Cvičení Algebra II — jaro 2008 — DÚ — Komentáře a řešení

A

Příklad A1 (autor: D. Sehnal)

Je $\sqrt{2} = \frac{(\sqrt{2}+\sqrt{3})+(\sqrt{2}-\sqrt{3})}{2}$ a $\sqrt{3} = \frac{(\sqrt{2}+\sqrt{3})-(\sqrt{2}-\sqrt{3})}{2}$, tedy $R = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
Nechť $\phi : R \to R$ je automorfismus R. Potom $\sigma(\sqrt{2})^2 = 2$, $\sigma(\sqrt{3})^2 = 3$ a tedy vztahy $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$ určují všechny automorfismy R. Jsou dvě možnosti kam poslat $\sqrt{2}$ nebo $\sqrt{3}$ a tedy $Aut(R) \simeq (\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$.
`Komentář`: *Pro všechny 4 možnosti by bylo vhodné ověřit, že předpis*

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + \epsilon b\sqrt{2} + \eta c\sqrt{3} + \epsilon\eta d\sqrt{6},$$

kde $\epsilon, \eta \in \{1, -1\}$ zadává homomorfismus. A také, že skládání homomorfismů odpovídá násobení v grupě $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$.

Příklad A2 (autor: T. Golembiovský)

Pro $x_1^2 + x_2^2 + x_3^2$ dostáváme:

x_1	x_2	x_3	s_1	s_2	s_3
2	0	0	2	0	0
1	1	0	0	1	0

$$x_1^2 + x_2^2 + x_3^2 = As_1^2 + Bs_2 = A(x_1 + x_2 + x_3)^2 + B(x_1x_2 + x_1x_3 + x_2x_3)$$

Hodnoty zvolíme následovně:
$x_1 = 1, x_2 = x_3 = 0 \ldots 1 = A$
$x_1 = x_2 = x_3 = 1 \ldots 3 = 9 + 3B \Rightarrow -2 = B$

Pro $x_1^3 + x_2^3 + x_3^3$ dostáváme:

x_1	x_2	x_3	s_1	s_2	s_3
3	0	0	3	0	0
2	1	0	1	1	0
1	1	1	0	0	1

$$x_1^3 + x_2^3 + x_3^3 = As_1^3 + Bs_1s_2 + Cs_3 =$$
$$= A(x_1 + x_2 + x_3)^3 + B(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) + Cx_1x_2x_3$$

Hodnoty zvolíme následovně:
$x_1 = 1, x_2 = x_3 = 0 \ldots 1 = A$
$x_1 = x_2 = 1, x_3 = 0 \ldots 2 = 8 + 2B \Rightarrow -3 = B$
$x_1 = x_2 = 1, x_3 = -1 \ldots 1 = 1 + 3 - C \Rightarrow 3 = C$
Dostaneme soustavu:

$$\begin{aligned} s_1 &= 0 \\ s_1^2 - 2s_2 &= s_1^3 - 3s_1s_2 + 3s_3 \\ s_3 &= 2 \end{aligned}$$

$$-2s_2 = 6$$
$$s_2 = -3$$

$$x_1 + x_2 + x_3 = 0$$

$$x_1x_2 + x_1x_3 + x_2x_3 = -3$$
$$x_1x_2x_3 = 2$$

$$x_2 + x_3 = -x_1$$
$$x_2x_3 = \frac{2}{x_1}$$
$$x_1(x_2 + x_3) + x_2x_3 = -3$$

$$-x_1^2 + \frac{2}{x_1} = -3$$
$$-x_1^3 + 3x_1 + 2 = 0$$

`Komentář`: *Polynom $f(x) = x^3 - 0x^2 - 3x - 2$ lze z podmínek $s_1 = 0, s_2 = -3, s_3 = 2$ sestavit rovnou na základě Vietových vztahů.*

Jeden kořen je viditelně $x_1 = 2$. Po vydělení $-x_1^3 + 3x_1 + 2/(x_1 - 2)$ dostáváme $x_1^2 + 2x_1 + 1 = 0$ a odtud pak:

$$x_1 = \frac{-2 \pm \sqrt{0}}{2} = -1$$

Dosazením do soustavy získáme

$$x_2 + x_3 = 1$$
$$-x_2 - x_3 + x_2x_3 = -3$$
$$x_2x_3 = -2$$

$$x_2 = 1 - x_3$$
$$(1 - x_3)x_3 = -2$$
$$-x_3^2 + x_3 + 2 = 0$$

$$x_3 = \frac{-1 \pm \sqrt{9}}{-2}$$
$$x_{3a} = -1$$
$$x_{3b} = 2$$

Nyní pro jednotlivé případy x_3:

1. pro $x_3 = -1$ jsou tedy zbylé dva kořeny $x_1 = -1$, $x_2 = 2$ (nebo naopak)
2. a pro $x_3 = 2$ jsou to $x_1 = -1$, $x_2 = -1$.

`Komentář`: *Soustavu není nutné řešit takto. x_1, x_2, x_3 jsou kořeny f, tj. jeden je 2 zbylé -1.*
Celkem máme tedy 3 řešení: $(-1, -1, 2), (-1, 2, -1), (2, -1, -1)$.

Příklad A3 (autor: M.Chmelík)
O kubickém polynomu $f(x) = x^3 - ux^2 + 1 \in \mathbb{C}[x]$, kde $u \in \mathbb{C}$, víme, že má 3 různé kořeny x_1, x_2, x_3. Sestavte normovaný kubický polynom, jež má kořeny:

$$\frac{x_1 + x_2}{x_3}, \frac{x_2 + x_3}{x_1}, \frac{x_1 + x_3}{x_2}$$

$$(x-x_1)(x-x_2)(x-x_3) = x^3 + (-x_1-x_2-x_3)x^2 + (x_1x_2+x_1x_3+x_2x_3)x + (-x_1x_2x_3)$$

Porovnáním získáme následující rovnosti:

$$\begin{aligned} x_1+x_2+x_3 &= u \\ x_1x_2+x_2x_3+x_1x_3 &= 0 \\ x_1x_2x_3 &= -1 \end{aligned}$$

Rádi bychom polynom tvaru:

$$x^3 - \left(\frac{x_1+x_2}{x_3} + \frac{x_2+x_3}{x_1} + \frac{x_1+x_3}{x_2}\right)x^2 + \left(\frac{(x_1+x_2)(x_2+x_3)}{x_1x_3} + \frac{(x_2+x_3)(x_1+x_3)}{x_1x_2} + \frac{(x_1+x_2)(x_1+x_3)}{x_2x_3}\right)x$$
$$-\frac{(x_1+x_2)(x_1+x_3)(x_2+x_3)}{x_1x_2x_3}$$

