ALGEBRA I PRO INFORMATIKY

JAN ŽEMLIČKA

Úvod

Velmi zhruba řečeno je centrálním objektem zájmu algebry množina opatřená jistým systémem operací. Přitom nás mohou zajímat nejen strukturní vlastnosti takové množiny popsané podmínkami vyjádřené právě pomocí operací, nýbrž i vztahy různých množin s podobnými systémy operací či vlastnosti tříd takových množin.

Dříve než se začneme systematicky zabývat abstraktními úvahami o takových algebraických objektech (které se budou zpravidla opírat o nějaký systém axiomatických požadavků na operace), uveďme několik motivačních příkladů, které by nám pomohly usnadnit porozumění důvodům (ať už praktickým tak historickým), proč právě tu či onu vlastnost sledujeme.

Příklad 0.1. Uvažme množinu celých čísel $\mathbf{Z}$ a na ní obvyklé operace sčítání $+$ a násobení $\cdot$. Pro libovolné přirozené číslo n položme $n\mathbf{Z} = \{n \cdot z |\ z \in \mathbf{Z}\}$. Nyní si můžeme všimnout, že je množina $n\mathbf{Z}$ „uzavřená" na obě uvažované operace, tj. pro každou dvojici $a, b \in n\mathbf{Z}$ platí, že $a + b, a \cdot b \in n\mathbf{Z}$, tedy operace $+$ a $\cdot$ můžeme uvažovat také omezeně na množině $n\mathbf{Z}$. Ačkoli pro žádné $n > 1$ množiny $n\mathbf{Z}$ a $\mathbf{Z}$ nesplývají, nelze pomocí vlastností operace $+$ obě množiny odlišit (tj. mají stejné „algebraické" vlastnosti vzhledem ke sčítání), což ozřejmíme, zavedeme-li zobrazení $f_n : \mathbf{Z} \to n\mathbf{Z}$ předpisem $f_n(k) = kn$. Zjevně se jedná o bijekci, která navíc splňuje podmínku $f_n(a + b) = f_n(a) + f_n(b)$.

Poznamenejme, že taková vlastnost zobrazení není nijak samozřejmá, například vzhledem k operaci násobení f_n obdobnou podmínku nesplňuje. Uvážíme-li navíc podmínku „existuje prvek e tak, že pro všechny prvky a platí $a \cdot e = a$", pak je tato podmínka na množině $\mathbf{Z}$ splněna pro $e = 1$, zatímco na množině $n\mathbf{Z}$ zjevně neplatí.

Příklad 0.2. V souladu se značením zavedeným na kurzu lineární algebry položme $\mathbf{Z}_n = \{0, 1, \ldots, n - 1\}$ pro nějaké celé číslo $n > 1$. Zaveďme na $\mathbf{Z}_n$ operace $+$ a $\cdot$ předpisem $a + b = (a + b) \mathrm{mod}\ n$ a $a \cdot b = (a \cdot b) \mathrm{mod}\ n$, kde mod n znamená zbytek po celočíselném dělení hodnotou n a v závorce uvažujeme vždy obvyklé sčítání a násobení celých čísel. Konečně definujme zobrazení $F_n : \mathbf{Z} \to \mathbf{Z}_n$ předpisem $F_n(k) = (k) \mathrm{mod}\ n$. Všimněme si, že tentokrát zobrazení F sice není bijekce, ale obě operace sčítání a násobenní „převádí" na nově zavedené $+$ a $\cdot$, tedy $F_n(a+b) = F_n(a)+F_n(b)$ i $F_n(a \cdot b) = F_n(a) \cdot F_n(b)$.

Definice. *Binární operací* na množině A budeme rozumět libovolné zobrazení $A \times A \to A$ (obvykle ji budeme zapisovat centrálně). Máme-li binární operaci $*$ na množině A, nějakou podmnožinu U množiny A a binární operaci $\circ$ na množině B. Řekneme, že U je *uzavřená* na operaci $*$, jestliže pro všechna $x, y \in U$ platí, že $x * y \in U$, a zobrazení $f : A \to B$ nazveme *slučitelné* s operacemi $*$ a $\circ$ je-li pro všechna $x, y \in A$ splněna rovnost $f(x * y) = f(x) \circ f(y)$.

Date: 19.1.2010.

Všimněme si, že zobrazení f_n z 0.1 je slučitelné s operacemi $+$ a není slučitelné s operacemi $\cdot$, zatímco zobrazení F_n z 0.2 je slučitelné s oběma páry operací $+$ i $\cdot$.

Příklad 0.3. Vezměme přirozené číslo $n \geq 2$ a označme $\sim_n$ relaci na množině celých čísel $\mathbf{Z}$ danou předpisem: $a \sim_n b \leftrightarrow n/(a-b)$. Není těžké si uvědomit, že se jedná o ekvivalenci (obvykle se jí říká kongruence na $\mathbf{Z}$), která splňuje pro všechna taková celá a_1, a_2, b_1, b_2, že $a_1 \sim_n b_1$ a $a_2 \sim_n b_2$ podmínky $(a_1 + a_2) \sim_n (b_1 + b_2)$ a $(a_1 \cdot a_2) \sim_n (b_1 \cdot b_2)$. Navíc si můžeme všimnout jejího těsného vztahu k zobrazení F_n z 0.2, neboť platí, že $a \sim_n b$, právě když $F_n(a) = F_n(b)$.

Připomeňme, že *relací na množině* A rozumíme libovolnou podmnožinu $A \times A$.

Definice. Uvažujme na množině A binární operaci $*$ a relaci $\sim$. Řekneme, že $\sim$ je *slučitelná s operací* $*$, jestliže pro všechny takové prvky $a_1, a_2, b_1, b_2 \in A$, pro něž $a_1 \sim b_1$ a $a_2 \sim b_2$ platí, že $(a_1 * a_2) \sim (b_1 * b_2)$.

V Příkladu 0.3 jsme tedy zjistili, že je „kongruence" $\sim_n$ slučitelná s oběma operacemi $+$ i $\cdot$.

Příklad 0.4. Mějme kladná celá čísla $n_1, \ldots, n_k$ a položme $n = n_1 \cdot n_2 \cdot \cdots \cdot n_k$. Zaveďme nyní na kartézském součinu $\prod_{i=1}^{k} \mathbf{Z}_{n_i}$ po složkách operace $+$ a $\cdot$: $(a_1, a_2, \ldots, a_k) + (b_1, b_2, \ldots, b_k) = (a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k)$ a $(a_1, a_2, \ldots, a_k) \cdot (b_1, b_2, \ldots, b_k) = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_k \cdot b_k)$ a definujme zobrazení $G : \mathbf{Z} \to \prod_{i=1}^{k} \mathbf{Z}_{n_i}$ předpisem $G(a) = ((a) \mathrm{mod}\ n_1, \ldots, (a) \mathrm{mod}\ n_k)$ a stejným předpisem zavedeme i zobrazení $H : \mathbf{Z}_n \to \prod_{i=1}^{k} \mathbf{Z}_{n_i}$. Obě zobrazení jsou opět slučitelná s $+$ a $\cdot$.

Tvrzení této a následující kapitoly budou bez důkazu využívat základních poznatků teorie čísel, především jednoznačnost (až na pořadí) ireducibilního rozkladu a Euklidova algoritmu na nalezení největšího společného dělitele.

V následující poznámce budeme uvažovat operace na kartézských součinech zavedené v Příkladu 0.4.

Poznámka 0.5 (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 bijekce slučitelná s operací $+$ a s operací $\cdot$.*

Důkaz. Přímo z definice snadno vidíme, že je f zobrazení slučitelné s oběma 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 ověřit, 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 $b = a$. □

Čínská věta o zbytcích nám umožňuje „algebraicky" přesně reprezentovat větší množinu $\mathbf{Z}_n$ pomocí počítání v menších množinách $\mathbf{Z}_{n_i}$, což je postup, který se při potřebě exaktního počítání s velkými čísly (například při práci s velkými prvočísly) často používá.

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

Poznámka 0.6. *Je-li p prvočíslo a k kladné celé číslo, pak $\varphi(p^k) = (p-1) \cdot p^{k-1}$.*

Důkaz. Číslo menší než p^k je soudělné s p^k, právě když je násobkem čísla p. Kladných násobků čísla p menších než p^k je zřejmě právě $p^{k-1}-1$. To znamená, že naopak kladných čísel nesoudělných s p^k máme $\varphi(p^k) = (p^k-1) - (p^{k-1}-1) = p^k - p^{k-1} = (p-1)p^{k-1}$. □

Věta 0.7. *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. Zvolme libovolné $a \in \mathbf{Z}_n$. Položme $n = \prod_{i=1}^k p_i^{r_i}$ a $(a_1, \ldots, a_k) = f(a)$. Podle 0.5 je zobrazení $f : \mathbf{Z}_n \to \prod_{i=1}^k \mathbf{Z}_{p_i^{r_i}}$ bijekce. Abychom ověřili rovnost $\varphi(\prod_{i=1}^k p_i^{r_i}) = \prod_{i=1}^k \varphi(p_i^{r_i})$, stačí nám nahlédnout, že $\mathrm{NSD}(a,n) = 1$ právě tehdy, když $\mathrm{NSD}(a_i, n_i) = 1$ pro všechna $i = 1, \ldots, k$, protože $\prod_{i=1}^k \varphi(n_i) = |\prod_{i=1}^k \{a \in \mathbf{Z}_{n_i} \setminus \{0\} |\ \mathrm{NSD}(a, n_i) = 1\}|$.

Jestliže $\mathrm{NSD}(a,n) \neq 1$, existuje prvočíslo p, které dělí n, a díky jednoznačnosti prvočíselného rozkladu tudíž existuje i, pro něž p dělí n_i. Tedy buď $a_i = 0$ nebo p dělí a_i, proto $\mathrm{NSD}(a_i, n_i) \neq 1$. Naopak, jesliže $\mathrm{NSD}(a_i, n_i) \neq 1$, pak existuje dělitel $c > 1$ čísel a_i i n_i, proto c dělí i $a = a_i + xn_i$ i $n = n_1 \ldots n_i \ldots n_k$.

Konečně rovnost $\prod_{i=1}^k \varphi(p_i^{r_i}) = \prod_{i=1}^k (p_i-1)p_i^{r_i-1}$ plyne okamžitě z 0.6 □

Příklad 0.8. Nechť X je neprázdná množina písmen a $M(X)$ je množina všech slov, tj. všech konečných posloupností písmen. Zaveďme na této množině binární operaci skládání $\cdot$: $x_1 \ldots x_n \cdot y_1 \ldots y_m = x_1 \ldots x_n y_1 \ldots y_m$ a dále označme λ prázdné slovo. Snadno nahlédneme, že je operace $\cdot$ asociativní (je-li X aspoň dvouprvková množina, pak operace není komutativní) a platí, že $\lambda \cdot s = s \cdot \lambda = s$ pro každé $s \in M(X)$.

Mějme dvě slova $a, b \in M(X)$. Obsahuje-li slovo s_a podposloupnost a, slovo s_b vznikne ze slova s_a tak, že podposloupnost a v s_a nahradíme podposloupností b. Ztotožníme-li všechny takové dvojice slov, t.j. zavedeme-li podmínkou $s_a \sim s_b$ a $s_b \sim s_c$ relaci $\sim$ na $M(X)$, pak $\sim$ bude ekvivalence slučitelná s operací $\cdot$.

1. Množiny s asociativní binární operací

Připomeňme, že binární operace $*$ na A je *asociativní* (resp. *komutativní*), platí-li pro všechna $x, y, z \in A$ rovnost $x * (y * z) = (x * y) * z$ (resp. $x * y = y * x$).

Definice. Uvažujme binární operací $*$ na množině A. *Neutrálním prvkem* operace $*$ rozumíme takový prvek $e \in A$, že $g * e = e * g = g$ pro všechna $g \in A$.

Poznámka 1.1. *Každá binární operace má nejvýše jeden neutrální prvek.*

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

Příklad 1.2. 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.

Definice. Nechť $\cdot$ je binární operace na množině S a 1 její neutrální prvek. Řekneme, že prvek $s \in S$ je *invertibilní*, existuje-li 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.

Definice. Množině G s binární operací $\cdot$ budeme říkat *grupoid* (a budeme psát $G(\cdot)$). O grupoidu $G(\cdot)$ řekneme, že je:

- *pologrupa*, je-li operace $\cdot$ asociativní,
- *monoid*, je-li operace $\cdot$ asociativní a v G leží její neutrální prvek,
- *grupa*, je-li $G(\cdot)$ monoid, jehož každý prvek je invertibilní,
- *komutativní grupa* (nebo *abelovská grupa*), je-li $G(\cdot)$ grupa a $\cdot$ je komutativní.

V Příkladech 0.1 a 0.3 jsme připomněli asociativní a komutativní operace $+$ a $\cdot$ na množině celých čísel (a v Příkladech 0.2 a 0.4 jsme si uvědomili, že asociativitu i komutativitu splňují jimi indukované operace na množinách $\mathbf{Z}_n$). Jistě zde není třeba opakovat, jak vypadají odpovídající neutrální a invertibilní prvky. Uveďme ještě několik dobře známých, ač méně elementárních příkladů asociativních binárních operací.

Příklad 1.3. (1) Množina $M(X)$ z Příkladu 0.8 tvoří s operací skládání (tzv. *slovní*) monoid.

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

(3) Čtvercové matice $M_n(T)$ nad tělesem T stupně n spolu s násobením tvoří monoid $M_n(T)(\cdot)$ (neutrálním prvkem je zde jednotková matice).

Nestanovíme-li jinak, bude v následujícím 1 označovat neutrální prvek operace $\cdot$ (a 0 pro operaci $+$) a s^{-1} bude inverzní prvek k s vzhledm k operaci $\cdot$ (a $-s$ bude inverz vzhledem k operaci $+$).

Poznámka 1.4. *Buď $S(\cdot)$ monoid a $a, b, c \in S$. Platí-li, že $a \cdot b = c \cdot a = 1$, potom $b = c$ je jednoznačně určený inverzní prvek k prvku a.*

Důkaz. Stačí ověřit, že $b = c$. S využitím asociativity počítejme: $c = c \cdot 1 = c \cdot (a \cdot b) = (c \cdot a) \cdot b = 1 \cdot b = b$. □

Příklad 1.5. 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 $\alpha\beta \neq Id$. Prvky α a β monoidu $T(\mathbf{N})$ splňují právě jednu z definitorických rovností invertibilního prvku, invertibilní tedy nejsou (a podle 1.4 být nemohou).

