

ALGEBRA I PRO INFORMATIKY

ÚVOD

Tento text si klade za cíl seznámit studenty informatiky s nezákladnějšími pojmy, koncepty a v neposlední řadě i konkrétními objekty, které jsou předmětem zkoumání současné algebry. Výběr a uspořádání teorie, kterou zde prezentujeme, je zvolen s ohledem na tři základní hlediska. Především se snažíme navázat na koncepty a způsoby uvažování, které jsou pro studenta informatiky přirozené, dále se v rámci velmi omezeného prostoru pokoušíme demonstrovat několik elementárních algebraických výsledků, které jsou užitečné v informatických aplikacích a konečně za nepominutelné považujeme přístup, který můžeme nepříliš přesně označit jako kontextuální, a jímž míníme seznámení studenta s terminologickými a historickými kontexty současné algebry.

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 algebraických objektech (které se budou zpravidla opírat o nějaký systém axiomatických požadavků na operace), uvedeme několik motivačních příkladů, které by nám pomohly usnadnit porozumění důvodům (ať už praktickým tak historickým), proč právě tu či onu vlastnost sledujeme.

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.

Nejprve se domluvíme, že *binární operací* na množině A budeme rozumět libovolné zobrazení $A \times A \rightarrow A$ (obvykle ji budeme zapisovat centrálně).

Příklad 0.1. Uvažujme množinu celých čísel \mathbf{Z} a na ní obvyklé operace sčítání $+$ a násobení \cdot . Pro libovolné přirozené číslo n položme $n\mathbf{Z} = \{n \cdot z \mid z \in \mathbf{Z}\}$. 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} nesplyvají, nelze pomocí vlastností operace $+$ obě množiny odlišit (tj. mají stejné „algebraické“ vlastnosti vzhledem ke sčítání), což ozřejmíme, zavedeme-li zobrazení $f_n : \mathbf{Z} \rightarrow n\mathbf{Z}$ 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 nespĺňuje. 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 $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$ pro nějaké celé číslo $n > 1$. Zaved' me na \mathbf{Z}_n operace $+$ a \cdot předpisem $a + b = (a + b) \bmod n$ a $a \cdot b = (a \cdot b) \bmod n$, kde $\bmod n$ znamená zbytek po celočíselném dělení hodnotou n a v závorce uvažujeme vždy obvyklé sčítání a násobení celých čísel. Konečně definujme zobrazení $F_n : \mathbf{Z} \rightarrow \mathbf{Z}_n$ předpisem $F_n(k) = (k) \bmod n$. Všimněme si, že tentokrát zobrazení F sice není bijekce, ale obě operace sčítání a násobení „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. 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 $f : A \rightarrow B$ nazveme *slučitelné* s operacemi $*$ a \circ je-li pro všechna $x, y \in A$ splněna rovnost $f(x * y) = f(x) \circ f(y)$.

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 . Navíc množina $n\mathbf{Z}$ je uzavřená na operace $+$ i \cdot . Uvedené pojmy jsou základním stavebním kamenem lineární algebry:

Příklad 0.3. Podprostor vektorového prostoru je zjevně podmnožinou uzavřenou na (vektorové) sčítání a lineární zobrazení jsou se sčítáním slučitelná.

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

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

Řekneme, že relace ρ je

- *symetrická*, jestliže $\rho^{-1} \subseteq \rho$,
- *reflexivní*, v případě, že $id \subseteq \rho$ a
- *tranzitivní*, pokud $\rho^+ \subseteq \rho$.

Ekvivalenci budeme nazývat každou symetrickou, reflexivní a tranzitivní relaci.

Příklad 0.4. Pro libovolné množiny A a B a zobrazení $f : A \rightarrow B$ množin jsou tvoří ekvivalenci relace

- (1) $id = \{(a, a) \mid a \in A\}$,
- (2) $A \times A$,
- (3) $\ker f = \{(x, y) \in A \times A \mid f(x) = f(y)\}$ (tzv. jádro zobrazení f).

