1. Algebry, homomorfismy, kongruence

Definice. Pro každé celé $n \geq 0$ nazveme *n-ární operací na množině A* každé zobrazení $A^n \to A$ (číslo n budeme nazývat *aritou* nebo *četností* operace). Nechť $(\alpha_i|\ i \in I)$ je systém operací na množině A. Pak dvojici $A(\alpha_i|\ i \in I)$ nazveme *algebrou*.

Příklad. Algebry tvoří například $\mathbf{Z}(+)$, $\mathbf{Z}(+,-)$, $\mathbf{Z}(+,\cdot,0,1)$. Je-li $\mathbf{T}$ těleso, pak je algebrou $\mathbf{T}(+,\cdot)$ či $\mathbf{T}(+,-,\cdot,0,1)$, pro vektorový prostor V nad $\mathbf{T}$, je algebrou $V(+,\cdot t|t \in \mathbf{T})$.

Definice. Buď α n-ární operace na A. Řekneme, že podmnožina $B \subseteq A$ je *uzavřená na operaci α*, pokud $\alpha(a_1,\ldots,a_n) \in B$ pro všechna $a_1,\ldots,a_n \in B$. Řekneme, že $B \subseteq A$ je *podalgebra* algebry $A(\alpha_i|\ i \in I)$, pokud je B uzavřená na všechny operace α_i, $i \in I$.

Označíme-li $\beta_i = \alpha_i|_{B^n}$ omezení n-ární operace α_i na B^n, potom pro podalgebru B leží všechny hodnoty zobrazení β_i opět v B. Zobrazení β_i tedy můžeme chápat jako operace na množině B a tak dostáváme strukturu algebry $B(\beta_i|\ i \in I)$ na každé podalgebře B.

Příklad. (1) Je-li $A(\alpha_i|\ i \in I)$ algebra, pak A zřejmě tvoří její podalgebru. Pokud navíc žádná z operací α_i není nulární, potom $\emptyset$ je podalgebrou algebry $A(\alpha_i|\ i \in I)$.

(2) Uvažujeme-li algebru $\mathbf{Z}(+,-)$, pak pro každé celé n tvoří množina všech násobků $n\mathbf{Z} = \{nz|\ z \in \mathbf{Z}\}$ podalgebru.

(3) Každý podprostor vektorového prostoru V nad tělesem $\mathbf{T}$, je podalgebrou algebry $V(+,\cdot t, t \in \mathbf{T})$.

Poznámka 1.1. *Nechť $A(\alpha_i|\ i \in I)$ je algebra a A_j je podalgebra A pro každé $j \in J$. Pak $\bigcap_{j\in J} A_j$ je rovněž podalgebra A.*

Důkaz. Viz [D, 2.1, 2.8]. □

Definice. Nechť symbol α označuje n-ární operaci na množině A. Řekneme, že zobrazení $f : A \to B$ je *slučitelné s α*, pokud $f(\alpha(a_1,\ldots,a_n)) = \alpha(f(a_1),\ldots,f(a_n))$.

Řekneme, že algebry $A(\alpha_i|\ i \in I)$ a $B(\alpha_i|\ i \in I)$ jsou *stejného typu*, pokud α_i označuje na množině A i na množině B dvě operace stejné arity. Zobrazení $f : A \to B$ mezi dvěma algebrami stejného typu budeme říkat *homomorfismus*, pokud je slučitelné se všemi operacemi α_i, $i \in I$.

Příklad. (1) Zobrazení $\pi : \mathbf{Z} \to \mathbf{Z}_n$ definované předpisem $\pi(z) = (z) mod\ n$ je homomorfismus algebry $\mathbf{Z}(+,\cdot)$ do $\mathbf{Z}_n(+,\cdot)$.

(2) Nechť U a V jsou dva vektorové prostory nad tělesem T. Potom každý homomorfismus vektorových prostorů je homomorfismem algeber $U(+,\cdot t|t \in T)$ a $V(+,\cdot t|t \in T)$.

(3) Označme $M_n(T)$ množinu všech čtvercových matic nad tělesem T a $\cdot$ budiž symbolem násobení matic. Potom zobrazení, které každé matici přiřadí její determinant, je homomorfismem algebry $M_n(T)(\cdot)$ do $T(\cdot)$.

Poznámka 1.2. *Buď $A(\alpha_i|\ i \in I)$, $B(\alpha_i|\ i \in I)$ a $C(\alpha_i|\ i \in I)$ algebry stejného typu. Jsou-li zobrazení $f : A \to B$ a $g : B \to C$ homomorfismy, pak i gf je homomorfismus. Je-li navíc f bijekce, je f^{-1} také homomorfismus.*

Důkaz. Viz [D, 2.2]. □

V případě, že nemůže dojít k omylu nebo jednotlivé operace na algebře nepotřebujeme uvažovat, budeme v následujícím označiovat algebru jen její nosnou množinou.

Poznámka 1.3. *Buď A a B dvě algebry stejného typu a buď $f : A \to B$ homomorfismus. Je-li C podalgebra algebry A a D podalgebra algebry B, pak $f(C)$ je podalgebrou B a $f^{-1}(D)$ je podalgebrou A.*

Důkaz. Viz [D, 2.3]. □

Definice. Bijektivní homomorfismus budeme nazývat *izomorfismus*. Pokud mezi dvěma algebrami A a B existuje izomorfismus, říkáme, že A a B jsou *izomorfní* (píšeme $A \cong B$).

Připomeňme, že *relací na množině A* rozumíme libovolnou podmnožinu $A \times A$. Nechť ρ je relace na A, označme:

- $\rho^{-1} = \{(b, a) |\ (a, b) \in \rho\}$ (opačná relace),
- $\rho^{+} = \{(a, b) |\ \exists a = a_0, a_1, \ldots, a_{n-1}, a_n = b \in A; (a_i, a_{i+1}) \in \rho\}$ (tranzitivní obal),
- $id = \{(a, a) |\ a \in A\}$ (identita).

Řekneme, že relace ρ je *symetrická*, pokud $\rho^{-1} \subseteq \rho$, *tranzitívní*, pokud $\rho^{+} \subseteq \rho$, a *reflexivní*, pokud $id \subseteq \rho$. *Ekvivalencí* budeme nazývat každou symetrickou, tranzitívní a reflexivní relaci.

Definice. Nechť ρ je ekvivalence na množině A. Definujme *faktor množiny* (často se říká také *kvocient*) A podle relace ρ jako množinu $A/\rho = \{[a]_\rho |\ a \in A\}$, kde $[a]_\rho = \{b \in A |\ (a, b) \in \rho\}$.

Všimněme si, že je-li ρ ekvivalence na A, pak $A/\rho = \{[a]_\rho |\ a \in A\}$ tvoří rozklad množiny A [D, 1.7]. Naopak máme-li $\{B_i |\ i \in I\}$ rozklad množiny A, pak relace ρ určená podmínkou: $(a, b) \in \rho \Leftrightarrow \exists i \in I : a, b \in B_i$ je ekvivalencí a $A/\rho = \{B_i |\ i \in I\}$.

Příklad. Na libovolné množině algeber stejného typu $\mathcal{M}$ je relace $\cong$ (tj. "být izomorfní") ekvivalencí (viz 1.2).

Definice. Je-li $f : A \to B$ zobrazení, rozumíme jeho *jádrem* $ker\ f$ relaci danou předpisem: $(a, b) \in ker\ f \Leftrightarrow f(a) = f(b)$. Mějme na A ekvivalenci ρ. *Přirozenou projekcí* nazveme zobrazení $\pi_\rho : A \to A/\rho$ dané předpisem $\pi_\rho(a) = [a]_\rho$.

Poznámka 1.4. *Nechť $f : A \to B$ je zobrazení a ρ ekvivalence na množině A. Pak platí:*

(1) *$ker\ f$ je ekvivalence,*
(2) *$ker\ f = id$, právě když je f prosté zobrazení,*
(3) *$ker\ \pi_\rho = \rho$,*
(4) *Zobrazení $g : A/\rho \to B$ splňující podmínku $g\pi_\rho = f$ existuje právě tehdy, když $\rho \subseteq ker\ f$.*

Důkaz. (1) $(a, a) \in ker\ f$, neboť $f(a) = f(a)$; pokud $(a, b) \in ker\ f$, pak $f(a) = f(b)$, tedy $(b, a) \in ker\ f$; je-li $f(a) = f(b) = f(c)$, potom zřejmě $(a, c) \in ker\ f$.
(2), (3) Plyne přímo z definice.
(4) Viz [D, 1.10]. □

Definice. Nechť $\rho \subseteq \sigma$ jsou dvě ekvivalence na A. Definujme relaci σ/ρ na A/ρ následovně: $([a]_\rho, [b]_\rho) \in \sigma/\rho \Leftrightarrow (a, b) \in \sigma$.

