25.10.

2. Součiny algeber

2.1 (Čínská věta o zbytcích)**.** Nechť $n_1, n_2, \ldots, n_k$ jsou po dvou nesoudělná kladná celá čísla a $n = n_1 \cdot n_2 \cdot \cdots \cdot n_k$, Dokažte, že zobrazení $f : \mathbf{Z}_n \to \prod_{i=1}^{k} \mathbf{Z}_{n_i}$ dané předpisem $f(x) = (x \bmod n_1,\ x \bmod n_2, \ldots, x \bmod n_k)$ je izomorfismus algeber $(\mathbf{Z}_n, +, \cdot, 0)$ a $(\prod_{i=1}^{k} \mathbf{Z}_{n_i}, +, \cdot, \mathbf{0})$, kde $\mathbf{0} = (0, \ldots, 0)$.

Přímo z definice snadno vidíme, že je f zobrazení slučitelné se všemi operacemi. Zbývá nahlédnout, že jde o bijekci. Protože jsou $\mathbf{Z}_n$ a $\prod_{i=1}^{k} \mathbf{Z}_{n_i}$ stejně velké konečné množiny, stačí nahlédnout, že je f prosté. Nechť pro $a \leq b \in \mathbf{Z}_n$ platí, že $f(a) = f(b)$. Potom $f(b-a) = 0$, tedy $n_i / b - a$ pro všechna $i = 1, \ldots, k$. Protože jsou n_i po dvou nesoudělná a $0 \leq b - a \leq n - 1$, máme i $n / b - a$, tudíž $b = a$. □

Ačkoli v předchozím důkaz stačilo ulázat, že je zobrazení prosté, v následujících příkladech si ukážeme, že pomocí Euklidova algoritmu lze pro zobrazení f najít vzor každého prvku.

2.2. Uvažujme zobrazení $f : \mathbf{Z}_{45} \to \mathbf{Z}_5 \times \mathbf{Z}_9$ z 2.1, tj.$f(a) = (a \bmod 5, a \bmod 9)$. Určete (jednoznačně určené) $a \in \mathbf{Z}_{45}$, pro které $f(a) = (3, 2)$.

Hledáme $a \in \mathbf{Z}_{45}$ pro něž existují taková $x \in \mathbf{Z}_9$ a $y \in \mathbf{Z}_5$, že $5x + 3 = a$ a $9y + 2 = a$, tedy musí platit $5x + 3 = 9y + 2$. Upravíme-li rovnici na tvar $9y - 5x = 1$, řešíme obvyklou úlohu. Snadno zjistíme, že $9 \cdot 4 - 5 \cdot 7 = 1$, tedy $a = 5 \cdot 7 + 3 = 9 \cdot 4 + 3 = 38$. □

1.11.

2.3. Uvažujme zobrazení $f : \mathbf{Z}_{720} \to \mathbf{Z}_5 \times \mathbf{Z}_9 \times \mathbf{Z}_{16}$ z 2.1. Najděte $b \in \mathbf{Z}_{720}$, pro které $f(b) = (3, 2, 13)$.

Definujme zobrazení $g : \mathbf{Z}_{45} \times \mathbf{Z}_{16} \to \mathbf{Z}_5 \times \mathbf{Z}_9 \times \mathbf{Z}_{16}$ předpisem $g(u, v) = (u \bmod 5, u \bmod 9, v)$ a zobrazení $h : \mathbf{Z}_{720} \to \mathbf{Z}_{45} \times \mathbf{Z}_{16}$ z Čínské věty o zbytcích, tj. $h(w) = (w \bmod 45, w \bmod 16)$. Všimněme si, že $f = gh$, navíc jsou obě zobrazení g a h bijekce a $f^{-1}(3, 2, 13) = h^{-1}(g^{-1}(3, 2, 13))$. Protože je zobrazení g součinem bijekce z 2.1 a identity a vzor dvojice $(3, 2)$ už jsme spočítali v předchozí úloze, vidíme, že $g^{-1}(3, 2, 13) = (38, 13)$. Zbývá nám tedy stejnou úvahou jako v předchozím příkladu najít vzor $h^{-1}(38, 13)$, tj. vyřešit rovnice $45x + 38 = b$ a $16y + 13 = b$ pomocí diofantické rovnice $16y - 45x + = 25$. Obvyklým způsobem zjistíme například, že $5 \cdot 45 - 14 \cdot 16 = 1$, proto $25 = 125 \cdot 45 - 350 \cdot 16 = 10 \cdot 16 - 3 \cdot 45$. Tedy $b = 45 \cdot 3 + 38 = 16 \cdot 10 + 13 = 173$. □