Je-li ρ ekvivalence na množině A , připomeňme, že *faktorem množiny* (často se také mluví o *kvocientu*) A podle ekvivalence ρ jako množinu $A/\rho = \{[a]_\rho \mid a \in A\}$, kde $[a]_\rho = \{b \in A \mid (a, b) \in \rho\}$ jsou rozkladové třídy (kosety), tedy A/ρ tvoří rozklad množiny A .

Naopak máme-li $\{B_i \mid i \in I\}$ rozklad množiny A , pak relace ρ určená podmínkou: $(a, b) \in \rho \Leftrightarrow \exists i \in I : a, b \in B_i$ je ekvivalenci a $A/\rho = \{B_i \mid i \in I\}$.

Příklad 0.5. Vezměme přirozené číslo $n \geq 2$ a označme $\equiv \pmod{n}$ relaci na množině celých čísel \mathbf{Z} danou předpisem: $a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$. Není těžké si uvědomit, že se jedná o ekvivalenci (obvykle se jí říká kongruence na \mathbf{Z}). Navíc si můžeme všimnout jejího těsného vztahu k zobrazení F_n z 0.2, neboť platí, že

$a \equiv b \pmod{n}$, právě když $F_n(a) = F_n(b)$, tedy kongruence $\equiv \pmod{n}$ je rovná právě ekvivalenci $\ker F_n$.

Teorie čísel, tedy otázky dělitelnosti na přirozených (nebo celých číslech), je jedním z historických zdrojů algebraických konceptů a terminologie. Dříve než začneme používat termín kongruence v mnohem obecnější situaci, připomeňme si několik jednoduchých vlastností, které kongruence na celých číslech má:

Poznámka 0.6. Pro každé $a, b, c, d \in \mathbf{Z}$ a $k, n \in \mathbf{N}$, kde $n > 1$, platí:

- (1) jestliže $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$, pak $a + c \equiv b + d \pmod{n}$,
 $a - c \equiv b - d \pmod{n}$, $a \cdot c \equiv b \cdot d \pmod{n}$ a $a^k \equiv b^k \pmod{n}$,
- (2) jestliže $c \neq 0$, pak $a \equiv b \pmod{n}$, právě když $a \cdot c \equiv b \cdot c \pmod{cn}$,
- (3) jestliže $\text{NSD}(c, n) = 1$, pak $a \equiv b \pmod{n}$, právě když $a \cdot c \equiv b \cdot c \pmod{n}$.

Důkaz. (1) Předpokládáme-li, že $n/(a-b), (c-d)$, pak

$$n/(a-b) + (c-d) = (a+c) - (b+d),$$

$$n/(a-b) - (c-d) = (a-c) - (b-d),$$

$$n/(a-b) \cdot c + b \cdot (c-d) = (a \cdot c) - (b \cdot d)$$

a poslední kongruenci dostaneme indukčním použitím předchozí pro $a = c$ a $b = d$.

(2) $a \equiv b \pmod{n} \Leftrightarrow n/(a-b) \Leftrightarrow nc/(ac-bc) \Leftrightarrow ac \equiv bc \pmod{cn}$.

(3) Přímá implikace plyne okamžitě z (1), protože $c \equiv c \pmod{n}$. Jakmile $n/ac - bc = (a-b)c$ a c a n jsou nesoudělná čísla, pak nutně $n/(a-b)$. \square

Definice. Uvažujme na množině A binární operaci $*$ a ekvivalenci \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 Poznámce 0.6 jsme tedy zjistili, že je kongruence $\equiv \pmod{n}$ slučitelná s přirozenými operacemi $+$, $-$ a \cdot na celých číslech.

