že existuje index $j \in \{1, \dots, k\}$ takový, že $i \ngeq m_j$, protože předpoklad $i \geq m_j$ pro všechna $j \in \{1, \dots, k\}$ implikuje $i \geq m_1 \vee m_2 \vee \cdots \vee m_k = m$, což není pravda. Našli jsem tedy $\vee$-nedosažitelný prvek $q = m_j$ v M, pro který platí $q \leq m$, $i \ngeq q$.

Uvažme nyní homomorfismus svazů $\alpha_q : \mathbf{M} \to \mathbf{2}$ definovaný v části c). Pro něj a libovolný prvek $x \in P$ platí: pokud $x \geq m$, pak $x \geq m \geq q$ a tedy $\alpha_q(x) = 1$ a pokud $x \leq i$, pak $x \ngeq q$ (neboť $x \geq q$ znamená $q \leq x \leq i$, spor) a tedy $\alpha_q(x) = 0$. Dostáváme tak v obou případech $\alpha_q(x) = \beta(x)$ pro všechna $x \in P$, a proto $\alpha_q|_P = \beta$.

Jiné řešení: V předchozím řešení lze druhý a třetí odstavec nahradit jinou úvahou, která používá větu o reprezentaci konečných distributivních svazů. Podle ní lze předpokládat, že $\mathbf{M}$ je (až na izomorfismus) podsvaz svazu $(\mathcal{P}(Z), \cup, \cap)$, pro vhodnou konečnou množinu Z. Je tedy $m = C \subseteq Z$ a $i = D \subseteq Z$. Přitom $i = D \not\supseteq C = m$ znamená, že existuje prvek $c \in C \subseteq Z$ takový, že $c \notin D$. Nyní můžeme definovat zobrazení α, a to dokonce s definičním oborem $\mathcal{P}(Z)$, takto: $\alpha(Y) = 1 \iff c \in Y$. Zřejmě se jedná o homomorfismus svazu $\mathcal{P}(Z)$ do svazu $\mathbf{2}$, a tím pádem i o homomorfismus svazu $\mathbf{M}$ do $\mathbf{2}$. Pro libovolný prvek $Y \leq i$ (tzn. $Y \subseteq i = D$) máme $c \notin Y$, a tudíž $\alpha(Y) = 0$; a pro prvek $Y \geq m$ (tzn. $Y \supseteq m = C$) máme $c \in Y$, a tedy $\alpha(Y) = 1$. Proto pro libovolné $Y \in P$ platí $\alpha(Y) = \beta(Y)$ a α je hledaný homomorfismus.

3. kolo — řešení

a) Označme X množinu ze zadání, tj.

$$X = \{\ (a_{11} \wedge a_{12} \wedge \cdots \wedge a_{1k_1}) \vee (a_{21} \wedge a_{22} \wedge \cdots \wedge a_{2k_2}) \vee \dots$$

$$\cdots \vee (a_{n1} \wedge a_{n2} \wedge \cdots \wedge a_{nk_n})\ ;\ n, k_1, \dots k_n \in \mathbb{N}, a_{11}, \dots a_{nk_n} \in A\ \}\ . \quad (*)$$

Chceme ukázat, že X je podsvaz svazu $(G, \vee, \wedge)$ generovaný množinou A, tzn. nejmenší podsvaz svazu $(G, \vee, \wedge)$, který obsahuje množinu A. Zřejmě platí $A \subseteq X$, neboť v $(*)$ lze vzít $n = 1$, $k_1 = 1$ a za prvek a_{11} brát postupně všechny prvky z množiny A.

Dokažme dále, že X je podsvaz $(G, \vee, \wedge)$. Předně si povšimněme, že (dle notace ze zadání části b)) množina X sestává právě z prvků, které jsou supremem několika prvků z množiny $A^\wedge$. Uvažujme nyní dva libovolné prvky x a y z X. Můžeme tedy psát $x = x_1 \vee x_2 \vee \cdots \vee x_n$ a $y = y_1 \vee y_2 \vee \cdots \vee y_m$, kde $x_i, y_j \in A^\wedge$ pro všechna $i \leq n$ a $j \leq m$.

Snadno se nahlédne, že $x \vee y = x_1 \vee x_2 \vee \cdots \vee x_n \vee y_1 \vee y_2 \vee \cdots \vee y_m$ je prvkem množiny X, neboť je supremem prvků z $A^\wedge$. Množina X je tedy uzavřena na suprema. Dále můžeme psát

$$x \wedge y = x \wedge (y_1 \vee y_2 \vee \cdots \vee y_m) = (x \wedge y_1) \vee (x \wedge y_2) \vee \cdots \vee (x \wedge y_m)\,,$$

kde jsme použili distributivitu svazu $(G, \vee, \wedge)$. Pro libovolné $j \leq m$ pak platí

$$x \wedge y_j = (x_1 \vee x_2 \vee \cdots \vee x_n) \wedge y_j = (x_1 \wedge y_1) \vee (x_2 \wedge y_j) \vee \cdots \vee (x_n \wedge y_j)\,.$$

Protože platí $x_1, \dots, x_n, y_1, \dots, y_m \in A^\wedge$, dostáváme, že pro libovolné $i \leq n$ a $j \leq m$ platí $x_i \wedge y_j \in A^\wedge$. Proto je $x \wedge y$ supremem prvků z $A^\wedge$ a tedy $x \wedge y \in X$. Tudíž X je podsvaz svazu $(G, \vee, \wedge)$.

Konečně předpokládejme, že M je podsvaz svazu $(G, \vee, \wedge)$, který obsahuje množinu A. Protože $A^\wedge$ obsahuje jen infima prvků z A, dostáváme $A^\wedge \subseteq M$. Podobně X obsahuje pouze suprema prvků z $A^\wedge$ a tedy $X \subseteq M$. Dostáváme tedy, že X je nejmenší podsvaz obsahující A.

b) Pro libovolnu neprázdnou podmnožinu B konečné množiny A máme jednoznačně dán prvek $\inf B \in A^\wedge$. Tím je tedy definováno zobrazení α z množiny $\mathcal{P}'(A)$, množiny všech neprázdných podmnožin n prvkové množiny A, do množiny $A^\wedge$. Uvažme libovolný prvek $a = a_1 \wedge a_2 \wedge \cdots \wedge a_n \in A^\wedge$. Pokud existují $1 \leq i < j \leq n$ takové, že $a_i = a_j$, potom díky základním vlastnostem operace $\wedge$, tj. asociativitě, komutativitě a idempotenci, platí $a = a_1 \wedge \cdots \wedge a_{j-1} \wedge a_{j+1} \wedge \cdots \wedge a_n$. Lze tedy jakýkoliv prvek z $A^\wedge$ psát jako infimum různých prvků a zobrazení α je proto surjektivní. Protože množina $\mathcal{P}'(A)$ má právě $2^n - 1$ prvků, má množina $A^\wedge$ nejvýše $2^n - 1$ prvků.

c) Pokud budeme uvažovat duální konstrukci ke konstrukci z části b), můžeme definovat, pro libovolnou podmnožinu $B \subseteq G$, množinu $B^\vee = \{b_1 \vee \cdots \vee b_m; m \in \mathbb{N}, b_1, \dots, b_m \in B\}$. Přitom duální tvrzení k tvrzení z části b) říká, že $|B^\vee| \leq 2^{|B|} - 1$.

Nechť $(G, \vee, \wedge)$ je generovaný n prvkovou množinou A. Tvrzení z části a) lze nyní zapsat takto: $G = \langle A \rangle = (A^\wedge)^\vee$. Protože $|A^\wedge| \leq 2^n - 1$, dostáváme $|G| \leq 2^{2^n - 1} - 1$. Zejména je množina G konečná.

d) Označme $A = \{a, b, c\}$. Víme, že $B = A^\wedge = \{a, b, c, a \wedge b, a \wedge c, b \wedge c, a \wedge b \wedge c\}$ má nejvýše sedm prvků. Navíc v podmnožině B uspořádané množiny $(G, \leq)$ je $a \wedge b \wedge c$ nejmenší prvek, a dále $x \wedge y \leq x$ pro libovolnou volbu $x, y \in A$. Pokud budeme uvažovat $B^\vee = \{b_1 \vee \cdots \vee b_m; m \in \mathbb{N}, b_1, \dots, b_m \in B\}$, pak ve výrazu $b_1 \vee \cdots \vee b_m$ lze brát prvky $b_1, b_2, \dots, b_m$ jako nesrovnatelné; v opačném případě, lze výsledný prvek zapsat jednodušeji, a to vypuštěním menšího z dvojice srovnatelných prvků. Určeme, kolik takových výrazů (s po dvou nesrovnatelnými prvky) existuje pro každé možné m. V těchto výrazech nebudeme, pro $m \geq 2$, používat prvek $a \wedge b \wedge c$, který je menší než všechny ostatní prvky, a také nebudeme rozlišovat mezi výrazy, které dávají – použitím asociativity, komutativity a idempotence – stejný prvek v G.

- Pro $m = 1$ dostaneme sedm výrazů $a, b, c, a \wedge b, a \wedge c, b \wedge c, a \wedge b \wedge c$, tj. vyjádření prvků množiny $A^\wedge$.
- Pro $m = 2$ máme k prvku a maximálně tři nesrovnatelné prvky, a to b, c a $b \wedge c$. Máme tedy tři výrazy $a \vee b$, $a \vee c$ a $a \vee (b \wedge c)$. Podobně pro b a c dostaneme navíc $b \vee c$, $b \vee (a \wedge c)$, $c \vee (a \wedge b)$. Pokud ve vyjádření $b_1 \vee b_2$ není žádný z prvků z množiny A, pak dostáváme tři možné výrazy $(a \wedge b) \vee (a \wedge c)$, $(a \wedge b) \vee (b \wedge c)$ a $(a \wedge c) \vee (b \wedge c)$. Celkem tedy máme devět výrazů pro $m = 2$.
- Pro $m = 3$, pokud výraz obsahuje dva prvky z množiny A, pak ten třetí také musí být z množiny A, tj. dostaneme výraz $a \vee b \vee c$. Podobně pokud výraz obsahuje dva prvky z množiny $\{a \wedge b, a \wedge c, b \wedge c\}$, pak ten třetí také musí být z této množiny, tj. máme výraz $(a \wedge b) \vee (a \wedge c) \vee (b \wedge c)$.
- Z předchozí úvahy také plyne, že pro $m \geq 4$ výraz $b_1 \vee \cdots \vee b_m$ nutně obsahuje srovnatelné prvky.