Poznámka 1.6. *Množina všech invertibilních prvků monidu $S(\cdot)$ je uzavřená na operaci $\cdot$. Je-li navíc s invertibilní prvek, pak i s^{-1} je invertibilní a $(s^{-1})^{-1} = s$.*

Důkaz. Označme S^* množinu invertibilních prvků monidu $S(\cdot)$ Vezmeme-li prvky g_1 a g_2 z S^*, platí, že existují prvky $h_1, h_2 \in S$, pro něž $g_i \cdot h_i = h_i \cdot g_i = 1$, kde $i = 1, 2$. Tedy $(g_1 \cdot g_2) \cdot (h_2 \cdot h_1) = g_1 \cdot (g_2 \cdot h_2) \cdot h_1 = g_1 \cdot 1 \cdot h_1 = g_1 \cdot h_1 = 1$ a symetricky $(h_2 \cdot h_1) \cdot (g_1 \cdot g_2) = 1$.

Druhá vlastnost plyne okamžitě z definitorické podmínky $s \cdot s^{-1} = s^{-1} \cdot s = 1$ a z 1.4. □

Poznámka 1.7. *Nechť $S(\cdot)$ je monoid a S^* množina všech jeho invertibilních prvků. Označíme-li $\cdot_{S^*}$ restrikci $\cdot|_{S^* \times S^*}$ operace $\cdot$ na množinu $S^* \times S^*$, pak $S^*(\cdot_{S^*})$ je grupa.*

Důkaz. Podle 1.6 je množina S^* uzavřená na operaci $\cdot$, proto je $\cdot|_{S^*\times S^*}$ dobře definovaná asociativní binární operace na S^*. Protože $1\cdot 1 = 1$, leží neutrální prvek 1 v množině S^*. Konečně, S^* obsahuje inverzní prvky opět díky 1.6. □

Příklad 1.8. (1) Grupa invertibilních prvků slovního monoidu $M(X)(\cdot)$ obsahuje pouze neutrální prvek e.

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

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

Definice. *Podgrupou* grupy $G(\cdot)$ budeme rozumět každou neprázdnou podmnožinu H množiny G, která je uzavřená na $\cdot$ a pro jejíž každý prvek $h \in H$ platí, že $h^{-1} \in H$. *Normální podgrupa* je podgrupa H grupy G splňující navíc podmínku $g \cdot h \cdot g^{-1} \in H$ pro každé $g \in G$ a $h \in H$.

Poznámka 1.9. *Nechť $G(\cdot)$ je grupa, H a H_i, $i \in I$ její podgrupy.*

(1) $1 \in H$,
(2) $H(\cdot)$ *tvoří s operací omezenou na množinu H opět grupu,*
(3) $\bigcap_{i\in I} H_i$ *je podgrupa grupy $G(\cdot)$,*
(4) *jsou-li všechny podgrupy H_i normální, pak je i podgrupa $\bigcap_{i\in I} H_i$ normální,*
(5) *je-li $G(\cdot)$ komutativní grupa, pak je podgrupa H vždy normální.*

Důkaz. (1) Protože je H neprázdná, obsahuje nějaké $h \in H$. Tedy $h^{-1} \in H$ a $1 = h \cdot h^{-1} \in H$.

(2) Díky (1) obsahuje H neutrální prvek vzhledem k $\cdot$, zbytek plyne okamžitě z definice podgrupy a vlastností operace $\cdot$ na G (srovnej s 1.6).

(3) $1 \in H_i$ pro všechna $i \in I$ podle (1), tedy $\bigcap_{i\in I} H_i$ je neprázdná. Zvolme libovolně $a, b \in \bigcap_{i\in I} H_i$. Potom $a \cdot b \in H_i$ pro každé $i \in I$ díky uzavřenosti H_i na operaci $\cdot$, tedy $a \cdot b \in \bigcap_{i\in I} H_i$. Podobně podle definice $a^{-1} \in H_i$ pro každé $i \in I$, proto $a^{-1} \in \bigcap_{i\in I} H_i$.

(4) Zvolme $h \in \bigcap_{i\in I} H_i$ a $g \in G$. Pak $g \cdot h \cdot g^{-1} \in H_i$ pro všechna $i \in I$, a tudíž $g \cdot h \cdot g^{-1} \in \bigcap_{i\in I} H_i$.

(5) Díky komutativitě binární operace platí pro každé $g \in G$ a $h \in H$, že $g \cdot h \cdot g^{-1} = g \cdot g^{-1} \cdot h = h \in H$. □

Příklad 1.10. (1) Všimněme si, že v každé grupě $G(\cdot)$ tvoří množiny $\{1\}$ a G (tzv. triviální) příklady normálních podgrup.

(2) Uvažujeme-li komutativní grupu celých čísel $\mathbf{Z}(+)$ (s neutrálním prvkem 0 a inverzními prvky značenými standardně symbolem $-$), potom množiny tvaru $n\mathbf{Z} = \{n \cdot z |\ z \in \mathbf{Z}\}$ jsou pro každé nezáporné celé n podgrupou grupy $\mathbf{Z}(+)$ (viz 0.1). Napak, uvažujme libovolnou nenulovou podgrupu P grupy $\mathbf{Z}(+)$. Protože P obsahuje nějaký nenulový prvek a s každým $a \in P$ je i $-a \in P$, leží v P jistě nějaký kladný prvek a my můžeme zvolit nejmenší kladné číslo obsažené v P, označme ho n. Ukažme, že nutně $P = n\mathbf{Z}$. Indukcí díky uzavřenosti P na sčítání nahlédneme, že $2n = n + n \in P$, $3n \in P$, …, $kn \in P$, …, pro každé přirozené k. Protože $-n \in P$, dostanem stejným argumentem, že $n\mathbf{Z} \subseteq P$. Nyní zvolme libovolně $a \in P$. Potom vydělíme se zbytkem číslo a číslem n, t.j. najdeme celé q a nezáporné celé $z < n$, pro která $a = qn + z$. Z uzavřenosti P na $+$ použité pro prvky $a, -qn \in P$ plyne, že $z = a + (-qn) \in P$, a z minimality volby n dostáváme, že $z = 0$, tedy $n\mathbf{Z} = P$.

(3) Uvažujme grupu permutací na množině $\{1, \dots, n\}$, obvykle se značí $S_n(\circ)$ (viz také 1.8(2)). Snadno nahlédneme, že množina všech sudých permutací A_n je normální podgrupou $S_n(\circ)$. Navíc lze (elemntárními prostředky) dokázat, že grupa $S_n(\circ)$ neobsahuje pro $n \neq 4$ jiné normální podgrupy než $\{\mathrm{Id}\}$, S_n a A_n (v případě S_4 se vyskytuje ještě jedna další výjimečná normální podgrupa). Uveďmě alespoň příklad zjevné podgrupy $T = \{Id, (12)\}$ grupy S_3, která není normální, protože například $(13) \circ (12) \circ (13)^{-1} = (23) \notin T$.

Definice. Nechť H a K jsou dvě podmnožiny grupy $G(\cdot)$ 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 $\mathrm{rmod}\, H$ (resp. $\mathrm{lmod}\, H$) podmínkou: $(a, b) \in \mathrm{rmod}\, H$ (resp. $(a, b) \in \mathrm{lmod}\, H$) $\Leftrightarrow a \cdot b^{-1} \in H$ (resp. $\cdot a^{-1}b \in H$).

Příklad 1.11. Mějme dvě normální podgrupy H a K grupy $G(\cdot)$. Pak pro každé $h_0 \in H$ a $k \in K$ existuje $h_1 \in H$, pro které $k \cdot h_0 \cdot k^{-1} = h_1$, tedy $k \cdot h_0 = h_1 \cdot k$ a $KH \subseteq HK$. Symetrický argument dokazuje i obrácenou inkluzi, proto $KH = HK$. Nyní snadno nahlédneme, že je součin HK rovněž podgrupou $G(\cdot)$: zřejmě je HK neprázdné a zvolíme-li $h_0, h_1 \in H$ a $k_0, k_1 \in K$, potom $(h_0 \cdot k_0)^{-1} = k_0^{-1} \cdot h_0^{-1} \in KH = HK$ a dále existuje takové $h_2 \in H$, že $k_0 \cdot h_1 = h_2 \cdot k_0$, proto $h_0 \cdot k_0 \cdot h_1 \cdot k_1 = h_0 \cdot h_2 \cdot k_0 \cdot k_1 \in HK$. Konečně vezmeme-li libovolné prvky $g \in G$, $h \in H$ a $k \in K$, pak platí $g \cdot h \cdot k \cdot g^{-1} = (g \cdot h \cdot g^{-1}) \cdot (g \cdot k \cdot g^{-1}) \in HK$ díky předpokládané normalitě obou podgrup. Vidíme, že „součin" normálních podgrup (například tedy součin libovolných podgrup komutativní grupy) dává opět normální podgrupu. Poznamenejme, že součin podgrup, které normální nejsou, vůbec nemusí být podgrupou (stačí uvážit například podgrupy $H = \{Id, (12)\}$ a $K = \{Id, (13)\}$ grupy S_3).

Relací na množině A budeme rozumět každou podmnožinu $A \times A$ Nechť ρ je relace na A, označme:

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

Řekneme, že relace ρ je *symetrická*, jestliže $\rho^{-1} \subseteq \rho$, *tranzitívní*, pokud $\rho^{+} \subseteq \rho$, a *reflexivní*, v případě, že $id \subseteq \rho$. *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 ekvivalence ρ jako množinu $A/\rho = \{[a]_\rho |\ a \in A\}$, kde $[a]_\rho = \{b \in A |\ (a, b) \in \rho\}$, a *přirozenou projekci* zobrazení $\pi_\rho : A \to A/\rho$ dané podmínkou $\pi_\rho(a) = [a]_\rho$.

Všimněme si, že je-li ρ ekvivalence na A, pak $A/\rho = \{[a]_\rho |\ a \in A\}$ tvoří rozklad množiny A. 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 $A/\rho = \{B_i |\ i \in I\}$.

Poznámka 1.12. *Nechť $G(\cdot)$ je grupa a H její podgrupa. Potom platí:*

(1) $\mathrm{rmod}\, H$ *i* $\mathrm{lmod}\, H$ *jsou ekvivalence na* G,
(2) $(a, b) \in \mathrm{rmod}\, H \Leftrightarrow (a^{-1}, b^{-1}) \in \mathrm{lmod}\, H$ *pro každé* $a, b \in G$,
(3) $|G/\mathrm{rmod}\, H)| = |G/\mathrm{lmod}\, H|$,
(4) $\mathrm{rmod}\, H = \mathrm{lmod}\, H$, *právě když je* H *normální podgrupa* $G(\cdot)$,

(5) $[a]_{\text{rmod } H} = Ha$ *a* $[a]_{\text{lmod } H} = aH$ *pro každé* $a \in G$,
(6) $|[a]_{\text{rmod } H}| = |[a]_{\text{lmod } H}| = |H|$ *pro každé* $a \in G$.

Důkaz. (1) Tvrzení dokážeme jen o rmod H, pro lmod H bude důkaz symetrický. Podle 1.9(1) podgrupa H obsahuje neutrální prvek 1, proto pro každé $a \in G$ máme $a \cdot a^{-1} = 1 \in H$, tedy $(a, a) \in \text{rmod } H$. Předpokládáme-li, že $(a, b) \in \text{rmod } H$, pak $a \cdot b^{-1} \in H$, proto i $b \cdot a^{-1} = (a \cdot b^{-1})^{-1} \in H$ (podle 1.4 a 1.6), tudíž $(b, a) \in \text{rmod } H$. Nyní předpokládejme, že $(a, b), (b, c) \in \text{rmod } H$, což podle definice naší relace znamená, že $a \cdot b^{-1}, b \cdot c^{-1} \in H$. Z uzavřenosti H na binární operaci plyne, že $(a \cdot b^{-1}) \cdot (b \cdot c^{-1}) \in H$, tedy $a \cdot c^{-1} = a \cdot b^{-1} \cdot b \cdot c^{-1} \in H$ a $(a, c) \in \text{rmod } H$. Tím jsme ověřili, že je relace rmod H reflexivním, symetrická a tranzitivní.

(2) Díky 1.6 máme rovnost $a \cdot b^{-1} = (a^{-1})^{-1} \cdot b^{-1}$, proto $a \cdot b^{-1} \in H \Leftrightarrow (a^{-1})^{-1} \cdot b^{-1} \in H$, čímž jsme dokončili důkaz.

(3) Podle (2) je zobrazení $[a]_{\text{rmod } H} \to [a^{-1}]_{\text{lmod } H}$ korektně definovanou bijekcí, tedy faktorové množiny $G/\text{rmod } H$ a $G/\text{lmod } H$ mají stejně prvků.

(4) Předpokládejme, že rmod H = lmod H a zvolme $h \in H$ a $g \in G$. Potom $(g \cdot h)^{-1} \cdot g = h^{-1} \cdot g^{-1} \cdot g = h^{-1} \in H$, tedy $(g \cdot h, g) \in \text{lmod } H = \text{rmod } H$. Z definice rmod H dostaneme $g \cdot h \cdot g^{-1} \in H$.

Nyní předpkládejme, že je H normální podgrupa grupy $G(\cdot)$. Zvolíme-li $(a, b) \in \text{rmod } H$, víme, že $a \cdot b^{-1} \in H$. Podle definice normální podgrupy $b^{-1} \cdot a = b^{-1} \cdot a \cdot b^{-1} \cdot (b^{-1})^{-1} \in H$, tedy $(b, a) \in \text{lmod } H$ a díky (1) $(a, b) \in \text{lmod } H$, čímž jsme ověřili, že rmod $H \subseteq$ lmod H. Symetrický argument dokazuje obrácenou implikaci.

(5) Opět se budeme věnovat jen ekvivalenci rmod H. Použijeme definici rozkladové třídy:

$$[a]_{\text{rmod } H} = \{b \in A |\ (a, b) \in \text{rmod } H\} = \{b \in A |\ \exists h \in H :\ a \cdot b^{-1} = h\} =$$
$$= \{b \in A |\ \exists h \in H :\ b = h^{-1} \cdot a\} = \{b \in A |\ \exists h' \in H :\ b = h' \cdot a\} = Ha.$$

(6) Definujme zobrazení $b : H \to Ha$ (resp. $H \to aH$) předpisem $b(h) = h \cdot a$ (resp. $b(h) = a \cdot h$). Zřejmě jde o zobrazení na Ha (resp. na aH) a předpokládejme, že $b(h_0) = b(h_1)$, tedy $h_0 \cdot a = h_1 \cdot a$. Tuto rovnost zprava (resp. zleva) přenásobíme hodnotou a^{-1}, abychom dostali $h_0 = h_0 \cdot a \cdot a^{-1} = h_1 \cdot a \cdot a^{-1} = h_1$. Tedy b je bijekce a všechny množiny H, aH, Ha mají stejný počet prvků. Nyní zbývá použít (5). □

Definice. Buď H podgrupa grupy $G(\cdot)$. Potom číslu $[G : H] = |G/\text{rmod } H|$ (= $|G/\text{lmod } H|$ podle 1.12) budeme říkat *index podgrupy* H v grupě G a velikosti $|G|$ množiny G budeme říkat *řád grupy* G.