3. Faktory algeber a kongruence

Uvažujme opět množinu $A = \{a, b, c\}$ s binární operací $\circ$ a dále množinu $B = \{1, 2, 3, 4\}$ s operací $\odot$ danými tabulkami:

$\circ$	**a**	**b**	**c**
a	c	b	a
b	b	a	b
c	a	b	c

$\odot$	**1**	**2**	**3**	**4**
1	2	1	1	3
2	1	4	1	1
3	4	1	4	1
4	3	4	4	2

3.1. Najděte všechny kongruence algebry $(A, \circ)$.

Snadno nahlédneme, že id a $A \times A$ tvoří kongruenci na každé algebře s nosnou množinou A. Budeme nyní probírat všechny zbývající ekvivalence na A, přičemž využijeme jednoznačné korespondence ekvivalence na A a rozkladu A. Existují tedy právě tři ekvivalence odpovídající rozkladu na ekvivalenční třídy $\{\{a\}, \{b, c\}\}$, $\{\{b\}, \{a, c\}\}$ a $\{\{c\}, \{a, b\}\}$.

Nechť $\sim$ je kongruence na A taková, že $a \sim b$. Uvědomíme-li si, že $a \sim a$ a že $\circ$ má být slučitelná s $\sim$, pak $a \circ a \sim a \circ b$, tedy $c \sim b$. Všimněme si, že tuto informaci můžeme vyčíst z prvního řádku tabulky operace $\circ$ (tj. sloupce odpovídající kongruentním prvkům musí v každém řádku obsahovat vzájemně kongruentní hodnoty). Podobně i $a \circ a \sim b \circ s$ (tj. stejnou úvahu můžeme provést i pro sloupce tabulky). V každém případě to znamená, že všechny prvky kongruence obsahující dvojici (a, b) leží v jedné ekvivalenční třídě, tedy dostáváme už zmíněnou kongruenci $A \times A$.

Nyní uvažujme kongruenci $\sim$ na A takovou, že $b \sim c$. Z tabululky okamžitě dostáváme, že $b = a \circ b \sim a \circ c = a$, tedy $a \sim b \sim c$, což opět znamená, že $\sim = A \times A$.

Konečně, pokud uvažujeme kongruenci splňující podmínku $a \sim c$, pak předchzím postupem nedostáváme žádnou novou nutnou podmínku. Zbývá nám nahlédnout, že rozklad $\{\{b\}, \{a, c\}\}$ skutečně určuje kongruenci. K tomu nám stačí zjistit, zda na množině $A/\sim = \{\{b\}, \{a, c\}\}$ můžeme zavést faktorovou operaci $\circ$ předpisem $[x]_\sim \circ [y]_\sim = [x \circ y]_\sim$. Jinak řečeno potřebujeme zjistit, zda všechny součiny prvků z každých dvou pevně zvolených rozkladových tříd leží vždy právě v jedné rozkladové třídě. To snadno nahlédneme z tabulky operace $\circ$, kde poněkud přeházíme řádky a sloupce:

$\circ$	**b**	**a** **c**
b	$[\, a \,]$	$\begin{bmatrix} b & b \end{bmatrix}$
a	$\begin{bmatrix} b \\ b \end{bmatrix}$	$\begin{bmatrix} c & a \\ a & c \end{bmatrix}$
c		

Vidíme, že v každém bloku tabulky máme jen prvky jedné rozkladové třídy, tedy rozkladu $\{\{b\}, \{a, c\}\}$ opravdu odpovídá kongruence $\sim = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$. Zjistili jsme, že na algebře $A(\circ)$ jsou právě tři různé kongruence. □

3.2. Najděte všechny kongruence algebry $(A, \circ, a)$.

Slučitelnost s nulární operací a představuje podmínka $a \sim a$, která je spněna pro každou ekvivalenci. Tedy kongruence na algebře $A(\circ, a)$ jsou stejné jako kongruence na algebře $(A, \circ)$. □

8.11.