Celkem tedy máme

$$B^\vee = \{a, b, c, a \wedge b, a \wedge c, b \wedge c, a \wedge b \wedge c, a \vee b, a \vee c, b \vee c, a \vee (b \wedge c), b \vee (a \wedge c), c \vee (a \wedge b),$$

$$(a \wedge b) \vee (a \wedge c), (a \wedge b) \vee (b \wedge c), (a \wedge c) \vee (b \wedge c), a \vee b \vee c, (a \wedge b) \vee (a \wedge c) \vee (b \wedge c)\}\,.$$

Zejména dostáváme $|G| = |B^\vee| \leq 18$.

e) Prázdná množina je dědičná, a také M je dědičná. Má proto $(H(M), \subseteq)$ nejmenší a největší prvek, což jsou navíc supremum a infimum prázdné množiny. Průnik a sjednocení libovolného neprázdného systému dědičných podmnožin uspořádané množiny $(M, \leq)$ je dědičná podmnožina – důkaz je snadný. Proto je $H(M)$ úplný svaz. Navíc se suprema a infima počítají stejně jako ve svazu $(\mathcal{P}(M), \subseteq)$, všech podmnožin množiny M, a je proto $H(M)$ podsvaz svazu $(\mathcal{P}(M), \cup, \cap)$. Protože $(\mathcal{P}(M), \cup, \cap)$ je distributivní svaz a podsvaz distributivního svazu je distributivní svaz, dostáváme, že $(H(M), \cup, \cap)$ je distributivním svazem.

Má-li uspořádaná množina $(M, \leq)$ nejmenší prvek a, pak a je prvkem každé neprázdné dědičné podmnožiny množiny M. Proto $H(M) = D(M) \cup \{\emptyset\}$ a $D(M)$ je podsvazem svazu $H(M)$ s nejmenším prvkem $\{a\}$. Je proto $D(M)$ distributivní svaz a navíc je i úplným svazem. Nicméně je vhodné si uvědomit, že supremum prázdné podmnožiny je nyní nejmenší prvek v $D(M)$, tj. $\{a\}$.

f) Za $(M, \leq)$ vezmeme sedmiprvkovou uspořádanou množinu $(\mathcal{P}'(\{1, 2, 3\}), \leq)$, kde $X \leq Y$ právě když $Y \subseteq X$. Je tedy $\{1, 2, 3\}$ nejmenším prvkem. Označme nyní dědičné podmnožiny

$$a = \{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}\,,$$

$$b = \{\{2\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}\,,$$

$$c = \{\{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}\,.$$

Zbývá ověřit, že všechny výrazy z vyjádření $B^\vee$ z části d) jsou po dvou různé dědičné podmnožiny v M (připomínáme, že operacemi jsou průnik a sjednocení):

$$a \wedge b = \{\{1, 2\}, \{1, 2, 3\}\}, \quad a \wedge c = \{\{1, 3\}, \{1, 2, 3\}\}, \quad b \wedge c = \{\{2, 3\}, \{1, 2, 3\}\},$$

$$a \wedge b \wedge c = \{\{1, 2, 3\}\},$$

$$a \vee b = \{\{1\}, \{2\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\},$$

$$a \vee c = \{\{1\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\},$$

$$b \vee c = \{\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\},$$
$$a \vee (b \wedge c) = \{\{1\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\},$$
$$b \vee (a \wedge c) = \{\{2\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\},$$
$$c \vee (a \wedge b) = \{\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\},$$
$$(a \wedge b) \vee (a \wedge c) = \{\{1,2\},\{1,3\},\{1,2,3\}\},$$
$$(a \wedge b) \vee (b \wedge c) = \{\{1,2\},\{2,3\},\{1,2,3\}\},$$
$$(a \wedge c) \vee (b \wedge c) = \{\{1,3\},\{2,3\},\{1,2,3\}\},$$
$$a \vee b \vee c = \{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\},$$
$$(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = \{\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}\,.$$

4. kolo — řešení

a) Pokud pro prvek $s \in S$ existuje $f \in F$ takové, že $s \geq f \wedge x$, pak zřejmě $s \in (F \cup \{x\})\!\uparrow$, neboť $f \wedge x \in (F \cup \{x\})\!\uparrow$. Naopak, pokud $s \in (F \cup \{x\})\!\uparrow$, pak podle věty 3.2 z učebního textu existuje $n \in \mathbb{N}$ a $a_1, \ldots, a_n \in F \cup \{x\}$ takové, že $s \geq a_1 \wedge \cdots \wedge a_n$. Pokud je $a_1 = \ldots = a_n = x$, pak zřejmě $s \geq x \geq x \wedge f$ pro libovolné $f \in F$ (takové existuje, neboť F je neprázdný). Pokud aspoň jeden z prvků $a_1, \ldots, a_n$ není roven x, pak musí patřit do F. Pak označme f infimum (neprázdné) množiny těch prvků z $a_1, \ldots, a_n$, které patří do F, Zřejmě pak $a_i \geq f \wedge x$ pro $1 \leq i \leq n$ (protože buď $a_i \geq f$ nebo $a_i = x$), takže $s \geq a_1 \wedge \cdots \wedge a_n \geq f \wedge x$.

b) (i) $\Rightarrow$ (ii): Nechť F je ultrafiltr $\boldsymbol{A}$ a předpokládejme sporem, že existují $x, y \in \boldsymbol{A}$ takové, že $x \vee y \in F$ a $x, y \notin F$. Potom je filtr $(F \cup \{x\})\!\uparrow$ ostře větší než F. Pokud ukážeme, že je to navíc vlastní filtr, tak dostaneme hledaný spor. Kdyby bylo $y \in (F \cup \{x\})\!\uparrow$, pak podle části a) existuje $f \in F$ takové, že $y \geq f \wedge x$. Potom z distributivity $\boldsymbol{A}$ plyne $y = (f \wedge x) \vee y = (f \vee y) \wedge (x \vee y) \in F$, neboť $f \vee y \in F$ (z uzavřenosti F nahoru) a $x \vee y \in F$ (podle předpokladu), což je spor. Takže $y \notin (F \cup \{x\})\!\uparrow$, a tedy $(F \cup \{x\})\!\uparrow$ je vlastní filtr.

Pozn.: V této části jsme nijak nevyužili komplementaritu svazu $\boldsymbol{A}$ ale pouze distributivitu, tato implikace tudíž platí pro všechny distributivní svazy.

(ii) $\Rightarrow$ (iii): Nechť je splněna podmínka (ii) a $x \in \boldsymbol{A}$. Platí $x \vee x' = 1 \in F$ (neboť F je neprázdný), takže podle (ii) platí $x \in F$ nebo $x' \in F$.

Pozn.: Všimněte si, že pro žádný prvek $x \in \boldsymbol{A}$ nemůže platit obojí $x \in F$ a $x' \in F$, protože potom by platilo $0 = x \wedge x' \in F$, a tak by F nebyl vlastní filtr.

(iii) $\Rightarrow$ (i): Nechť je splněna podmínka (iii) a předpokládejme sporem, že F není ultrafiltr, tedy existuje ostře větší vlastní filtr F' Booleovy algebry $\boldsymbol{A}$. Zvolme libovolný prvek $x \in F' \setminus F$. Potom $x \notin F$, a tedy podle (iii) je $x' \in F$, a tudíž $x' \in F'$. Je tedy $x, x' \in F'$, což je podle předchozí poznámky spor s tím, že F' je vlastní filtr.

c) Bez újmy na obecnosti můžeme předpokládat, že F je neprázdný, protože kdyby byl prázdný tak ho můžeme nahradit filtrem $\{1\}$ (který je vlastní, protože $\boldsymbol{A}$ je netriviální Booleova algebra), čímž neporušíme podmínku $F \cap I = \emptyset$, neboť I je vlastní ideál $\boldsymbol{A}$ a tak $1 \notin I$.

Nechť $\mathcal{F}$ je množina všech vlastních filtrů $\boldsymbol{A}$, které obsahují F a jsou disjunktní s I. Ukážeme, že uspořádaná množina $(\mathcal{F}, \subseteq)$ splňuje předpoklady Zornova lemmatu. Zřejmě $F \in \mathcal{F}$, takže $\mathcal{F}$ je neprázdná. Nechť $\emptyset \neq C \subseteq \mathcal{F}$ je libovolný neprázdný řetězec v $\mathcal{F}$. Ukážeme, že $M = \bigcup_{T \in C} T$ rovněž patří do $\mathcal{F}$, potom to zřejmě bude horní závora C. Nechť $x, y \in M$. Potom existují $T_1, T_2 \in C$ takové, že $x \in T_1$ a $y \in T_2$. Jelikož C je řetězec, tak platí $T_1 \subseteq T_2$ nebo $T_2 \subseteq T_1$. Potom $x, y \in \max(T_1, T_2)$, a tak $x \wedge y \in \max(T_1, T_2)$, tudíž $x \wedge y \in M$. Dále M je sjednocením nahoru uzavřených množin, a tak je rovněž nahoru uzavřená. Ukázali jsme tedy, že M je filtr $\boldsymbol{A}$. Zřejmě M obsahuje F (neboť C je neprázdná a každý její prvek obsahuje F) a je disjunktní s I (neboť každý prvek C je disjunktní s I). Navíc všechny prvky C jsou vlastní filtry $\boldsymbol{A}$, takže neobsahují 0, tudíž $0 \notin M$, a tak je M vlastní filtr $\boldsymbol{A}$. Celkem jsme tedy dokázali, že $M \in \mathcal{F}$.