Příklad 0.7. Mějme kladná celá čísla n_1, \dots, n_k a položme $n = n_1 \cdots n_k$. Zavedme nyní na kartézském součinu $\prod_{i=1}^k \mathbf{Z}_{n_i}$ po složkách operace $+$, $-$ a \cdot :

$$(a_1, a_2, \dots, a_k) + (b_1, b_2, \dots, b_k) = (a_1 + b_1, a_2 + b_2, \dots, a_k + b_k),$$

$$(a_1, a_2, \dots, a_k) - (b_1, b_2, \dots, b_k) = (a_1 - b_1, a_2 - b_2, \dots, a_k - b_k),$$

$$(a_1, a_2, \dots, a_k) \cdot (b_1, b_2, \dots, b_k) = (a_1 \cdot b_1, a_2 \cdot b_2, \dots, a_k \cdot b_k),$$

kde odčítání ve složkách definujeme rovněž modulo n_i . Definujme dále zobrazení $G : \mathbf{Z} \rightarrow \prod_{i=1}^k \mathbf{Z}_{n_i}$ předpisem $G(a) = ((a) \bmod n_1, \dots, (a) \bmod n_k)$ a stejným předpisem zavedeme i zobrazení $H : \mathbf{Z}_n \rightarrow \prod_{i=1}^k \mathbf{Z}_{n_i}$. Obě zobrazení jsou opět slučitelná s operacemi $+$, operacemi $-$ i operacemi \cdot .

V následující poznámce budeme uvažovat operace na kartézských součinech zavedené v Příkladu 0.7.

Poznámka 0.8 (Čínská věta o zbytcích). *Nechť n_1, n_2, \dots, n_k jsou kladná celá čísla a $n = n_1 \cdot n_2 \cdot \dots \cdot n_k$. Potom zobrazení H z 0.7 je bijekce slučitelná s operací $+$ a s operací \cdot , právě když jsou čísla n_1, n_2, \dots, n_k po dvou nesoudělná.*

Důkaz. Nejprve dokážeme zpětnou implikaci. V Příkladu 0.7 jsme si uvědomili, že je f zobrazení slčitelné 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 $H(a) = H(b)$. Potom $H(b - a) = 0$, tedy $n_i/b - a$ pro všechna $i = 1, \dots, k$. Protože jsou n_i po dvou nesoudělná a $0 \leq b - a \leq n - 1$, máme i $n/b - a$, tudíž $b = a$.

Přímou implikaci dokážeme nepřímou. Nechť existují indexy $i \neq j$, pro něž $c = \text{NSD}(n_i, n_j) > 1$. Potom $\frac{n}{c} \in \mathbf{Z}_n \setminus \{0\}$ a pro všechna $r = 1, \dots, k$ platí, že $n_r/\frac{n}{c}$. To znamená, že $H(0) = (0, \dots, 0) = H(\frac{n}{c})$, tedy H není prosté. \square

Uvedený důkaz Čínské věty o zbytcích sice není konstruktivní, následující příklad ovšem ukazuje, že hledat vzory zobrazení H není těžké.

Příklad 0.9. Uvědomme si, že podle Čínské věty o zbytcích existuje právě jedno $x \in \mathbf{Z}_{35}$ splňující kongruence $x \equiv 2 \pmod{5}$ a $x \equiv 3 \pmod{7}$. pokusíme se ho najít. Nejprve si všimněme, že z první kongruence plyne, že $x = 5y + 2$ pro vhodná $y \in \mathbf{Z}$ a toto vyjádření dosadíme do druhé kongruence a pomocí Poznámky 0.6 budeme kongruenci upravovat ekvivalentními úpravami:

$$5y + 2 \equiv 3 \pmod{7} \Leftrightarrow 5y \equiv 1 \pmod{7} \Leftrightarrow 3 \cdot 5y \equiv 3 \cdot 1 \pmod{7} \Leftrightarrow y \equiv 3 \pmod{7}.$$

Poznamenejme, že jsme v posledním kroku využili toho, že umíme najít „inverzu modulo 7 k číslu 5 jímž je 3 “. Hledaným řešením je tedy $x = 5 \cdot 3 + 2 = 17$.

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 při potřebě exaktního počítání s velkými čísly lze použít.

