5. Kvaziuspořádání a dělitelnost v komutativních monoidech

1. Dokažte, že všechna kvaziuspořádání množiny A tvoří uzávěrový systém nad A^2.

2. Dokažte, že kvaziuspořádání $\leq$ množiny A je noetherovské právě když platí, že každá neprázdná množina $B \subseteq A$ má alespoň jeden minimální prvek.

3. Buď $\leq$ kvaziuspořádání nějaké abecedy $\mathbb{A}$. Ať $\sigma : \mathbb{A}^* \to \mathbb{N}_0$ udává délku slova $w \in \mathbb{A}^*$. Místo $\sigma(w)$ pišme, jak je obvyklé, $|w|$. Na $\mathbb{A}^*$ definujme relaci $\preccurlyeq$ tak, že $s \preccurlyeq t$, jestliže:

(i) $s = t$ nebo
(ii) $|s| < |t|$ nebo
(iii) $|s| = |t|$, $s \neq t$ a je-li $s = a_1 \dots a_n$, $t = b_1 \dots b_n$, kde $n = |s|$ a $a_i, b_i \in \mathbb{A}$ pro $1 \leq i \leq n$, a $1 \leq j \leq n$ je nejmenší takové, že $a_j \neq b_j$, tak $a_j \leq b_j$.

Dokažte, že $\preccurlyeq$ je kvaziuspořádání $\mathbb{A}^*$, přičemž pro $a, b \in \mathbb{A}$ je $a \preccurlyeq b$ právě když $a \leq b$.
Dokažte, že je-li $\leq$ uspořádání, je i $\preccurlyeq$ uspořádání.
Dokažte, že je-li $\leq$ lineární uspořádání, je i $\preccurlyeq$ lineární uspořádání.
Dokažte, že je-li $\leq$ noetherovské, je i $\preccurlyeq$ noetherovské.

Relaci $\preccurlyeq$ se říká lexikografické (kvazi)uspořádání. Pojem lexikografického uspořádání ovšem není zcela jednoznačný, často se nejedná o zde definované uspořádání, ale o uspořádání skutečně odpovídající abecednímu řazení ve slovníku. Podejte přesnou definici lexikografického uspořádání v tomto smyslu.

4. Zkoumejte, jak vypadá ekvivalence $||$ v různých podmonoidech S multiplikativního monoidu reálných čísel $\mathbb{R}(\cdot, 1)$. (Vždy nejprve ověřte, že S je podmonoid.)

(i) Ať S je postupně $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{N}$, $\mathbb{Z}$,
(ii) Buď Π nějaká množina prvočísel a označme Σ podalgebru $\mathbb{N}(\cdot, 1)$ generovanou Π. Je zřejmé, že Σ je množina všech přirozených čísel, jejichž všechny prvočíselné dělitele leží v Π. Ať $S = \{\frac{a}{n}; a \in \mathbf{Z} \text{ a } n \in \Sigma\}$.
(iii) Buď n přirozené číslo, jež není dělitelné p^2 pro žádné prvočíslo p. Ať $S = \mathbb{Z} \cup \{a\sqrt{n};\ a \in \mathbb{Z}\}$.

5. Buď $S = S(\cdot, \mathbf{1})$ komutativní monoid. Ukažte, že

(i) množina invertibilních prvků S je podmonoid S,
(ii) $||$ je kongruence S,
(iii) $S/||$ je monoid, ve kterém je relace dělitelnosti uspořádáním.

6. Ujistěte se, že uspořádání $\mathbb{N}$ dělitelností indukuje na $\mathbb{N}$ svazové operace NSD a NSN. Pro $n \in \mathbb{N}$ ať $D(n) = \{d \in \mathbb{N};\ d \text{ dělí } n\}$. Ukažte, že $D(n)$ je podsvaz svazu $\mathbb{N}(NSD, NSN)$. Pro která n je uspořádání svazu $D(n)$ lineární? Pro která $n, m \in \mathbb{N}$ jsou svazy $D(n)$ a $D(m)$ izomorfní? Pro která n má svaz $D(n)$ tuto vlastnost: 'každý prvek je supremem nějaké množiny atomů'?

7. Relaci dělitelnosti jsme definovali tak, že $a|b$ právě když existuje c, že $b = ac$. Pišme $a|^{op}b$ právě když existuje c, že $b = ca$. Ukažte, že $|^{op}$ je rovněž kvaziuspořádání. Najděte co nejmenší monoid, aby se obě relace vzájemně lišily.

8. Zkoumejte relace $|$ a $|^{op}$ definované v předchozím cvičení pro monoid T_Ω (kde Ω je neprázdná množina). Vyjádřete relace $f|g$ a $g|^{op}f$ v T_Ω jako podmínky týkající se vztahů $\ker f$, $\ker g$, $\operatorname{Im} f$ a $\operatorname{Im} g$. Ukažte, že je-li množina Ω nekonečná, nejsou kvaziuspořádání $|$ a $|^{op}$ noetherovská.