Podle Zornova lemmatu existuje nějaký maximální prvek množiny $\mathcal{F}$, označme ho U. Budeme hotovi, když ukážeme, že U je ultrafiltr $\boldsymbol{A}$. Jelikož $F \subseteq U$ a $F \neq \emptyset$, tak $U \neq \emptyset$. Podle tvrzení z b) budeme hotovi, když ukážeme, že U splňuje podmínku (ii) z tohoto příkladu. Předpokládejme tedy sporem, že existují $x, y \in \boldsymbol{A}$ tak, že $x \vee y \in U$ a $x, y \notin U$. Stejně jako v důkazu implikace (i) $\Rightarrow$ (ii) v příkladu b) se ukáže, že potom $(U \cup \{x\})\uparrow$ a $(U \cup \{y\})\uparrow$ jsou vlastní filtry $\boldsymbol{A}$, které jsou ostře větší než U. Ani jeden z těchto filtrů nemůže být disjunktní s I, protože pak by patřil do $\mathcal{F}$ a dostali bychom spor s maximalitou U. Zvolme libovolné prvky $s_1 \in (U \cup \{x\})\uparrow \cap I$ a $s_2 \in (U \cup \{y\})\uparrow \cap I$. Potom podle příkladu a) existují $u_1, u_2 \in U$ takové, že $s_1 \geq u_1 \wedge x$ a $s_2 \geq u_2 \wedge y$. Jelikož I je uzavřený dolů, tak $u_1 \wedge x, u_2 \wedge y \in I$, z čehož plyne $(u_1 \wedge x) \vee (u_2 \wedge y) \in I$. Podle distributivity $\boldsymbol{A}$ platí $(u_1 \wedge x) \vee (u_2 \wedge y) = ((u_1 \wedge x) \vee u_2) \wedge ((u_1 \wedge x) \vee y) = (u_1 \vee u_2) \wedge (x \vee u_2) \wedge (u_1 \vee y) \wedge (x \vee y) \in U$, protože $u_1 \vee u_2, x \vee u_2, u_1 \vee y \in U$ (neboť U je uzavřená nahoru) a $x \vee y \in U$ podle předpokladu. Jelikož ale $U \cap I = \emptyset$, dostali jsme hledaný spor.

d) Nejprve ukážeme, že zobrazení i je injektivní. Nechť $x, y \in \boldsymbol{A}$, $x \neq y$. Potom je $x \not\leq y$ nebo $y \not\leq x$. V prvním případě platí $x\uparrow \cap\, y\downarrow = \emptyset$ (neboť kdyby existovalo nějaké $z \in x\uparrow \cap\, y\downarrow$, tak by bylo $x \leq z \leq y$), a tak podle tvrzení z příkladu c) existuje $U \in \mathcal{U}(\boldsymbol{A})$ tak, že $x\uparrow \subseteq U$ a $U \cap y\downarrow = \emptyset$, tedy $x \in U$ a $y \notin U$. Analogicky pokud $y \not\leq x$, tak existuje $U \in \mathcal{U}(\boldsymbol{A})$ tak, že $x \notin U$ a $y \in U$. Platí tedy $i(x) \neq i(y)$, a zobrazení i je tudíž injektivní.

Nyní ukážeme, že i je homomorfismus Booleových algeber. Ultrafiltry jsou podle definice vlastní filtry, a tak platí $i(0) = \emptyset$. Jelikož je $\boldsymbol{A}$ netriviální Booleova algebra, tak prázdný filtr není její ultrafiltr (neboť $\{1\}$ je ostře větší vlastní filtr $\boldsymbol{A}$). Tudíž všechny ultrafiltry $\boldsymbol{A}$ jsou neprázdné, a proto $i(1) = \mathcal{U}(\boldsymbol{A})$. Nechť $x, y \in \boldsymbol{A}$. Pro libovolný filtr F Booleovy algebry $\boldsymbol{A}$ zřejmě platí $x \wedge y \in F$ právě tehdy, když $x \in F$ a $y \in F$, a pro libovolný ultrafiltr U Booleovy algebry $\boldsymbol{A}$ platí podle příkladu b) $x \vee y \in U$ právě tehdy, když $x \in U$ nebo $y \in U$. Odtud dostaneme, že $i(x \wedge y) = \{U \in \mathcal{U}(\boldsymbol{A}); x \wedge y \in U\} = \{U \in \mathcal{U}(\boldsymbol{A}); x \in U \text{ a } y \in U\} =$
$\{U \in \mathcal{U}(\boldsymbol{A}); x \in U\} \cap \{U \in \mathcal{U}(\boldsymbol{A}); y \in U\} = i(x) \cap i(y)$ a $i(x \vee y) = \{U \in \mathcal{U}(\boldsymbol{A}); x \vee y \in U\} = \{U \in \mathcal{U}(\boldsymbol{A}); x \in U \text{ nebo } y \in U\} = \{U \in \mathcal{U}(\boldsymbol{A}); x \in U\} \cup \{U \in \mathcal{U}(\boldsymbol{A}); y \in U\} = i(x) \cup i(y)$. Dokázali jsme tedy, že zobrazení i je skutečně homomorfismus Booleových algeber.

Pozn.: V případě, že $\boldsymbol{A}$ je konečná, se snadno uvidí, že její ultrafiltry jsou právě filtry tvaru $a\uparrow$, kde a je atom $\boldsymbol{A}$, zobrazení i je tedy vlastně totožné se zobrazením h z důkazu věty 8.7 z učebního textu. V tom případě je tedy i dokonce izomorfismus Booleových algeber. Nicméně pokud je $\boldsymbol{A}$ nekonečná, pak už toto zobrazení nemusí být surjektivní. Lze ukázat, že na $\mathcal{U}(\boldsymbol{A})$ lze zavést jistou topologii tak, že potom pro každou množinu $P \subseteq \mathcal{U}(\boldsymbol{A})$ platí, že P leží v obrazu i právě tehdy, když je P v této topologii obojetná (tj. zároveň otevřená i uzavřená). Tato tvrzení jsou částí věty nazývané *Stoneova dualita*.

5. kolo — řešení

a) Abychom dokázali, že podokruh P je podtěleso, musíme pro libovolné $a \in P$, $a \neq 0$, ukázat, že $a^{-1} \in P$. Protože $K \subseteq T$ je algebraické rozšíření těles a $a \in T$, je a algebraický prvek nad K. Podle věty o jednoduchých rozšířeních z přednášky pak víme, že $K[a] = K(a)$, tedy podokruh tělesa T generovaný $K \cup \{a\}$ je podtělesem tělesa T. Protože P je podokruh tělesa T a platí $K \cup \{a\} \subseteq P$, je $K[a] \subseteq P$. Potřebné plyne z toho, že $a^{-1} \in K(a) = K[a] \subseteq P$.

b) plyne z d) níže volbou $n = 2$.

c) Položme $K = \mathbb{Q}$, $\alpha = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Pak $\alpha^3 = 1$, tedy $\mathbb{Q}(\alpha^3) = \mathbb{Q}$. Protože $x^3 - 1 = (x-1)(x^2+x+1)$ a $\alpha \neq 1$, je α kořenem polynomu x^2+x+1. Současně $\alpha \notin \mathbb{Q}$, tedy $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\alpha^3)$ a x^2+x+1 je minimální polynom prvku α nad $\mathbb{Q}$, proto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, což není dělitelné třemi.

d) Zřejmě $\alpha^n \in K(\alpha)$, a tedy $K(\alpha^n) \subseteq K(\alpha)$. Označme $m = [K(\alpha) : K(\alpha^n)]$. Protože α je kořenem polynomu $x^n - \alpha^n \in K(\alpha^n)$, minimální polynom f prvku α nad $K(\alpha^n)$ je dělitelem polynomu $x^n - \alpha^n$. Proto $m = \operatorname{st} f \leq \operatorname{st}(x^n - \alpha^n) = n$. Z inkluzí $K \subseteq K(\alpha^n) \subseteq K(\alpha)$ a věty o násobení stupňů plyne $[K(\alpha) : K] = m \cdot [K(\alpha^n) : K]$, a tedy žádné prvočíslo $p \leq n$ není dělitelem čísla m. To spolu s $m \leq n$ dává $m = 1$, což znamená $K(\alpha) = K(\alpha^n)$.

e) Protože v případě $\mu = \nu$ je tvrzení zřejmé, můžeme předpokládat, že $\mu \neq \nu$. Jistě platí $K(\mu+\nu) \subseteq K(\mu,\nu)$, budeme tedy dokazovat opačnou inkluzi. Protože

$$2\mu\nu = (\mu+\nu)^2 - \mu^2 - \nu^2 \in K(\mu+\nu)$$

a $\frac{1}{2} = \frac{1}{1+1} \in K$, platí $\mu\nu \in K(\mu+\nu)$. Pak

$$\mu(\mu^2 - \nu^2) = (\mu^2 - \mu\nu)(\mu+\nu) \in K(\mu+\nu),$$

což vzhledem k

$$0 \neq (\mu+\nu)(\mu-\nu) = \mu^2 - \nu^2 \in K$$

dává $\mu \in K(\mu+\nu)$, tedy také $\nu = (\mu+\nu) - \mu \in K(\mu+\nu)$. Dohromady $K(\mu,\nu) \subseteq K(\mu+\nu)$.

f) (i)$\Rightarrow$(iii) Z předpokladu máme $c \in K$ tak, že $a^2 - b = c^2$. Zvolme libovolně $\mu, \nu \in \mathbb{C}$ tak, aby $\mu^2 = \frac{a+c}{2}$, $\nu^2 = \frac{a-c}{2}$. Zřejmě $\mu^2, \nu^2 \in K$. Protože $(2\mu\nu)^2 = 4\mu^2\nu^2 = (a+c)(a-c) = a^2 - c^2 = b$, libovolné $\beta \in \mathbb{C}$ splňující $\beta^2 = b$ je tvaru $\beta = \pm 2\mu\nu$. Bez újmy na obecnosti lze předpokládat $\beta = 2\mu\nu$ (jinak zvolíme $-\nu$ místo ν). Pak $(\mu+\nu)^2 - \beta = \mu^2 + \nu^2 = \frac{a+c}{2} + \frac{a-c}{2} = a$.

(iii)$\Rightarrow$(ii) Plyne z toho, že jistě nějaké $\beta \in \mathbb{C}$ splňující $\beta^2 = b$ existuje.