Poznámka 1.5. (1) *Nechť $\rho \subseteq \sigma$ jsou dvě ekvivalence na A. Pak σ/ρ je dobře definovaná ekvivalence na A/ρ.*

(2) *Nechť ρ je ekvivalence na množině A a η je ekvivalence na A/ρ. Potom existuje právě jedna ekvivalence σ na A, pro níž $\eta = \sigma/\rho$.*

Důkaz. (1) viz [D, 1.8] a (2) viz [D, 1.9]. □

Definice. Nechť ρ je relace a α je n-ární operace na množině A. Řekneme, že ρ je *slučitelná s α*, pokud pro každý systém prvků $a_1, \ldots, a_n, b_1 \ldots, b_n \in A$, pro které $a_i \rho b_i$, $i = 1, \ldots, n$, platí, že $\alpha(a_1, \ldots, a_n) \rho \alpha(b_1, \ldots, b_n)$.

Je-li $A(\alpha_i |\ i \in I)$ algebra a ρ ekvivalence na množině A, pak ρ nazveme *kongruencí*, pokud je ρ slučitelná se všemi operacemi α_i, $i \in I$.

Příklad. (1) id a $A \times A$ jsou kongruence na libovolné algebře A.

(2) Vezměme přirozené číslo $n \geq 2$ a označme $\sim_n$ relaci na množině celých čísel $\mathbf{Z}$ danou předpisem: $a \sim_n b \leftrightarrow n/(a - b)$. Potom je $\sim_n$ kongruence na algebře $\mathbf{Z}(+, -, \cdot)$.

(3) Každá ekvivalence je slučitelná s libovolnou nulární operací.

Poznámka 1.6. *Nechť A a B jsou dvě algebry stejného typu a $f : A \to B$ je homomorfismus. Pak ker f je kongruence na algebře A.*

Důkaz. Viz [D, 2.5]. □

Definice. Nechť ρ je ekvivalence a α je n-ární operace na množině A. Pokud je ρ slučitelná s α definujeme operaci α na A/ρ následovně: $\alpha([a_1]_\rho, \ldots, [a_n]_\rho) = [\alpha(a_1, \ldots, a_n)]_\rho$. Je-li ρ kongruence na algebře A, pak stejným způsobem definujeme na A/ρ strukturu algebry.

Věta 1.7. *Je-li ρ kongruence na algebře A, pak je definice algebry A/ρ korektní, jde o algebru stejného typu jako A a přirozená projekce $\pi_\rho : A \to A/\rho$ je homomorfismus.*

Důkaz. Viz [D, 2.6]. □

Poznámka 1.8. *Buď ρ kongruence na algebře A a σ ekvivalence na A obsahující ρ. Pak je σ kongruence na algebře A právě tehdy, když je σ/ρ kongruence na algebře A/ρ.*

Důkaz. Viz [D, 3.4]. □

Poznámka 1.9. (Věta o homomorfismu) *Buď $f : A \to B$ homomorfismus dvou algeber stejného typu a nechť ρ je kongruence na algebře A. Pak existuje homomorfismus $g : A/\rho \to B$ splňující podmínku $g\pi_\rho = f$ právě tehdy, když $\rho \subseteq$ ker f. Navíc, pokud g existuje, je g izomorfismus, právě když f je na a ker $f = \rho$.*

Důkaz. Viz [D, 3.7]. □

Věta 1.10 (1. věta o izomorfismu)**.** *Nechť $f : A \to B$ je homomorfismus dvou algeber stejného typu. Pak $f(A)$ je podalgebra B (tedy algebra stejného typu) a $A/$ker f je izomorfní $f(A)$.*

Důkaz. Viz [D, 3.9]. □

Příklad. Mějme homomorfismus $f_n : \mathbf{Z} \to \mathbf{Z}_n$ algebry $\mathbf{Z}(+,\cdot,-,0)$ do algebry $\mathbf{Z}_n(+,\cdot,-,0)$ s počítáním modulo n daný předpisem $f_n(k) = (k) mod\ n$. Pak podle 1. věty o izomorfismu je $\mathbf{Z}/ker\ f_n \cong \mathbf{Z}_n$, navíc je zjevně $(a-b) \in ker\ f_n$, právě když $n/(a-b)$.

Věta 1.11 (2. věta o izomorfismu)**.** *Nechť $\rho \subseteq \sigma$ jsou dvě kongruence na algebře A. Pak algebra A/σ je izomorfní algebře $(A/\rho)/(\sigma/\rho)$.*

Důkaz. Viz [D, 3.10]. □

2. Algebry s jednou binární operací

Definice. Algebru $G(*)$ s jednou binární operací nazýváme *grupoid. Neutrálním prvkem* grupoidu $G(*)$ (nebo operace $*$) rozumíme takový prvek $e \in G$, že $g * e = e * g = g$ pro všechna $g \in G$. Algebru $G(*, e)$ nazveme *monoidem*, pokud je operace $*$ asociativní a e je neutrální prvek operace $*$. *Podgrupoidem (podmonoidem)* nazveme každou podalgebru grupoidu (monoidu).

Poznámka 2.1. *Každý grupoid obsahuje nejvýše jeden neutrální prvek.*

Důkaz. Jsou-li e, f dva neutrální prvky, pak $e = e \cdot f = f$. □

Příklad. Je-li X aspoň dvouprvková množina a definujeme-li na X binární operaci $*$ předpisem $x * y = x$, je operace $*$ asociativní, ale X neobsahuje žádný neutrální prvek. Přitom dokonce každý prvek X splňuje první z rovností, kterou je neutrální prvek definován.

Příklad. (1) Nechť X je neprázdná množina písmen a $M(X)$ je množina všech slov, tj. všech konečných posloupností písmen. Zaveďme na této množině operaci skládání $\cdot: x_1 \dots x_n \cdot y_1 \dots y_m = x_1 \dots x_n y_1 \dots y_m$ a dále označme λ prázdné slovo. Potom $M(X)(\cdot, \lambda)$ tvoří (tzv. slovní) monoid.

(2) Buď X nějaká neprázdná množina a označme $T(X)$ množinu všech zobrazení množiny X do sebe. Potom $T(X)(\cdot, Id)$ tvoří (s operací skládání $\cdot$) (tzv. transformační) monoid.

(3) Čtvercové matice $M_n(T)$ nad tělesem T stupně n spolu s násobením a jednotkovou maticí $M_n(T)(\cdot, Id)$ tvoří monoid.

Poznámka 2.2. *Buď $S(\cdot, 1)$ monoid a $a, b, c \in S$. Pokud platí, že $a \cdot b = c \cdot a = 1$, potom $b = c$.*

Důkaz. $c = c \cdot 1 = c \cdot (a \cdot b) = (c \cdot a) \cdot b = 1 \cdot b$. □

Příklad. Uvažujme transformační monoid $T(\mathbf{N})$ na množině všech přirozených čísel a nechť $\alpha(k) = 2k$ a $\beta(k) = [\frac{k}{2}]$. Pak $\beta\alpha = Id$ a $\alpha\beta \neq Id$.

Definice. Nechť $S(\cdot, 1)$ je monoid. Řekneme, že prvek $s \in S$ je *invertibilní*, pokud existuje takový prvek $s^{-1} \in S$, že $s^{-1} \cdot s = s \cdot s^{-1} = 1$. Prvek s^{-1} nazveme *inverzním prvkem* k prvku s.

Poznámka 2.3. *Množina všech invertibilních prvků monidu $S(\cdot, 1)$ tvoří jeho podmonoid. Navíc, je-li s invertibilní prvek, pak i s^{-1} je invertibilní.*

Důkaz. Viz [D, 2.16]. □

Definice. Algebra $G(\cdot,^{-1},1)$ je *grupa*, pokud $G(\cdot,1)$ je monoid a $^{-1}$ je unární operace, která každému prvku přiřadí prvek k němu inverzní, je-li operace $\cdot$ komutativní, mluvíme o *komutativní (Abelově) grupě*. *Podgrupou* budeme rozumět každou podalgebru algebry $G(\cdot,^{-1},1)$. *Normální podgrupa* je každá podgrupa H grupy G splňující navíc podmínku $ghg^{-1} \in H$ pro každé $g \in G$ a $h \in H$.

Poznámka 2.4. *Nechť $S(\cdot,1)$ je monoid a S^* označuje jeho podmonoid všech invertibilních prvků. Označme $\cdot_{S^*}$ restrikci $\cdot|_{S^*\times S^*}$ operace $\cdot$ na množinu $S^* \times S^*$ a definujeme unární operaci $^{-1}$ tak, že a^{-1} je inverzní prvek pro libovolné $a \in S^*$. Pak $S^*(\cdot_{S^*},^{-1},1)$ je grupa.*

Příklad. (1) Grupa invertibilních prvků (podle Poznámky 1.11) slovního monoidu $M(X)(\cdot,\lambda)$ obsahuje pouze neutrální prvek e.