Věta 1.13 (Lagrange)**.** *Je-li* H *podgrupa grupy* $G(\cdot)$*, pak* $|G| = [G : H] \cdot |H|$.

Důkaz. Podle 1.12(1) je rmod H ekvivalence, proto $G = \dot{\bigcup}_{A \in G/\text{rmod } H} A$, kde sjednocujeme disjunktní množiny. Využijeme-li dále poznatek 1.12(6), který říká, že všechny ekvivalenční třídy mají počet prvků stejný jako množina H, pak dostáváme

$$|G| = |\overset{\circ}{\bigcup}_{A \in G/\text{rmod } H} A| = \sum_{A \in G/\text{rmod } H} |A| = \sum_{A \in G/\text{rmod } H} |H| = [G : H] \cdot |H|.$$

□

Důsledek 1.14. *Je-li* G *konečná grupa, potom řád každé její podgrupy dělí řád grupy* G.

Všimněme si, že grupa prvočíselného řádu obsahuje jen triviální podgrupy.

Věta 1.15. *Nechť $G(\cdot)$ je grupa a ρ relace na G. Pak ρ je ekvivalence slučitelná s operací $\cdot$ právě tehdy, když $H = [1]_\rho$ je normální podgrupa $G(\cdot)$ a $\rho = \operatorname{rmod} H$.*

Důkaz. ($\Rightarrow$) Nejprve předpokládejme, že je ρ je ekvivalence slučitelná s operací $\cdot$. Protože je ρ reflexivní relace, leží 1 v třídě $[1]_\rho$ a ta je tudíž neprázdná. Zvolme $a, b \in [1]_\rho$ a $g \in G$. Vidíme, že $(1, a), (1, b) \in \rho$, navíc, z reflexivity ρ plyne, že $(a^{-1}, a^{-1}), (g^{-1}, g^{-1}), (g, g) \in \rho$. Nyní využijeme slučitelnosti ρ s $\cdot$, abychom dostali, že $(1 \cdot 1, a \cdot b) \in \rho$, dále že $(1 \cdot a^{-1}, a \cdot a^{-1}) \in \rho$ a $(g \cdot 1 \cdot g^{-1}, g \cdot a \cdot g^{-1}) \in \rho$. Využijeme-li vlastností neutrálního prvku a symetrie ρ, vidíme, že $(1, a \cdot b), (1, a^{-1}), (1, g \cdot a \cdot g^{-1}) \in \rho$, tedy $a \cdot b,\ a^{-1},\ g \cdot a \cdot g^{-1} \in [1]_\rho$, čímž máme ověřeno, že je $[1]_\rho$ normální podgrupa $G(\cdot)$. Připomeňme, že podle 1.12(4) $\operatorname{rmod} [1]_\rho = \operatorname{lmod} [1]_\rho$.

Nyní bychom měli dokázat, že $(a, b) \in \rho$, právě když $(a, b) \in \operatorname{lmod} [1]_\rho$. Jestliže nejprve $(a, b) \in \rho$, potom $(1, a^{-1} \cdot b) = (a^{-1} \cdot a, a^{-1} \cdot b) \in \rho$, protože je ρ ekvivalnce slučitelná s $\cdot$, tedy $(a, b) \in \operatorname{lmod} [1]_\rho$. Naopak, zvolíme-li $(a, b) \in \operatorname{lmod} [1]_\rho$, pak $(a, b) = (a \cdot 1, a \cdot a^{-1} \cdot b) \in \rho$.

($\Leftarrow$) Předpokládejme, že je H normální podgrupa $G(\cdot)$ a definujme relaci ρ jako $\operatorname{rmod} H$ (tj. $(a, b) \in \rho \leftrightarrow a \cdot b^{-1} \in H$). Podle 1.12(1) je ρ ekvivalence a přímým výpočtem zjistíme, že $[1]_\rho = H$. Zvolme nyní $(a_0, b_0), (a_1, b_1) \in \rho$, tj. $a_0 \cdot b_0^{-1}$ i $a_1 \cdot b_1^{-1}$ jsou prvky H. Nyní použijeme normalitu H, abychom dostali, že $b_0^{-1} \cdot a_0 = b_0^{-1} \cdot (a_0 \cdot b_0^{-1}) \cdot b_0 \in H$. Uzavřenost H na $\cdot$ zaručuje, že $b_0^{-1} \cdot a_0 \cdot a_1 \cdot b_1^{-1} \in H$ a dalším využitím normality získáme $a_0 \cdot a_1 \cdot (b_0 \cdot b_1)^{-1} = b_0 \cdot (b_0^{-1} \cdot a_0 \cdot a_1 \cdot b_1^{-1}) \cdot b_0^{-1} \in H$, tedy $(a_0 \cdot a_1, b_0 \cdot b_1) \in \rho$, čímž jsme ověřili slučitelnost ρ s s operací $\cdot$. □

Poznámka 1.16. *Nechť $G(\cdot)$ a $H(\cdot)$ jsou grupy a $f : G \to H$ je zobrazení slučitelné s operací $\cdot$. Pak je $f(1) = 1$ a $f(g^{-1}) = (f(g))^{-1}$ pro každé $g \in G$.*

Důkaz. Protože $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$, stačí rovnost $f(1) = f(1) \cdot f(1)$ přenásobit prvkem $f(1)^{-1}$, abychom dostali $1 = f(1) \cdot f(1)^{-1} = f(1) \cdot f(1) \cdot f(1)^{-1} = f(1)$. Dále $1 = f(1) = f(g^{-1} \cdot g) = f(g^{-1}) \cdot f(g)$ a podobně $1 = f(g) \cdot f(g^{-1})$, proto $f(g^{-1}) = (f(g))^{-1}$. □

Definice. Zobrazení $f : G \to H$ grup $G(\cdot)$ a $H(\cdot)$ slučitelné s jejich binárními operacemi se nazývá (grupový) *homomorfismus*. Bijektivní homomorfismus budeme nazývat *izomorfismus*. Podmnožině $\operatorname{Ker} f = \{g \in G |\ f(g) = 1\}$ i relaci $\ker f = \{(g_1, g_2) \in G \times G |\ f(g_1) = f(g_2)\}$ budeme říkat *jádro homomorfismu*.

Jestliže mezi dvěma grupami G_1 a G_2 existuje izomorfismus, říkáme, že G_1 a G_2 jsou *izomorfní* a píšeme $G_1 \cong G_2$.

Poznámka 1.17. *Nechť $G_1(\cdot)$, $G_2(\cdot)$ a $G_3(\cdot)$ jsou grupy, $f : G_1 \to G_2$ a $g : G_2 \to G_3$ jsou homomorfismy a H podgrupa grupy $G_2(\cdot)$.*

(1) *gf je také homomorfismus,*
(2) *je-li f bijekce, pak f^{-1} je izomorfismus,*
(3) *obraz $g(H)$ je podgrupa $G_3(\cdot)$ a úplný vzor $f^{-1}(H)$ je podgrupa $G_1(\cdot)$,*
(4) *$\operatorname{Ker} f$ je normální podgrupa $G_1(\cdot)$ a $\ker f = \operatorname{rmod} \operatorname{Ker} f$,*
(5) *$\ker f$ je ekvivalence slučitelná s operací $\cdot$ na G_1,*

Důkaz. (1) Je-li $a, b \in G_1$, pak $gf(a \cdot b) = g(f(a) \cdot f(b)) = g(f(a)) \cdot g(f(b))$.

(2) Stačí ověřit, že f^{-1} je homomorfismus. Zvolíme-li $c, d \in G_2$, potom $f(f^{-1}(c) \cdot f^{-1}(d)) = c \cdot d$, proto $f^{-1}(c) \cdot f^{-1}(d) = f^{-1}(c \cdot d)$.

(3) Nejprve ukážeme, že je $g(H)$ podgrupa $G_3(\cdot)$. $g(H)$ je zjevně neprázdná množina. Vezměme $u, v \in g(H)$, tj. existují $c, d \in H$, pro která $g(c) = u$ a $g(d) = v$. Protože $c \cdot d,\ c^{-1} \in H$, dostáváme přímo z definice, že $u \cdot v = g(c) \cdot g(d) = g(c \cdot d) \in g(H)$, a $u^{-1} = g(c)^{-1} = g(c^{-1}) \in g(H)$ podle 1.16.

Poznamenejme, že $1 \in f^{-1}(H)$, tedy jde o neprázdnou množinu a zvolme $a, b \in f^{-1}(H)$, tj. $f(a), f(b) \in H$. Potom opět $f(a) \cdot f(b) = f(a \cdot b) \in H$, a $f(a^{-1}) = f(a)^{-1} \in H$, tedy $a \cdot b,\ a^{-1} \in f^{-1}(H)$, tedy $f^{-1}(H)$ je podgrupa.

(4) Protože $\{1\}$ je podgrupa $G_2(\cdot)$ a $\mathrm{Ker} f = f^{-1}(\{1\})$, je $\mathrm{Ker} f$ podgrupa podle (3). Vezmeme-li libovolné $g \in G_1$ a $h \in \mathrm{Ker} f$, potom $f(g \cdot h \cdot g^{-1}) = f(g) \cdot f(h) \cdot f(g^{-1}) = f(g) \cdot 1 \cdot f(g)^{-1} = 1$, tedy $g \cdot h \cdot g^{-1} \in \mathrm{Ker} f$. Zbývá si uvědomit, že $f(a) = f(b) \Leftrightarrow f(a) \cdot f(b)^{-1} = 1 \Leftrightarrow f(a \cdot b^{-1}) = 1 \Leftrightarrow a \cdot b^{-1} \in \mathrm{Ker} f$.

(5) Plyne okamžitě z (4) a 1.15. □

Věta 1.18. *Nechť $G(\cdot)$ je grupa a ρ ekvivalence na G slučitelná s $\cdot$. Na faktorové množině G/ρ definujeme operaci $\odot$ předpisem $[a]_\rho \odot [b]_\rho = [a \cdot b]_\rho$. Tato definice je korektní, $G/\rho(\odot)$ je opět grupa a přirozená projekce π_ρ je homomorfismus.*

Důkaz. Abychom ověřili korektnost definice, musí ukázat, že definice nezávisí na volbě zástupce ekvivalenčních tříd. Mějme tedy $[a]_\rho = [c]_\rho$ a $[b]_\rho = [d]_\rho$, tj. (a, c), $(b, d) \in \rho$. Potom díky slučitelnosti ρ s operací máme $(a \cdot b, c \cdot d) \in \rho$, proto $[a \cdot b]_\rho = [c \cdot d]_\rho$.

Vezmeme-li $[a]_\rho, [b]_\rho, [c]_\rho \in \rho$, pak přímo z definice vidíme, že

$$[a]_\rho \odot ([b]_\rho \odot [c]_\rho]) = [a \cdot (b \cdot c)]_\rho = [(a \cdot b) \cdot c]_\rho = ([a]_\rho \odot [b]_\rho) \odot [c]_\rho,$$

tedy operace $\odot$ je asociativní. To, že je neutrálním prvkem právě $[1]_\rho$ a inverzním prvkem k prvku $[a]_\rho$ právě prvek $[a^{-1}]_\rho$, dostaneme přímým výpočtem. Konečně $\pi_\rho(a \cdot b) = [a \cdot b]_\rho = [a]_\rho \odot [b]_\rho = \pi_\rho(a) \odot \pi_\rho(b)$ z definice. □

Grupu zavedenou na faktorové množině budeme nazývat faktorovou grupou. Věta 1.15, která říká, že každé ekvivalenci ρ slučitelné s binární operací na grupě jednoznačně odpovídá normální podgrupa H, nám umožňuje faktorovou množinu zapisovat ve tvaru G/H, navíc je běžné, že se operace na faktorové grupě označuje stejně jako operace na původní grupě. Obvyklý zápis faktorové grupy $G/\rho(\odot)$ bude tedy $G/H(\cdot)$, kde $H = [1]_\rho$ a $[a]_\rho \cdot [b]_\rho = [a \cdot b]_\rho$. Podobně budeme přirozenou projekci G na G/H označovat symbolem π_H a místo $[a]_\rho$ budeme psát $[a]_H$.

Příklad 1.19. Uvážíme-li na grupě $\mathbf{Z}(+)$ ekvivalenci $\sim_n$ zavedenou v Příkladu 0.3, jedná se o ekvivalenci slučitelnou s operací $+$ a $[0]_{\sim_n} = n\mathbf{Z}$, proto $\sim_n = \mathrm{rmod}\ n\mathbf{Z}$ a na faktorové množině $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}/\sim_n$ máme dobře zavedenu strukturu grupy $\mathbf{Z}/n\mathbf{Z}(+)$ předpisem $[a]_{\sim_n} + [b]_{\sim_n} = [a + b]_{\sim_n}$.

Poznámka 1.20 (Věta o homomorfismu)**.** *Buď $f : G_1 \to G_2$ homomorfismus grup $G_1(\cdot)$ a $G_2(\cdot)$ a nechť H je normální podgrupa $G_1(\cdot)$. Pak existuje homomorfismus $g : G_1/H \to G_2$ splňující podmínku $g\pi_H = f$ právě tehdy, když $H \subseteq \mathrm{Ker} f$ (tj. $\mathrm{rmod} H \subseteq \mathrm{rmod}\ \mathrm{Ker} f$). Navíc, jestliže g existuje, je g izomorfismus, právě když f je na a $\mathrm{Ker} f = H$.*

Důkaz. Nejprve předpokládejme, že existuje homomorfismus $g : G_1/H \to G_2$ splňující $g\pi_H = f$, tedy $g([a]_H) = f(a)$. Zvolme $a \in H$. Pak $[a]_H = H = [1]_H$ je neutrální prvek grupy $G_1/H(\cdot)$, a proto $f(a) = g([a]_H) = 1$ podle 1.16. Tedy $a \in \mathrm{Ker} f$, čímž jsme ověřili, že $H \subseteq \mathrm{Ker} f$.

Naopak, nechť $H \subseteq \mathrm{Ker}f$. Musíme ověřit, že jediná možná definice g daná předpisem $g([a]_H) = f(a)$ je korektní. Vezměme proto $[a]_H = [b]_H$. Potom $a \cdot b^{-1} \in H \subseteq \mathrm{Ker}f$, tedy $1 = f(a \cdot b^{-1}) = f(a) \cdot f(b)^{-1}$ podle 1.16, a proto $f(a) = f(b)$. Konečně

$$g([a]_H \cdot [b]_H) = g([a \cdot b]_H) = f(a \cdot b) = f(a) \cdot f(b) = g([a]_H) \cdot g([b]_H),$$

tedy g je homomorfismus.