(ii)$\Rightarrow$(i) Platí tedy $a + \beta = (\mu+\nu)^2$, odkud $2\mu\nu = \beta + (a - \mu^2 - \nu^2)$, umocněním

$$4\mu^2\nu^2 = \beta^2 + (a - \mu^2 - \nu^2)^2 + 2\beta(a - \mu^2 - \nu^2).$$

Protože $a, \beta^2, \mu^2, \nu^2 \in K$, pokud by $a - \mu^2 - \nu^2 \neq 0$, dostali bychom úpravou

$$\beta = \frac{4\mu^2\nu^2 - \beta^2 - (a - \mu^2 - \nu^2)^2}{2(a - \mu^2 - \nu^2)} \in K,$$

což není pravda. Je tedy $a = \mu^2 + \nu^2$, odkud $\beta = 2\mu\nu$. Proto

$$a^2 - b = (\mu^2 + \nu^2)^2 - (2\mu\nu)^2 = \mu^4 + 2\mu^2\nu^2 + \nu^4 - 4\mu^2\nu^2 = (\mu^2 - \nu^2)^2.$$

6. kolo — řešení

a) Předpokládejme sporem, že $\operatorname{char} F = p > 0$ (kde p je prvočíslo). Potom v F platí $-1 = \underbrace{1^2 + \ldots + 1^2}_{p-1 \text{ sčítanců}}$, takže F není formálně reálné, spor.

b)-i) Nechť $a, b \in P$. Potom $a \geq 0$, z čehož plyne $a+b \geq b$. Zároveň $b \geq 0$, takže z tranzitivity dostáváme $a+b \geq 0$. Z podmínek $a \geq 0$, $b \geq 0$ rovněž plyne $ab \geq 0$. Platí tedy $a+b, ab \in P$, a tak $P{+}P \subseteq P$ a $P{\cdot}P \subseteq P$. Pro libovolné $a \in F$ platí $a \geq 0$ nebo $a \leq 0$, neboť jde o lineární uspořádání, tudíž $a \geq 0$ nebo $-a \geq 0$. Odtud plyne $P \cup (-P) = F$, a navíc platí $a^2 = a \cdot a = (-a) \cdot (-a)$, v obou případech tedy dostáváme $a^2 \geq 0$, tj. $a^2 \in P$. Zejména je tedy $1 = 1^2 > 0$, takže $-1 < 0$ a z antisymetrie dostáváme $-1 \notin P$.

ii) Z podmínky $P \cup (-P) = F$ plyne, že pro každé $a \in F$ je $a \in P$ nebo $-a \in P$, z podmínky $P \cdot P \subseteq P$ analogicky jako v předchozí části dostaneme, že $a^2 \in P$. Zejména tedy pro každé $a \in F$ platí $a - a = 0 = 0^2 \in P$, z čehož plyne, že relace $\leq$ je reflexivní. Pokud pro nějaká $a, b \in F$ platí $a \leq b$ a $b \leq a$, pak $b{-}a, a{-}b \in P$, tudíž z $P{\cdot}P \subseteq P$ plyne $-(b{-}a)^2 = (b{-}a){\cdot}(a{-}b) \in P$. Kdyby bylo $a \neq b$, tak by platilo $(1/(b-a))^2 \in P$, a tak z $P \cdot P \subseteq P$ by bylo $-1 = -(b-a)^2 \cdot (1/(b-a))^2 \in P$, což je spor. Je tedy $a = b$ a $\leq$ je antisymetrická relace. Dále pokud pro $a, b, c \in F$ máme $a \leq b$ a $b \leq c$, pak $b - a, c - b \in P$, takže z $P + P \subseteq P$ plyne $c - a = (c - b) + (b - a) \in P$, tj. $a \leq c$. Relace $\leq$ je tedy i tranzitivní, a dohromady je to tudíž uspořádání. Z podmínky $P \cup (-P) = F$ navíc plyne, že pro každé $a, b \in F$ je $b - a \in P$ nebo $a - b \in P$, takže $a \leq b$ nebo $b \leq a$, je to tedy lineární uspořádání. Dále pokud pro $a, b, c \in F$ platí $a\ leb$, pak $b - a \in P$. Jelikož $(b + c) - (a + c) = b - a$, platí pak $a + c \leq b + c$. Konečně z podmínky $P \cdot P \subseteq P$ dostaneme, že pro $a, b \geq 0$ je $ab \geq 0$. Relace $\leq$ je skutečně lineární uspořádání na F, vzhledem ke kterému je to uspořádané těleso.

c)-i) Označme $P = \{a \in \mathbb{R} \colon a \succeq 0\}$ a $\mathbb{R}_0^+ = \{a \in \mathbb{R} \colon a \geq 0\}$. Podle poznámky v komentáři stačí dokázat, že $P = \mathbb{R}_0^+$. Z důkazu části b)i) víme, že pro každé $a \in \mathbb{R}$ platí $a^2 \in P$, tudíž pro každé $a \geq 0$ platí $a = (\sqrt{a})^2 \in P$, takže $\mathbb{R}_0^+ \subseteq P$. Kdyby pro nějaké $a < 0$ platilo $a \in P$, pak by bylo $a, -a \in P$, takže $-1 = a \cdot (-a) \cdot (1/a)^2 \in P$, což je podle b)i) spor. Je tedy $P = \mathbb{R}_0^+$ a $\preceq = \leq$.

ii) Opět označme $P = \{a \in \mathbb{Q} \colon a \trianglerighteq 0\}$ a $\mathbb{Q}_0^+ = \{a \in \mathbb{Q} \colon a \geq 0\}$. Zřejmě $0 \in P$ a podle důkazu části b)i) platí $1 = 1^2 \in P$, z čehož se snadno indukcí dokáže, že $\mathbb{N}_0 \subseteq P$, kde $\mathbb{N}_0 = \mathbb{Q}_0^+ \cap \mathbb{Z}$. Každý prvek $\mathbb{Q}_0^+$ je tvaru r/s, kde $r \in \mathbb{N}_0$ a $s \in \mathbb{N}$. Platí $r/s = rs \cdot (1/s)^2 \in P$, a tak $\mathbb{Q}_0^+ \subseteq P$. Analogicky jako v c)i) se dokáže, že tato inkluze je dokonce rovnost, a proto $\trianglelefteq = \leq$.

d) Označme σ automorfismus tělesa $\mathbb{Q}(\sqrt{2})$ daný vztahem $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ pro $a, b \in \mathbb{Q}$. Zřejmě standardní uspořádání $\leq$ (zúžené na $\mathbb{Q}(\sqrt{2})$) je jedno možné uspořádání, vzhledem ke kterému je to uspořádané těleso. Jelikož je σ automorfismus, snadno se nahlédne, že relace $\trianglelefteq$ definovaná podmínkou, že $a \trianglelefteq b$ právě tehdy, když $\sigma(a) \leq \sigma(b)$, rovněž zadává možné uspořádání $\mathbb{Q}(\sqrt{2})$. Platí $\sqrt{2} > 0$ a $\sqrt{2} \lhd 0$, takže uspořádání $\leq$ a $\trianglelefteq$ jsou různé. Příslušné množiny nezáporných prvků v těchto uspořádáních potom jsou $\{a \in \mathbb{Q}(\sqrt{2}) \colon a \geq 0\}$, resp. $\{a \in \mathbb{Q}(\sqrt{2}) \colon \sigma(a) \geq 0\}$.

Ukážeme, že žádné jiné kompatibilní uspořádání na $\mathbb{Q}(\sqrt{2})$ neexistuje. Nechť tedy $\preceq$ je lineární uspořádání $\mathbb{Q}(\sqrt{2})$, vzhledem ke kterému je to uspořádané těleso. Vezměme si libovolné $a, b \in \mathbb{Q}$, z nichž aspoň jedno je nenulové. Potom platí $a + b\sqrt{2} \neq 0$, $a - b\sqrt{2} \neq 0$ (neboť $\sqrt{2} \notin \mathbb{Q}$) a navíc $(a + b\sqrt{2}) \cdot (a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Q}$. Z c)ii) plyne, že uspořádání $\preceq$ a $\leq$ se shodují na $\mathbb{Q}$ (neboť zúžení $\preceq$ na $\mathbb{Q}$ zadává kompatibilní uspořádání na $\mathbb{Q}$).

Pokud tedy $a^2 - 2b^2 > 0$, pak $a^2 - 2b^2 \succ 0$, a tudíž $a + b\sqrt{2}$ a $a - b\sqrt{2}$ mají v $\preceq$ stejná znaménka. Navíc toto znaménko bude stejné jako znaménko jejich součtu. Platí ale $(a + b\sqrt{2}) + (a - b\sqrt{2}) = 2a \in \mathbb{Q}$, tudíž tento součet bude mít v $\preceq$ stejné znaménko jako v $\leq$. V tomto případě je tedy $a + b\sqrt{2} \succeq 0$ právě tehdy, když $a + b\sqrt{2} \geq 0$.

Pokud $a^2 - 2b^2 < 0$, pak $a^2 - 2b^2 \prec 0$, a tudíž $a + b\sqrt{2}$ a $a - b\sqrt{2}$ mají v $\preceq$ opačná znaménka. To, které z nich je v $\preceq$ kladné a které záporné, můžeme poznat podle znaménka jejich rozdílu v $\preceq$. Jelikož $(a + b\sqrt{2}) - (a - b\sqrt{2}) = 2b\sqrt{2}$ a $2b \in \mathbb{Q}$, znaménko $a + b\sqrt{2}$ v $\preceq$ je v tomto případě jednoznačně určeno znaménkem $\sqrt{2}$ v $\preceq$.

Celkem jsme ukázali, že uspořádání $\preceq$ je jednoznačně určeno tím, jaké v něm má $\sqrt{2}$ znaménko. Z toho je jasné, že můžou existovat nejvýše dvě taková uspořádání, a tudíž platí $\preceq = \leq$ (to nastane, pokud $\sqrt{2} \succ 0$) nebo $\preceq = \trianglelefteq$ (pokud $\sqrt{2} \prec 0$).

e) Nechť $\leq$ je libovolné uspořádání F, vzhledem ke kterému je to uspořádané těleso (takové podle předpokladu existuje). Předpokládejme sporem, že F není formálně reálné, tj. existuje $n \in \mathbb{N}$ a $a_1, \dots, a_n \in F$ takové, že $-1 = \sum_{i=1}^n a_i^2$. V důkazu b)i) jsme ukázali, že $-1 < 0$ a $a^2 \geq 0$ pro každé $a \in F$, tudíž $\sum_{i=1}^n a_i^2 \geq 0 > -1$, spor.

f)-i) Ukážeme, že uspořádaná množina $(\mathcal{S}, \subseteq)$ splňuje předpoklady Zornova lemmatu.
Označme

$$S = \left\{ \sum_{i=1}^n a_i^2 : n \in \mathbb{N}; a_1, \dots, a_n \in F \right\}$$

množinu všech prvků F, které lze v F napsat jako součet čtverců. Nechť $a, b \in S$. Potom existují $m, n \in \mathbb{N}$ a $a_1, \dots, a_m, b_1, \dots, b_n \in F$ tak, že $a = \sum_{i=1}^m a_i^2$ a $b = \sum_{j=1}^n b_j^2$. Tudíž $a + b = \sum_{i=1}^m a_i^2 + \sum_{j=1}^n b_j^2 \in S$ a $ab = \sum_{i=1}^m \sum_{j=1}^n (a_i b_j)^2 \in S$, a tak $S + S \subseteq S$ a $S \cdot S \subseteq S$. Zřejmě $F^2 \subseteq S$ a jelikož je F formálně reálné, tak $-1 \notin S$. Dohromady tedy dostáváme, že platí $S \in \mathcal{S}$, zejména tedy $\mathcal{S} \neq \emptyset$.