(2) Grupu invertibilních prvků transformačního monoidu $T(X)(\cdot,Id)$ tvoří právě všechny bijekce $S(X)$ na množině X (mluvíme o symetrické grupě nebo grupě permutací).

(3) Grupu invertibilních prvků monoidu čtvercových matic $M_n(T)(\cdot,Id)$ stupně n tvoří právě všechny regulární matice stupně n.

Poznámka 2.5. *Všechny podgrupy komutativní grupy jsou normální.*

Věta 2.6. *Nechť $G(\cdot,^{-1},1)$ je grupa a ρ relace na G. Pak ρ je kongruence na $G(\cdot,^{-1},1)$ právě tehdy, když $[1]_\rho$ je normální podgrupa G a $(g,h) \in \rho \longleftrightarrow g^{-1}h \in [1]_\rho$.*

Důkaz. Viz [D, 6.10]. □

3. Uzávěrové systémy na algebře

Definice. Nechť A je množina a $\mathcal{C} \subseteq \mathcal{P}(A)$ je nějaký systém podmnožin množiny A. Řekneme, že $\mathcal{C}$ je *uzávěrovým systémem nad A*, pokud

(1) $A \in \mathcal{C}$,
(2) pro každý podsystém $\{B_i|\ i \in I\} \subseteq \mathcal{C}$, je $\bigcap\{B_i|\ i \in I\} \in \mathcal{C}$.

Pro uzávěrový systém $\mathcal{C}$ na množině A a každou podmnožinu $B \subseteq \mathcal{C}$ definujme *uzávěr B v $\mathcal{C}$* jako množinu $cl_{\mathcal{C}}B = \bigcap\{C \in \mathcal{C}|\ B \subseteq C\}$.

Zobrazení $\alpha : \mathcal{P}(A) \to \mathcal{P}(A)$ nazýváme *uzávěrovým operátorem*, pokud

(1) $B \subseteq \alpha(B)$, pro všechna $B \in \mathcal{P}(A)$,
(2) $\alpha(\alpha(B)) = \alpha(B)$, pro všechna $B \in \mathcal{P}(A)$,
(3) $\alpha(B) \subseteq \alpha(C)$, pro všechna $B \subseteq C \subseteq A$.

Příklad. Mějme nějaký vektorový prostor V a označme $\mathcal{C}$ množinu všech podprostorů V. Pak $\mathcal{C}$ je uzávěrový systém (platnost obou axiomů uzávěrového systému byla dokázána na přednášce lineární algebry). Prostor generovaný množinou $X \subseteq V$ je uzávěrem X v $\mathcal{C}$ a zobrazení, které každé podmnožině $X \subseteq V$ přiřadí podprostor generovaný množinou X, je uzávěrovým operátorem.

Poznámka 3.1. *Nechť $A(\alpha_i|\ i \in I)$ je algebra. Pak všechny podalgebry algebry $A(\alpha_i|\ i \in I)$ tvoří uzávěrový systém na A.*

Důkaz. Plyne přímo z 1.1 a z faktu, že A je uzavřená na libovolnou operaci na A. □

Věta 3.2. (1) *Je-li $\mathcal{C}$ uzávěrový systém nad A, pak $cl_{\mathcal{C}}$ tvoří uzávěrový operátor.*

(2) *Je-li α uzávěrový operátor na A, pak množina $\mathcal{C} = \{C \subseteq A |\ \alpha(C) = C\}$ tvoří uzávěrový systém nad A a $\alpha = cl_{\mathcal{C}}$.*

Důkaz. Viz [D, 1.1]. □

Poznámka 3.3. *Všechny uzávěrové systémy nad množinou A tvoří uzávěrový systém nad $\mathcal{P}(A)$.*

Důkaz. Viz [D, 1.2]. □

Poznámka 3.4. *Nechť $\mathcal{A}$ a $\mathcal{B}$ jsou takové dva uzávěrové systémy nad A, že $\mathcal{A} \subseteq \mathcal{B}$, a nechť $C \subseteq D \subseteq A$. Potom $cl_{\mathcal{B}}(C) \subseteq cl_{\mathcal{A}}(D)$.*

Důkaz. Viz [D, 1.3]. □

Poznámka 3.5. *Všechny ekvivalence na množině A a všechny kongruence na algebře $A(\alpha_i |\ i \in I)$ tvoří uzávěrový systém na $A \times A$.*

Důkaz. Důkaz, že symetrické (tranzitívní, reflexivní) relace tvoří uzávěrový systém viz [D, 1.4]. Ekvivalence jsou průnikem všech symetrických, tranzitívních a reflexivních relací, proto tvoří uzávěrový systém podle 3.3. Že jsou kongruence uzávěrovým systémem viz [D, 2.4]. □

Věta 3.6. *Buď ρ relace na množině A. Potom $((\rho \cup id) \cup (\rho \cup Id)^{-1})^{+} = (\rho \cup \rho^{-1} \cup id)^{+}$ je nejmenší ekvivalence na A obsahující relaci ρ.*

Důkaz. Viz [D, 1.6]. □

Definice. Buď A algebra a $X \subseteq A$. Označme $\mathcal{A}$ uzávěrový systém všech podalgeber A. Potom budeme říkat, že X *generuje* (podalgebru) $cl_{\mathcal{A}}(X)$.

Poznámka 3.7. *Buď $f, g : A \to B$ dva homomorfismy algeber stejného typu a nechť $X \subseteq A$ generuje algebru A. Jestliže $f(x) = g(x)$ pro všechna $x \in X$, potom $f = g$.*

Důkaz. Viz [D, 3.3]. □

Příklad. Uvažujme grupu celých čísel $\mathbf{Z}(+, -, 0)$ a $G(+, -, 0)$ nějaká další algebra s jednou binární operací $+$, unární operací $-$ a nulární operací 0. Nechť $f, g : \mathbf{Z} \to G$ je homomorfismus. Uvědomme si, že nejmenší podgrupa obsahující prvek 1 je už rovna celému $\mathbf{Z}$. Podle předchozí poznámky jsou tedy f a g shodné, pokud $f(1) = g(1)$.

4. Svazy

Definice. Relaci $\leq$ na množině M budeme říkat *uspořádání*, pokud je to reflexivní a tranzitivní relace, pro níž platí podmínka $a \leq b,\ b \leq a \Rightarrow a = b$ pro každé $a, b \in M$ (tj. jde o slabě antisymetrickou relaci).

Příklad. Následující relace jsou uspořádáním:

- $\subseteq$ na množině všech podmnožin $\mathcal{P}(X)$ množiny X,
- / na množině všech přirozených čísel $\mathbf{N}$,
- $\leq$ na množině všech celých (reálných, racionálních) čísel $\mathbf{Z}$ ($\mathbf{R}$, $\mathbf{Q}$),

- Id na libovolné neprázdné množině M.

Definice. Nechť $\leq$ je uspořádání na množině M a $A \subseteq M$. Řekneme, že $m \in A$ je *nejmenší* (resp. *největší*) prvek množiny A, pokud $m \leq a$ (resp. $a \leq m$) pro všechna $a \in A$. *Supremem* (resp. *infimem*) množiny A budeme rozumět nejmenší prvek množiny $\{n \in M |\ \forall a \in A :\ a \leq n\}$ (resp. největší prvek množiny $\{n \in M |\ \forall a \in A :\ n \leq a\}$), supremum značíme $sup_{\leq}$ a infimum $inf_{\leq}$. Dvojici $(M, \leq)$ budeme říkat *svaz*, pokud pro každé dva prvky $a, b \in A$ existuje supremum a infimum množiny $\{a, b\}$. Svaz $(M, \leq)$ je úplným svazem, existuje-li supremum a infimum každé podmnožiny M.

Příklad. Snadno nahlédneme, že svazem jsou následující dvojice
- $(\mathcal{P}(X), \subseteq)$, kde $sup_{\subseteq}(A, B) = A \cup B$ a $inf_{\subseteq}(A, B) = A \cap B$,
- $(\mathbf{N}, /)$, kde $sup_{/}(n, m) = nsn(n, m)$ a $inf_{/}(a, b) = NSD(n, m)$,
- $(\mathbf{Z}, \leq)$, $(\mathbf{R}, \leq)$, $(\mathbf{Q}, \leq)$, kde $sup_{\leq}(a, b) = max(a, b)$ a $inf_{\leq}(a, b) = min(a, b)$.

Příklad. $(\mathcal{P}(X), \subseteq)$ je dokonce úplný svaz, kde $sup_{\subseteq}(\mathcal{B}) = \bigcup \mathcal{B}$ a $inf_{\subseteq}(\mathcal{B}) = \bigcap \mathcal{B}$ pro každou podmnožinu $\mathcal{B} \subseteq \mathcal{P}(X)$.

Definice. Nechť $(M, \leq)$ je svaz. Pro každé dva prvky $m, n \in M$ označme $m \vee n = sup_{\leq}(\{m, n\})$ a $m \wedge n = inf_{\leq}(\{m, n\})$. Potom binární operaci $\vee$ nazveme *spojení* a $\wedge$ *průsek*.