Zbývá ověřit závěrečnou ekvivalenci. Předně si uvědomme, že $g(G_1/H) = f(G_1)$, tedy g je na, právě když je f na. Nechť je g navíc prosté a zvolme $a \in \mathrm{Ker}f$. Pak $g([a]_H) = f(a) = 1$. Protože $g([1]_H) = g(H) = 1$, plyne z prostoty g, že $[a]_H = H$, tedy $a \in H$. Ověřili jsme, že $\mathrm{Ker}f \subseteq H$, a protože už víme, že $H \subseteq \mathrm{Ker}f$, máme rovnost $H = \mathrm{Ker}f$. Konečně předpokládejme, že $g([a]_H) = g([b]_H)$. Potom $f(a) = f(b)$ a $a \cdot b^{-1} \in \mathrm{Ker}f = H$. Tudíž $(a, b) \in \mathrm{rmod}H$ a $[a]_H = [b]_H$, čímž jsme ověřili, že je g prosté. □

Věta 1.21 (1. věta o izomorfismu)**.** *Nechť $f : G_1 \to G_2$ homomorfismus grup $G_1(\cdot)$ a $G_2(\cdot)$. Pak $f(G_1)$ je podgrupa G_2 (tedy opět grupa) a $G_1/\mathrm{Ker}f(\cdot)$ je izomorfní $f(G_1)(\cdot)$.*

Důkaz. Z 1.17(3) dostáváme, že $f(G_1)$ je podgrupa G_2. Omezíme-li obor hodnot zobrazení f, můžeme ho chápat jako homomorfismus $f : G_1 \to f(G_1)$. Nyní aplikujeme 1.20 pro $H = \mathrm{Ker}f$ a dostaneme přímo požadovaný izomorfismus $g : G_1/\mathrm{Ker}f \to f(G_1)$. □

Příklad 1.22. Mějme homomorfismus $f_n : \mathbf{Z} \to \mathbf{Z}_n$ grupy $\mathbf{Z}(+)$ do grupy $\mathbf{Z}_n(+)$ s počítáním modulo n daný předpisem $f_n(k) = (k) mod\ n$. Pak máme podle 1.21 izomorfismus $\mathbf{Z}/\mathrm{Ker}\ f_n(+) \cong \mathbf{Z}_n(+)$, navíc je zjevně $(a, b) \in ker\ f_n$, právě když $n/(a - b)$, a $\mathrm{Ker}\ f_n = n\mathbf{Z}$.

Věta 1.23 (2. věta o izomorfismu)**.** *Nechť $G(\cdot)$ je grupa a H, K její normální podgrupy. Jestliže $H \subseteq K$, pak K/H je normální podgrupa grupy $G/H(\cdot)$ a faktorová grupa $G/K(\cdot)$ je izomorfní grupě $(G/H)/(K/H)(\cdot)$.*

Důkaz. Opět nejprve použijeme 1.20 pro homomorfismy $\pi_K : G \to G/K$ (jako f z 1.20) a $\pi_H : G \to G/H$ (jako π_H z 1.20). Protože podle předpokladu $H \subseteq K = \mathrm{Ker}\pi_K$, dává nám 1.20 homomorfismus $g : G/H \to G/K$ splňující vztah $g([a]_H) = [a]_K$. Všimněme si, že je g zjevně na. Nyní přímočaře spočítáme $\mathrm{Ker}g = \{[a]_H \in G/H |\ g([a]_H) = [a]_K = [1]_K\} = K/H$. Poznamenejme, že je $\mathrm{Ker}g = K/H$ normální podgrupa $G/H(\cdot)$ podle 1.17(3). Nyní pro homomorfismus g využijeme 1.21, abychom dostali $G/K = g(G/H) \cong (G/H)/\mathrm{Ker}g = (G/H)/(K/H)$. □

2. Cyklické grupy

Připomeňme, že podle 1.9(3) je průnik libovolného systému podgrup zase podgrupou. Uvážíme-li grupu $G(\cdot)$ a podmnožinu $X \subseteq G$, pak průnik všech podgrup $G(\cdot)$ obsahujících X je rovněž podgrupou obsahující X, označme ho $\langle X \rangle$, zjevně se jedná o nejmenší takovou podgrupu vzhledem k inkluzi. Speciálně budeme psát $\langle g \rangle$ místo $\langle \{g\} \rangle$, je-li $g \in G$.

Definice. Buď $G(\cdot)$ grupa a $X \subseteq G$. Podgrupu $\langle X \rangle$ nazveme podgrupu $G(\cdot)$ *generovanou* množinou X. Řekneme, že $G(\cdot)$ je *cyklická grupa*, existuje-li takový prvek $g \in G$, že $\langle g \rangle = G$.

Nechť $G(\cdot)$ je grupa $a \in G$. Definujme indukcí:

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

Poznámka 2.1. *Nechť $G(\cdot)$ je grupa a $a \in G$. Zobrazení $\phi : \mathbf{Z} \to G$ dané předpisem $\phi(n) = a^n$ je homomorfismus grupy $\mathbf{Z}(+)$ do grupy $G(\cdot)$ a $\phi(\mathbf{Z}) = \langle a \rangle = \{a^n |\ n \in \mathbf{Z}\}$.*

Důkaz. Potřebujeme pro každou dvojici $m, n \in \mathbf{Z}$ ověřit, že $\phi(n+m) = a^{n+m} = a^n \cdot a^m = \phi(n) \cdot \phi(m)$. Přitom $a^{n+m} = a^n \cdot a^m$ zjevně platí pro obě nezáporná a obě záporná m, n. Je-li n záporné a $m+n$ nezáporné, pak $a^n \cdot a^m = (a^{-1})^{-n} \cdot a^m = a^{n+m}$. Podobně pro n záporné, m kladné a $m+n$ záporné máme $a^n \cdot a^m = (a^{-1})^{-n} \cdot a^m = (a^{-1})^{-n-m} = a^{n+m}$.

Závěrem poznamenejme, že $\phi(\mathbf{Z})$ je právě tvaru $\phi(\mathbf{Z}) = \{a^n |\ n \in \mathbf{Z}\}$, a proto se jedná o nejmenší podgrupu $G(\cdot)$ obsahující a. □

Důsledek 2.2. *Nechť $G(\cdot)$ je grupa $a \in G$. Potom pro každé $n, m \in \mathbf{Z}$ platí, že $a^{-n} = (a^n)^{-1}$ a $(a^n)^m = a^{nm}$.*

Příklad 2.3. (1) $\mathbf{Z}(+)$ je cyklická grupa, kde $\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

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

Věta 2.4. *Buď $G(\cdot)$ cyklická grupa.*

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

Důkaz. Vezměme nějaký generátor g cyklické grupy $G(\cdot)$, tedy $\langle g \rangle = G$ a definujme zobrazení $\phi : \mathbf{Z} \to G$ dané předpisem $\phi(n) = g^n$. Podle 2.1 jde o homomorfismus a $\phi(\mathbf{Z}) = \langle g \rangle = G$, tedy ϕ je zobrazení na. Nyní podle 1.21 je $\mathbf{Z}/\mathrm{Ker}\phi(+) \cong G(\cdot)$. Zbývá si rozmyslet, jak vypadá $\mathbf{Z}/\mathrm{Ker}\phi$. Z 1.10(2) víme, že $\mathrm{Ker}\phi = n\mathbf{Z}$ pro vhodné nezáporné celé n. V případě, že $n = 0$, pak $\mathbf{Z}/\mathrm{Ker}\phi = \mathbf{Z}/\{0\} \cong \mathbf{Z}$, a v případě kladného n je $\mathbf{Z}/\mathrm{Ker}\phi = \mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$ podle 1.22. □

Poznámka 2.5. *Každá faktorová grupa i podgrupa cyklické grupy je opět cyklická.*

Důkaz. Snadno nahlédneme, že je-li g generátor cyklické grupy $G(\cdot)$, pak $[g]_H$ je generátor její faktorové grupy $G/H(\cdot)$.

Díky 2.4 stačí tvrzení o podgrupách dokázat pro grupy $\mathbf{Z}(+)$ a $\mathbf{Z}_n(+)$. Nejprve ho dokažme pro grupu $\mathbf{Z}(+)$. V 1.10(2) jsme ověřili, že $\mathbf{Z}(+)$ jiné podgrupy než podgrupy tvaru $n\mathbf{Z}$ neobsahuje. Přitom $\langle n \rangle = n\mathbf{Z}$ je cyklická grupa, čímž je tvrzení ověřeno.

Nyní využijeme homomorfismu $f_n : \mathbf{Z} \to \mathbf{Z}_n$ z 1.22. Zvolíme-li podgrupu H grupy $\mathbf{Z}_n(+)$, pak $f_n^{-1}(H)$ je podle předchozí úvahy a 1.17(3) cyklická podgrupa $\mathbf{Z}$, tedy $H = f_n(f_n^{-1}(H))$ je cyklická podgrupa $\mathbf{Z}_n(+)$. □

Poznámka 2.6. *Buď $G(\cdot)$ konečná grupa. Potom $g^{|G|} = 1$ pro každý prvek $g \in G$.*

Důkaz. $\langle g \rangle$ je cyklická grupa řádu n, tedy je podle 2.4 izomorfní $\mathbf{Z}_n(+)$, proto $g^n = 1$. Podle 1.13 $n/|G|$, tedy $g^{|G|} = (g^n)^{\frac{|G|}{n}} = 1^{\frac{|G|}{n}} = 1$, kde 1. rovnost plyne z 2.2. □

Věta 2.7. *Nechť $G(\cdot)$ je konečná cyklická grupa. Pak pro každé přirozené k, které dělí řád grupy G, existuje právě jedna podgrupa grupy G řádu k.*

Důkaz. K důkazu využijeme charakterizace cyklických grup 2.4, díky němuž stačí tvrzení dokázat pro (izomorfní) grupu $\mathbf{Z}_n(+)$. Jestliže $k = 1$, je tvrzení triviální, předpokládejme tedy, že $k > 1$. Potom snadno nahlédneme, že množina $\langle \frac{n}{k} \rangle = \{0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}\}$ je podgrupa a $|\langle \frac{n}{k} \rangle| = k$. Mějme nyní nějakou podgrupu H grupy $\mathbf{Z}_n(+)$ řádu k. Podle 2.6 $(k \cdot h)\mathrm{mod}\ n = 0$, proto $k \cdot h = c \cdot n$ pro vhodné celé číslo c. Tedy $h = c \cdot \frac{n}{k}$. Tím jsme ověřili, že H je částí podgrupy $\langle \frac{n}{k} \rangle$. Protože se jedná o dvě konečné stejně velké množiny, dostáváme, že $H = \langle \frac{n}{k} \rangle$, čímž jsme ověřili jednoznačnost volby. □

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 2.8. *Nechť $n \in \mathbf{N}$, $a \in \mathbf{Z}_n \setminus \{0\}$ 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 generuje grupu $\mathbf{Z}_n(+)$), právě když $NSD(a, n) = 1$.*

Důkaz. Nejprve předpokládejme, že $a\mathbf{Z}_n = k\mathbf{Z}_n$. Potom $k \in a\mathbf{Z}_n$, tedy existuje celé x, pro které $(a \cdot x)\mathrm{mod}\ n = k$. Proto také existuje takové celé y, že $a \cdot x + n \cdot y = k$. Odtud plyne, že $\mathrm{NSD}(a, n)/k$. Podobně, protože $a \in k\mathbf{Z}_n$ existují celá u a v, pro něž $k \cdot u + n \cdot v = a$, a protože k/n, nutně musí k/a. Vidíme, že $k/\mathrm{NSD}(a, n)$, tudíž $\mathrm{NSD}(a, n) = k$.

Nyní předpokládejme, že $\mathrm{NSD}(a, n) = k$. Potom díky Euklidovu algoritmu existují $x \in \mathbf{Z}_n$ a celé y, pro něž $a \cdot x + n \cdot y = k$. Proto $(a \cdot x)\mathrm{mod}\ n = k$, tudíž $k \in a\mathbf{Z}_n$ a $k\mathbf{Z}_n \subseteq a\mathbf{Z}_n$. Konečně, protože k/a, vidíme, že $a \in k\mathbf{Z}_n$, a proto $a\mathbf{Z}_n \subseteq k\mathbf{Z}_n$, což znamená, že $k\mathbf{Z}_n = a\mathbf{Z}_n$. □

Důsledek 2.9. *Je-li $n \in \mathbf{N}$, pak číslo $\varphi(n)$ udává počet prvků, které generují grupu $\mathbf{Z}_n(+)$ a počet invertibilních prvků monoidu $\mathbf{Z}_n(\cdot)$.*

Příklad 2.10. (1) Uvažujme konečnou cyklickou grupu $G(\cdot)$. Potom nám 2.9 říká, že $G(\cdot)$ obsahuje právě $\varphi(|G|)$ generátorů, a podle 2.7 $G(\cdot)$ obsahuje právě tolik podgrup, kolik je dělitelů jejího řádu.

(2) Vezměme cyklickou grupu $\mathbf{Z}_{50}(+)$. V bodu (1) jsme nahlédli, že $\mathbf{Z}_{50}(+)$ obsahuje $\varphi(50) = 20$ generátorů a právě 6 podgrup. Vezmeme-li například podgrupu $\langle 42 \rangle$ grupy $\mathbf{Z}_{50}(+)$ (a jiné než cyklické podgrupy tato grupa podle 2.5 neobsahuje), pak díky 2.8 víme, že $\langle 42 \rangle = \langle \mathrm{NSD}(42, 50) \rangle = \langle 2 \rangle = 2\mathbf{Z}_{50}$, a jedná se tedy o podgrupu řádu $25 = \frac{50}{2}$.