3.3. Najděte všechny izomorfismy algebry $(A, \circ)$ do sebe.

Uvažujme nějaký izomorfismus $\varphi : A \to A$. Připomeňme, že izomorfismus „zachovává všechny vlastnosti" algebry, tedy například obrazů jejích jednotlivých prvků. Všimneme-li si, že v A leží právě jeden prvek x, pro který $x \circ x = x$, tj. prvek x, potom $\varphi(c) = c$, konkrétně

$$\varphi(c) = \varphi(c \circ c) = \varphi(c) \circ \varphi(c) \in A.$$

Dále $a \circ a = c$ a $b \circ b \neq c$ a konečně $\varphi(a) \circ \varphi(a) = \varphi(a \circ a) = \varphi(c) = c$, proto $\varphi(a) = a$, a tedy $\varphi(b) = b$, protože φ je bijekce. Zjistili jsme, že jediný izomorfismus $A(\circ)$ do sebe je identické zobrazení. □

3.4. Najděte všechny homomorfismy algebry $(A, \circ)$ do sebe.

V minulé úloze už jsme zjistili, že izomorfismus $(A, \circ)$ do sebe exsituje pouze identický. Uvažujme tedy nějaký homomorfismus $\varphi : A \to A$, který není na, což znamená, že počet prvků $\varphi(A)$ je 1 či 2. Poznamenejme, že $\varphi(A)$ musí být podalgebra A.

Nejprve předpkládejme, že $|\varphi(A)| = 1$. V úloze 1.15 jsme našli jedinou jednoprvkovou podalgebru algebry $A(\circ)$, jíž je podalgebra $\{c\}$. To znamená, že $\varphi(x) = c$ pro všechna $x \in A$.

Nyní předpkládejme, že $|\varphi(A)| = 2$ a opět připomeňme, že v 1.15 jsme zjistili, že množina $\{a, c\}$ je jediná dvouprvková podalgebra algebry $A(\circ)$. Víme, že jádro homomorfismus $ker\varphi = \{(x, y) \in A \times A |\ \varphi(x) = \varphi(y)\}$ 3.1 je kongruence a faktor $A/ker\varphi$ musí být dvouprvkový, tedy rozkladové třídy jádra jsou podle 3.1 nutně $\{a, c\}$ a $\{b\}$, tj. $\varphi(a) = \varphi(c) \neq \varphi(b)$. Nyní spočítáme

$$\varphi(b) \circ \varphi(b) = \varphi(b \circ b) = \varphi(a) \neq \varphi(b),$$

ale $c \circ c = c$, proto $\varphi(b) \neq c$ a nutně tedy $\varphi(b) \neq a$ a $\varphi(a) = \varphi(c) = c$. Nyní už prověřením jednotlivých případů snadno nahlédneme, že je φ posledním hledaným homomorfismem.

3.5. Rozhodněte, zda existuje homomorfismus algebry $(A, \circ)$ do algebry $(X, \circ)$, kde $X = \{x, y\}$, $x \circ y = x \circ x = y$ a $y \circ y = y \circ x = x$.

Naše úvaha bude stejná jako v předchozí úloze. Předpokládejme, že máme nějaký homomorfismus $f : A \to X$. Potom obraz $f(A)$ musí být podalgebrou algebry $(A, \circ)$. Okamžitě vidíme, že $x \circ x \neq x$ a $y \circ y \neq y$, tedy jedinou podalgebrou algebry $(X, \circ)$ je X a $f(A) = X$. Zjistili jsme, že jedinou faktorovou algebrou algebry $(A, \circ)$, která je dvouprvková je faktor A podle kongruence $\cong$ určené rozkladem $\{a, c\}$ a $\{b\}$. Nyní stačí srovnat tabulky binární operace nutně izomorfních algeber $(A/\cong, \circ)$ a $(X, \circ)$:

$\odot$	$\{\mathbf{a}, \mathbf{c}\}$	$\{\mathbf{b}\}$
$\{\mathbf{a}, \mathbf{c}\}$	$\{a, c\}$	$\{b\}$
$\{\mathbf{b}\}$	$\{b\}$	$\{a, c\}$

a

$\odot$	$\mathbf{x}$	$\mathbf{y}$
$\mathbf{x}$	y	y
$\mathbf{y}$	x	x

,

z nichž snadno nahlédneme, že algebry nejsou izomorfní. Podrobněji, kdyby $f(a) = f(c) = x$, pak by $y = f(a) \circ f(a) = f(a \circ a) = f(c) = x$, a kdyby $f(b) = x$, pak by $f(a) = f(c) = y$ a $x = f(b) = f(b \circ a) = f(b) \circ f(a) = x \circ y = y$.