Poznámka 4.1. *Buď $(M, \leq)$ svaz. Pak pro všechna $a, b, c \in M$ platí:*

(S1) $a \vee b = b \vee a$, $a \wedge b = b \wedge a$,
(S2) $a \vee a = a = a \wedge a$,
(S3) $a \vee (b \vee c) = (a \vee b) \vee c$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$,
(S4) $a \vee (b \wedge a) = a = a \wedge (b \vee a)$.

Důkaz. Viz [D, s.29]. □

Poznámka 4.2. *Nechť $M(\wedge, \vee)$ je algebra s dvěma binárními operacemi, které splňují podmínky* (S1) – (S4). *Definujme na M relaci $\leq$ předpisem: $a \leq b \Leftrightarrow b = a \vee b$. Pak $(M, \leq)$ je svaz, kde $sup_{\leq}(\{m, n\}) = m \vee n$ a $inf_{\leq}(\{m, n\}) = m \wedge n$.*

Důkaz. Viz [D, s.29]. □

Předchozí dvě poznámky ukazují vzájemně jednoznačnou korespondenci mezi svazy a algebrami $M(\wedge, \vee)$ splňujícími podmínky (S1) – (S4). Proto budeme svazem nazývat i algebru $M(\wedge, \vee)$ a na množině M budeme zároveň používat operace $\wedge$ a $\vee$ i odpovídající relaci $\leq$.

Příklad. U uvedených příkladů svazů máme tedy dva způsoby jak na svaz nahlížet:
- $(\mathcal{P}(X), \subseteq)$ odpovídá algebře $\mathcal{P}(X)(\cap, \cup)$,
- $(\mathbf{N}, /)$ odpovídá algebře $\mathbf{N}(NSD, nsn)$,
- $(\mathbf{Z}, \leq)$ (respektive $(\mathbf{R}, \leq)$, $(\mathbf{Q}, \leq)$) odpovídá algebře $\mathbf{Z}(min, max)$ (respektive $\mathbf{R}(min, max)$, $\mathbf{Q}(min, max)$).

Věta 4.3. *Nechť $\mathcal{C}$ je uzávěrový systém. Pak $(\mathcal{C}, \subseteq)$ tvoří úplný svaz, kde $sup_{\subseteq}(\mathcal{B}) = cl_{\mathcal{C}}(\bigcup \mathcal{B})$ a $inf_{\subseteq}(\mathcal{B}) = \bigcap \mathcal{B}$.*

Důkaz. Viz [D, 4.2]. □

Příklad. Podle předchozí věty je systém všech podalgeber i systém všech kongruencí na algebře spolu s inkluzí svazem.

Poznámka 4.4. *Nechť $M(\wedge, \vee)$ je svaz. Pak i $M(\vee, \wedge)$ tvoří svaz (mluvíme o opačném svazu s opačným uspořádáním $\geq$).*

Důkaz. Zřejmé. □

Definice. Nechť $(M, \leq)$ je svaz a $a, b, c \in M$. Řekneme, že prvek b *pokrývá* prvek a (píšeme $a <\cdot\, b$), pokud $a \leq b$, $a \neq b$ a $a \leq c \leq b \Rightarrow c = a$ nebo $c = b$.

Hasseovým diagramem svazu $(M, \leq)$ rozumíme graf, jehož vrcholy tvoří prvky množiny M a a je s b spojen takovou hranou, že b se nachází výše než a, pokud b pokrývá a.

Poznámka 4.5. *Nechť $M(\wedge, \vee)$ je svaz, $a, b, c \in M$ a $a \leq c$. Potom $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.*

Důkaz. Viz [D, 14.1]. □

Definice. O svazu $S(\wedge, \vee)$ řekneme, že je *modulární*, jestliže pro každé $a, b, c \in S$ takové, že $a \leq c$ platí, že $a \vee (b \wedge c) = (a \vee b) \wedge c$. Řekneme, že je svaz *distributivní*, platí-li pro každé $a, b, c \in S$, že $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Příklad. (1) Svaz všech podprostorů vektorového prostoru je modulární.

(2) Svaz $(N_5, \leq)$, kde $N_5 = \{0, 1, a, b, c\}$, daný relacemi: $0 <\cdot\, a <\cdot\, c <\cdot\, 1$, $0 <\cdot\, b <\cdot\, 1$ (tzv. pentagon, $\mathcal{N}_5$) není modulární.

(3) Nechť $M_5 = \{\mathbf{0}, \mathbf{1}, u, v, w\}$, buď $\mathbf{0}$ nejmenší prvek, $\mathbf{1}$ největší prvek a $u \vee v = u \vee w = v \vee w = \mathbf{1}$ a $u \wedge v = u \wedge w = v \wedge w = \mathbf{0}$. Pak $M_5(\wedge, \vee)$ je modulární svaz, který není distributivní (říká se mu obvykle diamant a značí se $\mathcal{M}_5$).

Poznámka 4.6. *Svaz $S(\wedge, \vee)$ je distributivní, právě když pro každé $a, b, c \in S$ platí, že $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ (tj. svaz $S(\wedge, \vee)$ je distributivní, právě když je opačný svaz $S(\vee, \wedge)$ distributivní).*

Důkaz. Viz [D, 14.6]. □

Poznámka 4.7. *Každý distributivní svaz je modulární.*

Důkaz. Viz [D, 14.6]. □

Věta 4.8. *Svaz je modulární právě tehdy, když neobsahuje podsvaz izomorfní svazu $\mathcal{N}_5$.*

Důkaz. Viz [D, 14.4]. □

Obdobné tvrzení lze (obdobnými prostředky) dokázat i pro distributivní svazy: svaz je distributivní, právě když neobsahuje ani podsvaz izomorfní svazu $\mathcal{N}_5$, ani podsvaz izomorfní svazu $\mathcal{M}_5$.

Definice. Nechť má svaz $S(\wedge, \vee)$ nejmenší prvek $\mathbf{0}$ a největší prvek $\mathbf{1}$. Prvek $a \in S$ nazveme *atomem* (resp. *koatomem*), pokud a pokrývá 0 (resp. 1 pokrývá a). *Komplementem* prvku $a \in S$ nazveme takový prvek $a' \in S$, že $a \vee a' = \mathbf{1}$ a $a \wedge a' = \mathbf{0}$.

Poznámka 4.9. *Každý prvek distributivního svazu má nejvýše jeden komplement.*

Důkaz. Viz [D, 14.8]. □

Definice. *Booleovou algebrou* nazveme takovou algebru $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$, že $S(\wedge, \vee)$ je distributivní svaz s největším prvkem $\mathbf{1}$ a nejmenším prvkem $\mathbf{0}$ a unární operace $'$ přiřadí každému prvku jeho komplement.

Příklad. Nechť $\mathcal{P}(X)$ je množina všech podmnožin množiny X a pro každou podmnožinu $Y \subseteq X$ definujme $Y' = X \setminus Y$. Pak $\mathcal{P}(X)(\cup, \cap, \emptyset, X, \ ')$ je Booleova algebra.

Poznámka 4.10. *Nechť $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ je Booleova algebra. Pak pro každé $a, b \in S$ platí:*

(1) $(a')' = a$,
(2) $(a \vee b)' = a' \wedge b'$,
(3) $(a \wedge b)' = a' \vee b'$,
(4) $(\mathbf{1})' = \mathbf{0}$ *a* $(\mathbf{0})' = \mathbf{1}$.

Důkaz. Viz [D, 14.9]. □

Definice. Nechť $f : A \to B$ je zobrazení a $(A, \leq)$ a $(B, \leq)$ jsou svazy. Řekneme, že φ je *monotónní* zobrazení, platí-li implikace $a_1 \leq a_2 \Rightarrow f(a_1) \leq f(a_2)$.

Vezmeme-li $M = \{m_1, \ldots, m_n\}$ neprázdnou konečnou podmnožinu Booleovy algebry, pak značme $\bigwedge M = m_1 \wedge m_2 \wedge \cdots \wedge m_n$ a $\bigvee M = m_1 \vee m_2 \vee \cdots \vee m_n$. Dále $\bigwedge \emptyset = \mathbf{1}$ a $\bigvee \emptyset = \mathbf{0}$.