Vyjádříme si výraz:

$$-\frac{(x_1+x_2)(x_1+x_3)(x_2+x_3)}{x_1x_2x_3}$$

Víme, že $x_1x_2x_3 = -1$, proto budeme upravovat výraz:

$$(x_1+x_2)(x_1+x_3)(x_2+x_3) = (x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) - x_1x_2x_3 = u \cdot 0 - (-1) = 1$$

Vyjádříme si výraz:

$$\frac{(x_1+x_2)(x_2+x_3)}{x_1x_3} + \frac{(x_2+x_3)(x_1+x_3)}{x_1x_2} + \frac{(x_1+x_2)(x_1+x_3)}{x_2x_3} =$$
$$\frac{{x_1}^3 + x_2{x_1}^2 + x_3{x_1}^2 + {x_2}^2x_1 + {x_3}^2x_1 + 3x_2x_3x_1 + {x_2}^3 + {x_3}^3 + x_2{x_3}^2 + {x_2}^2x_3}{x_1x_2x_3} =$$
$$-((x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) + {x_1}^3 + {x_2}^3 + {x_3}^3) =$$
$$-({x_1}^3 + {x_2}^3 + {x_3}^3)$$

$$-({x_1}^3 + {x_2}^3 + {x_3}^3) = -({\sigma_1}^3 - 3\sigma_1\sigma_2 + 3\sigma_3) = -(u^3 + 3(-1)) = -u^3 + 3$$

Vyjádříme si výraz:

$$-\left(\frac{x_1+x_2}{x_3} + \frac{x_2+x_3}{x_1} + \frac{x_1+x_3}{x_2}\right) = \frac{(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) - 3x_1x_2x_3}{x_1x_2x_3} =$$
$$-3(-1) = 3$$

Proto hledaný polynom bude tvaru:

$$x^3 + 3x^2 + (3-u^3)x + 1$$

Příklad A4 (autor: D. Sehnal)
$(Reg(A), \subseteq)$ tvoří svaz, protože regularní jazyky jsou uzavřeny na (konečné) sjednocení a průnik. Tedy $\sup\{X,Y\} = X \cup Y$ a $\inf\{X,Y\} = X \cap Y$. Největší prvek je A^* a nejmenši je prázdný jazyk.

$(Reg(A), \subseteq)$ netvoří úplný svaz.

Nechť $A = \{a\}$. Uvažujme třídu $X = \{X_i | i \in \mathbb{N}\}$ regulárních jazyků, kde

$$X_i = \begin{cases} A^* & \text{je-li i prvočíslo;} \\ A^* - \{a^i\} & \text{jinak.} \end{cases}$$

Nyní $L = \bigcap_{i\in\mathbb{N}} X_i = \{a^p | p \text{ je prvočíslo}\}$ není regulární jazyk. Dále $\inf X$ musí ležet pod L. Nechť $Y_i = \{a^p | p \text{ je prvočíslo menší než i-té prvočíslo}\}$. Každý Y_i je regulární, protože je konečný. Posloupnost $Y_1 \subset Y_2 \subset Y_3 \subset \cdots$ tvoří posloupnost dolních závor X. Nutně tedy $Y_i \subseteq \inf X$, ovšem $\bigcup_{i\in\mathbb{N}} Y_i = L$, což je spor s předchozím pozorováním $\inf X \subset L$.

Příklad A5 (autor: M.Šmérek)

Nechť $(A, \subseteq)$ je neprázdný svaz neobsahující nekonečné podřetězce. Ukážeme, že $(A, \subseteq)$ má největší a nejmenší prvek. Nechť X je libovolný maximální (vzhledem k inkluzi) podřetězec $(A, \subseteq)$ a x je jeho největší prvek. Pak x je maximální prvek $(A, \subseteq)$ (jinak spor s maximalitou X). Zároveň $(\forall a \in A)(\ a \leq x\ )$, jinak pro nějaké $b \in A$, které toto porušuje bychom dostali $(x \vee b) > x$ a X není maximální. Tedy x je největší prvek $(A, \subseteq)$. Obdobně bychom dokázali, že $(A, \subseteq)$ má i nejmenší prvek.

Nyní předpokládejme, že existuje $M \subseteq A$ tak, že M nemá supremum v A (M je neprázdná, neboť supremum prázdné množiny je nejmenší prvek v A). Nechť H je množina horních závor M. Protože $(A, \subseteq)$ má největší prvek (označme jej 1), máme $1 \in H$. Dále musí existovat $x_1 \in H$ tak, že $x_1 \leq 1$ a $x_1 \neq 1$, jinak je 1 supremum množiny M. Navíc existuje $y_1 \in H$ tak, že $y_1 < x_1$ nebo x_1 a y_1 jsou nesrovnatelné. Pokud by takové y_1 neexistovalo, tak by x_1 bylo supremum M. Pak ale $(\forall m \in M)(\ m \leq (x_1 \wedge y_1)\ )$ a tedy $(x_1 \wedge y_1) \in H$. Máme tedy řetězec délky 3, ale obdobně můžeme pokračovat a získat tak nekonečný řetězec, což by byl spor a taková množina M nemůže existovat. $(A, \subseteq)$ je tedy úplný svaz.

`Komentář`: *První čás lze dokázat i tak, že*

1. *existuje nějaký maximální prvek uspořádané množiny A,*
2. *každý prvek je menší než nějaký maximální a*
3. *nemohou existovat dva maximální prvky, protože ve svazu A existuje jejich supremum.*

Druhá část důkazu lze dokončit elegantně tak, že konstatujeme, že H je podsvaz svazu A a podle první části má tedy nejmenší prvek. To je hledané supremum.

Příklad A6 (autor: L. Caha)
Příloha mimo tento soubor.

Příklad A7 (autor: J. Krčál)

$(\mathbb{N}_0, |)$

Supremem podmnožiny $X \subseteq \mathbb{N}_0$ je nejmenší společný násobek (lcm), nebo 0, pokud lcm X neexistuje.

Prvek 1 je zřejmě kompaktní, je to nejmenší prvek. Ukažme, že lib. prvek $x \in \mathbb{N} \setminus \{1\}$ není kompaktní. Každé číslo je zřejmě součin konečně mnoha prvočísel, tedy existuje prvočíslo p, tak že $p \nmid x$. Pak $sup\{p^n \mid n \in \mathbb{N}\} = 0 \geq x$. Ovšem pro lib. konečnou podmnožinu Y je $supY$ rovno největšímu prvku podmnožiny a pro lib. n máme $x \nmid p^n$, tedy neplatí $supY \geq x$.