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

Poznámka 0.10. 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 tehdy, 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 $\varphi(p^k) = (p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1} = (p - 1)p^{k-1}$. \square

Věta 0.11. Bud' $p_1 < p_2 < \dots < p_k$ prvočísla a r_1, r_2, \dots, 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. Položme $n = \prod_{i=1}^k n_i$ a zvolme libovolné $a \in \mathbf{Z}_n$. Dále položme $n_i = p_i^{r_i}$ a uvažujme zobrazení $f : \mathbf{Z}_n \rightarrow \prod_{i=1}^k \mathbf{Z}_{p_i^{r_i}}$ z Poznámky 0.8. Protože jsou n_1, \dots, n_k nesoudělná čísla, je f podle 0.8 bijekce. Nyní položme $(a_1, \dots, a_k) = f(a)$. 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 $\text{NSD}(a, n) = 1$ právě tehdy, když $\text{NSD}(a_i, n_i) = 1$ pro všechna $i = 1, \dots, k$, protože

$$\prod_{i=1}^k \varphi(n_i) = \left| \prod_{i=1}^k \{a \in \mathbf{Z}_{n_i} \setminus \{0\} \mid \text{NSD}(a, n_i) = 1\} \right|.$$

Jestliže $\text{NSD}(a, n) \neq 1$, existuje index i , pro něž prvočíslo p_i dělí a , a díky jednoznačnosti prvočíselného rozkladu, tudíž buď $a_i = 0$ nebo p_i dělí a_i , proto $\text{NSD}(a_i, n_i) \neq 1$.

Naopak, jestliže $\text{NSD}(a_i, n_i) \neq 1$, pak existuje dělitel $c > 1$ čísel a_i i n_i , proto c dělí i $a = a_i + xn_i$ i $n = n_1 \dots n_i \dots n_k$.

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 0.10 \square

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 operaci $*$ 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 $e = e * f = f$. \square

Následující příklad ukazuje, že se v definici neutrálního prvku nemůžeme omezit jen na jednu ze dvou rovností:

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 je 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 .

Příklad 1.3. Uvažujme $T(\mathbf{N})$ množinu všech zobrazení přirozených čísel do sebe s operací skládání \circ a nechť $\alpha(k) = 2k$ a $\beta(k) = \lfloor \frac{k}{2} \rfloor$. Pak identické zobrazení Id je neutrální vzhledem k \circ , a platí, že $\beta\alpha = Id$ a $\alpha\beta \neq Id$. Prvky α a β tedy splňují právě jednu z definitorických rovností invertibilního prvku, ovšem invertibilní nejsou.

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 0.5 jsme připomněli asociativní a komutativní operace $+$ a \cdot na množině celých čísel (a v Příkladech 0.2 a 0.7 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 1.4. Nechť $n > 1$ je přirozené číslo a X neprázdná množina.

(1) Nechť $M(X)$ je množina všech slov, tj. všech konečných posloupností písmen z množiny X . Zaveďme na této množině binární operaci skládání \cdot : $x_1 \dots x_n \cdot y_1 \dots y_m = x_1 \dots x_n y_1 \dots y_m$ a dále označme ϵ prázdné slovo. Snadno nahlédneme,

že je operace \cdot asociativní (je-li X aspoň dvouprvková množina, pak operace není komutativní) a platí, že $\epsilon \cdot s = s \cdot \epsilon = s$ pro každé $s \in M(X)$, tedy $M(X)(\cdot)$ je tzv. *slovní monoid*.

(2) 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).

(4) $\mathbf{Z}_n(\cdot)$ je konečný komutativní monoid, který není grupou, protože prvek 0 není invertibilní.