Věta 4.11. *Buď $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ konečná Booleova algebra a A buď množina všech atomů svazu S. Potom zobrazení $\varphi : \mathcal{P}(A) \to S$ dané předpisem $\varphi(B) = \bigvee B$ je izomorfismus Booleových algeber $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ a $P(A)(\cup, \cap, \emptyset, X, \ ')$.*

Důkaz. Viz [D, 15.2]. □

Poznámka 4.12. *Homomorfismus svazů je monotónní zobrazení.*

Důkaz. Viz [D, 4.3]. □

Příklad. Uvažujme svazy $(S_1, \leq)$ a $(S_2, \leq)$, kde $S_1 = \{0, 1, a, b\}$, $S_2 = \{\mathbf{0}, \mathbf{1}, \mathbf{A}, \mathbf{B}\}$ a daný relacemi: $0 < \cdot\ a < \cdot\ 1$, $0 < \cdot\ b < \cdot\ 1$ a $\mathbf{0} < \cdot\ \mathbf{A} < \cdot\ \mathbf{B} < \cdot\ \mathbf{1}$. Potom zobrazení $f(0) = \mathbf{0}$, $f(1) = \mathbf{1}$, $f(a) = \mathbf{A}$, $f(b) = \mathbf{B}$ je monotónní, ale není to homomorfismus svazů ($f(a \wedge b) = f(0) = \mathbf{0} \neq \mathbf{A} = f(a) \wedge f(b)$).

Věta 4.13. *Bijekce svazů f je izomorfismus, právě když f i f^{-1} jsou monotónní zobrazení.*

Důkaz. Viz [D, 4.4]. □

Poznámka 4.14. *Buď $\mathcal{C}$ uzávěrový systém obsažený v systému všech ekvivalencí na množině A. Nechť $\mathcal{N} \subseteq \mathcal{P}(A)$ a $e \in A$ tak, že platí:*

(a) $[e]_\rho \in \mathcal{N}$ *pro každé* $\rho \in \mathcal{C}$,
(b) *pro každé* $N \in \mathcal{N}$ *existuje takové* $\rho \in \mathcal{C}$, *že* $N = [e]_\rho$,
(c) *pro každé* $\rho, \eta \in \mathcal{C}$ *platí, že* $[e]_\rho \subseteq [e]_\eta \Rightarrow \rho \subseteq \eta$.

Pak $\mathcal{N}$ je uzávěrový systém na A (a tedy svaz) a zobrazení $\varphi : \mathcal{C} \to \mathcal{N}$ dané předpisem $\varphi(\rho) = [e]_\rho$ je izomorfismus svazů.

Důkaz. Viz [D, 4.7]. □

Věta 4.15. *Všechny normální podgrupy libovolné grupy G tvoří svaz izomorfní svazu všech kongruencí na grupě G.*

Důkaz. Podle [D, 1.13] systém všech kongruencí $\mathcal{C}$ a systém všech normálních podgrup $\mathcal{N}$ grupy $G(\cdot, ^{-1}, 1)$ spolu s $e = 1$ splňuje předpoklady Poznámky 4.14. Závěr tedy plyne ze 4.14. □

Příklad (Galoisova korespondence)**.** Uvažujme množina nějakých objektů O a množina vlastností, které mohou objekty mít V. Definujme $\rho \subseteq O \times V$ tak, že $(o, v) \in \rho$, právě když objekt o má vlastnost v. Dále definujme $\alpha_\rho(O_1) = \{v \in V |\ (o, v) \in \rho\ \forall o \in O_1\}$ (tj. vezmeme všechny vlastnosti, které mají všechny objekty z O_1) a $\beta_\rho(V_1) = \{v \in A |\ (o, v) \in \rho\ \forall v \in V_1\}$ (tj. vezmeme všechny objekty splňující všechny vlastnosti z V_1). Ukážeme, že takto definovanou struktura lze popsat prostřednictvím pojmu svazu. Nejprve si uvědomíme zřejmé vlastnosti zobrazení α_ρ a β_ρ a shrneme je do obecné definice tzv. *Galoisovy korespondence*:

Nechť A a B jsou množiny. Dvojici zobrazení $\alpha : \mathcal{P}(A) \to \mathcal{P}(B)$ a $\beta : \mathcal{P}(B) \to \mathcal{P}(A)$ se říká *Galoisova korespondence*, jsou-li pro každé $A_1, A_2 \in \mathcal{P}(A)$ a $B_1, B_2 \in \mathcal{P}(B)$ splněny následující podmínky:

(i) $A_1 \subseteq A_2 \Rightarrow \alpha(A_2) \subseteq \alpha(A_1)$ a $B_1 \subseteq B_2 \Rightarrow \beta(B_2) \subseteq \beta(B_1)$,
(ii) $A_1 \subseteq \beta\alpha(A_1)$ a $B_1 \subseteq \alpha\beta(B_1)$.

Nyní si uvědomíme, že Galoisova korespondence má následující vlastnosti (důkaz viz [D, 4.9]):

Tvrzení. Buď $\alpha : \mathcal{P}(A) \to \mathcal{P}(B)$ a $\beta : \mathcal{P}(B) \to \mathcal{P}(A)$ Galoisova korespondence. Potom jsou zobrazení $\beta\alpha$ a $\alpha\beta$ uzávěrové operátory. Označme $\mathcal{A}$ a $\mathcal{B}$ uzávěrové systémy příslušné uzávěrovým operátorům $\beta\alpha$ a $\alpha\beta$. Pak $\alpha(\mathcal{A}) \subseteq \mathcal{B}$ a $\beta(\mathcal{B}) \subseteq \mathcal{A}$. Označíme-li $\alpha' : \mathcal{A} \to \mathcal{B}$ a $\beta' : \mathcal{B} \to \mathcal{A}$ příslušné restrikce zobrazení α a β, pak α' a β' jsou bijekce a $\alpha' = (\beta')^{-1}$. Navíc pro každé $A_1, A_2 \in \mathcal{A}$ a $B_1, B_2 \in \mathcal{B}$ platí, že $A_1 \subseteq A_2 \Leftrightarrow \alpha(A_2) \subseteq \alpha(A_1)$ a $B_1 \subseteq B_2 \Leftrightarrow \beta(B_2) \subseteq \beta(B_1)$.

5. Grupy

Poznámka 5.1. *Nechť $G(\cdot, ^{-1}, 1)$ a $H(\cdot, ^{-1}, 1)$ jsou grupy a $f : G \to H$ je zobrazení slučitelné s operací $\cdot$. Pak je f homomorfismus grup.*

Důkaz. Viz [D, 6.1]. □

Definice. Nechť H a K jsou dvě podmnožiny grupy $G(\cdot, ^{-1}, 1)$ a $g \in G$. Definujme množiny $HK = \{h \cdot k |\ h \in H,\ k \in K\}$, $gH = \{g\}H$ a $Hg = H\{g\}$. Je-li H podgrupa G, definujme na G relaci $rmod\ H$ (resp. $lmod\ H$) podmínkou: $(a, b) \in rmod\ H$ (resp. $(a, b) \in lmod\ H$) $\Leftrightarrow a \cdot b^{-1} \in H$ (resp. $\cdot a^{-1}b \in H$).

Poznámka 5.2. *Nechť $G(\cdot, ^{-1}, 1)$ je grupa a H její podgrupa. Potom pro každé $a, b \in G$ platí:*

(1) *$rmod\ H$ i $lmod\ H$ jsou ekvivalence na G,*
(2) *$(a, b) \in rmod\ H \Leftrightarrow (a^{-1}, b^{-1}) \in lmod\ H$,*
(3) *$card(G/rmod\ H) = card(G/lmod\ H)$,*
(4) *$[a]_{rmod\ H} = Ha$ a $[a]_{lmod\ H} = aH$,*
(5) *$card([a]_{rmod\ H}) = card([a]_{lmod\ H}) = card(H)$.*

Důkaz. (1) a (2) viz [D, 6.6]. Podle (2) je zobrazení $[a]_{rmod\ H} \to [a^{-1}]_{lmod\ H}$ korektně definovanou bijekcí, tedy platí (3). Body (4) a (5) viz [D, 6.7]. □

Definice. Buď H podgrupa grupy G. Potom číslu $[G : H] = card(G/rmod\ H)$ budeme říkat *index podgrupy H* v grupě G a číslu $|G| = card(G)$ budeme říkat *řád grupy G*.

Věta 5.3 (Lagrange)**.** *Je-li H podgrupa grupy $G(\cdot,^{-1},1)$, pak $|G| = [G:H] \cdot |H|$.*

Důkaz. Viz [D, 6.8]. □

Důsledek 5.4. *Je-li G konečná grupa, potom řád každé její podgrupy dělí řád grupy G.*

Definice. Nechť $G(\cdot,^{-1},1)$ je grupa a $a \in G$. Definujme indukcí:

$a^0 = 1$,
$a^n = a^{n-1} \cdot a$ pro každé $n > 0$,
$a^n = (a^{-1})^{-n} \cdot a$ pro každé $n < 0$.

Poznámka 5.5. *Nechť $G(\cdot,^{-1},1)$ je grupa $a \in G$. Zobrazení $\varphi : \mathbf{Z} \to G$ dané předpisem $\varphi(n) = a^n$ je homomorfismus grupy $\mathbf{Z}(+,-,0)$ do grupy $G(\cdot,^{-1},1)$ a $\varphi(\mathbf{Z}) = \langle a \rangle = \{a^n |\ n \in \mathbf{Z}\}$.*

Důkaz. Viz [D, 6.3]. □

Definice. Buď $G(\cdot,^{-1},1)$ grupa. Označme $\langle a \rangle$ nejmenší podgrupu grupy G obsahující prvek $a \in G$. Řekneme, že G je *cyklická grupa*, pokud existuje takový prvek $g \in G$, že $\langle g \rangle = G$.