Tedy $(\mathbb{N}_0, |)$ není algebraický.

$(\mathbb{N}_0, |)^d$

Supremem je největší společný dělitel (gcd).

Prvek 0 je zřejmě kompaktní, ukažme, že libovolné $x \in \mathbb{N}$ je kompatní. Nechť $X \subseteq \mathbb{N}_0$, $supX \geq x \iff gcdX \mid x$.

Vezměme lib. $a \in X$, pouze u konečně mnoha prvočísel má rozklad a na prvočísla vyšší mocninu než $gcdX$. Pro každé takové prvočíslo p a mocninu m v $gcdX$ musí existovat $y \in X$, tak že rozklad y na prvočísla obsahuje právě p^m. Tyto prvky přidáme k prvku a, postupně získáme $Y = \{a, y_1, y_2, y_3, ..., y_k\}$, tak že $gcdY = gcdX$.

Všechny prvky jsou kompaktní, tedy zřejmě $(\mathbb{N}_0, |)^d$ je algebraický.

Příklad A8 (autor: O. Klíma dle různých řešení)
Pro $n \leq 2$ je svaz distributivní. Pro $n \leq 3$ je svaz modulární. Pro $n \geq 3$ obsahuje svaz podsvaz izomorfní M_5 a tedy není distributivní. Pro $n \geq 4$ obsahuje svaz podsvaz izomorfní N_5 a tedy není modularní. Konkrétně: pro $A = \{1, 2, 3, \dots, n\}$ je např. podsvaz izomorfní M_5 dán prvky $\triangle$, $\rho_1 = \{(2, 3), (3, 2)\} \cup \triangle$, $\rho_2 = \{(1, 3), (3, 1)\} \cup \triangle$, $\rho_3 = \{(1, 2), (2, 1)\} \cup \triangle$ a $\rho = \{1, 2, 3\} \times \{1, 2, 3\} \cup \triangle$.

Podobně, pro modularitu lze uvažovat $\triangle$, $\tau_1 = \{(1, 2), (2, 1)\} \cup \triangle$, $\tau_2 = \{(1, 2), (2, 1), (3, 4), (4, 3)\} \cup \triangle$, $\tau_3 = \{(1, 3), (3, 1), (2, 4), (4, 2)\} \cup \triangle$, $\tau = \{1, 2, 3, 4\} \times \{1, 2, 3, 4\} \cup \triangle$.

Příklad A9 (autor: O. Klíma podle A. Hericha)

Svaz podsvazů svazu S je distributivní, právě když S je řetězec.

Důkaz: Pokud je S řetězec, pak každá podmnožina tvoří podsvaz. Tj. Svaz podsvazů svazu S je $(\mathcal{P}(S), \cap, \cup)$, který je distributivní.

Pokud S není řetězec, pak obsahuje dva nesrovnatelné prvky a, b. Potom následujíci podmnžiny tvoří podsvazy S: $\emptyset$, $\{a\}$, $\{b\}$, $\{a, a \vee b\}$, $\{a \wedge b, a, b, a \vee b\}$. A ty tvoří podsvaz svazu všech podsvazů svazu S, který je izomorfní svazu N_5. (Pardon, neodolal jsem této formulaci.)

Příklad A10 (autor: O. Klíma podle A. Hericha)

Nechť a je $\vee$-ireducibilní a nechť $a \leq x \vee y$.
Pak $a = a \wedge (x \vee y)$ a z distributivity máme $a = (a \wedge x) \vee (a \wedge y)$. Odtud ($a$ je $\vee$-ireducibilní) máme $a = a \wedge x$ nebo $a = a \wedge y$. Čili $a \leq x$ nebo $a \leq y$.

Naopak, nechť a je $\vee$-primitivní a nechť $a = x \vee y$.
Pak 1. $a \geq x$ a $a \geq y$.
2. $a \leq x \vee y$ a tedy (a je $\vee$-primitivní) máme $a \leq x$ nebo $a \leq y$.
Dohromady $a = x$ nebo $a = y$.

Všimněte si, že distributivita se využila pouze v jedné implikaci.

Příklad A11 (autor: O. Klíma podle mnohých)

Označme $b = (a \vee a)$. Pak $c = a \wedge b = a \wedge (a \vee a) = a$ podle absorbčního zákona.
Proto $a \vee c = a \vee a$. Na druhé straně $a \vee c = a \vee (a \wedge b) = a$ opět podle absorbčního zákona.
Tzn. $a \vee a = a \vee c = a$.

Stejným způsobem lze dokázat $a \wedge a = a$. Případně to lze odvodit pomocí dokázaného: $a \wedge a = a \wedge (a \vee a) = a$.

Příklad A12 (autor: O. Klíma podle mnohých)

V obou případech vyjde osmiprvkový svaz izomorfní $\mathcal{P}_3$ (krychle postavená na špičku).

Příklad A13 (autor: O. Klíma podle mnohých)

i) Neplatí. Například (nekomplementární) tříprvkový řetězec je podsvazem komplementárního svazu N_5.

ii) Platí. Nechť $\varphi : S \to S'$ je surjektivní homomorfismus z komplementárního svazu S do svazu S'. Pokud 1 je největší prvek S, potom $\varphi(1)$ je největší prvek S' (plyne z izotonie zobrazení φ). Stejně tak $\varphi(0)$ je nejmenší prvek S' a svaz S' je tedy omezený.

Nyní pro libovolný prvek $a \in S'$ existuje prvek $s \in S$ tak, že $\varphi(s) = a$. Pro něj máme komplement s' ve svazu S. Ukážeme, že $\varphi(s')$ je komplement a ve svazu S'. Stačí ověřit, že

$$\varphi(s') \wedge a = \varphi(s') \wedge \varphi(s) = \varphi(s' \wedge s) = \varphi(0).$$

Podobně $\varphi(s') \vee a = \varphi(1)$.

iii) Pro libovolný svaz S uvažujeme $S' = S \cup \{0, 1, k\}$ kde $0, 1, k$ jsou nové prvky, tj. $0, 1, k \notin S$. Rozšíříme definici operací $\wedge$ a $\vee$ na množinu S' tak, že 0 bude nejmenší prvek, 1 bude největší prvek a k je prvek nesrovnatelný se všemi prvky z S. Přesněji, pro libovolné $t \in S'$ resp. $s \in S$ definujeme:

$$t \wedge 0 = 0 \wedge t = 0, \quad t \wedge 1 = 1 \wedge t = t, \quad s \wedge k = k \wedge s = 0,$$

$$t \vee 0 = 0 \vee t = t, \quad t \vee 1 = 1 \vee t = 1, \quad s \vee k = k \vee s = 1.$$

`Komentář`: *Nejmenší a největší prvek musíme přidat, protože nikde nebylo řečeno, že S je omezený.*

Příklad A14 (autor:)

Počty postupně 27,29,5,5.