Nechť $\mathcal{C}$ je libovolný neprázdný řetězec v $\mathcal{S}$. Ukážeme, že $U = \bigcup_{M \in \mathcal{C}} M \in \mathcal{S}$. Nechť $a, b \in U$. Potom existují $M_1, M_2 \in \mathcal{C}$ tak, že $a \in M_1$ a $b \in M_2$. Jelikož $\mathcal{C}$ je řetězec, platí $a, b \in \max(M_1, M_2)$, a proto $a + b, ab \in \max(M_1, M_2) \subseteq U$. Tudíž $U + U \subseteq U$, $U \cdot U \subseteq U$. Jelikož $\mathcal{C} \neq \emptyset$ a $F^2 \subseteq M$ pro každé $M \in \mathcal{C}$, tak $F^2 \subseteq U$. Konečně $-1 \notin M$ pro každé $M \in \mathcal{C}$, a tak $-1 \notin U$. Skutečně tedy $U \in \mathcal{S}$, a navíc U je zřejmě horní závora $\mathcal{C}$.

Podle Zornova lemmatu tedy existuje $P \in \mathcal{S}$, které je maximální prvek $\mathcal{S}$ vzhledem k inkluzi.

ii) Vezměme si libovolné takové P a předpokládejme sporem, že existuje $a \in F$ takové, že $a, -a \notin P$. Dokážeme, že potom $P + a \cdot P \in \mathcal{S}$.

Nechť $b, c \in P + a \cdot P$. Pak existují $p_1, p_2, p_3, p_4 \in P$ takové, že $b = p_1 + ap_2$ a $c = p_3 + ap_4$. Pak $b + c = (p_1 + p_3) + a(p_2 + p_4) \in P + a \cdot P$ (neboť $p_1 + p_3, p_2 + p_4 \in P$) a $bc = (p_1p_3 + a^2p_2p_4) + a(p_1p_4 + p_2p_3) \in P + a \cdot P$ (neboť $a^2 \in P$, a tak $p_1p_3 + a^2p_2p_4, p_1p_4 + p_2p_3 \in P$). Dále platí $F^2 \subseteq P$ a $P \subseteq P + a \cdot P$ (protože $0 \in P$), takže $F^2 \subseteq P + a \cdot P$. Konečně předpokládejme sporem, že $-1 \in P + a \cdot P$. Potom existují $p_1, p_2 \in P$ takové, že $-1 = p_1 + ap_2$. Jelikož $-1 \notin P$, musí být $p_2 \neq 0$. Potom ale $-a = (p_1 + 1) \cdot p_2 \cdot (1/p_2)^2 \in P$ (neboť $F^2 \subseteq P$, a tedy zejména $1 \in P$, čehož plyne $p_1 + 1 \in P$). Platí ale $-a \notin P$, takže dostáváme spor, a tedy $-1 \notin P + a \cdot P$. Celkem tak dostáváme $P + a \cdot P \in \mathcal{S}$.

Jelikož $a = 0 + a \cdot 1 \in P + a \cdot P$ (neboť $0, 1 \in P$), tak je $P \subsetneq P + a \cdot P$. Ovšem P je maximální prvek $\mathcal{S}$, což je spor. Tudíž žádné takové a neexistuje, a tedy platí $P \cup (-P) = F$. Z b)ii) potom plyne, že F je uspořádatelné těleso.

7. kolo — řešení

a) Nechť $a, b \in R + I$. Pak existují $r_1, r_2 \in R$ a $i_1, i_2 \in I$ takové, že $a = r_1 + i_1$ a $b = r_2 + i_2$. Pak $a + b = (r_1 + r_2) + (i_1 + i_2) \in R + I$ (protože $r_1 + r_2 \in R$ a $i_1 + i_2 \in I$), $-a = -r_1 - i_1 \in R + I$ (protože $-r_1 \in R$, $-i_1 \in I$) a navíc $0 = 0 + 0 \in R + I$ (protože $0 \in R$, $0 \in I$), takže $(R + I, +)$ je podgrupa $(S,+)$. Dále $ab = r_1r_2 + (r_1i_2 + i_1r_2 + i_1i_2) \in R+I$ (neboť $r_1r_2 \in R$ a $r_1i_2, i_1r_2, i_1i_2 \in I$) a $1 = 1+0 \in R+I$ (neboť $1 \in R$, $0 \in I$), takže $(R+I,\cdot)$ je podmonoid $(S,\cdot)$. Dohromady je tedy $R+I$ podokruh S.

Jelikož $I \subseteq R+I \subseteq S$, I je ideál S a $R+I$ je podokruh S, tak zřejmě I je rovněž ideál $R+I$.

Označme f homomorfismus okruhů $R \to (R+I)/I$, který vznikne složením inkluze $R \to R+I$ a kanonické projekce $R+I \to (R+I)/I$. Dokážeme, že f je surjektivní. Vezměme si libovolné $a \in (R+I)/I$. Pak existují $r \in R$ a $i \in I$ tak, že $a = (r+i)+I$. Pak $a = r+I = f(r)$, takže f je skutečně surjektivní. Jádro projekce $R+I \to (R+I)/I$ je I, tudíž jádro f tvoří právě ty prvky R, které se v inkluzi $R \to R+I$ zobrazí do I, tedy přesně prvky $R \cap I$. Tudíž $R \cap I$ je ideál R a platí $R/(R\cap I) \cong (R+I)/I$, viz diagram.

$$\begin{tikzcd}
R \arrow[r, hook] \arrow[d, two heads] \arrow[dr, two heads, "f"] & R+I \arrow[d, two heads] \\
R/(R\cap I) \arrow[r, dashed, "\sim"] & (R+I)/I
\end{tikzcd}$$

b)-i) Jelikož $(I,+)$ je zřejmě podgrupa komutativní grupy $(J+I,+)$, tak je kvocient $(J+I)/I$ korektně definovaný. Dokážeme, že platí $p(J) = (J+I)/I$. Mějme libovolné $a \in p(J)$. Pak existuje $j \in J$ takové, že $a = j+I$, a zřejmě platí $a \in (J+I)/I$. Naopak, vezměme si libovolné $a \in (J+I)/I$. Potom existují $j \in J$ a $i \in I$ takové, že $a = (j+i)+I$. Pak $a = j+I = p(j) \in p(J)$. Skutečně tedy $p(J) = (J+I)/I$, navíc jelikož obraz ideálu v surjektivním homomorfismu okruhů je rovněž ideál, tak $(J+I)/I$ je ideál R/I.

ii) Jelikož $I \subseteq J$, tak zřejmě $J+I = J$, takže podle b)i) je J/I ideál R/I. Označme p kanonickou projekci $R \to R/J$ a q kanonickou projekci $R \to R/I$. Jelikož $I \subseteq J = \ker p$, tak existuje homomorfismus $\varphi\colon R/I \to R/J$ takový, že $p = \varphi \circ q$. Jelikož je p surjektivní, tak je φ taky surjektivní. Ukážeme, že platí $\ker\varphi = J/I$. Nechť $a \in \ker\varphi$. Potom existuje $r \in R$ takové, že $a = r+I$ a platí $0+J = \varphi(a) = \varphi(q(r)) = p(r)$, a proto $r \in J$ a $a = r+I \in J/I$. Naopak nechť $a \in J/I$. Pak existuje $j \in J$ takové, že $a = j+I$. Z toho plyne $\varphi(a) = \varphi(q(j)) = p(j) = 0+J$, a tedy $a \in \ker\varphi$. Skutečně tedy $\ker\varphi = J/I$ a dohromady dostáváme, že platí $(R/I)/(J/I) \cong R/J$, viz diagram.

$$\begin{tikzcd}
R \arrow[r, two heads, "p"] \arrow[d, two heads, "q"'] & R/J \\
R/I \arrow[ur, dashed, two heads, "\varphi"] \arrow[d, two heads] & \\
\frac{R/I}{J/I} \arrow[uur, dashed, "\sim"'] &
\end{tikzcd}$$

c)-i) Jelikož obraz ideálu v surjektivním homomorfismu okruhů je zase ideál, je zobrazení α korektně definované. Podobně vzor ideálu v homomorfismu okruhů je rovněž ideál, navíc pro každé $K \in \mathcal{L}(R/I)$ platí $I = p^{-1}(0) \subseteq p^{-1}(K) = \beta(K)$, takže zobrazení β je taky korektně definované. Navíc přímo z definic je zřejmé, že α i β jsou izotonní. Ukážeme, že jsou i navzájem inverzní.

Mějme libovolné $J \in \mathcal{L}_I(R)$. Zřejmě platí $J \subseteq p^{-1}(p(J)) = \beta(\alpha(J))$. Naopak nechť $r \in \beta(\alpha(J)) = p^{-1}(p(J))$. Pak $p(r) \in p(J)$, takže existuje $j \in J$ takové, že $p(r) = p(j)$. Tudíž $p(r-j) = 0+I$, proto $r-j \in I$. Jelikož $I \subseteq J$, tak $r-j \in J$, a tak $r = j+(r-j) \in J$. Dostáváme $\beta(\alpha(J)) \subseteq J$, a proto $\beta(\alpha(J)) = J$.

Nyní nechť $K \in \mathcal{L}(R/I)$. Jelikož je p surjektivní, platí $K \subseteq p(p^{-1}(K)) = \alpha(\beta(K))$. Inkluze $\alpha(\beta(K)) = p(p^{-1}(K)) \subseteq K$ je zřejmá, a tedy $\alpha(\beta(K)) = K$.

Zobrazení α a β jsou tedy skutečně navzájem inverzní, takže $\mathcal{L}_I(R)$ a $\mathcal{L}(R/I)$ jsou izomorfní jako uspořádané množiny, a tudíž i jako svazy.

ii) Maximální ideály R obsahující I jsou právě maximální prvky uspořádané množiny, která vznikne z $\mathcal{L}_I(R)$ odebráním největšího prvku (tj. ideálu R). Analogicky maximální ideály R/I jsou právě maximální prvky uspořádané množiny, která vznikne z $\mathcal{L}(R/I)$ odebráním největšího prvku (tj. ideálu R/I). Jelikož jsou uspořádané množiny $\mathcal{L}_I(R)$ a $\mathcal{L}(R/I)$ izomorfní, tak si skutečně tyto ideály vzájemně odpovídají.