Příklad. (1) $\mathbf{Z}(+,-,0)$ je cyklická grupa, kde $\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

(2) $\mathbf{Z}_n(+,-,0)$ je pro každé přirozené n cyklická grupa s operacemi definovanými modulo n, kde $\mathbf{Z}_n = \langle a \rangle$, pokud $NSD(a,n) = 1$.

Pro každé přirozené k (resp. $k \in \mathbf{Z}_n$) označujme $k\mathbf{Z} = \langle k \rangle = \{kz |\ z \in \mathbf{Z}\}$ (resp. $k\mathbf{Z}_n = \langle k \rangle = \{k \cdot z |\ z \in \mathbf{Z}_n\}$)

Poznámka 5.6. (1) *Je-li $A \subseteq \mathbf{Z}$, pak A je podgrupa $\mathbf{Z}$, právě když existuje $k \geq 0$ tak, že $A = k\mathbf{Z}$.*

(2) *Je-li $A \subseteq \mathbf{Z}_n$, pak A je podgrupa $\mathbf{Z}_n$, právě když existuje $k \in \mathbf{Z}_n$ tak, že k je buď 0 nebo k dělí n a $A = k\mathbf{Z}_n$.*

Důkaz. Viz [D, 8.1]. □

Věta 5.7. *Buď $G(\cdot,^{-1},1)$ cyklická grupa.*

(1) *Je-li G nekonečná, pak $G(\cdot,^{-1},1) \cong \mathbf{Z}(+,-,0)$.*
(2) *Je-li $n = |G|$ konečné, pak $G(\cdot,^{-1},1) \cong \mathbf{Z}_n(+,-,0)$.*

Důkaz. Viz [D, 8.2]. □

Důsledek 5.8. *Podgrupa i faktorová grupa každé cyklické grupy je opět cyklická.*

Důkaz. Viz [D, 8.3]. □

Důsledek 5.9. *Buď $G(\cdot,^{-1},1)$ konečná grupa. Potom $g^{|G|} = 1$ pro každý prvek $g \in G$.*

Důkaz. $\langle g \rangle$ je cyklická grupa řádu n, tedy je podle 5.8 izomorfní $\mathbf{Z}_n(+,-,0)$, proto $g^n = 1$. Podle 5.4 $n/|G|$, tedy $g^{|G|} = (g^n)^{\frac{|G|}{n}} = 1^{\frac{|G|}{n}} = 1$ □

Věta 5.10. *Nechť $G(\cdot,^{-1},1)$ je konečná cyklická grupa. Pak pro každé přirozené k, které dělí řád grupy G, existuje právě jedna podgrupa grupy G řádu k.*

Důkaz. Viz [D, 8.4]. □

Poznámka 5.11. *Nechť $n \in \mathbf{N}$, $a, b \in \mathbf{Z}_n - \{0\}$ a k/n. Pak $a\mathbf{Z}_n = k\mathbf{Z}_n$ právě když $NSD(a,n) = k$. Speciálně platí, že $a\mathbf{Z}_n = \mathbf{Z}_n$ (tj. a je generuje $\mathbf{Z}_n$), právě když $NSD(a,n) = 1$.*

Důkaz. Viz [D, 8.7]. □

Definice. Funkci $\varphi : \mathbf{N} \to \mathbf{N}$ danou předpisem $\varphi(n) = |\{0 < k < n |\ NSD(k,n) = 1\}|$ nazveme *Eulerovou funkcí.*

Poznámka 5.12. *Je-li $n \in \mathbf{N}$, pak číslo $\varphi(n)$ udává počet prvků, které generují grupu $\mathbf{Z}_n(+,-,0)$ a počet invertibilních prvků $\mathbf{Z}_n(\cdot,1)$.*

Důkaz. Důsledek 5.11. □

Věta 5.13 (Malá Fermatova věta)**.** *Pro nesoudělná kladná celá čísla $a < n$ je $(a^{\varphi(n)}) mod\ n = 1$.*

Důkaz. Viz [D, 8.13]. □

Definice. Nechť $A_j(\alpha_i | i \in I)$, $j \leq k$ jsou algebry stejného typu. Definujme na $\prod_{j=1}^{k} A_j$ strukturu algebry algebry stejného typu předpisem

$$\alpha_i((a_{11}, \ldots, a_{k1}),\ (a_{12}, \ldots, a_{k2}), \ldots,\ (a_{1n}, \ldots, a_{kn})) =$$
$$= (\alpha_i(a_{11}, \ldots, a_{1n}), \alpha_i(a_{21}, \ldots, a_{2n}), \ldots, \alpha_i(a_{k1}, \ldots, a_{kn}))$$

pro každou n-ární operaci α_i.

Poznámka 5.14. *Mějme $M_j(\cdot,1)$ pro $j \leq k$ monoidy. Pak $\prod_{j=1}^{k} M_i(\cdot,(1,\ldots,1))$ je opět monoid a platí:*

(1) *$(m_1, m_2, \ldots, m_k) \in \prod_{j=1}^{k} M_i$ je invertibilní, právě když jsou všechny prvky m_j, $j = 1, \ldots, k$ invertibilní.*
(2) *$(m_1, m_2, \ldots, m_k)^n = (m_1, m_2, \ldots, m_k)$ právě když $m_j^n = m_j$ pro každé $j = 1, \ldots, k$, každé $m_j \in M_j$ a $n \in \mathbf{N}$.*

Důkaz. Stačí uvážit, že $(m_1, m_2, \ldots, m_k) \cdot (r_1, r_2, \ldots, r_k) = (m_1 \cdot r_1, m_2 \cdot r_2, \ldots, m_k \cdot r_k) = (1, 1, \ldots, 1)$, respektive $(m_1, m_2, \ldots, m_k)^n = (m_1^n, m_2^n, \ldots, m_k^n)$. □

Věta 5.15 (Čínská věta o zbytcích)**.** *Nechť $n_1, n_2, \ldots, n_k$ jsou po dvou nesoudělná kladná celá čísla a $n = n_1 \cdot n_2 \cdot \cdots \cdot n_k$, potom zobrazení $f : \mathbf{Z}_n \to \prod_{i=1}^{k} \mathbf{Z}_{n_i}$ dané předpisem $f(x) = (x\ mod\ n_1,\ x\ mod\ n_2, \ldots, x\ mod\ n_k)$ je izomorfismus algeber $\mathbf{Z}_n(+,-,0,\cdot,1)$ a $\prod_{i=1}^{k} \mathbf{Z}_{n_i}(+,-,\mathbf{0},\cdot,\mathbf{1})$.*

Důkaz. 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 $b = a$. □

Poznámka 5.16. *Je-li p prvočíslo a r kladné celé číslo, pak $\varphi(p^r) = (p-1) \cdot p^{r-1}$.*

Důkaz. Viz [D, 8.10]. □

Věta 5.17. *Buď $p_1 < p_2 < \cdots < p_k$ prvočísla a $r_1, r_2, \ldots, r_k$ kladná celá čísla. Potom $\varphi(\prod_{i=1}^{k} p_i^{r_i}) = \prod_{i=1}^{k} \varphi(p_i^{r_i}) = \prod_{i=1}^{k} (p_i - 1) p_i^{r_i - 1}$.*

Důkaz. Podle 5.15 jsou monoidy $\mathbf{Z}_{\prod_{i=1}^k p_i^{r_i}}(\cdot,1)$ a $\prod_{i=1}^k \mathbf{Z}_{p_i^{r_i}}(\cdot,(1,\dots,1)$ izomorfní, proto mají stejné počty invertibilních prvků. Použijeme-li dále 5.14 dostáváme: $\varphi(\prod_{i=1}^k p_i^{r_i}) = |(\mathbf{Z}_{\prod_{i=1}^k p_i^{r_i}})^*| = |\prod_{i=1}^k \mathbf{Z}^*_{p_i^{r_i}}| = \prod_{i=1}^k |\mathbf{Z}^*_{p_i^{r_i}}| = \prod_{i=1}^k \varphi(p_i^{r_i})$. Druhou rovnost dostaneme aplikací předchozí poznámky. (Viz také [D, 8.9].) □

Příklad (Rivest, Shamir, Adleman)**.** Zvolme p a q dvě různá lichá prvočísla a položme $m = nsn(p-1, q-1)$, potom je podle 5.13 (x^m)mod p = 1 a (y^m)mod q = 1 pro nenulová x a y, a proto i (x^{m+1})mod p = x a (y^{m+1})mod q = y pro každé $x \in \mathbf{Z}_p$ a $y \in \mathbf{Z}_q$. Z 5.15 a 5.14 potom plyne, že (a^{m+1})mod pq = a pro každé $a \in \mathbf{Z}_{pq}$. Dále zvolme $e < m$ nesoudělné s m a pak (například pomocí Euklidova algoritmu) najdeme takové $d < m$, že (ed)mod m = 1. Nyní pro každé $a \in \mathbf{Z}_{pq}$ platí, že $(a^e)^d = a^{ed} = a^{um+1} = a$ (počítáno v $\mathbf{Z}_{pq}$, tedy modulo pq).