Příklad A15 (autor: O. Klíma)

V libovolné unární algebře (A, f) platí, že sjednocení dvou podalgeber je podalgebra. Skutečně, pokud $B, C \subseteq A$ jsou nosiče podalgeber, pak pro libovolné $x \in B \cup C$, máme $x \in B$ nebo $x \in C$, tj. $f(x) \in B$ nebo $f(x) \in C$, odkud $f(x) \in B \cup C$.

Proto supremum ve svazu všech podalgeber algebry (A, f) je sjednocení. Víme, že infimum je průnik (platí obecně pro libovolnou algebru). Tedy svaz S všech podalgeber (A, f) je podsvaz svazu všech podmnožin množiny A, který je distributivní, a tedy je i S je distributivní.

Příklad A16 (autor: O. Klíma)

Uvažujeme-li unární algebru (A, id_A), pak snadno nahlédneme, že každá relace ekvivalence na množině A je kongruencí algebry (A, id_A). Víme, že svaz všech relací ekvivalencí na čtyřprvkové množině není modulární. Stačí tedy vzít $A = \{1, 2, 3, 4\}$ a algebru (A, id_A).

Jiné řešení (několik studentů): (A, f), kde $A = \{1, 2, 3, 4\}$, $f(1) = 2, f(2) = 1, f(3) = 4, f(4) = 3$.

Příklad A17 (autor: O. Klíma)

Pro libovolnou kongruenci ρ (různou od Δ) označme $n, d \in \mathbb{N}$ nejmenší čísla s vlastností $n\rho(n+d)$. (Přesněji, n nechť je nejmenší číslo, pro které existuje $k \in \mathbb{N}$ takové, že $n\rho(n+k)$, a pro toto n nechť d je nejmenší takové k.) Snadno se nahlédne, že tato dvojice jednoznačně zadává kongruenci.

Platí, že kongruence ρ daná dvojicí (n, d) je menší než kongruence σ daná dvojicí (n', d') právě tehdy, když $n' \leq n$ a $d' \mid d$. Proto je hledaný svaz izomorfní svazu $(\mathbb{N}, \leq)^d \times (\mathbb{N}, |)^d \cup \{\perp\}$.

Příklad A18 (autor: O. Klíma podle mnohých)

a) Ne. V součinu dvou těles nemají prvky tvaru $(a, 0)$ inverze. Lze také argumentovat konečností.
b) Ne. $\alpha(1) + \alpha(1) = 2 + 2 = 4 \neq 3 = \alpha(2) = \alpha(1 + 1)$.
c) Ano. Ověří se že ρ je relace ekvivalence. Poté se ověří, že platí $a\rho a' \wedge b\rho b' \implies ab\rho a'b'$.

Příklad A19 (autor: O. Klíma)

a) Ano, ano, ano. Jde o varietu danou identitou $f(x) = g(x)$.

b) H: Ne. Obrazem může být triviální algebra, která není v naší třídě.

P: Ne. Zlobí součin přes prázdnou množinu, kdy výsledkem je triviální algebra. Pro neprázné součiny uvažovanou třídu neopustíme.

S: Ano.

c) H: Ne. Pro $(\mathbb{Z}, succ)$ lze uvažovat kongruenci ρ, která má v relaci všechna kladná čísla; přesněji

$$x\rho y \iff (x = y \vee (x > 0 \wedge y > 0)).$$

Potom příslušná faktoralgebra (cyklus délky 1 s nekonečným ocáskem) nemá bijektivní operaci.

P: Ano.

S: Ne. $\mathbb{N}$ je podalgebra $(\mathbb{Z}, succ)$.

Příklad A20 (autor: O. Klíma)

a) H: Ano; S: Ano; P_f Ano; P Ne.

b) H: Ne!!!! (příklad je netriviální-viz konec); S: Ano — každý minimální automat obsahuje pouze jeden podautomat, tj. celý automat; P,P_f: Ne — příklad na cvičení.

c) H, S: Ne — viz. A19-c); P, P_f: Ano.

d) H: Ano; S: Ano; P_f Ano; P Ne.

e) H: Ano (automat je generován prázdnou množinou, tj. i homomorfní obraz má tuto vlastnost); S: Ano(viz b)); P_f, P Ne (viz b)).

Příklad k b-H:

$\Omega = \{a, b, c\}$, $L = \Omega^*(ab + bc + ca)$.

Minimální automat má 7 stavů: $\{0, 1, 2, 3, 4, 5, 6\}$, kde 0 je iniciální, a dále $a(0) = a(1) = a(2) = a(4) = a(5) = 1$, $a(3) = a(6) = 4$; $b(0) = b(2) = b(3) = b(5) = b(6) = 2$, $b(1) = b(4) = 5$; $c(0) = c(1) = c(3) = c(4) = c(6) = 3$, $c(2) = c(5) = 6$.

Nyní kongruence ρ je dána/generována vztahy $1\rho 4$, $2\rho 5$, $3\rho 6$. Tzn. faktoralgebra má 4 prvky kde všechny tři unární operace jsou konstantní. O tomto automatu lze ukázat, že není minimální. Ať zvolíme množinu finálních stavů jakoukoli, vždy půjde faktorizovat. (Např. stav, který je třídou obsahující 1, lze ztotožnit se stavem, který je třídou obsahující 2, pokud jsou oba tyto stavy finální nebo naopak oba nefinální.)

Příklad A21 (autor: O. Klíma, T.Golembiovský)

`Komentář`: *Při práci s unárními operacemi je možné uvažovat dvě různé interpretace. Buď vše chápeme klasicky, tj. např $a^3b^2(x)$ znamená $a(a(a(b(b(x)))))$, nebo uvažujeme pohled přes automaty, tj. že na prvek x postupně aplikuje „písmenka“, tj. např $a^3b^2(x)$ znamená, že z x jdeme postupně podle a, a, a, b a na konec b. Je nutné si předem jednu interpretaci zvolit a té se poté držet po celý příklad- autor předkládaného řešení zvolil druhou interpretaci.*

Rozebereme $f^kg^l(x) = g^mf^n(x)$ ve dvou případech, kdy za x dosazujeme prvek z množiny $\{1, 2, 3, 4\}$ nebo $\{5, 6\}$.