9. O prvku z monoidu $S(\cdot, \mathbf{1})$ řekneme, že je nulou, jestliže $az = za = z$ pro každé $a \in S$. Ukažte, že:

(i) Monoid S má nanejvýš jednu nulu.
(ii) Je-li z nula monoidu S, tak $a|z$ pro každé $a \in S$, ale $z|a$ jedině pro $a = z$.
(iii) Má-li monoid S alespoň dva prvky a obsahuje-li nulu, není to monoid s krácením.
(iv) Je-li $S(\cdot, \mathbf{1})$ monoid a $z \notin S$, tak na množině $S' = S \cup \{z\}$ definujeme operaci $\cdot$ tak, aby $a \cdot z = z \cdot a = z = z \cdot z$ pro každé $a \in S$, a aby S byla podalgebra $S'(\cdot, \mathbf{1})$. Ukažte, že $S'(\cdot, \mathbf{1})$ je také monoid.

10. Jestliže z každého z monoidů S zkoumaných ve cvičení 4 vypustíme nulu, dostaneme opět monoid – označme ho například S'. S' je komutativní monoid s krácením. Ukažte, že relace $|$ je ve všech zkoumaných případech noetherovská. Popište všechny ireducibilní prvky monoidu S'. Zjistěte, kdy jsou ireducibilní prvky monoidu S' prvočiniteli.

Řešení

4. (i) Pro $\mathbb{R}$ a $\mathbb{Q}$ je $a||b$ právě když $a = 0 = b$ nebo $a \neq 0 \neq b$. Pro $\mathbb{N}$ je $||$ rovno $\mathrm{id}_\mathbb{N}$. Pro $\mathbb{Z}$ je $a||b$ právě když $a = \pm b$. (ii) Buď $\alpha = \frac{a}{n}$ a $\beta = \frac{b}{m}$ prvky S a ať a', b' jsou největší taková, že $a'|a$, $b'|b$ a a' ani b' nemají prvočíselného dělitele z Π. Pak $\frac{a}{n}||\frac{b}{m}$ právě když $a' = \pm b'$. (iii) Pro $\alpha, \beta \in S$ je $\alpha||\beta$ právě když $\alpha = \pm\beta$.

6. $D(n)$ je lineární, je-li n mocninou prvočísla. Jsou-li $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $1 \leq \alpha_1 \leq \dots \leq \alpha_k$ a $m = q_1^{\beta_1} \dots q_r^{\beta_r}$, $1 \leq \beta_1 \leq \dots \leq \beta_r$ prvočíselné rozklady n a m, tak $D(n) \simeq D(m)$ právě když $r = k$ a $\alpha_1 = \beta_1, \dots, \alpha_k = \beta_k$. Každý prvek mimo 1 je v $D(n)$ spojením atomů právě když p^2 nedělí n pro žádné prvočíslo p. (Poznámka: Vyšetřování $D(n) \simeq D(m)$ provádíme tak, že dokážeme, že $D(n)$ a $D(m)$ musí mít stejně atomů, a že nad odpovídajícími atomy musí ležet stejný počet prvků, které mají s každým jiným atomem průsek 1.)

7. Uvažme binární operaci na $S = \{1, a, b\}$ takovou, že $e = 1 \cdot e = e \cdot 1$ pro každé $s \in S$ a $a \cdot a = a \cdot b = a$, $b \cdot a = b \cdot b = b$. Pak $S(\cdot, 1)$ je monoid, $a|^{op}b$, ale $a|b$ neplatí.

8. $f|g$ právě když $\operatorname{Im} g \subseteq \operatorname{Im} f$ a $f|^{op}g$ právě když $\ker f \subseteq \ker g$. Je-li Ω nekonečná, tak jistě lze sestrojit posloupnosti $f_0, f_1, \dots$ a $g_0, g_1, \dots$ transformací množiny Ω tak, aby $\operatorname{Im} f_{i+1} \supsetneq \operatorname{Im} f_i$ a $\ker g_{i+1} \subsetneq \ker g_i$.

10. (ii) Ireducibilní prvky jsou (až na $||$ ekvivalenci) všechna prvočísla mimo Π a všechny ireducibilní prvky jsou prvočinitelé. (iii) Je-li $n = p$ prvočíslo, tak prvočinitele se shodují s ireducibilními prvky a jsou to: $\sqrt{p}$ a všechna prvočísla mimo p. Ať n není prvočíslo. Pak ireducibilními prvky jsou jednak všechna prvočísla, jednak číslo $\sqrt{n}$. Prvočiniteli jsou ovšem toliko prvočísla, jež n nedělí.