Věta 2.11 (Malá Fermatova věta)**.** *Pro nesoudělná kladná celá čísla $a, n > 1$ je $(a^{\varphi(n)})\mathrm{mod}\ n = 1$.*

Důkaz. Nejprve uvážíme, že $(a^{\varphi(n)})\mathrm{mod}\ n = ((a)\mathrm{mod}\ n^{\varphi(n)})\mathrm{mod}\ n$, což znamená, že tvrzení stačí dokázat pro $a < n$. Nyní vezmem jako grupu G z 2.6 grupu invertibillních prvků $\mathbf{Z}_n^*(\cdot)$ monoidu $\mathbf{Z}_n(\cdot)$ tj. prvků nesoudělných s n podle 2.9. Protože $a \in \mathbf{Z}_n^*$, je $(a^{\varphi(n)})\mathrm{mod}\ n = (a^{|\mathbf{Z}_n^*|})\mathrm{mod}\ n = 1$ díky 2.6 a 2.9. □

Poznámka 2.12. *Buď p a q dvě různá lichá prvočísla a $m = \mathrm{nsn}(p - 1, q - 1)$. Potom pro každé $a \in \mathbf{Z}_{pq}$ platí, že $(a^{m+1})\mathrm{mod}\ \mathrm{pq} = \mathrm{a}$.*

Důkaz. Podle 2.11 (x^m)mod p = 1 a (y^m)mod q = 1 pro x, která nejsou násobkem p a y, která nejsou násobkem q. Dále zřejmě platí $((up)^{m+1})$modp = 0 a proto i (x^{m+1})mod p = (x)mod p a (y^{m+1})mod q = (y)mod q pro každé nezáporné celé x a y. Vezměme nyni $a \in \mathbf{Z}_{pq}$. Z předchozího pozorování plyne, že $((a)\text{mod } p, (a)\text{mod } q) = ((a^{m+1})\text{mod } p, (a^{m+1})\text{mod } q)$, a díky Větě 0.5 použité pro bijekci $\mathbf{Z}_{pq} \to \mathbf{Z}_p \times \mathbf{Z}_q$ dostáváme, že shodné jsou i vzory prvků $((a)\text{mod } p, (a)\text{mod } q)$ a $((a^{m+1})\text{mod } p, (a^{m+1})\text{mod } q)$, tedy, že (a^{m+1})mod pq = a. □

Příklad 2.13 (Rivest, Shamir, Adleman)**.** Opět zvolme p a q dvě různá lichá prvočísla a položme $m = \text{nsn}(p-1, q-1)$. Indukcí díky 2.12 a 2.2 dostaneme, že $a^{um+1} = a^{(u-1)m} \cdot a^{m+1} = a^{(u-1)m+1} = a$ pro každé $u \in \mathbf{N}$ a $a \in \mathbf{Z}_{pq}$.

Vezměme $e < m$ 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. Položíme-li $n = p \cdot q$, je veřejným klíčem je dvojice čísel (pq, e) a soukromý klíč tvoří *tajný exponent* d. Chceme-li informaci vyjádřenou posloupností hodnot $a_1, \ldots, a_k \in \mathbf{Z}_{pq}$ 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 $pq, \ldots, (a_k^e)$mod pq. K jejímu rozluštění stačí umocnit v $\mathbf{Z}_{pq}(\cdot, 1)$ pomocí tajného exponentu, protože $(a_i^e)^d = a_i^{ed} = a_i$. Naopak, zveřejnění-li majitel soukromého klíče zašifrovanou zprávu $(a_1^d)mod\ pq, \ldots,$ $(a_k^d)mod\ pq$, mohou si příjemci zprávy stejným způsobem (tj. umocněním na veřejně známý exponent e: $((a_1^d)^e)mod\ pq, \ldots, ((a_k^d)^e)mod\ pq = a_1, \ldots, a_k$) 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), zatímco 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 2.14. *Nechť $T(+, \cdot)$ je komutativní těleso a nechť G je konečná podgrupa multiplikativní grupy $T \setminus \{0\}(\cdot, ^{-1}, 1)$. Potom G je cyklická grupa.*

3. Univerzální pohled: pojem algebry

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*.

1-ární operace se obvykle nazývají unárními operacemi, 2-árním operacím se říká binární operace a 3-ární se nazývají ternárními operacemi. Uvědomme si, že nulární operace vyznačuje v algebře jeden její prvek, proto ji můžeme se tímto vyznačeným prvkem ztotožnit.

Příklad 3.1. (1) Uvážíme-li grupu $G(\cdot)$ s unární operací inverzního prvku $^{-1}$ a nulární operací 1, pak $G(\cdot)$, $G(\cdot,^{-1})$, $G(\cdot,^{-1},1)$ tvoří (formálně různé) příklady algeber.

(2) 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, jestliže $\alpha(a_1,\dots,a_n)\in B$ pro všechna $a_1,\dots,a_n\in B$. Řekneme, že $B\subseteq A$ je *podalgebra* algebry $A(\alpha_i|\ i\in I)$, je-li 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.

Definice. Nechť symbol α označuje n-ární operaci na množině A i B. Řekneme, že zobrazení $f:A\to B$ je *slučitelné s operací* α, jestliže $f(\alpha(a_1,\dots,a_n))=\alpha(f(a_1),\dots,f(a_n))$. 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*, je-li slučitelné se všemi operacemi α_i, $i\in I$. Bijektivní homomorfismus budeme nazývat *izomorfismus*. Jestliže mezi dvěma algebrami A a B existuje izomorfismus, říkáme, že A a B jsou *izomorfní* a píšeme $A\cong B$.

Příklad 3.2. (1) Buď $G_i(\cdot)$ pro $i=1,2$ grupy s unární operací inverzního prvku $^{-1}$ a nulární operací 1. pak každý homomorfimus grup $G_1(\cdot)$ a $G_2(\cdot)$ je podle 1.16 homomorfismem algeber $G_1(\cdot)$ a $G_2(\cdot)$, $G_1(\cdot,^{-1})$ a $G_2(\cdot^{-1})$ i $G_1(\cdot,^{-1},1)$ a $G_2(\cdot^{-1},1)$

(2) Nechť U a V jsou dva vektorové prostory nad tělesem T. Potom každé lineární zobrazení (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 $T(\cdot)$ (poznamenejme, že se jedná právě o monoidy).

Definice. Nechť ρ je relace a α je n-ární operace na množině A. Řekneme, že ρ je *slučitelná s* α, jestliže pro každý systém prvků $a_1,\dots,a_n,b_1\dots,b_n\in A$, pro které $(a_i,b_i)\in\rho$, $i=1,\dots,n$, platí, že $(\alpha(a_1,\dots,a_n),\alpha(b_1,\dots,b_n))\in\rho$. Je-li $A(\alpha_i|\ i\in I)$ algebra a ρ ekvivalence na množině A, pak ρ nazveme *kongruencí*, je-li ρ slučitelná se všemi operacemi α_i, $i\in I$.

Příklad 3.3. (1) id a $A\times A$ jsou kongruence na libovolné algebře A.

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

(3) Ekvivalence slučitelná s operací $\cdot$ na grupě $G(\cdot)$ je kongruencí algeber $G(\cdot)$, $G(\cdot,^{-1})$ a $G(\cdot,^{-1},1)$.

Připomeňme, že je-li $f:A\to B$ zobrazení, rozumíme jeho *jádrem* $\ker f$ relaci danou předpisem: $(a,b)\in ker\ f\Leftrightarrow f(a)=f(b)$. Nyní jsme připraveni vyslovit obdobu Poznámky 1.17 pro obecné algebry:

Poznámka 3.4. *Nechť $A_1(\alpha_i|\ i\in I)$, $A_2(\alpha_i|\ i\in I)$ a $A_3(\alpha_i|\ i\in I)$ jsou algebry stejného typu, $f:A_1\to A_2$ a $g:A_2\to A_3$ jsou homomorfismy a B je podalgebra algebry $A_2(\cdot)$.*

(1) *gf je také homomorfismus,*
(2) *je-li f bijekce, pak f^{-1} je izomorfismus,*
(3) *obraz $g(B)$ je podalgebra algebry $A_3(\alpha_i|\ i \in I)$ a úplný vzor $f^{-1}(B)$ je podalgebra algebry $A_1(\alpha_i|\ i \in I)$,*
(4) *$\ker f$ je kongruence na algebře $A_1(\alpha_i|\ i \in I)$.*

Důkaz. Důkaz je snadným zobecněním důkazu příslušných bodů 1.17.

(1) Je-li α_i n-ární operace na A_1, A_2 a A_3 a vezmeme-li $a_1, \dots a_n \in A_1$, pak $gf(\alpha_i(a_1, \dots a_n)) = g(\alpha_i(f(a_1), \dots f(a_n))) = \alpha_i(gf(a_1), \dots gf(a_n))$.

(2) Stačí opět ověřit, že f^{-1} je homomorfismus. Zvolíme-li libovolně n-ární operaci α_i a prvky $a_1, \dots a_n \in A_2$, potom $f(\alpha_i(f^{-1}(a_1), \dots, f^{-1}(a_n))) = \alpha_i(a_1, \dots a_n)$, proto $\alpha_i(f^{-1}(a_1), \dots, f^{-1}(a_n)) = f^{-1}(\alpha_i(a_1, \dots a_n))$.

(3) Nechť je opět α_i libovolná n-ární operace na A_2 i A_3. Vezměme nejprve $c_1, \dots c_n \in g(B)$, tj. existují $b_1, \dots b_n \in B$, pro která $g(b_j) = c_j$, $j = 1, \dots, n$. Protože $\alpha_i(b_1, \dots b_n) \in B$, dostáváme bezprostředně z definice, že $\alpha_i(c_1, \dots c_n) = \alpha_i(g(b_1), \dots g(b_n)) = g(\alpha_i(b_1, \dots b_n)) \in g(B)$.

Nyní zvolme $a_1, \dots a_n \in f^{-1}(B)$, tj. $f(a_j) \in B$. Potom $f(\alpha_i(a_1, \dots a_n)) = \alpha_i(f(a_1), \dots f(a_n)) \in B$.

(4) Vezměme n-ární operaci α_i na A_1 a A_2 a prvky $a_1, \dots a_n, b_1, \dots b_n \in A_1$, o nichž víme, že $(a_j, b_j) \in \ker f$, tedy $f(a_j) = f(b_j)$, pro každé $j = 1 \dots n$. Potom z definice homomorfismu dostaneme rovnost

$$f(\alpha_i(a_1, \dots a_n)) = \alpha_i(f(a_1), \dots f(a_n)) = \alpha_i(f(b_1), \dots f(b_n)) = f(\alpha_i(b_1, \dots b_n)),$$

čímž jsme ověřili, že $(\alpha_i(a_1, \dots a_n), \alpha_i(b_1, \dots b_n)) \in \ker f$. Že se jedná o ekvivalenci je snadné cvičení. □

Poznámka 3.5. *Nechť $A(\alpha_i|\ i \in I)$ je algebra a A_j jsou podalgebray A a ρ_j ekvivalence na A pro každé $j \in J$.*

(1) *$\bigcap_{j\in J} A_j$ je podalgebra A,*
(2) *jsou-li ρ_j kongruence na A, pak i $\bigcap_{j\in J} \rho_j$ je kongruence.*

Důkaz. (1) Obdoba Poznámky 1.9(3). Nechť α_i je libovolná n-ární operace na A a $a_1, \dots a_n \in \bigcap_{j\in J} A_j$. Protože $\bigcap_{j\in J} A_j \subseteq A_k$ pro každé $k \in J$ a A_k je podalgebra $A(\alpha_i|\ i \in I)$ máme $\alpha_i(a_1, \dots a_n) \in A_k$, tedy $\alpha_i(a_1, \dots a_n) \in \bigcap_{j\in J} A_j$.

(2) Protože $\mathrm{id} \subseteq \rho_j$ pro všechna $j \in J$, máme $\mathrm{id} \subseteq \bigcap_{j\in J} \rho_j$, tedy relace $\bigcap_{j\in J} \rho_j$ je reflexivní. Je-li $(a, b) \in \bigcap_{j\in J} \rho_j$, máme $(a, b) \in \rho_j$, ze symetrie potom ρ_j i $(b, a) \in \rho_j$ pro všechna $j \in J$, tudíž $(b, a) \in \bigcap_{j\in J} \rho_j$. Konečně platí-li, že $(a, b), (b, c) \in \bigcap_{j\in J} \rho_j$, pak tranzitivita jednotlivých relací ρ_j, které všechny obsahují průnik $\bigcap_{j\in J} \rho_j$ implikuje, že $(a, c) \in \rho_j$, a proto $(a, c) \in \bigcap_{j\in J} \rho_j$.

Mějme α_i nějakou n-ární operaci na A a vezměme prvky $a_1, \dots a_n, b_1, \dots b_n \in A$, pro něž platí, že $(a_k, b_k) \in \bigcap_{j\in J} \rho_j$ ($\subseteq \rho_j$ pro všechna $j \in J$). Potom pro všechna $j \in J$ máme $(\alpha_i(a_1, \dots a_n), \alpha_i(b_1, \dots b_n)) \in \rho_j$, tedy $(\alpha_i(a_1, \dots a_n), \alpha_i(b_1, \dots b_n)) \in \bigcap_{j\in J} \rho_j$. □

Definice. Nechť je A 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 $\bigcap\{B_i|\ i \in I\} \in \mathcal{C}$.

Důsledek 3.6. *Nechť $A(\alpha_i|\ i \in I)$ je algebra. Pak všechny podalgebry algebry $A(\alpha_i|\ i \in I)$ tvoří uzávěrový systém na A a všechny kongruence na algebře $A(\alpha_i|\ i \in I)$ tvoří uzávěrový systém na $A \times A$.*

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

Nyní zobecníme definici ze začátku 2.kapitoly.

Definice. Buď A algebra a $X \subseteq A$. Potom podalgebru $\langle X\rangle$ algebry A, kterou dostaneme jako průnik všech podalgeber A obsahujících množinu X nazveme podalgebrou *generovanou* X (nebo budeme říkat, že X *generuje* podalgebru $\langle X\rangle$).

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. Nejprve ukážeme, že je množina $C = \{a \in A|\ f(a) = g(a)\}$ podalgebrou algebry A. Vezměme n-ární operaci α algebry A a nechť $a_1, \dots, a_n \in C$. Pak $f(\alpha(a_1, \dots, a_n)) = \alpha(f(a_1), \dots, f(a_n)) = \alpha(g(a_1), \dots, g(a_n)) = g(\alpha(a_1, \dots, a_n))$, proto $\alpha(a_1, \dots, a_n) \in C$. Všimneme-li si, že $X \subseteq C$, dostaneme $A = \langle X\rangle \subseteq C$, čímž jsme dokončili důkaz. □

Příklad 3.8. (1) Uvažujme grupu celých čísel $\mathbf{Z}(+)$ a $G(+)$ nějaký grupoid, tedy algebru s jednou binární operací $+$. Nechť $f, g : \mathbf{Z} \to G$ je homomorfismus. Uvědomme si, že nejmenší podalgebra $\mathbf{Z}(+)$ obsahující množinu $\{-1, 1\}$ je už rovna celému $\mathbf{Z}$ tj. $\langle\{-1, 1\}\rangle = \mathbf{Z}$. Podle předchozí poznámky jsou tedy f a g shodné, jestliže $f(1) = g(1)$ a $f(-1) = g(-1)$.

(2) Uvažujme-li nyní dva homomorfismy $f, g : \mathbf{Z} \to G$ na algebře celých čísel $\mathbf{Z}(+, -)$ a obecné algebře $G(+, -)$ s jednou binární operací $+$ a jednou unární operací $+$. Nechť $f, g : \mathbf{Z} \to G$ je homomorfismus. Potom $\langle\{-1, 1\}\rangle = \mathbf{Z}$, a podle 3.7 jsou f a g shodné, jestliže $f(1) = g(1)$.

Definice. Nechť ρ je ekvivalence a α je n-ární operace na množině A. Je-li ρ slučitelná s α, definujeme operaci α na faktoru A/ρ předpisem $\alpha([a_1]_\rho, \dots, [a_n]_\rho) = [\alpha(a_1, \dots, a_n)]_\rho$. Je-li ρ kongruence na algebře A, pak tímto způsobem definujeme na A/ρ strukturu algebry stejného typu.