- Pro $s \in \{1, 2, 3, 4\}$ platí $a^kb^l(s) = b^ma^n(s)$ právě když $k - l \equiv n - m0(mod4)$.
- Pro $x \in \{5, 6\}$ musí platit $k = 0 \Leftrightarrow n = 0$.

  Je-li $k = n = 0$ dostáváme podmínku $l = 0 \Leftrightarrow m = 0$.

  Je-li $k, n > 0$ dostáváme podmínku $|k - l - n| \equiv 0 \pmod 4$.

Všechny identity rozdělíme na několik typů. Je vidět, že algebra nesplňuje žádnou identitu s termy v různých proměnných (viz. cvičení). Podobě nesplňuje žádnou identitu s termy v jedné proměnné, kde f je jen v jednom termu (stačí dosatit prvek 5). Tj. zbývá diskutovat

1. $g^m fu(x) = g^n fv(x)$, kde $u, v \in \{f, g\}^*$.

2. $g^m(x) = g^n(x)$

1. Platí pokud jsou splňeny dvě podmínky

$$\#_f(u) + 1 - m - \#_g(u) \equiv \#_f(v) + 1 - n - \#_g(v) \pmod 4$$

(případ dosazení prvku z množiny $\{1, 2, 3, 4\}$)

$$\#_f(u) - \#_g(u) \equiv \#_f(v) - \#_g(v) \pmod 4$$

(případ $\{5, 6\}$)

Tyto dvě podmínky lze tedy ekvivalentně přepsat:

$$\#_f(u) - \#_g(u) \equiv \#_f(v) - \#_g(v) \pmod 4, \quad m \equiv n \pmod 4.$$

2.
Platí pokud $m - n \equiv 0 \pmod 4$ a $m = 0 \Leftrightarrow n = 0$

Příklad A22 (autor: O. Klíma)

Pokud $m \mid n$ potom algebra Z_m je faktoralgebra Z_n (zde zobrazení $[x]_n \mapsto [x]_m$ je surjektivní homomorfismus). V tomto případě tedy každá identita, která platí v Z_n, platí i v Z_m a hledaná identita tedy neexistuje.

Pokud $m \not| n$ pak hledanou identitou je např. $f^n(x) = x$. Ta jistě platí v Z_n, ale neplatí v Z_m (za x dosadíme např. $[0]_m$ a rovnost $f^n([0]_m) = [0]_m$ by znamenala $[n]_m = [0]_m$, tj. $m \mid n$.)

Příklad A23 (autor: O. Klíma)

i) Intuitivně kontrolujeme první písmenko a množinu všech písmen, které se ve slově objeví. Definujeme h zobrazení („první písmenko“) z množiny všech termů do množiny proměnných X takto: $h(x) = x$ pro $x \in X$, $h(t_1 \cdot t_2) = h(t_1)$ pro termy t_1, t_2.

Podobně c je zobrazení („obsah“) z množiny všech termů do množiny proměnných $\mathcal{P}(X)$ definované takto: $c(x) = \{x\}$ pro $x \in X$, $c(t_1 \cdot t_2) = c(t_1) \cup c(t_2)$ pro termy t_1, t_2.

Identita $t = s$ je splněna v uvažované varietě, právě když $h(t) = h(s)$ a $c(t) = c(s)$.

DK: $' \leftarrow'$ použijí se identity.

$' \rightarrow'$ pokud $h(t) \neq h(s)$, pak stačí vzít pologrupu levých nul (která je v naší varietě), ve které nebude identita $t = s$ platit. Pokud $c(t) \neq c(s)$ pak vhodnou pologrupou je polosvaz $(\mathcal{P}(X), \cup)$.

Poznamenejme, že lze také rovnou brát volnou pologrupu v této varietě — viz. doc. Polák-1.termín, úloha B, 2003.

ii) nemám kapacitu: intuitivně kontrolujeme posloupnost prvních výskytů všech písmen ve slově.

Příklad B1 (autor: D. Sehnal)

Minimální polynom (s koeficienty v $\mathbb{Q}$) mající $\alpha = 2^{1/4}$ jako kořen je $f(x) = x^4 - 2$. Podobně pro i máme $g(x) = x^2 + 1$. Je tedy $R = \mathbb{Q}(\alpha, i) = \mathbb{Q}/\langle (x^4 - 2)(x^2 + 1) \rangle$. Kořeny $f(x)$ jsou $\alpha, -\alpha, \alpha i, -\alpha i$ a pro $g(x)$ jsou kořeny $i, -i$. To znamená, že α můžeme poslat na nějaký prvek z $\{\alpha, -\alpha, \alpha i, -\alpha i\}$ a i na $\{i, -i\}$.

Nechť $\varphi : R \to R, \alpha \mapsto \alpha i, i \mapsto i$ a $\psi : R \to R, \alpha \mapsto \alpha, i \mapsto -i$ jsou automorfismy R. Pak φ a ϕ generují grupu $Aut(R)$, která není nic jiného než grupa symetrií čtverce tvořeného vrcholy o souřadnicích kořenů polynomu $f(x)$ v komplexní rovině, kde rotaci o 90 stupňů odpovídá φ a ϕ osové symetrii podle osy x. Je tedy $Aut(R) \simeq D_4$, kde D_n je dihedralní grupa (grupa symetrií pravidelného n-úhelníku). Prvky $Aut(R)$ jsou $\{1, \varphi, \varphi^2, \varphi^3, \psi, \varphi\psi, \varphi^2\psi, \varphi^3\psi\}$.

Příklad B2 (autor: O. Klíma)

Pokud není R obor integrity, snadno se takový příklad nalezne. Např. $2x$ nad $\mathbb{Z}_8$.

Pokud R je obor integrity, pak takový polynom neexistuje. Předpokládejme naopak, že f má takovou vlastnost, tj. $f(x, y, z_1, \ldots, z_k) \neq f(y, x, z_1, \ldots, z_k)$, pro nějaké x, y, přičemž f^3 je symetrický polynom. Uvažujme $g(x, y) = f(x, y, \ldots)$ jako polynom nad $R[z_1, z_2, \ldots, z_k]$. Pak $g(x, y)$ má také naši vlastnost jako f. Budeme pracovat s tímto polynomem ve dvou proměnných. Navíc místo oboru integrity přesuneme naše úvahy do příslušného podílového tělesa. Pro polynom $\alpha = \frac{g(x,y)}{g(y,x)} \neq 1$ máme $\alpha^3 = 1$.

Lze dokázat, že pokud $\alpha^3 = 1$ pak $\alpha \in R$. (Není to úplně jednoduché.)