Nyní ukážeme, že prvoideály R obsahující I odpovídají prvoideálům R/I. Mějme libovolné $J \in \mathcal{L}_I(R)$, který je navíc prvoideál R. Ukážeme, že pak je $p(J)$ prvoideál R/I. Víme, že J je vlastní ideál R, takže z c)i) plyne, že $p(J)$ vlastní ideál R/I. Nechť $a, b \in R/I$ jsou takové, že $ab \in p(J)$. Potom existují $r, s \in R$ takové, že $a = r + I$, $b = s + I$. Pak $ab = rs + I \in p(J)$, takže s využitím výsledku s c)i) dostáváme $rs \in p^{-1}(p(J)) = J$. Jelikož je J prvoideál, tak je $r \in J$ nebo $s \in J$, a tedy $a = p(r) \in p(J)$ nebo $b = p(s) \in p(J)$. Ideál $p(J)$ je tedy skutečně prvoideál R/I. Nechť naopak $K \in \mathcal{L}(R/I)$, který je navíc prvoideál R/I. Jelikož je K vlastní ideál R/I, tak $p^{-1}(K)$ je vlastní ideál R. Mějme $r, s \in R$ takové, že $rs \in p^{-1}(K)$. Potom s využitím c)i) dostaneme, že platí $p(r)p(s) = p(rs) \in p(p^{-1}(K)) = K$, a jelikož je K prvoideál, dostáváme $p(r) \in K$ nebo $p(s) \in K$, takže $r \in p^{-1}(K)$ nebo $s \in p^{-1}(K)$. Dokázali jsme tedy, že $p^{-1}(K)$ je prvoideál R, a dohromady tedy prvoideály R obsahující I odpovídají v popsaném izomorfismu prvoideálům R/I.

Pozn.: V případě kdy je R komutativní okruh, lze tvrzení z c)ii) dokázat alternativně pomocí b). Skutečně, pro každé $J \in \mathcal{L}_I(R)$ platí $R/J \cong (R/I)\big/(J/I) = (R/I)\big/p(J)$, takže R/J je těleso, resp. obor integrity právě tehdy, když je $(R/I)\big/p(J)$ těleso, resp. obor integrity, a tudíž J je maximální ideál, resp. prvoideál okruhu R právě tehdy, když je $p(J)$ maximální ideál, resp. prvoideál okruhu R/I. Tato úvaha lze zobecnit i na nekomutativní okruhy, místo těles je třeba uvažovat netriviální okruhy, které nemají žádné nenulové vlastní ideály, a místo oborů integrity netriviální okruhy, které nemají dělitele nuly.

d)-i) Vezměme $R = \mathbb{Z}$, $S = \mathbb{Z}_2$, f kanonickou projekci $\mathbb{Z} \to \mathbb{Z}_2$ a $M = 3\mathbb{Z}$ (což je maximální ideál $\mathbb{Z}$, neboť $\mathbb{Z}/M \cong \mathbb{Z}_3$ je těleso). Pak $f(M) = \mathbb{Z}_2$ (protože $f(0) = [0]_2$ a $f(3) = [3]_2 = [1]_2$) je nevlastní ideál $\mathbb{Z}_2$, takže to není maximální ideál $\mathbb{Z}_2$.

ii) Vezměme $R = \mathbb{Z}[x]$, $S = \mathbb{Z}_4[x]$. Označme g homomorfismus okruhů $\mathbb{Z} \to \mathbb{Z}_4[x]$, který vznikne složením kanonické projekce $\mathbb{Z} \to \mathbb{Z}_4$ a inkluze $\mathbb{Z}_4 \to \mathbb{Z}_4[x]$. Dále označme i inkluzi $\mathbb{Z} \to \mathbb{Z}[x]$. Potom existuje jediný homomorfismus okruhů $f\colon \mathbb{Z}[x] \to \mathbb{Z}_4[x]$ takový, že $f(x) = x$ a $g = f \circ i$, tj. následují diagram komutuje.

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[r, dashed, "f"] & \mathbb{Z}_4[x] \\
\mathbb{Z} \arrow[u, hook, "i"] \arrow[ur, "g"] \arrow[r, two heads] & \mathbb{Z}_4 \arrow[u, hook]
\end{tikzcd}$$

Pro každý polynom $p(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ tudíž platí $f(p(x)) = [a_n]_4 x^n + \ldots + [a_0]_4$, z čehož je snadno vidět, že f je surjektivní. Vezměme $P = x\mathbb{Z}[x]$. Zřejmě $P \neq \{0\}$ a navíc je P jádro surjektivního homomorfismu $\mathbb{Z}[x] \to \mathbb{Z}$ daného vztahem $p(x) \to p(0)$ pro každé $p(x) \in \mathbb{Z}[x]$, takže $\mathbb{Z}[x]/P \cong \mathbb{Z}$ je obor integrity a tedy P je prvoideál $\mathbb{Z}[x]$. Zřejmě platí $f(P) = x\mathbb{Z}_4[x]$, což je vlastní ideál $\mathbb{Z}_4[x]$, navíc je tento ideál jádro surjektivního homomorfismu $\mathbb{Z}_4[x] \to \mathbb{Z}_4$ určeného vztahem $p(x) \to p(0)$ pro každé $p(x) \in \mathbb{Z}_4[x]$, takže $\mathbb{Z}_4[x]/f(P) \cong \mathbb{Z}_4$ není obor integrity, a tedy $f(P)$ není prvoideál $\mathbb{Z}_4[x]$ (nebo alternativně můžeme ukázat přímo z definice, že $f(P)$ není prvoideál $\mathbb{Z}_4[x]$, platí totiž $[2]_4 \cdot [2]_4 = [4]_4 = [0]_4 \in f(P)$, ale $[2]_4 \notin f(P)$).

8. kolo — řešení

a) Označme $\mathcal{P}$ množinu všech vlastních ideálů okruhu R, které obsahují I. Ukážeme, že $(\mathcal{P}, \subseteq)$ splňuje předpoklady Zornova lemmatu. Zřejmě $I \in \mathcal{P}$, takže $\mathcal{P} \neq \emptyset$. Nechť $\mathcal{C}$ je libovolný neprázdný řetězec v $(\mathcal{P}, \subseteq)$. Označme $Q = \bigcup_{J \in \mathcal{C}} J$. Ukážeme, že Q je ideál R. Mějme $x, y \in Q$ a $r \in R$. Pak existují $J_1, J_2 \in \mathcal{C}$ takové, že $x \in J_1$ a $y \in J_2$. Pak $x + y, rx, xr \in \max(J_1, J_2) \subseteq Q$, takže Q je skutečně ideál R. Jelikož $I \subseteq J$ a $1 \notin J$ (neboť jde o vlastní ideály) pro každé $J \in C$, tak $I \subseteq Q$ a $1 \notin Q$. Tudíž skutečně $Q \in \mathcal{P}$, a zřejmě Q je horní závora $\mathcal{C}$ v $\mathcal{P}$. Podle Zornova lemmatu tedy existuje ideál M, který je maximální prvek $(\mathcal{P}, \subseteq)$. Je evidentní, že M je maximální ideál okruhu R obsahující I.

b) Nechť $x \in J(R)$ a předpokládejme sporem, že existuje $r \in R$ takové, že $1 + rx \notin R^\times$. Potom je ideál $(1 + rx)$ vlastní, a tak podle a) existuje maximální ideál M okruhu R takový, že $(1 + rx) \subseteq M$, tj. $1 + rx \in M$. Kdyby bylo $x \in M$, tak by platilo $1 = (1 + rx) - rx \in M$, což je spor. Platí tedy $x \notin M$, a tak $x \notin J(R)$.

Naopak předpokládejme, že pro každé $r \in R$ je $1 + rx \in R^\times$, a mějme maximální ideál M okruhu R. Ukážeme, že platí $x \in M$, z čehož pak vyplyne $x \in J(R)$. Kdyby bylo $x \notin M$, tak by ideál $M + (x)$ byl ostře větší než M. Jelikož je ale M maximální ideál, tak pak musí být $M + (x) = R$, tedy $1 \in M + (x)$. Jelikož je R komutativní, tak to znamená, že existují $m \in M$ a $s \in R$ takové, že $m + sx = 1$. Odtud plyne $1 - sx = m \in M$, a tak $1 - sx \notin R^\times$ (jelikož M je vlastní ideál), což je spor.

c)-i) Zřejmě $0 \in N(R)$. Mějme $x, y \in N(R)$ a $r \in R$. Potom existují $m, n \in \mathbb{N}$ takové, že $x^m = y^n = 0$. Jelikož je R komutativní okruh, tak podle binomické věty platí $(x + y)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} x^i y^{m+n-1-i}$. Pro každé $i \in \{0, \dots, m+n-1\}$ platí buď $i \geq m$ nebo $m+n-1-i \geq n$, takže všechny sčítance v této sumě jsou nulové, a tak $(x + y)^{m+n-1} = 0$, a tedy $x + y \in N(R)$. Dále opět z komutativity R máme $(rx)^m = r^m x^m = r^m \cdot 0 = 0$, takže $rx \in N(R)$. Tudíž $N(R)$ je skutečně ideál okruhu R.

ii) Pro každé $x \in R$ a $n \in \mathbb{N}$ platí $x^n \in I$ právě tehdy, když $p(x)^n = p(x^n) = 0 + I$, a tak $x \in \sqrt{I}$ právě tehdy, když $p(x) \in N(R/I)$. Skutečně tedy $\sqrt{I} = p^{-1}(N(R/I))$. Podle c)i) aplikovaného na okruh R/I je $N(R/I)$ ideál R/I, a tak $\sqrt{I} = p^{-1}(N(R/I))$ je ideál okruhu R.