Pomocí vlastnosti čísel p, q, m, d, e můžeme nyní popsat protokol asymetrického šifrování známý pod zkratkou RSA: veřejným klíčem je dvojice čísel (pq, e), soukromý klíč tvoří *tajný exponent* d. Chceme-li informaci vyjádřenou posloupností hodnot $a_1, \dots, a_k \in \mathbf{Z}_{pq}$ adresovat majiteli soukromého klíče, stačí ji zašifrovat pomocí mocnění veřejně známou hodnotou e v monoidu $\mathbf{Z}_{pq}(\cdot, 1)$, tj. odeslat zprávu $(a_1^e) mod\ pq, \dots, (a_k^e) mod\ pq$. K jejímu rozluštění stačí umocnit v $\mathbf{Z}_{pq}$ pomocí tajného exponentu, protože $(a_i^e)^d = a_i^{ed} = a_i$. Naopak, zveřejnění-li majitel soukromého klíče zašifrovanou zprávu $(a_1^d) mod\ pq, \dots, (a_k^d) mod\ pq$, mohou si příjemci zprávy stejným způsobem (tj. umocněním na veřejně známý exponent e: $((a_1^d)^e) mod\ pq, \dots, ((a_k^d)^e) mod\ pq = a_1, \dots, a_k$) ověřit, že odesilatel zprávy opravdu zná tajný exponent.

Poznamenejme, že je ze znalosti n a e obtížné najít d (odpovídá to nalezení prvočíselného rozkladu čísla n, což je úloha, pro níž není znám algoritmus polynomiální složitosti), zattímco mocnění čísel v $\mathbf{Z}_{pq}$ je (i pro velké exponenty a velké pq) velmi snadné a rychlé.

Důkaz následujícího tvrzení o cyklických grupách, který vyžaduje znalosti z teorie polynomů nad obecným tělesem, provedeme až v příštím semestru:

Věta 5.18. *Nechť $T(+,\cdot)$ je těleso a nechť G je konečná podgrupa multiplikativní grupy $T \setminus \{0\}(\cdot,^{-1},1)$. Potom G je cyklická grupa.*

6. Okruhy a ideály

Definice. *Okruhem* budeme nazývat každou takovou algebru $R(+,\cdot,-,0,1)$, že $R(+,-,0)$ je komutativní grupa, $R(\cdot,1)$ je monoid a pro každé $a,b,c \in R$ platí, že $a \cdot (b+c) = a \cdot b + a \cdot c$ a $(a+b) \cdot c = a \cdot c + b \cdot c$. $R(+,\cdot,-,0,1)$ je *komutativní okruhem*, je-li operace $\cdot$ komutativní.

Příklad. (1) $\mathbf{Z}(+,\cdot,-,0,1)$ je komutativní okruh.

(2) $\mathbf{Z}_n(+,\cdot,-,0,1)$ je pro každé přirozené n komutativní okruh s operacemi definovanými modulo n.

(3) Je-li T těleso a $M_n(T)$ značí množinu všech čtvercových matic nad T řádu n, pak $M_n(T)(+,\cdot,-,\mathbf{0}_n,\mathbf{I}_n)$ je okruh.

(4) Nechť V je vektorový prostor. Označme $End(V)$ množinu všech homomorfismů prostoru V do sebe (tzv. endomorfismů). Na této množině můžeme definovat sčítání a opačný prvek předpisem $[f+g](\mathbf{v}) = f(\mathbf{v}) + g(\mathbf{v})$ a $[-f](\mathbf{v}) = -f(\mathbf{v})$

pro každé $\mathbf{v} \in V$. Označíme-li nulový homomorfismus symbolem 0_V a $\circ$ označuje skládání, pak $End(V)(+, \circ, -, 0_V, Id)$ je okruh.

Poznámka 6.1. *Nechť $R(+, \cdot, -, 0, 1)$ je okruh. Pak pro každé $a, b \in R$ platí:*

(1) $0 \cdot a = a \cdot 0 = 0$,
(2) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$,
(3) $(-1) \cdot a = a \cdot (-1) = -a$,
(4) $(-a) \cdot (-b) = a \cdot b$,
(5) $1 \neq 0$, *právě když* $card(R) > 1$ *(tj. R je netriviální okruh).*

Důkaz. Viz [D, 7.2] a [D, 7.3]. □

Definice. Nechť $R(+, \cdot, -, 0, 1)$ je okruh. Řekneme, že množina $I \subseteq R$ je *pravý* (resp. *levý*) *ideál* okruhu R, pokud I je podgrupa grupy $R(+, -, 0)$ a pro každé $i \in I$ a $r \in R$ platí, že $i \cdot r \in I$ (resp. $r \cdot i \in I$). Množinu I nazveme *ideálem*, pokud je pravým a zároveň levým ideálem.

Příklad. (1) $\{0\}$ a R jsou (tzv. *triviálními*) ideály každého okruhu R.

(2) Množiny $aR = \{a \cdot r |\ r \in R\}$ (resp. $Ra = \{r \cdot a |\ r \in R\}$) jsou (tzv. *hlavní*) pravé (resp. levé) ideály okruhu R pro každé $a \in R$.

(3) Ideály okruhu celých čísel $\mathbf{Z}(+, \cdot, -, 0, 1)$ jsou právě tvaru $k\mathbf{Z}$.

(4) Ideály okruhu $\mathbf{Z}_n(+, \cdot, -, 0, 1)$ jsou právě tvaru $k\mathbf{Z}_n$, kde $k < n$ je 0 nebo dělitel čísla n.

Definice. Nechť $R(+, \cdot, -, 0, 1)$ je okruh. O (levém, pravém) ideálu I řekneme, že je *vlastní*, pokud $I \neq \{0\}$ a $I \neq R$.

Věta 6.2. *Nechť $R(+, \cdot, -, 0, 1)$ je okruh. Všechny ideály okruhu R tvoří uzávěrový systém a zobrazení $\rho \to [0]_\rho$ je izomorfismus svazu všech kongruencí na $R(+, \cdot, -, 0, 1)$ a svazu všech ideálů okruhu R. Navíc ρ je kongruence na okruhu R, právě když $[0]_\rho$ je ideál a $(a, b) \in \rho \longleftrightarrow a - b \in [0]_\rho$.*

Důkaz. Viz [D, 7.4]. □

Faktor okruhu R podle kongruence jednoznačně odpovídající ideálu I budeme značit (obdobně jako v případu faktorizace grup podle normálních podgrup) R/I. *Ideálem generovaným množinou $A \subset R$* rozumíme nejmenší ideál obsahující A.

Definice. Řekneme, že prvek okruhu $R(+, \cdot, -, 0, 1)$ je *invertibilní*, jedná-li se o invertibilní prvek monoidu $R(\cdot, 1)$. Řekneme, že okruh R je *tělesem*, jsou-li všechny prvky množiny $R \setminus \{0\}$ invertibilní. Konečně ideál okruhu $R(+, \cdot, -, 0, 1)$ je *maximální*, pokud je to koatom svazu všech ideálů okruhu R.

Poznámka 6.3. *Nechť $R(+, \cdot, -, 0, 1)$ je okruh a $a \in R$. Pak $a \in R$ je invertibilní, právě když $aR = Ra = R$.*

Důkaz. Viz [D, 7.6 (i)]. □

Věta 6.4. *V netriviálním okruhu $R(+, \cdot, -, 0, 1)$ je ekvivalentní:*

(1) *R je těleso,*
(2) *R neobsahuje žádné vlastní pravé ideály,*
(3) *R neobsahuje žádné vlastní levé ideály.*

Důkaz. Viz [D, 7.11] a [D, 7.13]. □

Věta 6.5. *Nechť $R(+,\cdot,-,0,1)$ je komutativní okruh. Potom R/I je těleso právě tehdy, když I je maximální ideál.*

Důkaz. Viz [D, 7.14]. □

Definice. Nechť $R(+,\cdot,-,0,1)$ je okruh. Definujme pro každé $n \in \mathbf{Z}$:

$0 \times a = 0$,
$n \times a = ((n-1) \times a) + a$ pro každé $n > 0$,
$n \times a = |n| \times (-a)$ pro každé $n < 0$.

Poznámka 6.6. *Nechť $R(+,\cdot,-,0,1)$ je okruh. Definujme zobrazení $\varphi : \mathbf{Z} \to R$ předpisem $\varphi(n) = n \times 1$. Pak φ je homomorfismus okruhů a $\varphi(\mathbf{Z})$ je nejmenší podokruh R obsahující prvek 1. Navíc $(Ker\varphi =) \{n \in \mathbf{Z} |\ \varphi(n) = 0\} = p\mathbf{Z}$ pro jednoznačně určené celé $p \geq 0$.*

Důkaz. Viz [D, 7.18]. □

Jednoznačně určené číslo p z předchozí poznámky se nazývá *charakteristika okruhu R*.