Nyní z $g(x, y) = \alpha g(y, x)$ plyne výměnou x a y, že $g(y, x) = \alpha g(x, y)$ (zde použijeme, že α je konstanta). Teď již snadno: $g(x, y) = \alpha g(y, x) = \alpha^2 g(x, y) = \alpha^3 g(y, x) = g(y, x)$. Spor.

`Komentář`: *Zajímavé je, že pro druhou mocninu to funguje. Tj. existuje polynom f nad oborem integrity který není symetrický ale f^2 symetrický je.*

Příklad B3 (autor: J. Konečný)

$\mathcal{S}$ — množina všech vektorových podprostorů vektorového prostoru $\mathbb{Q}^3$
$a = \langle (1, 0, 0) \rangle$, $b = \langle (0, 1, 0) \rangle$, $c = \langle (0, 0, 1) \rangle$, $d = \langle (1, 1, 1) \rangle$

Podsvaz svazu $(\mathcal{S}, \wedge, \vee)$ generovaný množinou $\{a, b, c\}$ má osm prvků ($\mathcal{M} = \{\{\vec{0}\}, a, b, c, \langle a, b \rangle, \langle a, c \rangle, \langle b, c \rangle, \mathbb{Q}^3\}$) a je izomorfní se svazem $(\mathcal{P}(a, b, c), \subseteq)$.

`Komentář`: *Zde se zápisem $\langle a, b \rangle$ myslí podprostor generovaný $a \cup b$. Bylo by přesnější asi psát* $\sup\{a, b\}$ *nebo $a \vee b$ nebo třeba $\langle a \cup b \rangle$ místo $\langle a, b \rangle$.*

$(\mathcal{N}, \wedge, \vee)$ je podsvaz svazu $(\mathcal{S}, \wedge, \vee)$ generovaný množinou $\{a, b, c, d\}$. Zřejmě $\mathcal{M} \subseteq \mathcal{N}$. Pomocí průseků a spojení lze nagenerovat další prvky náležící do $\mathcal{N}$:

- $\langle a, d \rangle = a \vee d = \langle (1, 0, 0), (0, 1, 1) \rangle$
  $\langle b, d \rangle = b \vee d = \langle (1, 0, 1), (0, 1, 0) \rangle$
  $\langle c, d \rangle = c \vee d = \langle (1, 1, 0), (0, 0, 1) \rangle$
- $e = \langle a, d \rangle \wedge \langle b, c \rangle = \langle (0, 1, 1) \rangle$
  $f = \langle b, d \rangle \wedge \langle a, c \rangle = \langle (1, 0, 1) \rangle$
  $g = \langle c, d \rangle \wedge \langle a, b \rangle = \langle (1, 1, 0) \rangle$
- $\langle e, f \rangle = e \vee f = \langle (1, 0, 1), (0, 1, 1) \rangle$
  $\langle e, g \rangle = e \vee g = \langle (1, 0, -1), (0, 1, 1) \rangle$
  $\langle f, g \rangle = f \vee g = \langle (1, 0, 1), (0, 1, -1) \rangle$

- $h = \langle e, f\rangle \wedge \langle a, b\rangle = \langle (1, -1, 0)\rangle$
  $i = \langle e, g\rangle \wedge \langle a, c\rangle = \langle (1, 0, -1)\rangle$
  $j = \langle f, g\rangle \wedge \langle b, c\rangle = \langle (0, 1, -1)\rangle$

Aplikací průseků a spojení lze generovat do nekonečna další podprostory. Pro popis podsvazu bude třeba přesně popsat operace spojení jednorozměrných a průseku dvourozměrných podprostorů. Spojení dvou jednorozměrných podprostorů lze snadno popsat $U \vee V = \langle U \cup V\rangle$. Pro popis průseků budou dále dvourozměrné prostory zapisovány v normovaném tvaru $\langle (1, 0, x), (0, 1, y)\rangle$ kde $x, y \in \mathbb{Q}$. Kromě $\langle a, c\rangle$ a $\langle b, c\rangle$ lze takto popsat všechny dvourozměrné podprostory z $\mathbb{Q}^3$.

`Komentář`: *Kromě všech obsahujících c.*

Nechť $p = \langle (1, 0, x), (0, 1, y)\rangle$ a $q = \langle (1, 0, u), (0, 1, v)\rangle$. Rovinu p lze parametricky vyjádřit $(x_1, x_2, x_3) = s(1, 0, x) + t(0, 1, y)$. Rovina q má normálový vektor $n = (u, v, -1)$ a je popsána rovnicí $ux_1 + vx_2 - x_3 = 0$. Po dosazení p do q dostaneme $s(u - x) = t(y - v)$, $t = s(\frac{u-x}{y-v})$.

`Komentář`: *Přesněji pro $y \neq v$. Pro $u = x$ ale nemá smysl průsek počítat.*

$s(1, 0, x) + t(0, 1, y) = s(1, 0, x) + s(\frac{u-x}{y-v})(0, 1, y) = s(1, \frac{u-x}{y-v}, x + \frac{(u-x)y}{y-v}) \in p \wedge q$, proto

$$p \wedge q = \left\langle (1, \frac{u - x}{y - v}, x + \frac{(u - x)y}{y - v})\right\rangle .$$

Způsob, jakým je počítán průsek, dává velké možnosti dalšího generování podprostorů.

Lze dokázat, že $\langle (1, 0, x), (0, 1, y)\rangle \in \mathcal{N}$ pro $x, y \in \mathbb{Z}$: Pro $x, y \in \{-1, 0, 1\}$ platí (spojení podprostorů a, b, e, f, i, j). Předpokládejme, že tvrtení platí pro $x, y \in \{-n, \dots, n\}$, dokážeme že platí i pro $x, y \in \{-n - 1, \dots, n + 1\}$.

$v = \langle (1, 0, n - 1), (0, 1, -1)\rangle \wedge \langle (1, 0, n), (0, 1, 0)\rangle = \langle (1, -1, n)\rangle$.
$(v \vee e) \wedge (c \vee f) = \langle (1, 0, n + 1)\rangle$, $(v \vee i) \wedge (c \vee e) = \langle (0, 1, -n - 1)\rangle$. Při volbě $v = \langle (1, 0, -n + 1), (0, 1, -1)\rangle \wedge \langle (1, 0, -n), (0, 1, 0)\rangle = \langle (1, 1, -n)\rangle$ dostaneme stejným způsobem i $\langle (1, 0, -n - 1)\rangle$ a $\langle (0, 1, n + 1)\rangle$.