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

Poznámka 1.5. *Bud' $S(\cdot)$ 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: $c = c \cdot 1 = c \cdot (a \cdot b) = (c \cdot a) \cdot b = 1 \cdot b = b$. \square

Poznámka 1.6. *Je-li $S(\cdot)$ monoid a $s, t \in S$ jeho invertibilní prvky, pak $s \cdot t$ a s^{-1} jsou také invertibilní. Navíc $(s \cdot t)^{-1} = t^{-1} \cdot s^{-1}$ a $(s^{-1})^{-1} = s$.*

Důkaz. Protože $s \cdot s^{-1} = s^{-1} \cdot s = 1$, je zřejmě s^{-1} invertibilní a díky 1.5 máme $(s^{-1})^{-1} = s$. Nyní stačí dokázat, že je prvek $t^{-1} \cdot s^{-1}$ inverzní k $s \cdot t$:

$$(s \cdot t) \cdot (t^{-1} \cdot s^{-1}) = s \cdot (t \cdot t^{-1}) \cdot s^{-1} = s \cdot 1 \cdot s^{-1} = s \cdot s^{-1} = 1$$

a symetricky

$$(t^{-1} \cdot s^{-1}) \cdot (s \cdot t) = t^{-1} \cdot (s^{-1} \cdot s) \cdot t = t^{-1} \cdot 1 \cdot t = t^{-1} \cdot t = 1.$$

\square

Množinu všech invertibilních prvků monoidu $S(\cdot)$ budeme značit S^* . Všimněme si, že jsme v předchozí úvaze dokázali, že množina S^* je uzavřená na operaci \cdot , uvědomíme-li si navíc, že $1 \in S^*$, protože $1 \cdot 1 = 1$, dostáváme díky předchozí poznámce následující pozorování:

Důsledek 1.7. *Nechť $S(\cdot)$ je monoid. Označíme-li \cdot_{S^*} restrikci $\cdot|_{S^* \times S^*}$ operace \cdot na množinu $S^* \times S^*$, pak $S^*(\cdot_{S^*})$ je grupa.*

Příklad 1.8. Nechť $n > 1$ je přirozené číslo a X neprázdná množina.

(1) Grupa invertibilních prvků $M(X)(\cdot)$ obsahuje pouze neutrální prvek ϵ .

(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 (značíme je $GL_n(T)$).

(4) Ukážeme, že $\mathbf{Z}_n^*(\cdot) = \{0 < a < n \mid \text{NSD}(a, n) = 1\}$. Jestliže $a \in \mathbf{Z}_n^*$, existují $x \in \mathbf{Z}_n$ a $y \in \mathbf{Z}$, pro něž $ax + by = 1$. Je-li s společný dělitel čísel a, n , pak $s \mid (ax + ny) = 1$, proto $\text{NSD}(a, n) = 1$. Nechť naopak $\text{NSD}(a, n) = 1$, potom díky Euklidovu algoritmu existují $x \in \mathbf{Z}_n$ a $y \in \mathbf{Z}$, pro které $ax + ny = 1$, proto $a^{-1} = x \bmod n$, tudíž $a \in \mathbf{Z}_n^*$. Jednoduchým důsledkem tohoto pozorování je fakt, že $|\mathbf{Z}_n^*| = \varphi(n)$.

Definice. Podgrupou grupy $G(\cdot)$ budeme rozumět každou podmnožinu H množiny G , která je uzavřená na \cdot , obsahuje prvek 1 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 $h \in H$.

Protože podle 1.6 pro každý prvek g grupy $G(\cdot)$ platí, že $(g^{-1})^{-1} = g$, mohli jsme normální podgrupu H také ekvivalentně definovat také symetrickou podmínkou $g^{-1} \cdot h \cdot g \in H$ 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) $H(\cdot)$ tvoří s operací omezenou na množinu H opět grupu,
- (2) $\bigcap_{i \in I} H_i$ je podgrupa grupy $G(\cdot)$,
- (3) jsou-li všechny podgrupy H_i normální, pak je i podgrupa $\bigcap_{i \in I} H_i$ normální,
- (4) je-li $G(\cdot)$ komutativní grupa, pak je podgrupa H vždy normální.

Důkaz. (1) Plyne okamžitě z definice podgrupy a vlastností operace \cdot na G (srovnej s 1.6).