Věta 3.9. *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. Vezměme libovolnou n-ární operaci α algebry A a nechť $[a_j]_\rho = [b_j]_\rho$, $j = 1, \dots n$. Potom $(a_j, b_j) \in \rho$, kde $j = 1, \dots n$, proto $[\alpha(a_1, \dots, a_n)]_\rho = [\alpha(b_1, \dots, b_n)]_\rho$, tedy definice operací na A/ρ je korektní. Zbytek tvrzení je přímý důsledek definice. □

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 3.10. *Buď ρ kongruence na algebře A.*

(1) *Je-li σ kongruence na A obsahující ρ, je σ/ρ dobře definovaná kongruence na algebře A/ρ.*

(2) *Je-li η kongruence na algebře A/ρ, potom existuje právě jedna kongruence σ na algebře A obsahující ρ, pro níž $\eta = \sigma/\rho$.*

Důkaz. (1) Stačí ověřit, že je σ/ρ dobře definovaná, zbytek je okamžitým důsledkem definice σ/ρ a operace na faktorové algebře A/ρ. Mějme $[a_1]_\rho = [a_2]_\rho$ $[b_1]_\rho = [b_2]_\rho$. Potom $(a_1, a_2), (b_1, b_2) \in \rho \subseteq \sigma$, tedy díky tranzitivitě a symetrii σ platí, že $(a_1, b_1) \in \sigma \Leftrightarrow (a_2, b_2) \in \sigma$.

(2) Jediný možný způsob, jak definovat σ nám dává předpis $(a, b) \in \sigma \Leftrightarrow ([a]_\rho, [b]_\rho) \in \eta$. Nyní stačí přímočaře nahlédnout, že jsme takto zavedli kongruenci na A. □

Nyní už můžeme vyslovit obecné verze Věty o homomorfismus a Vět o izomorfismus:

Poznámka 3.11. (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. Tvrzení dokážeme stejně jako Větu o homomorfismu pro grupy (1.20).

Nejprve předpokládejme, že existuje homomorfismus $g : A/\rho \to B$ splňující podmínku $g\pi_\rho = f$, tedy $g([a]_\rho) = f(a)$ a vezměme $(a_1, a_2) \in \rho$. Pak $[a_1]_\rho = [a_2]_\rho$, a proto $f(a_1) = g([a_1]_\rho) = g([a_2]_\rho) = f(a_2)$. Tedy $(a_1, a_2) \in \ker f$.

Je-li naopak $\rho \subseteq \ker f$, ověřujeme, že definice g daná předpisem $g([a]_\rho) = f(a)$ je korektní. Vezmeme-li $[a_1]_\rho = [a_2]_\rho \subseteq \ker f$, pak $g([a_1]_\rho) = f(a_1) = f(a_2) = g([a_2]_\rho)$. Že je g homomorfismus je zjevné z jeho definice.

Konečně dokážeme závěrečnou ekvivalenci. Protože $g(G_1/\rho) = f(G_1)$, opět vidíme, že g je na, právě když je f na. Je-li g navíc prosté a zvolíme-li $(a_1, a_2) \in \ker f$, pak $g([a_1]_\rho) = f(a_1) = f(a_2) = g([a_2]_\rho)$, a proto $(a_1, a_2) \in \rho$. Ověřili jsme, že $\ker f \subseteq \rho$, a protože už víme, že $\rho \subseteq \ker f$, máme rovnost $\rho = \ker f$. Konečně předpokládejme, že $g([a_1]_\rho) = g([a_2]_\rho)$. Potom $f(a_1) = f(a_2)$, a proto $(a_1, a_2) \in \rho$ a $[a_1]_\rho = [a_2]_\rho$, čímž jsme ověřili, že je g prosté. □

Věta 3.12 (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. Rozmyslíme si, že podle 3.4(3) je $f(A)$ je podalgebra B a poté stejně jako v důkazu 1.21 použijeme Větu o homomorfismu 3.11 na $\rho = \ker f$. □

Věta 3.13 (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. I tentokrát postupujeme stejně jako v důkazu Věty o izomorfismu pro grupy 1.23: nejprve použijeme 3.11 pro homomorfismy $\pi_\sigma : A \to A/\sigma$ a $\pi_\rho : A \to A/\rho$, která nám dává homomorfismus $g : A/\rho \to A/\sigma$ splňující vztah $g([a]_\rho) = [a]_\sigma$. Zbývá spočítat $\ker g = \sigma/\rho$ a použít 3.12. □

4. Svazy

Definice. Relaci $\leq$ na množině M budeme říkat *uspořádání*, je-li reflexivní a tranzitivní a splňuje-li podmínku $a \leq b,\ b \leq a \Rightarrow a = b$ pro každé $a, b \in M$ (tj. jde o slabě antisymetrickou relaci).

Příklad 4.1. Následující relace jsou uspořádáním:

(1) / na množině všech přirozených čísel $\mathbf{N}$,
(2) $\leq$ na množině všech celých (reálných, racionálních) čísel $\mathbf{Z}$ ($\mathbf{R}$, $\mathbf{Q}$),
(3) $\subseteq$ na množině všech podmnožin $\mathcal{P}(X)$ množiny X,
(4) 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, jestliže $m \leq a$ (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 množiny M.

Příklad 4.2. (1) $(\mathbf{N}, /)$, kde $\sup_{/}(n, m) = nsn(n, m)$ a $\inf_{/}(a, b) = NSD(n, m)$, je příkladem svazu

(2) $(\mathbf{Z}, \leq)$, $(\mathbf{R}, \leq)$, $(\mathbf{Q}, \leq)$, kde $\sup_{\leq}(a, b) = \max(a, b)$ a $\inf_{\leq}(a, b) = \min(a, b)$, je rovněž (dokonce lineárně uspořádaný) svaz.

(3) $(\mathcal{P}(X), \subseteq)$, je 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 4.3. *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. Vlastnosti (S1) a (S2) jsou okamžitým důsledkem definice $\wedge$ a $\vee$.

(S3) Položme $d = a \vee (b \vee c)$. Dokážeme, že je d supremem množiny $\{a, b, c\}$. Podle definice $\vee$ je $a \leq d$ a $b, c \leq b \vee c \leq d$, tedy d je horní odhad množiny $\{a, b, c\}$. Zvolme nějaké e, pro něž $a, b, c \leq e$. Pak $(b \vee c) \leq e$, protože je e horní odhad množiny $\{b, c\}$ a $(b \vee c)$ je supremem této množiny. Stejným argumentem dostaneme $a \vee (b \vee c) \leq e$, tedy $a \vee (b \vee c) = \sup_{\leq}(\{a, b, c\}) = c \vee (a \vee b) = (a \vee b) \vee c$ díky (S1). Důkaz druhé podmínky je symetrický.

(S4) Protože $b \wedge a \leq a$ a $a \leq a$, máme $a \vee (b \wedge a) \leq a$. Naopak $a \leq a \vee (b \wedge a)$, tedy ze slabé antisymetrie plyne, že $a = a \vee (b \wedge a)$. I tentokrát pro ověření druhé podmínky stačí zaměnit spojení průsekem a relaci $\leq$ relací $\geq$. □

Poznámka 4.4. *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 $\sup_{\leq}(a, b) = a \vee b$ a $\inf_{\leq}(a, b) = a \wedge b$.*

Důkaz. Nejprve ukážeme, že je $\leq$ uspořádání. Protože $a = a \vee a$ díky (S2), máme podle definice $a \leq a$. Vezmeme-li $a \leq b$ a $b \leq c$, tj. $b = a \vee b$, $c = b \vee c$, pak $c = (a \vee b) \vee c = a \vee (b \vee c) = a \vee c$ díky (S3), tedy $a \leq c$. Konečně platí-li, že $a \leq b$ a $b \leq a$, dostáváme z (S2), že $b = a \vee b = b \vee a = a$.

Nyní ověříme, že $b = a \vee b \Leftrightarrow a = a \wedge b$. Za symetrie podmínek pro $\wedge$ a $\vee$ plyne, že stačí abychom ověřili jen jednu implikaci. Nechť například $b = a \vee b$. Potom $a \wedge b = a \wedge (a \vee b) = a \wedge (b \vee a) = a$ podle (S1) a (S4). Vidíme, že je definice $\leq$ symtericky formulovatelná pomocí podmínky $a \leq b \Leftrightarrow a = a \wedge b$.

Zbývá dokázat, že $\sup_{\leq}(a, b) = a \vee b$ (tvrzení pro $\wedge$ se dokáže symetricky). Předně $a \vee (a \vee b) = (a \vee a) \vee b = a \vee b$ díky (S3) a (S2) a $b \vee (a \vee b) = (a \vee b) \vee b = a \vee (b \vee b) = a \vee b$ díky (S1), (S3) a (S2), tudíž $a, b \leq (a \vee b)$. Vezmeme-li prvek c, pro který $a, b \leq c$, pak $c = a \vee c$ a $c = b \vee c$, proto $c = a \vee (b \vee c) = (a \vee b) \vee c$ podle (S3). Tím jsme ověřili, že $(a \vee b) \leq c$, což znamená, že $\sup_{\leq}(a, b) = a \vee b$. □

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 $\leq$. Všimněme si, že je-li $M(\wedge, \vee)$ svaz, pak i $M(\vee, \wedge)$ tvoří svaz (mluvíme o *opačném svazu* s opačným uspořádáním $\geq$).

Příklad 4.5. U příkladů svazů uvedených v 4.2 máme tedy dva způsoby jak na svaz nahlížet:

(1) $(\mathbf{N}, /)$ odpovídá algebře $\mathbf{N}(\mathrm{NSD}, \mathrm{nsn})$,
(2) $(\mathbf{Z}, \leq)$ (respektive $(\mathbf{R}, \leq)$, $(\mathbf{Q}, \leq)$) odpovídá algebře $\mathbf{Z}(\min, \max)$ (respektive $\mathbf{R}(\min, \max)$, $\mathbf{Q}(\min, \max)$).
(3) $(\mathcal{P}(X), \subseteq)$ odpovídá algebře $\mathcal{P}(X)(\cap, \cup)$,

Věta 4.6. *Nechť $\mathcal{C}$ je uzávěrový systém. Pak $(\mathcal{C}, \subseteq)$ tvoří úplný svaz, kde $\sup_{\subseteq}(\mathcal{B}) = \bigcap\{C \in \mathcal{C} | \bigcup \mathcal{B} \subseteq C\}$ a $\inf_{\subseteq}(\mathcal{B}) = \bigcap \mathcal{B}$ pro každé $\mathcal{B} \subseteq \mathcal{C}$.*

Důkaz. $\subseteq$ je uspořádání a $\bigcap \mathcal{B}$ je zjevně infimem. Protože je $\mathcal{C}$ uzavřené na průniky, je $\bigcap\{X \in \mathcal{C} | \bigcup \mathcal{B} \subseteq X\}$ nejmenším prvkem $\mathcal{C}$ obsahujícím všechna $B \in \mathcal{B}$, což je podle definice právě supremum vzhledem k inkluzi. □

Důsledek 4.7. *Systém všech podalgeber i systém všech kongruencí na algebře spolu s inkluzí je díky 3.6 svazem.*

Definice. Nechť $(M, \leq)$ je svaz a $a, b, c \in M$. Řekneme, že prvek b *pokrývá* prvek a (píšeme $a <\cdot\, b$), jestliže $a \leq b$, $a \neq b$ a $a \leq c \leq b \Rightarrow c = a$ nebo $c = b$. *Hasseovým diagramem* svazu $(M, \leq)$ rozumíme orientovaný graf, jehož vrcholy tvoří prvky množiny M a a je s b spojen takovou hranou, že b se nachází výše než a, právě když b pokrývá a.

Poznámka 4.8. *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. Protože $a \leq a \vee b$ a $b \wedge c \leq b \leq a \vee b$, máme z definice suprema $a \vee (b \wedge c) \leq a \vee b$. Podobně $a \leq a \vee c$ a $b \wedge c \leq c$, proto $a \vee (b \wedge c) \leq c$. Využijeme-li nyní definici infima množiny $\{a \vee b, c\}$, pak dostaneme $a \vee (b \wedge c) \leq (a \vee b) \wedge c$. □

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

Poznámka 4.9. *Každý distributivní svaz je modulární.*

Důkaz. Předpokládejme, že $a \leq c$, tj. $(a \vee c) = c$. Potom nám distributivita dává rovnost $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$. □

Příklad 4.10. (1) Svaz $\mathcal{P}(X)(\cap,\cup)$, kde $\mathcal{P}(X)$ je množina všech podmnožin množiny X, je distributivní.

(2) Množina všech podprostorů vektorového prostoru je uzávěrový systém, a proto tvoří díky Větě 4.6 spolu s inkluzí svaz. Tento svaz je modulární.

(3) 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, protože $a\leq c$ a $a\vee(b\wedge c)=a\neq c=(a\vee b)\wedge c$.

(4) 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 $u\wedge v=u\wedge w=v\wedge w=\mathbf{0}$. Protože $u\vee(v\wedge w)=u\vee\mathbf{0}\neq\mathbf{1}=\mathbf{1}\wedge\mathbf{1}(u\vee v)\wedge(u\vee w)$, není $M_5(\wedge,\vee)$ distributivní svaz. Elemntárními prostředku můžeme dokázat, že je modulární. (říká se mu obvykle diamant a značí se $\mathcal{M}_5$).

Poznámka 4.11. *Svaz $S(\wedge,\vee)$ je distributivní, právě když pro každé $a,b,c\in S$ platí, že $a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)$, tedy svaz $S(\wedge,\vee)$ je distributivní, právě když je opačný svaz $S(\vee,\wedge)$ distributivní.*

Důkaz. Ze symetrie vlastností operací plyne, že stačí dokázat pouze jednu implikaci. Nechť je svaz distributivní. Budeme s využitím definice distributivity a 4.3 upravovat: $(a\wedge b)\vee(a\wedge c)=((a\wedge b)\vee a)\wedge((a\wedge b)\vee c)=(a\vee a)\wedge(b\vee a)\wedge(a\vee c)\wedge(b\vee c)=a\wedge(b\vee c)$, kde poslední rovnost plyne ze vztahů $a\leq(b\vee a)$ a $a\leq(a\vee c)$. □

Definice. Nechť $f:A\to B$ je zobrazení a $(A,\leq)$ a $(B,\leq)$ jsou svazy. Řekneme, že je f *homomorfismus* (*izomorfismus*) jde-li o homorfismus (izomorfismus) algeber $A(\wedge,\vee)$ a $B(\wedge,\vee)$ a f nazveme *monotónním* zobrazením, platí-li implikace $a_1\leq a_2\Rightarrow f(a_1)\leq f(a_2)$.