Definice. Komutativní okruh $R(+,\cdot,-,0,1)$ nazveme *oborem integrity*, platí-li, že $a \cdot b = 0$ implikuje $a = 0$ nebo $b = 0$

Příklad. (1) Každé komutativní těleso je oborem integrity.
(2) $\mathbf{Z}(+,\cdot,-,0,1)$ je oborem integrity.
(3) Okruh reálných polynomů $\mathbf{R}[x](+,\cdot,-,0,1)$ je obor integrity.

Uvažujme obor integrity $R(+,\cdot,-,0,1)$, a definujme algebru $F(+,\cdot,-,\mathbf{0},\mathbf{1})$, kde $F = R \times (R - \{0\})$ s operacemi: $(a,b) \cdot (c,d) = (a \cdot c, b \cdot d)$, $(a,b) + (c,d) = (a \cdot d + b \cdot c, b \cdot d)$, $-(a,b) = (-a,b)$, $\mathbf{0} = (0,1)$ a $\mathbf{1} = (1,1)$. Na algebře $F(+,\cdot,-,\mathbf{0},\mathbf{1})$ konečně definujme relaci $\sim$ předpisem $(a,b) \sim (c,d) \Leftrightarrow a \cdot d = b \cdot c$.

Věta 6.7. *Pro algebru $F(+,\cdot,-,\mathbf{0},\mathbf{1})$ platí:*

(1) *$F(+,\mathbf{0})$ a $F(\cdot,\mathbf{1})$ jsou komutativní monoidy,*
(2) *$\sim$ je kongruence na $F(+,\cdot,-,\mathbf{0},\mathbf{1})$,*
(3) *$(0,a) \sim \mathbf{0}$ a $(a,a) \sim \mathbf{1}$ pro každé $a \in R \setminus \{0\}$,*
(4) *$F/\sim$ je komutativní těleso,*
(5) *zobrazení $\sigma : R \to F/\sim$ dané předpisem $\sigma(r) = [(r,1)]_\sim$ je prostý okruhový homomorfismus.*

Důkaz. (1) viz [D, 9.2], (2) viz [D, 9.3], (3) viz [D, 9.4], (4) viz [D, 9.5] a (5) viz [D, 9.7]. □

Definice. Komutativní těleso $F/\sim$ budeme nazývat *podílovým tělesem* okruhu R a jeho prvky budeme značit $\frac{a}{b} = [(a,b)]_\sim$.

Příklad. Těleso racionálních čísel $\mathbf{Q}(+,\cdot,-,0,1)$ je podílovým tělesem okruhu celých čísel $\mathbf{Z}(+,\cdot,-,0,1)$.

7. Dělitelnost

Definice. Řekneme, že $S(\cdot,1)$ je *komutativní monoid s krácením*, pokud je $S(\cdot,1)$ monoid s komutativní operací $\cdot$ splňující pro každé $a,b,c \in S$ podmínku $a \cdot c = b \cdot c \ \Rightarrow\ a = b$.

Buď $S(\cdot,1)$ komutativní monoid s krácením a nechť $a,b \in S$. Řekneme, že a *dělí* b (píšeme a/b), pokud existuje takové $c \in S$, že $b = a \cdot c$. Řekneme že a *je asociován s* b (píšeme $a\|b$), pokud a/b a zároveň b/a.

Příklad. 1) $\mathbf{N}(\cdot,1)$ a $\mathbf{Z} \setminus \{0\}(\cdot,1)$ jsou komutativní monoidy s krácením.

2) Je-li $R(+,\cdot,-,0,1)$obor integrity, pak je $R \setminus \{0\}(\cdot,1)$ komutativní monoid s krácením.

Poznámka 7.1. *Buď $R\setminus\{0\}(\cdot,1)$ multiplikativní monoid (tedy komutativní monoid s krácením) nějakého oboru integrity $R(+,\cdot,-,0,1)$ (například okruhu celých čísel nebo reálných polynomů). Pak a/b právě když $bR \subseteq aR$ a $a\|b$ právě když $bR = aR$.*

Důkaz. Přímý důsledek definice. □

Poznámka 7.2. *Nechť $S(\cdot,1)$ je komutativní monoid s krácením.*

(1) *Pro každé $a,b \in S$ existuje nejvýše jeden takový prvek $c \in S$, že $a = b \cdot c$.*
(2) *Nechť $a,b \in S$. Pak $a\|b$ právě tehdy, když existuje invertibilní prvek $u \in S$ tak, že $a = b \cdot u$.*
(3) *$\|$ je kongruence na $S(\cdot,1)$.*
(4) *$S/\|(\cdot,[1]_\|)$ je komutativní monoid s krácením a relace "dělí" na něm tvoří uspořádání.*

Důkaz. (1) viz [D, 5.10], (2) viz [D, 5.2], (3) viz [D, 5.5]. □

Příklad. Komutativní monoidy $\mathbf{N}(\cdot,1)$ a $\mathbf{Z} \setminus \{0\}/\|(\cdot,1)$ jsou izomorfní.

Definice. Buď $S(\cdot,1)$ komutativní monoid s krácením (nebo $S(+,\cdot,-,0,1)$ obor integrity) a nechť $a,b,c,a_1,\ldots,a_n \in S$. Prvek c nazveme *největší společný dělitel prvků* $a_1,\ldots,a_n$ (píšeme $NSD(a_1,\ldots,a_n)$), jestliže c/a_i pro všechna i, a každý prvek $d \in S$, který dělí všechna a_i, dělí i prvek c. Prvek c nazveme *ireducibilním* prvkem, jestliže c není invertibilní (ani nulový v oboru integrity) a $c = a \cdot b \;\Rightarrow\; c\|a$ nebo $c\|b$. Prvek c nazveme *prvočinitelem*, jestliže c není invertibilní (ani nulový) a $c/a \cdot b \;\Rightarrow\; c/a$ nebo c/b.

Poznámka 7.3. *Nechť $S(\cdot,1)$ je komutativní monoid s krácením a $a,b,c \in S$.*

(1) *Nechť d je $NSD(a,b)$ a e je $NSD(a \cdot c, b \cdot c)$. Potom $(d \cdot c)\|e$*
(2) *Nechť 1 je $NSD(a,b)$ a $a/b \cdot c$. Existuje-li $NSD(a \cdot c, b \cdot c)$, pak a/c.*

Důkaz. (1) viz [D, 5.12] a (2) viz [D, 5.13]. □

Poznámka 7.4. *Mějme $S(\cdot,1)$ komutativní monoid s krácením. Potom je každý prvočinitel ireducibilní. Pokud navíc pro každé $a,b \in S$ existuje $NSD(a,b)$ pak je každý ireducibilní prvek prvočinitelem.*

Důkaz. Viz [D, 5.14]. □

Následující větu letos dokážu až v letním semestru (tedy její důkaz nebudu samozřejmě zkoušet):

Věta 7.5. *Nechť je každý ireducibilní prvek komutativního monoidu s krácením $S(\cdot,1)$ prvočinitelem a nechť $p_1,\ldots,p_r,q_1,\ldots,q_s \in S$ jsou ireducibilní prvky takové, že $p_1 \cdot p_2 \cdot \cdots \cdot p_r \| q_1 \cdot q_2 \cdot \cdots \cdot q_s$. Potom $r = s$ a existuje bijekce σ tak, že $p_i \| q_{\sigma(i)}$ pro všechna $i = 1,\ldots,r$.*

Důkaz. Viz [D, 5.16]. □

Příklad. Uvažujme podokruh $\mathbf{Z}[\sqrt{5}] = \{a + \sqrt{5}b |\ a, b \in \mathbf{Z}\}$ okruhu reálných čísel. Zřejmě se jedná o obor integrity, tedy $\mathbf{Z}[\sqrt{5}] \setminus \{0\}(\cdot, 1)$ je komutativního monoidu s krácením. Lze ukázat, že prvky 2, $\sqrt{5}+1$ a $\sqrt{5}-1$ jsou ireducibilní, ale nejde o prvočinitele, protože $2/4 = (\sqrt{5}+1)\cdot(\sqrt{5}-1)$, ale 2 nedělí $\sqrt{5}+1$, ani $\sqrt{5}-1$ (podobně pro $\sqrt{5}+1$ a $\sqrt{5}-1$).

Zároveň dostáváme dva neasocivané ireducibilní rozklady prvku $4 = 2 \cdot 2 = (\sqrt{5}+1)\cdot(\sqrt{5}-1)$.

[D] - odkazuje na skripta profesora Drápala na adrese
http://www.karlin.mff.cuni.cz/∼drapal/skripta/