Zjistili jsme, že žádný homomorfismus algebry $(A, \circ)$ do algebry $(X, \circ)$ neexistuje. □

3.6. Najděte všechny podalgebry a kongruence algebry $(B, \odot)$.

Postupujeme stejně jako v předchzích úlohách.

Celá nosná množina B je zřejmě podalgebrou $(B, \odot)$.

Algebra $(B, \odot)$ zjevně neobsahuje žádný idempotent (tj. prvek s vlastností $x \odot x = x$), tedy žádná jednoprvková podalgebra neexistuje. Snadno nahlédneme, že každá množina uzavřená na operaci obsahující dva prvky z $\{1, 2, 3, 4\}$ musí obsahovat další prvek, tedy $(B, \odot)$ neobsahuje ani žádnou dvouprvkovou podalgebru. Podobně každá trojice prvků z B už generuje celé B, tedy B neobsahuje žádnou tříprvkovou podalgebru.

Zjistili jsme, že $(B, \odot)$ obsahuje jen triviální podalgebru B.

Zřejmě id a $B \times B$ tvoří kongruenci na $(B, \odot)$. Uvažujeme-li nejmenší kongruenci $\sim$ obsahující dvojici $(1, 2)$ pak $1 = 1 \odot 2 \sim 2 \odot 2 = 4$ a $3 = 1 \odot 4 \sim 2 \odot 4 = 1$, proto 1 2 3 4 a tedy $\langle (1, 2) \rangle = \sim = B \times B$.

Nejmenší kongruence obsahující dvojici $(1, 4)$ zřejmě nutně obsahuje i dvojici $(1 \odot 1, 4 \odot 1) = (2, 3)$. Na faktoru B podle ekvivalence dané rozkladem $\{1, 4\}$ a $\{2, 3\}$ už ovšem můžeme dobře definovat faktorovou operaci, jak je vidět například z tabulky operace s permutovanými řádky a sloupci (každý z bloků obsahuje jen prvky jedné rozkladové třídy):

$\odot$	**1**	**4**	**2**	**3**
1	2	3	1	1
4	3	2	4	4
2	1	1	4	1
3	4	1	1	4

Obdobně nahlédneme, že nejmenší kongruence obsahující dvojici $(2, 3)$ je táž jako předchozí. Konečně vezmeme-li kongruenci s trojicí kongruentních prvků, pak díky předchzím úvahám dostáváme maximální kongruenci $B \times B$.

Tedy na algebře $(B, \odot)$ máme právě tři kongruence: dvě triviální (id, $B \times B$) a poslední $id \cup \{(1, 4),\ (4, 1),\ (2, 3), (3, 2)\}$.

15.11.

3.7. Popište všechny faktory algebry $(B, \odot)$.

V předchozí úloze jsme našli právě tři kongruence, tedy mánme 3 ekvivalence podle nichž můžeme faktorizovat.

Nejprve uvážíme triviální případy. Vidíme, že $(B, \odot) \cong (B/\mathrm{id}, \odot)$, kde uvažujeme izomorfismus $x \to \{x\}$, a dále $(\{*\}, \odot) \cong (B/B \times B, \odot)$, kde $* \cdot * = *$.

Nyní uvážíme kongruenci $\sim$, která odpovídá rozkladu $\{\{1, 4\}, \{2, 3\}\}$ (tj. $B/\sim = \{\{1, 4\}, \{2, 3\}\}$) a vytvoříme tabulku faktorové operace na prvcích $X = \{\{1, 4\}$ a

$Y = \{2, 3\} \in B/\sim$ pomocí definitorického vztahu $[a]_\sim \odot [b]_\sim = [a \odot b]_\sim$:

$\odot$	$\mathbf{X}$	$\mathbf{Y}$
$\mathbf{X}$	Y	X
$\mathbf{Y}$	X	X

□

3.8. Spočítejte všechny ekvivalence na množině B.

Potřebujeme uvážit kolik existuje disjunktních rozkladů čtyřprvkové množiny. Provedeme diskuzi podle počtu množin v rozkladu Nejprve poznamenejme, že existje právě jeden jednočlenný (celé B) a právě jeden čtyřčlenný ($\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$,) rozklad. Dvoučlenné rozklady sestávají buď ze dvou dvouprvkových množin (a ty najdeme právě 3) nebo z jedné jednoprvkové množiny a jedné tříprvkové (vybírámeli jednoprvkovou, vidíme, že takové rozklady jsou k dispozici 4). Dvoučlenných rozkladů tedy existuje 7. Konečně tříčlené rozklady jsou tvořeny jednou jednoprvkovou a dvěmi dvouprvkovými množinami, jsou tedy jednoznačně určeny dvouprvkovou podmnožinu, jichž existuje 6. Spočítali jsme, že ekvivalencí na na množině B je právě 1+1+7+6=15. □

3.9. Popište všechny faktory algebry $(B, \odot, 2)$.

Provedeme-li stejnou úvahu jako v 3.2, tedy, že podmínka slučitelnosti s nulární operací platí pro každou ekvivalenci, pak vidíme, že faktorové algebry $(B, \odot, 2)$ jsou stejně jako u algebry $(B, \odot)$ právě 3, dva triviální (tedy jeden izomorfní $(B, \odot, 2)$ a druhý izomorfní jednoprvkové algebře $(\{*\}, \odot, *)$) a jeden daný kongruencí $\sim$ s rozkladem $B/\sim = \{\{1, 4\}, \{2, 3\}\}$, tedy $(B/\sim, \odot, [2]_\sim)$. □

3.10. Mějme pro každé celé číslo $z \in \mathbf{Z}$ jednu nulární operaci, která vybírá v $\mathbf{Z}$ právě prvek z a uvažujme algberu $(\mathbf{Z}, z; z \in \mathbf{Z})$. Popište všechny její podalgebry a všechny její kongruence.

V minulém příkladu jsme nahlédli, že každá ekvivalence je slučitelná s každou nulární operací, proto je každá ekvivalence na $\mathbf{Z}$ kongruencí na $(\mathbf{Z}, z; z \in \mathbf{Z})$, poznamenejme, že rozkladů a tedy i ekvivalencí na spočetné množině na $\mathbf{Z}$ je nespočetně mnoho.

Nyní si uvědomme, že každá podalgebra $(\mathbf{Z}, z; z \in \mathbf{Z})$ musí obsahovat všechny nulární operace, tedy všechna celá čísla. To znamená, že $(\mathbf{Z}, z; z \in \mathbf{Z})$ obsahuje pouze podalgebru $\mathbf{Z}$. □

3.11. Popište všechny kongruence algebry $(\mathbf{Z}, +)$.

Nejprve si rozmyslíme, že „kongruence modulo přirozené číslo n" tvoří kongruence na algebře $(\mathbf{Z}, +)$. Připomeňme, že se jedná o relaci definovanou předpisem $a \equiv b \pmod{n}$, jestliže $n/a - b$. Snadno nahlédneme, že jde o reflexivní, tranzitivní a symetrickou relaci, tedy o ekvivalenci. Jakmile $a_1 \equiv b_1 \pmod{n}$ a $a_2 \equiv b_2 \pmod{n}$, pak $n/a_1 - b_1$ a $n/a_2 - b_2$, proto $n/(a_1 + a_2) - (b_1 + b_2)$, tedy $(a_1 + a_2) \equiv (b_1 + b_2) \pmod{n}$.

Nyní ukážeme, že jiné kongruemce než kongruence modulo přirozené číslo n a identita na algebře $(\mathbf{Z}, +)$ neexistují. Zvolme tedy neidentickou kongruenci $\sim$.

Potom určitě existují celá čísla $a < b$, pro něž $a \sim b$, Jelikož $-a \sim -a$, dostáváme z definice kongruence nan algebře vztah $0 = a + (-a) \sim b + (-a) = b - a > 0$. To znamená, že exsituje kladné celé číslo kongruentní s nulou a můžeme zvolit nejmenší kladné n, pro které $n \sim 0$. Dokážeme, že $\sim$ je právě kongruence modulo přirozené číslo n.