Dále lze vygenerovat libovonlý prostor $\left\langle (1, 0, \frac{r}{s})\right\rangle$, $r, s \in \mathbb{Z}, s \neq 0$. Pak $v = \langle (1, 0, 0), (0, 1, 0)\rangle \wedge \langle (1, 0, r), (0, 1, s)\rangle = \left\langle (1, -\frac{r}{s}, 0)\right\rangle$ a dále $(v \vee e) \wedge (a \vee c) = \left\langle (1, 0, \frac{r}{s})\right\rangle$. Výrazem $(\left\langle (1, 0, \frac{r}{s})\right\rangle \vee h) \wedge (b \vee c)$ dostaneme $\left\langle (0, 1, \frac{r}{s})\right\rangle$.

Z výše uvedeného plyne, že dokážeme nagenerovat libovolný dvourozměrný podprostor v $\mathbb{Q}^3$. Průsekem dostaneme libovolný jednorozměrný. Proto $(\mathcal{N}, \wedge, \vee) = (\mathcal{S}, \wedge, \vee)$.

Příklad B4 (autor: M. Šmérek)

Jedná se o svaz. Existence spojité funkce, která je supremem definovaným

$$(\forall f, g \in C) sup\{f, g\} = h, \text{ kde } h(x) = max\{f(x), g(x)\}$$

plyne ze spojitosti f a g. Obdobně pro infimum.

Nejedná se o úplný svaz, neboť

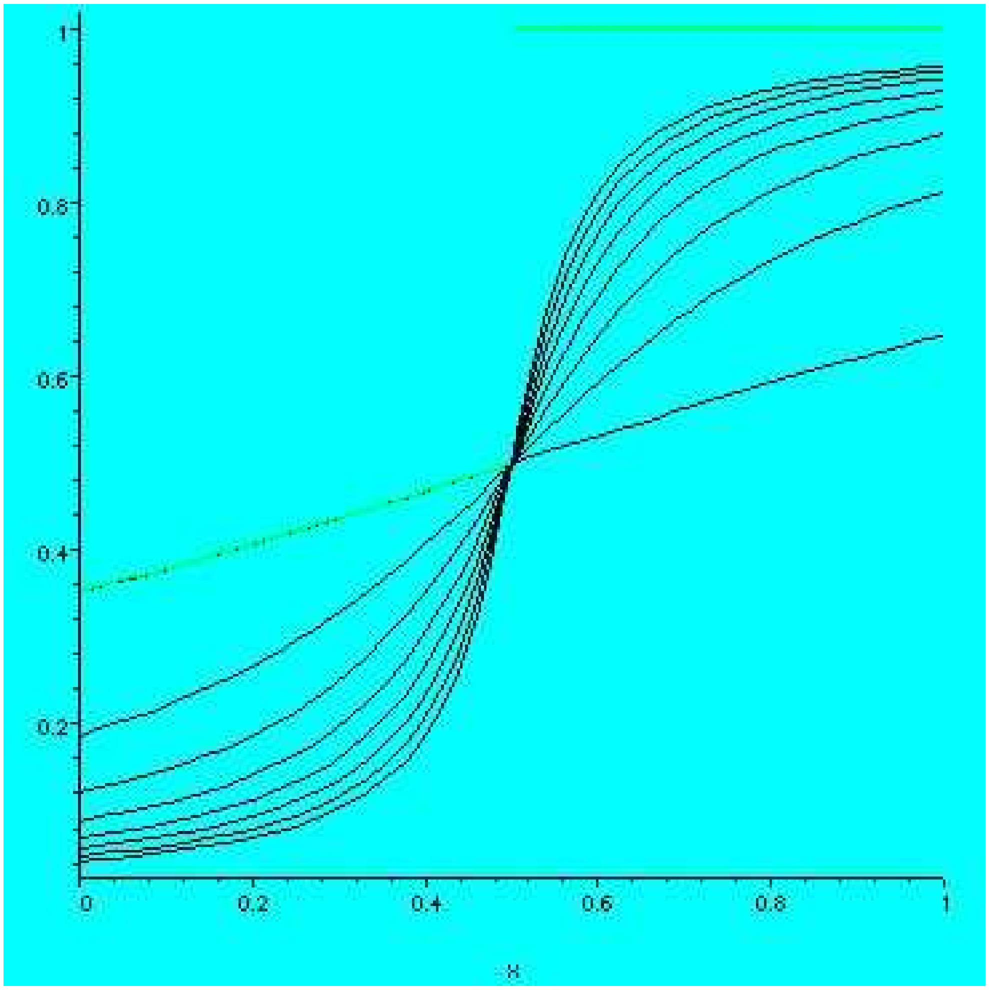
$$sup\{f_i\}_{i\in\mathbb{N}}, \text{ kde } f_i = \frac{1}{\pi} arctan(i(x - \frac{1}{2})) + \frac{1}{2}$$

neexistuje. Na obrázku je zeleně vyznačeno supremum v nespojitých funkcích. Pro libovolnou funkci $f \in C$ takovou, že $(\forall i \in \mathbb{N})(\ f \geq f_i\ )$ existuje f' různé od f tak, že $(\forall i \in \mathbb{N})(\ f \geq f' \geq f_i\ )$. Takové f' začne „stoupat k jedničce“ později jak f.

`Komentář`: *Pro uvažované f máme $f(x) = 1$ pro $x \geq \frac{1}{2}$. Potom $f'(x) = 1$ pro $x \geq \frac{1}{2}$ a pro $x < \frac{1}{2}$ lze definovat $f'(x)$ například takto: $f'(x) = \frac{f_1(x)+f(x)}{2}$.*

Možná trochu přehlednější je uvažovat „lineární“ funkce tvaru $f(x) = i(x - \frac{1}{2}) + \frac{1}{2}$, „ořízlé“ do intervalu $\langle 0, 1\rangle$.

Příklad B5 (autor: R. Benkovský)



Obrázek 1: Obrázek k příkladu B-4

Nechť $(G, +)$ je libovolná grupa, potom svaz podgrup grupy $(G, +)$ je algebraický svaz.
Tvrzení : Kompaktní prvky svazu podgrup $(Sub(G), \subseteq)$ jsou právě konečně generované podgrupy (tedy podgrupy, které mají konečnou množinu generátorů).
Důkaz: (Jen jedné implikace, kterou pro náš příklad potřebujeme.)

Pokud je S konečně generovaná podgrupa, potom pro libovolnou množinu podgrup X platí : pokud $\sup X \geq S$, potom tedy $\sup X \supseteq S$, tedy $\sup X$ obsahuje všechny prvky podgrupy S, tedy obsahuje i (konečně mnoho) generátorů podgrupy $S =< R >$.