d)-i) Ukážeme, že $(\mathcal{T}, \subseteq)$ splňuje předpoklady Zornova lemmatu. Jelikož $x \notin N(R)$, tak $0 \notin S$, takže $(0) \in \mathcal{T}$, a tak $\mathcal{T} \neq \emptyset$. Nechť dále $\mathcal{C}$ je libovolný neprázdný řetězec v $(\mathcal{T}, \subseteq)$. Označme $Q = \bigcup_{J \in \mathcal{C}} J$. Stejně jako v části a) se dokáže, že Q je ideál okruhu R. Jelikož $J \cap S = \emptyset$ pro každé $J \in \mathcal{C}$, tak $Q \cap S = \emptyset$. Je tedy $Q \in \mathcal{T}$, a zřejmě je to horní závora $\mathcal{C}$ v $\mathcal{T}$. Podle Zornova lemmatu tedy existuje ideál P, který je maximální prvek $(\mathcal{T}, \subseteq)$.

ii) Jelikož je $x \notin P$, je P vlastní ideál okruhu R. Předpokládejme sporem, že existují $y, z \in R$ takové, že $y, z \notin P$ a $yz \in P$. Potom jsou ideály $P + (y)$ a $P + (z)$ ostře větší než P. Kdyby ani jeden z těchto ideálů nepatřil do $\mathcal{T}$, tak by existovaly $m, n \in \mathbb{N}$ takové, že $x^m \in P + (y)$ a $x^n \in P + (z)$, tudíž by existovaly $p_1, p_2 \in P$ a $r, s \in R$ takové, že $x^m = p_1 + ry$ a $x^n = p_2 + sz$. Potom by bylo $x^{m+n} = (p_1 + ry) \cdot (p_2 + sz) = p_1p_2 + p_1sz + ryp_2 + rsyz \in P$ (neboť každý z těchto sčítanců leží v P). To ale nemůže nastat, protože $P \cap S = \emptyset$. Platí tedy $P + (y) \in \mathcal{T}$ nebo $P + (z) \in \mathcal{T}$, což je spor s maximalitou P. Dokázali jsme tedy, že P je prvoideál okruhu R.

e)-i) Nechť P je prvoideál okruhu R a $x \in N(R)$. Pak existuje $n \in \mathbb{N}$ takové, že $x^n = 0$. Platí tedy $x^n \in P$, a tak $x \in P$ (snadno se indukcí dokáže, že pokud prvoideál obsahuje součin konečně mnoha prvků daného okruhu, tak obsahuje některý z nich). Tudíž platí $N(R) \subseteq P$, a tedy $N(R)$ je obsaženo v průniku všech prvoideálů okruhu R (jelikož je R netriviální okruh, tak z a) a z komutativity R plyne, že existuje aspoň jeden prvoideál tohoto okruhu, takže jde o průnik přes neprázdnou množinu).

Nechť naopak $x \in R$, $x \notin N(R)$. Potom z d) plyne, že existuje prvoideál P okruhu R takový, že $x \notin P$, takže x neleží v průniku všech prvoideálů R.

Dohromady tedy dostáváme, že $N(R)$ je rovno průniku všech prvoideálů okruhu R.

ii) Z c)ii) víme, že $\sqrt{I} = p^{-1}(N(R/I))$, a podle e)i) aplikovaného na okruh R/I (jelikož je I vlastní ideál R, tak je R/I netriviální okruh) je $N(R/I)$ rovno průniku všech prvoideálů R/I. Jelikož je vzor průniku je roven průniku vzorů, tak je $\sqrt{I}$ rovno průniku všech ideálů okruhu R tvaru $p^{-1}(P)$, kde P probíhá přes všechny prvoideály R/I. Podle příkladu c)ii) ze 7. kola soutěže jsou tyto ideály právě prvoideály R obsahující I, a tedy $\sqrt{I}$ je rovno jejich průniku.

9. kolo — řešení

a) Označme $M = \{r \cdot s;\ r \in I,\ s \in J\}$. Podle definice je $I \cdot J = (M)$, ideál generovaný množinou M. Protože každý ideál okruhu R je podgrupou grupy $(R, +)$, pro podgrupu $\langle M \rangle$ grupy $(R, +)$ generovanou množinou M platí $\langle M \rangle \subseteq (M)$. Protože $I \neq \emptyset$, $J \neq \emptyset$, platí $M \neq \emptyset$, navíc pro libovolné $r \in I$, $s \in J$ je $-(r \cdot s) = (-r) \cdot s \in M$, podle věty o podgrupě grupy generované podmnožinou grupy z přednášky Algebra I víme, že

$$\begin{aligned}\langle M \rangle &= \Big\{\sum_{i=1}^{n} m_i;\ n \in \mathbb{N},\ m_1, \ldots, m_n \in M\Big\} = \\ &= \Big\{\sum_{i=1}^{n} r_i \cdot s_i;\ n \in \mathbb{N},\ r_1, \ldots, r_n \in I,\ s_1, \ldots, s_n \in J\Big\}.\end{aligned}$$

Abychom ukázali, že $\langle M \rangle = (M)$, stačí ověřit, že $\langle M \rangle$ je ideál, což vzhledem k tomu, že je to podgrupa $(R, +)$, znamená ověřit uzavřenost na násobení zvenčí. Pro libovolné $r \in R$ a libovolná $r_1, \ldots, r_n \in I$, $s_1, \ldots, s_n \in J$ platí

$$\begin{aligned} r \cdot \Big(\sum_{i=1}^{n} r_i \cdot s_i\Big) &= \sum_{i=1}^{n} (r \cdot r_i) \cdot s_i \in \langle M \rangle, \\ \Big(\sum_{i=1}^{n} r_i \cdot s_i\Big) \cdot r &= \sum_{i=1}^{n} r_i \cdot (s_i \cdot r) \in \langle M \rangle, \end{aligned}$$

neboť $r \cdot r_i \in I$, $s_i \cdot r \in J$.

Z uzavřenosti ideálu na násobení zvenčí plyne $M \subseteq I$, a tedy $(M) \subseteq I$, podobně $(M) \subseteq J$, dohromady $I \cdot J \subseteq I \cap J$.

b) Z definice součinu ideálů víme, že ideál $(I \cdot J) \cdot K$ je generován součiny

$$\Big(\sum_{i=1}^{n} r_i \cdot s_i\Big) \cdot t = \sum_{i=1}^{n} r_i \cdot s_i \cdot t,$$

kde $r_1, \ldots, r_n \in I$, $s_1, \ldots, s_n \in J$, $t \in K$. Každý sčítanec $r_i \cdot s_i \cdot t$ leží v $I \cdot (J \cdot K)$, proto zde leží i jejich součet, odkud $(I \cdot J) \cdot K \subseteq I \cdot (J \cdot K)$. Opačná inkluze se dokáže analogicky.

c) Označme $N = \{a_i \cdot b_j;\ i = 1, \dots, n,\ j = 1, \dots, m\}$, nechť M má stejný význam jako v části a). Pak z $N \subseteq M$ plyne $(N) \subseteq (M)$. Naopak libovolný prvek množiny M je tvaru $r \cdot s$, kde $r \in I$, $s \in J$. Pro tyto prvky r, s existují $u_1, \dots, u_n, v_1, \dots, v_m \in R$ tak, že $r = \sum_{i=1}^{n} u_i a_i$, $s = \sum_{j=1}^{m} v_j b_j$, tedy $r \cdot s = \sum_{i=1}^{n} \sum_{j=1}^{m} u_i v_j a_i b_j \in (N)$. Z $M \subseteq (N)$ plyne $(M) \subseteq (N)$, vždyť (M) je nejmenší ideál obsahující množinu M. Dohromady dostáváme rovnost $(M) = (N)$.

d) Z předpokladu nesoudělnosti ideálů plyne existence $r, r' \in I$, $s \in J$ a $t \in K$ tak, že platí $r + s = 1 = r' + t$. Pak dostáváme $1 = (r+s) \cdot (r'+t) = rr' + sr' + rt + st$, přitom $rr' + sr' + rt \in I$, $st \in J \cdot K$. Tedy ideál I je nesoudělný s ideálem $J \cdot K$.

e) Z předpokladu nesoudělnosti ideálů plyne existence $r \in I$, $s \in J$ tak, že platí $r + s = 1$. Pro libovolné $t \in I \cap J$ pak dostaneme $t = (r + s) \cdot t = r \cdot t + t \cdot s \in I \cdot J$. Využitím a) odtud plyne $I \cdot J = I \cap J$.

f-i) To, že φ je homomorfismus okruhů, plyne z univerzální vlastnosti součinu: označíme-li součin faktorokruhů $S = R/I_1 \times \cdots \times R/I_n$ a projekce ze součinu $\mu_j : S \to R/I_j$, $j = 1, \dots, n$, pak pro n-tici projekcí na faktorokruh $\pi_j : R \to R/I_j$, $j = 1, \dots, n$ je φ jediné zobrazení splňující $\mu_j \circ \varphi = \pi_j$ pro každé $j = 1, \dots, n$. Snadno se však tento fakt odvodí přímo z toho, že v součinu jsou operace definovány po složkách a ve faktorokruhu pomocí reprezentantů. Pro libovolné $r, s \in R$ platí

$$\begin{aligned}
\varphi(r + s) &= (r + s + I_1,\ r + s + I_2,\ \dots,\ r + s + I_n) = \\
&= (r + I_1,\ r + I_2,\ \dots,\ r + I_n) + (s + I_1,\ s + I_2,\ \dots,\ s + I_n) = \\
&= \varphi(r) + \varphi(s), \\
\varphi(r \cdot s) &= (r \cdot s + I_1,\ r \cdot s + I_2,\ \dots,\ r \cdot s + I_n) = \\
&= (r + I_1,\ r + I_2,\ \dots,\ r + I_n) \cdot (s + I_1,\ s + I_2,\ \dots,\ s + I_n) = \\
&= \varphi(r) \cdot \varphi(s), \\
\varphi(1) &= (1 + I_1,\ 1 + I_2,\ \dots,\ 1 + I_n),
\end{aligned}$$

což je jednička okruhu S.

Prvek $x \in R$ patří do jádra φ, právě když $x + I_j = 0 + I_j$ pro každé $j = 1, \dots, n$, což nastane právě když $x \in I_j$ pro každé $j = 1, \dots, n$, tedy když $x \in I_1 \cap I_2 \cap \cdots \cap I_n$.

f-ii) Jestliže je φ surjektivní, pak pro každé $1 \leq j < k \leq n$ existuje $r \in R$ tak, že $\varphi(r) = (\dots, 0 + I_j, \dots, 1 + I_k, \dots)$ má v j-té složce nulu a v k-té složce jedničku dotyčného faktorokruhu (ostatní složky nejsou pro nás podstatné). Označme $s = 1 - r$. Pak platí $r \in I_j$, $r \in 1 + I_k$, tedy $s \in I_k$ a $r + s = 1$, ideály I_j a I_k jsou tedy nesoudělné.