Příští semestr dokážeme, že je svaz modulární, právě když neobsahuje podsvaz izomorfní svazu $\mathcal{N}_5$, a že je distributivní, právě když neobsahuje ani podsvaz izomorfní $\mathcal{N}_5$, ani podsvaz izomorfní $\mathcal{M}_5$.

Poznámka 4.12. *Homomorfismus svazů je monotónní zobrazení.*

Důkaz. Je-li $f:A\to B$ homomorfismus svazů a $a_1\leq a_2\in A$, pak $a_2=a_1\vee a_2$. Proto $f(a_2)=f(a_1\vee a_2)=f(a_1)\vee f(a_2)$ a tedy $f(a_1)\leq f(a_2)$. □

Příklad 4.13. 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, protože $f(a\wedge b)=f(0)=\mathbf{0}\neq\mathbf{A}=f(a)\wedge f(b)$.

Věta 4.14. *Bijekce svazů f je izomorfismus, právě když jsou f i f^{-1} monotónní zobrazení.*

Důkaz. Díky 4.12 stačí dokázat zpětnou implikaci. Ověříme slučitelnost f například s $\vee$. Mějme $f:A\to B$ takovou bijekci svazů, že f i f^{-1} jsou monotónní, a zvolme $a,b\in A$. Protože $a,b\leq a\vee b$, je $f(a),f(b)\leq f(a\vee b)$, tudíž $f(a)\vee f(b)\leq f(a\vee b)$. Podobně $f(a),f(b)\leq f(a)\vee f(b)$, proto $a,b\leq f^{-1}(f(a)\vee f(b))$ a $a\vee b\leq f^{-1}(f(a)\vee f(b))$. Použijeme-li na poslední vztah znovu monotonii f, dostaneme $f(a\vee b)\leq f(a)\vee f(b)$. Ze slabé antisymetrie $\leq$, potom plyne, že $f(a\vee b)=f(a)\vee f(b)$. □

Definice. Nechť má svaz $S(\wedge,\vee)$ nejmenší prvek $\mathbf{0}$ a největší prvek $\mathbf{1}$. Prvek $a\in S$ nazveme *atomem* (resp. *koatomem*), jestliže a pokrývá $\mathbf{0}$ (resp. $\mathbf{1}$ 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 4.15. *Každý prvek distributivního svazu má nejvýše jeden komplement.*

Důkaz. Nechť $a \vee b_i = \mathbf{1}$ a $a \wedge b_i = \mathbf{0}$ pro $i = 1, 2$. Pak $b_i \wedge (a \vee b_j) = (b_i \wedge a) \vee (b_i \wedge b_j) = \mathbf{0} \vee (b_i \wedge b_j) = b_i \wedge b_j$, tedy $b_i \leq b_j$ pro všechna $i, j \in \{1, 2\}$, což znamená, že $b_1 = b_2$. □

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. *Homomorfismem* (*izomorfismem*) Booleových algeber rozumíme homorfismus (izomorfismus) algeber v obvyklém smyslu.

Příklad 4.16. 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 4.17. *Nechť $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ je Booleova algebra. Pak pro každé $a, b \in S$ platí:*

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

Důkaz. (1) a (2) plyne přímo z definice a 4.15 a (4) je symetrické k (3).

(3) $(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$ a podobně $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = \mathbf{1} \vee \mathbf{1} = \mathbf{1}$. □

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

Důkaz. Definujme nejprve zobrazení $\psi : S \to \mathcal{P}(A)$ předpisem $\psi(s) = \{a \in A |\ a \leq s\}$. Okamžitě vidíme, že zobrazení ϕ i ψ jsou monotónní vzhledem k inkluzi a $\phi(\emptyset) = \mathbf{0}$. Ukážeme-li navíc, že je ϕ bijekce slučitelná s průsekem a spojením, pak nutně $\phi(A) = \mathbf{1}$ a $\phi(B') = \phi(B)'$ pro každé $B \in \mathcal{P}(A)$. Podle 4.14 tedy zbývá ověřit, že $\phi \circ \psi = \mathrm{Id}_S$ i $\psi \circ \phi = \mathrm{Id}_{\mathcal{P}(A)}$, tedy že ϕ je bijekce a $\phi^{-1} = \psi$.

Položme $t = \phi\psi(s) = \bigvee \{a \in A |\ a \leq s\}$. Potom $t = \bigvee \{a \in A |\ a \leq s\} \leq s$. Všimněme si, že díky distributivitě $s = s \wedge \mathbf{1} = s \wedge (t \vee t') = (s \wedge t) \vee (s \wedge t') = t \vee (s \wedge t')$. Předpokládáme-li, že $t \neq s$, pak z předchozího vidíme, že $(s \wedge t') \neq \mathbf{0}$, a díky konečnosti S najdeme nějaký atom a_0, který leží pod prvkem $s \wedge t'$, tedy $a \leq t'$ a $a \in \psi(s)$, a proto $a \leq t$. Zjistili jsme, že $a \leq t \wedge t' = \mathbf{0}$, což je spor, tudíž $s = t$.

Nyní položme $C = \psi\phi(B) = \{a \in A |\ a \leq \bigvee B\}$. Vezmeme-li $b \in B$, pak $b \leq \bigvee B$, a proto $b \in C$, čímž jsme ověřili inkluzi $B \subseteq C$. Zvolme tedy $c \in C$ a uvažme, že $\mathbf{0} \neq c = c \wedge \bigvee B = \bigvee \{c \wedge b |\ b \in B\}$ díky distributivitě a konečnosti B. To ovšem znamená, že existuje $b \in B$, pro něž $c \wedge b \neq \mathbf{0}$. Protože jsou oba prvky b a c atomy, máme $b = c$, čímž jsme dokázali, že $B = C$. □

Poznámka 4.19. *Buď $\mathcal{C}$ uzávěrový systém obsažený v systému všech ekvivalencí na množině A. Nechť pro $\mathcal{N} \subseteq \mathcal{P}(A)$ a $e \in A$ 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. Nejprve ukážeme, že je $\mathcal{N}$ uzávěrový systém. Protože $A \times A \in \mathcal{C}$, máme $A = [e]_{A\times A} \in \mathcal{N}$ díky (a). Vezmeme-li $N_i \in \mathcal{N}$, $i \in I$, pak podle (b) existuje pro každé $i \in I$ taková ekvivalence $\rho_i \in \mathcal{C}$, že $N_i = [e]_{\rho_i}$. Protože je $\mathcal{C}$ uzávěrový systém, tedy $\bigcap_{i\in I} \rho_i \in \mathcal{C}$, dostáváme $\bigcap_{i\in I} N_i = \bigcap_{i\in I} [e]_{\rho_i} = [e]_{\bigcap_{i\in I}\rho_i} \in \mathcal{N}$ opět díky (a).

Nyní stačí podle 4.14 ověřit, že je φ dobře definovaná bijekce a že φ i φ^{-1} jsou monotónní vzhledem k inkluzi. Korektnost definice přitom zaručuje podmínka (a), podmínka (b) říká, že je φ na $\mathcal{N}$, a z podmínky (c) plyne, že jde o prosté zobrazení. Konečně, je-li $\rho \subseteq \eta$, pak $[e]_\rho \subseteq [e]_\eta$ pro každou dvojici ekvivalencí ρ a η, což zaručuje monotónii φ, a monotónie φ^{-1} je přímo obsahem podmínky (c). □

Věta 4.20. *Všechny normální podgrupy libovolné grupy* $G(\cdot)$ *tvoří svaz izomorfní svazu všech kongruencí na grupě* $G(\cdot)$.

Důkaz. Označme symbolem $\mathcal{C}$ množinu všech kongruencí na $G(\cdot)$, tj. ekvivalencí slučitelných s operací $\cdot$ (viz 3.3(3)), symbolem $\mathcal{N}$ množinu všech normálních podgrup $G(\cdot)$ a symbolem e neutrální prvek $G(\cdot)$. Z 4.7 plyne, že je $\mathcal{C}$ uzávěrový systém a 1.15 zaručuje, že jsou splněny předpoklady (a), (b), (c) Poznámky 4.19, odkud plyne závěr. □

5. Okruhy a ideály

Definice. *Okruhem* budeme nazývat každou takovou algebru $R(+, \cdot, -, 0, 1)$, že $R(+)$ je komutativní grupa s neutrálním prvkem 0 a operací opačného prvku $-$, $R(\cdot)$ je monoid s neutrálním prvkem 1 a pro každé $a, b, c \in R$ platí, že $a\cdot(b+c) = a\cdot b+a\cdot c$ a $(a+b)\cdot c = a\cdot c+b\cdot c$. Okruh se nazývá *komutativní*, je-li operace $\cdot$ komutativní.

Příklad 5.1. (1) $\mathbf{Z}(+, \cdot, -, 0, 1)$ a $\mathbf{Z}_n(+, \cdot, -, 0, 1)$ pro každé přirozené $n > 1$ jsou komutativní okruhy.

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

Poznámka 5.2. *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) $1 \neq 0$, *právě když* $|R| > 1$ *(tj. R je netriviální okruh).*

Důkaz. U bodů (1)–(3) dokážeme jen jednu rovnost, důkaz druhé je symetrický.

(1) Využijeme-li definitorickou vlastnost prvku 0 a distributivitu, dostaneme $a\cdot 0 = a\cdot(0+0) = a\cdot 0+a\cdot 0$. Přičteme-li k levé a pravé straně rovnosti $a\cdot 0 = a\cdot 0+a\cdot 0$ prvek $-(0 \cdot a)$, vidíme, že $a \cdot 0 = 0$.

(2) Opět díky distributivitě máme $(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0$, kde poslední rovnost plyne z (1).

(3) Dostáváme přímo z (2) pro $b = 1$.

(4) Přímá implikace je triviální, předpokládejme tedy, že $1 = 0$ a vezměme libovolné $a \in R$. Potom $a = a \cdot 1 = a \cdot 0 = 0$ podle definice a (1). □

Definice. Nechť $R(+, \cdot, -, 0, 1)$ je okruh. Řekneme, že množina $I \subseteq R$ je *pravý* (resp. *levý*) *ideál* okruhu R, jestliže je I podgrupa grupy $R(+)$ 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*, je-li pravým a zároveň levým ideálem. *Homomorfismus* (*izomorfismus*) okruhů bude homorfismus (izomorfismus) příslušných algeber.

Příklad 5.3. (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 $a \in R$. Ověříme to například pro aR. Je-li $ar, as \in aR$, pak díky distributivitě $ar + as = a(r + s) \in aR$ a $-ar = a(-r) \in aR$ podle 5.2(2). Dále $0 = a0 \in aR$ díky 5.2(1) a $(ar)x = a(rx) \in aR$ díky asociativitě pro libovolné $x \in R$.

(3) Podle (2) a 2.5 jsou ideály okruhu celých čísel $\mathbf{Z}(+, \cdot, -, 0, 1)$ právě tvaru $k\mathbf{Z}$ a ideály okruhu $\mathbf{Z}_n(+, \cdot, -, 0, 1)$ tvaru $k\mathbf{Z}_n$, kde $k < n$ je 0 nebo dělitel čísla n.

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

Věta 5.4. *Nechť $R(+, \cdot, -, 0, 1)$ je okruh. Všechny kongruence a všechny ideály okruhu R tvoří spolu s inkluzí svazy a zobrazení $\rho \to [0]_\rho$ je izomorfismus svazu všech kongruencí na svazu všech ideálů okruhu R. Přitom ekvivalence ρ je kongruence na $R(+, \cdot, -, 0, 1)$, právě když $[0]_\rho$ je ideál a $(a, b) \in \rho \Leftrightarrow a - b \in [0]_\rho$.*

Důkaz. Nejprve dokážeme závěrečnou ekvivalenci. Je-li ρ je kongruence na okruhu R, pak jde také o kongruenci grupy $R(+)$, proto je $[0]_\rho$ podle 1.15 podgrupou $R(+)$ a $(a, b) \in \rho \Leftrightarrow a - b \in [0]_\rho$. Zbývá ověřit, že jde o ideál. Zvolme $i \in [0]_\rho$ a $r \in R$, tedy $(i, 0) \in \rho$ a $(r, r) \in \rho$, proto $(ir, 0) = (ir, 0r) \in \rho$ a $(ri, 0) = (ri, r0) \in \rho$, tedy $ir, ri \in I$.

Předpokládejme, že je I je ideál a definujme $(a, b) \in \rho \Leftrightarrow a - b \in I$. Potom $I = [0]_\rho$ a podle 1.15 je ρ slučitelné s $+$. Zvolme $(a, b), (c, d) \in \rho$. Pak $a - b, c - d, (a - b)c, b(c - d) \in [0]_\rho$, a tudíž $-a + b \in [0]_\rho$ a $ac - bd = (a - b)c + b(c - d) \in [0]_\rho$, proto $(-a, -b), (a \cdot c, b \cdot d) \in \rho$, čímž jsme ověřili, že je ρ kongruence na $R(+, \cdot, -, 0, 1)$.

Nyní stejným způsobem jako v důkazu 4.20 nahlédneme že jsou pro $e = 0$, $\mathcal{C}$ množinu všech kongruencí a $\mathcal{N}$ množinu všech ideálů okruhu $R(+, \cdot, -, 0, 1)$ splněny předpoklady 4.19, odkud dostáváme závěr. □

Obdobně jako v případu faktorizace grup podle normálních podgrup budeme faktor okruhu R podle kongruence jednoznačně odpovídající ideálu I značit R/I. Poznamenejme, že faktorová algebra R/I je opět okruh.

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

Poznámka 5.5. *Je-li $R(+, \cdot, -, 0, 1)$ okruh a I jeho pravý nebo levý ideál, pak $I = R$, právě když $1 \in I$.*

Důkaz. Přímá implikace je triviální. Jestliže $1 \in I$ a $r \in R$, potom $r = 1 \cdot r = (r \cdot 1) \in I$, je-li I pravý (levý) ideál. □

Věta 5.6. *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. Stačí dokázat ekvivalenci (1) a (2).

Předpokládejme, že je R těleso a mějme nějaký nenulový pravý ideál I. Pak existuje $0 \neq i \in I$ a k němu inverzní prvek $i^{-1} \in R$, tedy $1 = i \cdot i^{-1} \in I$ a proto $I = R$ podle 5.5.