Z množiny podgrup X nám tedy stačí vybrat podgrupy X_i, které obsahují prvky množiny R. Dostáváme tedy (zřejmě konečnou, protože množina R je konečná) množinu indexů I tak, že

$$\left\langle \bigcup_{i \in I} X_i \right\rangle = \sup\{X_i \in X | i \in I\} \geq S$$

.
Tvrzení : Každý prvek $(Sub(G), \subseteq)$ je supremem kompaktních prvků.
Důkaz : Nechť $H \in Sub(G)$, rozlišíme 2 případy :

- H je konečně generovaná $\Rightarrow$ H je kompaktní prvek $\Rightarrow$ H je tedy zřejmě supremem kompaktních prvků
- H je nekonečně generovaná : Nechť tedy $\forall i \in H$ (prvky grupy H) jsou $H_i =< i >$ (podgrupy H generované prvkem i). Potom zřejmě H_i pro libovolné $i \in H$ je podgrupa H a je konečně generovaná. Dále tedy

$H = \sup X$, kde $X = \{H_i \mid i \in H\}$ a tedy H je supremem kompaktních prvků (H_i jsou konečně generované, tedy jsou kompaktní).

Příklad B6 (autor: T. Golembiovský)

- Součin dvou algebraických svazů je algebraický.
  Nechť $(A, \leq)$ a $(B, \sqsubseteq)$ jsou algebraické svazy a mějme součin $(A \times B, \preceq)$.

  Ve svazu $(A \times B, \preceq)$ je prvek $c \in A \times B$, $c = (a, b)$, kompaktní pokud jsou kompaktní a v $(A, \leq)$ a b v $(B, \sqsubseteq)$.
  Je-li $\sup C \geq c$ a $c = (a, b)$ pak vezměme

  $$X = \{x \in A | (\exists b \in B)((x, b) \in C)\} \text{ a } Y = \{y \in B | (\exists a \in A)((a, y) \in C\})$$

  a pak konečné podmnožiny $X_f \subseteq X$ a $Y_f \subseteq Y$ tak, že $\sup X_f \geq a$ a $\sup Y_f \geq b$.

  (`Komentář`: *Zde častá chyba: pak* $\sup X_f \times Y_f \geq c$ *a* $X_f \times Y_f$ *je konečné. To nelze použít, protože* $X_f \times Y_f$ *nemusí být podmnožina* C.)

  Nyní pro libovolné $x \in X_f$ existuje $b \in B$ tak, že $(x, b) \in C$; vyberme nějaké takové b a vložme dvojici (x, b) do množiny X_f'. Podobně zkonstruujeme množinu Y_f'. Konečně $\sup(X_f' \cup Y_f') \geq c$, kde $X_f' \cup Y_f' \subseteq C$.

  Potom pro každý prvek $c \in A \times B$, $c = (a, b)$ vezměme množiny kompaktních prvků $X_a \subseteq A$ a $Y_b \subseteq B$ takových, že $\sup X_a = a$ a $\sup Y_b = b$, pak $\sup X_a \times Y_b = c$ a každý prvek je tedy supremem kompaktních prvků.

- Podsvaz algebraického svazu není algebraický.
  $(P(\mathrm{N}), \subseteq)$ je algebraický svaz, ale podsvaz $(P_\infty(\mathrm{N}) \cup \{\emptyset\}, \subseteq)$ není algebraický.

Příklad B7 (autor: V. Baisa)
Příloha mimo tento soubor.

Příklad B8,B9,B10,B11 (autor: Nemám kapacitu)
Návody: zkuste B9 idnukcí.
B10ii) funguje obecně, stačí ukázat, že

$$\rho_{a,b} = \bigcap \{\ \rho \ \mid \ \rho \ \text{ kongruence}, (a, b) \in \rho\ \}$$

je kompaktní prvek.

Příklad B12 (autor: O. Klíma, P. Troubil)

Úlohu vyřešíme rovnou obecně. Dokážeme, že pro každou podalgebru $\mathcal{A}$ Boolovy algebry $(\mathcal{P}_n, \cup, \cap, 0, 1,')$ platí, že ty prvky $\mathcal{P}_n$, které v $\mathcal{A}$ pokrývají 0, tvoří rozklad na množině $X_n = \{1, \ldots, n\}$. Množinu těchto prvků označme $\mathcal{A}_0$. Musíme ukázat, že prvky v $\mathcal{A}_0$ jsou neprázdné (zřejmé), disjunktní (část 1) jejichž sjednocení je rovno X_n (část 2).

1) Nechť existuje takové $i \in X_n$ a $a \neq b \in \mathcal{A}_0$, tak že $i \in a \cap b$. Protože a, b jsou různé prvky pokrývající v $\mathcal{A}$ prvek 0, musí v $\mathcal{A}$ platit $a \wedge b = 0$. To je spor s $i \in a \cap b = a \wedge b$.

2) Předpokládejme, že $\bigcup \mathcal{A}_0 = C \neq X_n$. Je zřejmé, že (v každém konečném svazu) lze ke každému prvku $x \neq 0$ najít (důkaz indukcí) prvek $y \leq x$, který pokrývá 0. V našem případě aplikujme tento poznatek na

prvek $(\bigvee \mathcal{A}_0)' = C'$ svazu $\mathcal{A}$. Podle předpokladu $C' \neq 0$, tzn. existuje $a \in \mathcal{A}_0$, $a \subseteq C'$. To je spor poněvadž $C' = \bigcap_{b \in \mathcal{A}_0} b' \subseteq a'$.

Výčet všech prvků, které pokrývají v podalgebře $\mathcal{A}$ prvek 0, jednoznačně určuje všechny prvky nosiče této podlagebry. Podalgeber Boolovy algebry $\mathcal{P}_n$ existuje tedy právě tolik, kolik existuje rozkladů množiny $X_n = \{1, \dots, n\}$. Tento počet udává n-té Bellovo číslo $B(n)$. To může být vypočteno např. pomocí rekurzivního vzorce

$$B(n+1) = \sum_{k=0}^{n} \binom{n}{k} B(k)$$

nebo formulí

$$B(n) = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}.$$

Konkrétně potom $B(5) = 52$.

Příklad B13 (autor: Nemám kapacitu)

Příklad B14 (autor: O. Klíma)

H: ne - netriviální příklad je uveden v B13.
S: ne, např $\mathbb{N}$ podsvaz $(\mathbb{N}_0, |)$.
P: ano, lze dokázat, počítáme po složkách.

Příklad B15 (autor: Nemám kapacitu)
Je to jednoduché.

Příklad B16 (autor: Nemám kapacitu)