Předpokládejme, že $c \sim d$ a $d > c$. Potom stejnou úvahou jako výše dostáváme, že $d - c \sim 0$. Vydělíme-li číslo $d - c$ se zbytkem číslem n dostaneme $q, r \in \mathbf{Z}$, kde $0 \leq r < n$, pro která $d - c = qn + r$, tedy $r = d - c - qn$. Víme, že $d - c \sim 0$ a opakovanou úvahou zjsitíme, že $-qn \sim 0$, proto $r = d - c - qn \sim 0$. Z minimality volby n plyne, že $r = 0$, tedy $n/d - c$.

Jakmile $n/d - c$, dostaneme $d - c \sim 0$ zcela přímočarou úvahou. □

22.11.

3.12. Popište všechny kongruence algebry $(\mathbf{R}, +, \cdot)$, kde $\mathbf{R}$ je množina všech reálných čísel.

Víme, že id je vždy kongruence. Uvažujme tedy kongruenci $\sim \neq \mathrm{id}$, to znamená, že existují různé prvky $a, b \in \mathbf{R}$, pro které $a \sim b$. Protože $-a \sim -a$, dostáváme díky vlastnosti kongruence pro operaci sčítaní, že $0 = a + (-a) \sim b + (-a) = b - a$, kde $b - a \neq 0$. Vezmem-li dále libovolné $r \in \mathbf{R}$, potom stejnou úvahou pro operaci násobení ze vztahu $\frac{r}{b-a} \sim \frac{r}{b-a}$ plyne, že $0 = 0 \cdot \frac{r}{b-a} \sim b - a \cdot \frac{r}{b-a} = r$. Zjistili jsme, že $\sim = \mathbf{R} \times \mathbf{R}$, tedy na algebře $(\mathbf{R}, +, \cdot)$ máme jen dvě triviální kongruence.

3.13. Rozhodněte, zda jsou izomorfní algebry $(\mathbf{N}, +)$ a $(\mathbf{N}, \cdot)$.

Předpokládejme, že mezi danými algebrami izomorfismus existuje a označme ho φ. Všimněme si, že v algebře $(\mathbf{N}, \cdot)$ leží prvek 1 splňující podmínku $1 \cdot 1 = 1$, tedy musí existovat nějaký jeho vzor $n \in \mathbf{N}$, tj. $\varphi(n) = 1$. Protože je φ homomorfismus, platí, že

$$\varphi(n) = 1 = 1 \cdot 1 = \varphi(n) \cdot \varphi(n) = \varphi(n + n),$$

tudíž $n + n = n$. To ovšem pro žádné kladné celé číslo neplatí, proto izomorfismus mezi algebrami $(\mathbf{N}, +)$ a $(\mathbf{N}, \cdot)$ neexistuje. □

3.14. Rozhodněte, zda jsou izomorfní algebry $(\mathbf{N} \cup \{0\}, +)$ a $(\mathbf{N}, \cdot)$.

Opět předpokládejme, že mezi danými algebrami izomorfismus existuje a označme ho φ. Určitě musí existovat nějaký prvek $n \in \mathbf{N}$, pro který $\varphi(1) = n$, každý prvek nenulový prvek z algebry $(\mathbf{N} \cup \{0\}, +)$ dostaneme jako součet 1, tedy $\langle 1 \rangle = \mathbf{N}$ a $\langle 0, 1 \rangle_{(\mathbf{N} \cup \{0\}} = \mathbf{N} \cup \{0\}$. To ovšem znamená, že bychom každý prvek různý od 1 museli dostat jako součin kopií prvku $\varphi(1) = n$, tj. $\langle 1, n \rangle_{(\mathbf{N}, \cdot)} = \mathbf{N}$. Stačí abychom vzali prvočíslo p, které se nenalézá v prvočíselném rozkladu čísla p, abychom nahlédli, že $p \notin \langle 1, n \rangle_{(\mathbf{N}, \cdot)}$, což je spor. Ani tentokrát algebry izomorfní nejsou.

Poznamenejme, že stačilo najít tvrzení, které v jedné algebře platilo a v druhé neplatilo, konkrétně algebra $(\mathbf{N} \cup \{0\}, +)$ je konečně generovaná, zatímco algebra $(\mathbf{N}, \cdot)$ konečně generovaná není, tedy se nomůže jednat o izomorfní algebry. □

3.15. Dokažte, že pro každé přirozené n je $(\mathbf{Z}[\sqrt{n}], +, \cdot)$, kde $\mathbf{Z}[\sqrt{n}] = \{a+b\sqrt{n} |\ a, b \in \mathbf{Z}\}$, podalgebrou algebry $(\mathbf{R}, +, \cdot)$.