Opačnou implikaci dokážeme indukcí vzhledem k n, a to dokonce pro všechna $n \geq 1$. Je-li $n = 1$, je $\varphi : R \to R/I_1$ projektce na faktorokruh, a proto je φ surjektivní. Dále předpokládejme, že $n > 1$ a že pro součin $n-1$ faktorokruhů bylo tvrzení dokázáno, tedy že jsou-li ideály $I_1, I_2, \dots, I_{n-1}$ po dvou nesoudělné, pak máme surjektivní homomorfismus $\bar{\varphi}\colon R \to R/I_1 \times \cdots \times R/I_{n-1}$ definovaný předpisem $\bar{\varphi}(x) = (x + I_1,\ x + I_2,\ \dots,\ x + I_{n-1})$ pro každé $x \in R$. Tvrzení dokážeme pro n. Mějme tedy další ideál I_n okruhu R, který je nesoudělný s každým z ideálů $I_1, I_2, \dots, I_{n-1}$. Indukcí z části d) dostáváme, že I_n je nesoudělný se součinem $I_1 \cdot I_2 \cdots I_{n-1}$, existují tedy $r \in I_1 \cdot I_2 \cdots I_{n-1}$ a $s \in I_n$ tak, že $r + s = 1$. Nechť $a_1, \dots, a_n \in R$ jsou libovolné. Z indukčního předpokladu existuje $d \in R$ tak, že $\bar{\varphi}(d) = (a_1 + I_1,\ a_2 + I_2,\ \dots,\ a_{n-1} + I_{n-1})$, tedy $d - a_j \in I_j$ pro každé $j = 1, \dots, n-1$. Označme $c = r \cdot a_n + s \cdot d$. Pak pro každé $j = 1, \dots, n-1$ podle inkluze z části a) platí $r \in I_j$, a tedy $c = r \cdot a_n + (1 - r) \cdot d = d + r \cdot (a_n - d)$, proto $c - d = r \cdot (a_n - d) \in I_j$, což spolu s $d - a_j \in I_j$ dává $c - a_j \in I_j$. Podobně $c = (1 - s) \cdot a_n + s \cdot d = a_n + s \cdot (d - a_n)$, odkud $c - a_n \in I_n$. Proto $\varphi(c) = (a_1 + I_1,\ a_2 + I_2,\ \dots,\ a_n + I_n)$.

f-iii) Požadovanou rovnost dokážeme indukcí vzhledem k n. Je-li $n = 2$, jde o výsledek části e).

Předpokládejme, že $n > 2$ a že $I_1 \cdot I_2 \cdots I_{n-1} = I_1 \cap I_2 \cap \cdots \cap I_{n-1}$. Už jsme zmiňovali, že z části d) indukcí dostáváme, že I_n je nesoudělný se součinem $I_1 \cdot I_2 \cdots I_{n-1}$, a tedy podle části e) platí $I_1 \cdot I_2 \cdots I_n = (I_1 \cdot I_2 \cdots I_{n-1}) \cap I_n$. Dosazením dostaneme dokazované.

Protože φ je surjektivní homomorfismus a $\ker \varphi = I_1 \cap I_2 \cap \cdots \cap I_n = I_1 \cdot I_2 \cdots I_n$, hlavní věta o faktorokruzích nám dává izomorfismus $R/(I_1 \cdot I_2 \cdots I_n) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n$.

10. kolo — řešení

a) Je-li $f(x) \in R[[x]]^\times$, pak existuje mocninná řada $g(x) = \sum_{i=0}^{\infty} b_i x^i \in R[[x]]$ tak, že platí $f(x) \cdot g(x) = 1$, odkud $a_0 b_0 = 1$, a tedy $a_0 \in R^\times$.

Naopak, je-li $a_0 \in R^\times$, pak existuje $b_0 \in R$ tak, že $a_0 b_0 = 1$. Pro každé $n \in \mathbb{N}$ definujme rekurentně

$$b_n = -b_0 \cdot \sum_{i=1}^{n} a_i b_{n-i} \in R.$$

Pak $a_0 b_n = -\sum_{i=1}^{n} a_i b_{n-i}$, tedy $\sum_{i=0}^{n} a_i b_{n-i} = 0$, což pro $g(x) = \sum_{i=0}^{\infty} b_i x^i \in R[[x]]$ znamená, že $f(x) \cdot g(x) = 1$. Z komutativity také $g(x) \cdot f(x) = 1$.

b) Předpokládejme, že $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]^\times$. Protože $R[x]$ je podokruhem $R[[x]]$, plyne odtud užitím a), že $a_0 \in R^\times$. Abychom ukázali, že $a_1, \ldots, a_n \in N(R)$, podle tvrzení z e)i) z 8. kola soutěže stačí ukázat pro libovolný prvoideál P okruhu R, že $a_1, \ldots, a_n \in P$. Projekci na faktorokruh $\pi : R \to R/P$ lze rozšířit na homomorfismus $\tilde{\pi} : R[x] \to (R/P)[x]$ aplikující π na koeficienty polynomu, tedy

$$\tilde{\pi}\Big(\sum_{i=0}^{m} b_i x^i\Big) = \sum_{i=0}^{m} \pi(b_i) x^i.$$

Obrazem jednotky v homomorfismus okruhů je jednotka, tedy $\tilde{\pi}(f(x)) \in (R/P)[x]^\times$. Protože P je prvoideál, je faktorokruhem R/P obor integrity. Podle věty 5.13 ze skript k Algebře I (J. Rosický: Algebra) jsou jednotky v okruhu polynomů nad oborem integrity pouze konstantní polynomy (které jsou navíc jednotkami v tomto oboru integrity). Proto pro každé $i = 1, \ldots, n$ platí $\pi(a_i) = 0$, tedy $a_i \in P$.

Předpokládejme, že $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ a že platí $a_0 \in R^\times$ a $a_i \in N(R)$ pro všechna $1 \le i \le n$. Podle definice nilradikálu je prvek a_i nilpotentní, tj. existuje $m_i \in \mathbb{N}$ tak, že $a_i^{m_i} = 0$. Pro jednoduchost označme m největší číslo z čísel $m_1, \ldots, m_n$, pak $a_i^m = 0$ pro každé $1 \le i \le n$. Potřebnou úvahu vyložíme nejsnadněji pomocí pojmu součin ideálů, který je zaveden v komentáři k devátém kolu soutěže. Označme $I = (a_1, \ldots, a_n)$ ideál generovaný prvky $a_1, \ldots, a_n$. Z úlohy b) devátého kola plyne, že množina všech ideálů okruhu R tvoří vzhledem k operaci součin ideálů pologrupu, můžeme tedy hovořit o mocnině I^r ideálu I pro každé $r \in \mathbb{N}$. Z úlohy c) devátého kola indukcí snadno plyne, že pro každé $r \in \mathbb{N}$ je ideál I^r generován součiny $\prod_{i=1}^{n} a_i^{k_i}$, kde $(k_1, \ldots, k_n)$ probíhá n-tice nezáporných celých čísel splňujících $k_1 + \cdots + k_n = r$, přičemž a_i^0 zde znamená 1. Z Dirichletova principu plyne, že $I^r = \{0\}$ pro každé $r > n(m-1)$.

Podle části a) existuje formální mocninná řada $g(x) = \sum_{i=0}^{\infty} b_i x^i \in R[[x]]$ tak, že platí $f(x) \cdot g(x) = 1$. Ukážeme, že $g(x)$ je polynom. Platí

$$\begin{aligned}
b_1 &= -b_0 \cdot a_1 b_0 \in I, \\
b_2 &= -b_0 \cdot (a_1 b_1 + a_2 b_0) \in I, \\
&\vdots \\
b_n &= -b_0 \cdot (a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_n b_0) \in I
\end{aligned}$$

a pro každé $k > n$ platí

$$b_k = -b_0 \cdot (b_{k-1}a_1 + \cdots + b_{k-n}a_n).$$

Jestliže tedy pro nějaké r platí $b_{k-1}, b_{k-2}, \ldots, b_{k-n} \in I^r$, pak odtud $b_k \in I^{r+1}$. Dostáváme tedy

$$\begin{gathered} b_1, b_2, \ldots, b_n \in I, \\ b_{n+1}, b_{n+2}, \ldots, b_{2n} \in I^2, \\ b_{2n+1}, b_{2n+2}, \ldots, b_{3n} \in I^3, \ldots \end{gathered}$$

Odtud plyne, že pro každé $t > n^2(m-1)$ platí $b_t \in I^{n(m-1)+1}$, tedy $b_t = 0$. Proto $g(x)$ je polynom.

c) Je-li $cf(x) = 0$ pro nějaké nenulové $c \in R$, pak je $f(x)$ dělitel nuly v okruhu $R[x]$.

Předpokládejme naopak, že $f(x)$ je dělitel nuly v okruhu $R[x]$. Zvolme nenulový polynom $g(x) = \sum_{i=0}^{m} b_i x^i \in R[x]$ co nejmenšího stupně m takový, že $f(x)g(x) = 0$. Tedy $b_m \neq 0$ a je-li $m = 0$, jsme hotovi. Proto předpokládejme $m > 0$. Kdyby pro všechna $\ell \in \{0, \ldots, n\}$ platilo $a_\ell g(x) = 0$, pak by $a_\ell b_m = 0$, tedy $f(x)b_m = 0$, spor s volbou $g(x)$. Proto existuje takové $\ell \in \{0, \ldots, n\}$, že $a_\ell g(x) \neq 0$. Volbou největšího takového ℓ lze předpokládat, že pro každé r splňující $\ell < r \leq n$ je $a_r g(x) = 0$. Pro koeficient u $x^{\ell+m}$ součinu $f(x)g(x)$ platí

$$\sum_{i=0}^{\ell+m} a_i b_{\ell+m-i} = 0,$$

kde klademe $a_i = 0$ pro $i > n$ a $b_{\ell+m-i} = 0$ pro $i < \ell$. Ovšem pro $i > \ell$, $i \leq n$ víme, že $a_i g(x) = 0$, a tedy $a_i b_{\ell+m-i} = 0$. Proto i pro poslední zbylý sčítanec tohoto součtu platí $a_\ell b_m = 0$. Odtud plyne, že nenulový polynom $a_\ell g(x)$ má stupeň menší než m a současně platí $f(x) \cdot (a_\ell g(x)) = 0$, což je spor s volbou polynomu $g(x)$.