Předpokládejme, že R neobsahuje žádné vlastní pravé ideály a vezměme libovolně nenulový prvek $a \in R$. Potom $0 \neq a = a \cdot 1 \in aR$, tedy podle předpokladu $aR = R$. Proto existuje $b \in R$, pro nějž $a \cdot b = 1$. Poznamenejme, že díky 5.2(1) a (4) opět $b \neq 0$, a tudíž můžeme stejným argumentem najít $c \in R$, pro které $b \cdot c = 1$. Nyní $a = c$ podle 1.4 a b je tedy inverzní k a. □

Věta 5.7. *Nechť $R(+,\cdot,-,0,1)$ je komutativní okruh a I jeho ideál. Potom faktorový okruh R/I je těleso právě tehdy, když I je maximální ideál.*

Důkaz. Připomeňme, že podle 5.4 je svaz ideálů izomorfní svazu kongruencí okruhu, označme ρ_I kongruenci, která v tomto izomorfismu odpovídá ideálu I. Dále si uvědomme, že díky tomuto izomorfismu je I maximální ideál, právě když je ρ_I koatom svazu kongruencí a to je podle 3.10 ekvivalentní tomu, že faktorokruh $R/\rho_I = R/I$ obsahuje pouze triviální kongruence. Tato podmínka ovšem díky 5.6 a opětovnému použití 5.4 tentokrát na okruh R/I nastává právě tehdy, když je R/I těleso. □

Definice. Komutativní okruh $R(+,\cdot,-,0,1)$ nazveme *oborem integrity*, platí-li, že $a \cdot b = 0$ implikuje $a = 0$ nebo $b = 0$. Prvek $c \in R$ nazveme *ireducibilním* prvkem, jestliže c není invertibilní ani nulový a $c = a \cdot b$ implikuje, že a nebo b je invertibilní.

Poznamenejme, že každé komutativní těleso stejně jako okruh $\mathbf{Z}(+,\cdot,-,0,1)$ jsou obory integrity.

Označme $\mathbf{N}_0$ množinu nezáporných celých čísel.

Poznámka 5.8. *Jestliže je $R(+,\cdot,-,0,1)$ obor integrity, jehož každý ideál je hlavní, a a je ireducibilní prvek, pak aR je maximální ideál.*

Důkaz. Vezměme libovolný (hlavní) ideál uR, pro který $aR \subset uR$ a $aR \neq uR$. Potom $a \in uR$, tedy existuje $v \in R$, pro nějž $a = u \cdot v$. Protože je a ireducibilní musí být buď u nebo v invertibilní. Kdyby bylo invertibilní v, potom by $u = u \cdot v \cdot v^{-1} = a \cdot v^{-1} \in aR$, což je ve sporu s předpokladem. Tedy je invertibilní u, a proto $1 = u \cdot u^{-1} \in uR$ a $uR = R$ díky 5.5 □

Definice. Buď $R(+,\cdot,-,0,1)$ okruh. Položme $R[x] = \{p : \mathbf{N}_0 \to R |\ \{n | p(n) \neq 0\}$ je konečné$\}$. Prvek $p \in R[x]$ budeme zapisovat také ve tvaru $p = \sum_{n\in\mathbf{N}_0} p_n x^n$, kde $p_n = p(n)$, tedy $R[x]$ obsahuje právě všechny formální nekonečné sumy s konečným nosičem. Na $R[x]$ definujme binární operace $+$ a $\cdot$, unární operaci $-$ a nulární operace $\mathbf{0}$ a $\mathbf{1}$ pro $p = \sum_{n\in\mathbf{N}_0} p_n x^n$ a $q = \sum_{n\in\mathbf{N}_0} q_n x^n$:

$$p + q = \sum_{n\in\mathbf{N}_0} (p_n + q_n)x^n, \qquad p \cdot q = \sum_{n\in\mathbf{N}_0} (\sum_{i=0}^{n} p_i \cdot q_{n-i})x^n,$$

$$-p = \sum_{n\in\mathbf{N}_0} -p_n x^n, \quad \mathbf{0} = \sum_{n\in\mathbf{N}_0} 0x^n, \quad \mathbf{1} = 1x^0 + \sum_{n>0} 0x^n.$$

Je-li $p \neq \mathbf{0}$, budeme největší takové $n \in \mathbf{N}_0$, že $p_n \neq 0$, nazývat stupněm polynomu p. Stupeň polynomu $\mathbf{0}$ položíme roven -1. Stupeň polynomu p budeme označovat $\operatorname{st} p$.

Poznámka 5.9. *Nechť $R(+,\cdot,-,0,1)$ je okruh a $p,\ q \in R[x]$.*

(1) *$R[x](+,\cdot,-,\mathbf{0},\mathbf{1})$ je okruh a množina $\{sx^0|\ s \in R\}$ jeho podokruh izomorfní okruhu $R(+,\cdot,-,0,1)$,*
(2) *$\operatorname{st} p + q \leq \max(\operatorname{st} p,\ \operatorname{st} q)$,*
(3) *je-li $p, q \neq \mathbf{0}$, pak $\operatorname{st} p \cdot q \leq \operatorname{st} p + \operatorname{st} q$, je-li navíc R oborem integrity, potom $\operatorname{st} p \cdot q = \operatorname{st} p + \operatorname{st} q$,*
(4) *$R[x]$ je obor integrity právě tehdy, když je R obor integrity,*

Důkaz. Mějme $p = \sum_{n\in\mathbf{N}_0} p_n x^n$, $q = \sum_{n\in\mathbf{N}_0} q_n x^n$, $r = \sum_{n\in\mathbf{N}_0} r_n x^n \in R[x]$.

(1) Nejprve poznamenejme, že jsou všechny operace dobře definované a přímočaře ověřme komutativitu a asociativitu operace $+$:

$$p + q = \sum_{n\in\mathbf{N}_0} (p_n + q_n)x^n = \sum_{n\in\mathbf{N}_0} (q_n + p_n)x^n = q + p,$$

$$(p + q) + r = \sum_{n\in\mathbf{N}_0} ((p_n + q_n) + r_n)x^n = \sum_{n\in\mathbf{N}_0} (p_n + (q_n + r_n))x^n = p + (q + r).$$

Protože $\mathbf{0}$ je zjevně neutrální prvek operace $+$ a vidíme, že $p + (-p) = \mathbf{0}$, je $R(+,-,0)$ komutativní grupa. Podobně

$$r \cdot (p + q) = r \cdot \sum_{n\in\mathbf{N}_0} (p_n + q_n)x^n = \sum_{n\in\mathbf{N}_0} (\sum_{i=0}^{n} r_i \cdot (p_{n-i} + q_{n-i}))x^n =$$

$$= \sum_{n\in\mathbf{N}_0} (\sum_{i=0}^{n} r_i \cdot p_{n-i})x^n + \sum_{n\in\mathbf{N}_0} (\sum_{i=0}^{n} r_i \cdot q_{n-i})x^n = p \cdot r + q \cdot r,$$

důkaz druhé distributivity je symetrický. Konečně zbývá ověřit, že je $R(\cdot,1)$ monoid:

$$(p \cdot q) \cdot r = \sum_{n\in\mathbf{N}_0} (\sum_{i+j=n} p_i \cdot q_j)x^n) \cdot r = \sum_{n\in\mathbf{N}_0} (\sum_{i+j+k=n} p_i \cdot q_j \cdot r_k)x^n) = p \cdot (q \cdot r).$$

a

$$p \cdot \mathbf{1} = \sum_{n\in\mathbf{N}_0} (\sum_{i=0}^{n} p_i \cdot \mathbf{1}_{n-i})x^n \sum_{n\in\mathbf{N}_0} (p_n \cdot 1)x^n = p = \mathbf{1} \cdot p,$$

kde $\mathbf{1} = \sum_n \mathbf{1}_n x^n$, tedy $\mathbf{1}_0 = 1$ a $\mathbf{1}_n = 0$ pro všechna $n > 0$. Bezprostředně z konstrukce okruhu $R[x]$ vidíme, že zobrazení $\nu : R \to R[x]$ dané vztahem $\nu(r) = rx^0$ je prostý okruhový homomorfismus, proto díky 3.12 dostáváme izomorfismus okruhu $R(+,\cdot,-,0,1)$ s podokruhem $\nu(R) = \{sx^0|\ s \in R\}$.

(2) Plyne z inkluze $\{n|\ p_n + q_n \neq 0\} \subseteq \{n|\ p_n \neq 0\} \cup \{n|\ q_n \neq 0\}$.

(3) Označme $\nu = \operatorname{st} p$ a $\mu = \operatorname{st} q$ a uvědomme si pro každé $n > \nu + \mu$, že koeficient u x^n v polynomu $p \cdot q$ je $\sum_{k=0}^{n}(p_k \cdot q_{n-k}) = \sum_{k=0}^{n-\mu}(p_k \cdot 0) + \sum_{k=n-\mu+1}^{n}(0 \cdot q_{n-k}) = 0$, proto $\operatorname{st} p \cdot q \leq \nu + \mu$.

Je-li R obor integrity, máme koeficient polynomu $p \cdot q$ u $x^{\nu+\mu}$:

$$\sum_{k=0}^{\nu+\mu}(p_k \cdot q_{n-k}) = \sum_{k=0}^{n-\mu-1} (p_k \cdot 0) + p_\nu \cdot q_\mu + \sum_{k=n-\mu+1}^{n} (0 \cdot q_{n-k}) = p_\nu \cdot q_\mu \neq 0,$$

neboť $p_\nu \neq 0$ a $q_\mu \neq 0$.

(4) Je-li $R[x]$ obor integrity, je každý jeho podokruh oborem integrity, tedy i okruh R podle (1). Je-li R obor integrity a $p, q \neq \mathbf{0}$, máme podle (3) $\operatorname{st} p \cdot q = \operatorname{st} p + \operatorname{st} q \geq 0$, proto $p \cdot q \neq 0$. □

Okruhu $R[x](+, \cdot, -, \mathbf{0}, \mathbf{1})$ budeme říkat *okruhem polynomů* jedné neurčité) a jeho prvkům *polynomy.*

Věta 5.10 (Dělení se zbytkem)**.** *Nechť $R(+, \cdot, -, 0, 1)$ je obor integrity, $a,\ b \in R[x]$, kde $b = \sum b_n x^n$. Předpokládejme, že $m = \operatorname{st} b \geq 0$ a b_m je invertibilní v R. Pak existují takové jednoznačně určené polynomy $q,\ r \in R[x]$, že $a = b \cdot q + r$ a $\operatorname{st} r < \operatorname{st} b$.*

Důkaz. Tvrzení dokážeme indukcí podle $n = \operatorname{st} a - \operatorname{st} b$. Jestliže $\operatorname{st} a < \operatorname{st} b$, a tedy $n < 0$, stačí položit $q = 0$ a $r = a$. Platí-li existenční tvrzení pro všechna $i < n$, dokážeme ho pro n. Buď $a = \sum a_n x^n$ a položme $q_0 = a_{n+m} b_m^{-1} x^n$ a $t = a - q_0 \cdot b$. Podle 5.9(2) a (3) je $\operatorname{st} t \leq \max(\operatorname{st} a, \operatorname{st} q_0 + \operatorname{st} b) = n + m$ a koeficient polynomu t u mocniny x^{n+m} je $a_{n+m} - a_{n+m} b_m^{-1} b_m = 0$, tedy $\operatorname{st} t - \operatorname{st} b < n$ a můžeme pro polynom t užít indukčního předpokladu, podle nějž existují takové polynomy q_1 a r, že $t = b \cdot q_1 + r$ a $\operatorname{st} r < \operatorname{st} b$. Položíme-li nyní $q = q_0 + q_1$, dostáváme

$$b \cdot q + r = b \cdot q_0 + b \cdot q_1 + r = b \cdot q_0 + t = a.$$

Konečně předpokládejme, že $a = b \cdot q' + r'$ a $\operatorname{st} r' < \operatorname{st} b$. Potom $b \cdot (q - q') = r' - r$ a podle 5.9(3) a protože $st(r' - r) < \operatorname{st} b$, dostáváme $r' - r = 0$, a proto $q - q' = 0$ □

Věta 5.11. *Nechť $T(+, \cdot, -, 0, 1)$ je komutativní těleso. Pak je každý ideál okruhu $T[x](+, \cdot, -, \mathbf{0}, \mathbf{1})$ hlavní.*

Důkaz. Vezměme libovolný nenulový ideál I a v ideálu I zvolme nenulový polynom p nejmenšího možného stupně. Zřejmě $pT[x] \subseteq I$. Nechť $i \in I$. Pak podle 5.10 existují takové polynomy $q, r \in T[x]$, že $i = p \cdot q + r$ a $\operatorname{st}(r) < \operatorname{st}(p)$. Protože $r = i - p \cdot q \in I$ a $\operatorname{st}(p)$ byl minimální, je nutně $r = 0$ a $pT[x] = I$. □

Uvážíme-li, že podle 5.7 je faktor komutativního okruhu podle maximálního ideálu těleso, dostáváme s využitím 5.8 důsledek předchozí věty:

Důsledek 5.12. *Je-li $T(+, \cdot, -, 0, 1)$ komutativní těleso a $p \in T[x]$ ireducibilní polynom, pak $T[x]/pT[x]$ je komutativní těleso.*

Příklad 5.13 (Konstrukce tělesa o p^n prvcích)**.** Buď p prvočíslo a uvažujme těleso $\mathbf{Z}_p(+, \cdot, -, 0, 1)$. Najdeme-li ireducibilní polynom $u \in \mathbf{Z}_p[x]$ stupně n, pak je podle 5.12 okruh $\mathbf{Z}_p[x]/u\mathbf{Z}_p[x]$ tělesem. Označíme-li si $[a]_u$ rozkladové třídy faktoru $\mathbf{Z}_p[x]/u\mathbf{Z}_p[x]$, pak díky 5.4 snadno nahlédneme, že $\mathbf{Z}_p[x]/u\mathbf{Z}_p[x] = \{[a]_u |\ \operatorname{st} a < n\}$ a že $|\mathbf{Z}_p[x]/u\mathbf{Z}_p[x]| = p^n$.

Vezmeme-li polynom $x^3 + x + 1 \in \mathbf{Z}_2[x]$ snadno ověříme, že není součinem polynomu stupně 1 a polynomu stupně 2, tedy že je ireducibilní. Rozkladové třídy $[a]_{x^3+x+1}$ tělesa $T = \mathbf{Z}_2[x]/(x^3 + x + 1)\mathbf{Z}_p[x]$ budeme značit $[a]$. Vidíme, že rozkladové třídy T reprezentuje množina polynomů $P = \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$, t.j. $T = \{[a] |\ a \in P\}$. Připomeňme, že $[a] \pm [b] = [a \pm b]$, tedy vezmeme-li $a, b \in P$, pak $a \pm b \in P$. Díky 5.4 snadno nahlédneme, že $[a] = [(a) \bmod (x^3 + x + 1)]$, kde $(a) \bmod (x^3 + x + 1)$ znamená zbytek po dělení polynomu a polynomem $x^3 + x + 1$ podle 5.10. Proto $[a] \cdot [b] = [a \cdot b] = [(a \cdot b) \bmod (x^3 + x + 1)]$, tedy vezmeme-li $a, b \in P$, pak $(a \cdot b) \bmod (x^3 + x + 1) \in P$, čímž jsme kompletně popsali okruhovou strukturu pomocí reprezentantů P.