Stačí pro libovolné $a_1, a_2, b_1, b_2 \in \mathbf{Z}$ nahlédnout, že

$$(a_1 + b_1\sqrt{n}) + (a_2 + b_2\sqrt{n}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{n} \in \mathbf{Z}[\sqrt{n}]$$

a dále, že

$$(a_1 + b_1\sqrt{n}) \cdot (a_2 + b_2\sqrt{n}) = (a_1a_2 + b_1b_2n) + (a_1b_2 + a_2b_1)\sqrt{n} \in \mathbf{Z}[\sqrt{n}].$$

□

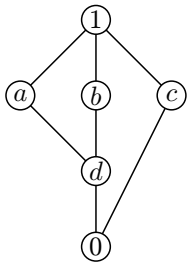
3.16. Rozhodněte, zda jsou izomorfní algebry $(\mathbf{Z}, +, \cdot)$ a $(\mathbf{Z}[\sqrt{2}], +, \cdot)$.

Tentokrát se omezíme na hledání tvrzení, které platí v algebře $(\mathbf{Z}[\sqrt{2}], +, \cdot)$ a neplatí v algebře $(\mathbf{Z}, +, \cdot)$. Všimnene si, že v první algebře existuje prvek α (konkrétně $\alpha = \sqrt{2}$) a prvek β (konkrétně $\beta = 1$) tak, že pro všechny prvky algebry γ je $\beta \cdot \gamma = \gamma$ a $\alpha \cdot \alpha = \beta + \beta$ (tedy $1 \cdot \gamma = \gamma$ a $\sqrt{2} \cdot \sqrt{2} = 1 + 1$). Takové tvrzení v algebře $(\mathbf{Z}, +, \cdot)$ ovšem neplatí, najdeme tam sice neutrální prvek vzhledem k násobení, jímž je opět 1, ale $2 = 1 + 1$ zde odmocnit neumíme. □

4. Svazy

Připomeňme, že *Hasseovým diagramem* uspořádané množiny $(S, \leq)$ rozumíme orientovaný graf, jehož vrcholy tvoří prvky množiny S a a je s b spojen takovou hranou, že b se nachází výše než a, právě když $a <\cdot\, b$. Přitom $a <\cdot\, b$, jestliže $a \leq b$, $a \neq b$ a $a \leq c \leq b \Rightarrow c = a$ nebo $c = b$.

Uvažujme v následujícím na nosné množině $S = \{0, 1, a, b, c, d\}$ uspořádání Hasseovým diagramem $(S, \leq)$, tj.



4.1. Ověřte, že je $(S, \leq)$ dobře definovaný svaz.

Zřejmě diagram dobře popisuje uspořádání na množině S (tj. $x \leq y$ právě když z vrcholu x stoupá cesta do vrcholu y). Zbývá tedy vyšetřit, že pro každou dvojici prvků existuje supremum a infimum. Jestliže $x \leq y$, pak snadno nahlédneme, že $sup_{\leq}(\{x, y\}) = y$ a $inf_{\leq}(\{x, y\}) = x$. Pro nesrovnatelné dvojice prvků je třeba provést diskuzi. □

4.2. Spočítejte ve svazu z předchozího příkladu hodnoty $a \wedge b$, $a \vee b$, $a \wedge c$, $a \vee c$, $b \wedge d$, $b \vee d$,

Podle definice je spojení nejmenší horní odhad (tedy supremum) příslušné dvojice prvků. Konkrétně $a \vee b = 1$, $a \vee c = 1$, $b \vee d = b$.

Průsek je naopak největším dolním odhadem (tj. infimem), proto $a \wedge b = d$, $a \wedge c = 0$, $b \wedge d = d$. □

4.3. Najděte všechny podalgebry (tj. podsvazy) svazu $(S, \leq)$.

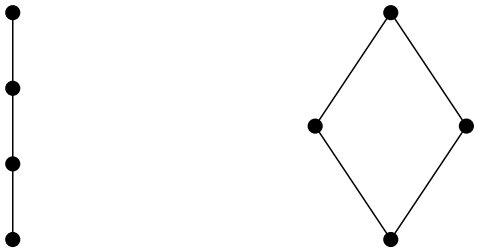
Budene obvyklým způsobem vyšetřovat podmnožiny svazu. Uvědomme si, že každý nenulový podsvaz je zároveň svazem, tedy můžeme namalovat jeho Hasseův diagram.

Předně zřejmě je prázdná množina $\emptyset$ podsvazem. Dále všech prvky svazu jsou vzhledem k oběma binárním operacím idempotentní, proto jsou všechny jednoprvkové podmnožiny daného svazu podsvazy.

Podsvazem je dále každá dvojice prvků spojených cestou vedoucí ze shora dolů. Jde o dvojice $\{1, a\}$, $\{1, d\}$, $\{1, 0\}$, $\{1, b\}$, $\{1, c\}$, $\{a, d\}$, $\{a, 0\}$, $\{b, d\}$, $\{b, 0\}$, $\{c, 0\}$ a $\{d, 0\}$. Žádný další dvouprvkový podsvaz neexistuje. Hasseův diagram příslušného svazu má tvar:

Podobně, jedinými podsvazy o třech prvcích jsou právě tři prvky ležící na cestě, která vede ze zhora dolů. Konkrétně dostáváme $\{1, a, d\}$, $\{1, a, 0\}$, $\{1, b, d\}$, $\{1, b, 0\}$, $\{1, d, 0\}$, $\{a, d, 0\}$, $\{b, d, 0\}$, $\{1, c, 0\}$. Hasseův diagram příslušné třídy svazů má tvar:

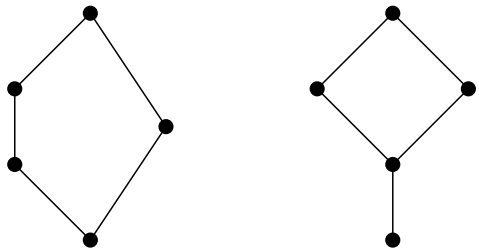
Podsvazy o čtřech prvcích mohou být dvojího typu, který můžeme vyjádřit Hasseovými diagramy:



Tedy čtyři vrcholy ležící na cestě vedoucí shora dolů tvoří podsvazy $\{1, a, d, 0\}$ a $\{1, b, d, 0\}$ a čtverec je Hasseovým diagramem podsvazů $\{1, a, b, d\}$, $\{1, a, 0, c\}$, $\{1, b, 0, c\}$ a $\{1, d, 0, c\}$.

Podsvazy o pěti prvcích mohou být v daném svazu opět dvojího typu, který popisují Hasseovy diagramy (například cestu shora dolů obsahující pět vrcholů už v Hasseově diagramu našeho svazu nenajdeme). Snadno zjistíme, že pětiprvkové

podsvazy tvoří množiny $\{1, a, b, d, 0\}$, $\{1, a, d, 0, c\}$ a $\{1, b, d, 0, c\}$ s následujícími Hasseovými diagramy:



Konečně celá nosná množina svazu S je samozřejmě podsvazem. □

Další úlohy

(1) Uvažujme množinu $\mathbf{Z}_n$ s unární operací $^+$ definovanou předpisem $a^+ = (a+1) mod\ n$. Popište všechny podalgebry a všechny kongruence na $(\mathbf{Z}_n, ^+)$.
(2) Označme $\sim_A$ jedinou netriviální kongruenci algebry $(A, \circ)$ a $\sim_B$ jedinou netriviální kongruenci algebry $B(\odot)$. Rozhodněte, zda jsou faktorové algebry $(A/\sim_A, \circ)$ a $(B/\sim_B, \odot)$ izomorfní.
(3) Najděte všechny homomorfismy algebry $(X, \circ)$ do algebry $(A, \circ)$ z příkladu 3.5.
(4) Najděte pro každé přirozené n nějakou algebru, pro níž existuje právě n různých faktorových algeber.
(5) Rozhodněte, zda jsou izomorfní algebry $(\mathbf{Z}[\sqrt{3}], +, \cdot)$ a $(\mathbf{Z}[\sqrt{5}], +, \cdot)$.
(6) Nakreslete Hasseovy diagramy všech svazů o pěti (šesti, sedmi) prvcích.
(7) Najděte všechny čtyřprvkové podsvazy svaz s Hasseovým diagramem