(2) $1 \in H_i$ pro všechna $i \in I$ podle, tedy $1 \in \bigcap_{i \in I} H_i$. 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 $a^{-1} \in \bigcap_{i \in I} H_i$.

(3) 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 $g \cdot h \cdot g^{-1} \in \bigcap_{i \in I} H_i$.

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

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

(2) 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 (elementárními prostředky) dokázat, že grupa $S_n(\circ)$ neobsahuje pro $n \neq 4$ jiné normální podgrupy než $\{\text{Id}\}$, S_n a A_n (v případě S_4 se vyskytuje ještě jedna tzv. Kleinova normální podgrupa $K = \{\text{Id}, (12)(34), (13)(24), (14)(23)\}$). Uveďme alespoň příklad zjevné podgrupy $T = \{\text{Id}, (12)\}$ grupy S_3 , která není normální, protože například $(13) \circ (12) \circ (13)^{-1} = (23) \notin T$.

(3) Protože $\det(\mathbf{A} \cdot \mathbf{B}) = \det(\mathbf{A}) \cdot \det(\mathbf{B})$, snadno spočítáme, že množiny $S = \{\mathbf{A} \in GL_n(T) \mid \det(\mathbf{A}) = 1\}$ a $P = \{\mathbf{A} \in GL_n(T) \mid \det(\mathbf{A}) = \pm 1\}$ jsou normální podgrupy grupy $GL_n(T)(\cdot)$.

(4) Uvažujme-li komutativní grupu celých čísel $\mathbf{Z}(+)$ (s neutrálním prvkem 0 a inverzními prvky značenými standardně symbolem $-$), potom množiny tvaru $n\mathbf{Z} = \{n \cdot z \mid z \in \mathbf{Z}\}$ jsou pro každé nezáporné celé n podgrupou grupy $\mathbf{Z}(+)$ (viz 0.1). Naopak, 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 $2n = n + n \in P$, $3n \in P$, \dots , $kn \in P$, \dots , pro každé přirozené k . Protože $-n \in P$, dostaneme 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 $a = qn + z$. \mathbf{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 $n\mathbf{Z} = P$.

Definice. Je-li H podgrupa G , definujme na G relaci $\text{rmod } H$ (resp. $\text{lmod } H$) podmínkou: $(a, b) \in \text{rmod } H$ (resp. $(a, b) \in \text{lmod } H$) $\Leftrightarrow a \cdot b^{-1} \in H$ (resp. $a^{-1} \cdot b \in H$).

Nechť H a K jsou dvě podmnožiny grupy $G(\cdot)$ a $g \in G$. Označme množiny $H \cdot K = \{h \cdot k \mid h \in H, k \in K\}$, $gH = \{g\}H$ a $Hg = H\{g\}$. V případě grup s operací \cdot budeme často psát hk místo $h \cdot k$ a HK místo $H \cdot K$.

Věta 1.11. *Nechť $G(\cdot)$ je grupa a H její podgrupa. Potom platí:*

- (1) $\text{rmod } H$ i $\text{lmod } H$ jsou ekvivalence na G ,
- (2) $(a, b) \in \text{rmod } H \Leftrightarrow (a^{-1}, b^{-1}) \in \text{lmod } H$ pro každé $a, b \in G$,
- (3) $|G/\text{rmod } H| = |G/\text{lmod } H|$,
- (4) $\text{rmod } H = \text{lmod } H$, 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) Tvzení dokážeme jen o $\text{rmod } H$, pro $\text{lmod } H$ bude důkaz symetrický. 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 1.5 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 $\text{rmod } H$ reflexivní, 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 $[a]_{\text{rmod } H} \rightarrow [a^{-1}]_{\text{lmod } H}$ korektně definovanou bijekcí, tedy faktorové množiny $G/\text{rmod } H$ a $G/\text{lmod } H$ mají stejně prvků.

(4) Předpokládejme, že $\text{rmod } H = \text{lmod } H$ 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 $\text{rmod } H$ dostaneme $g \cdot h \cdot g^{-1} \in H$.

Nyní předpokládejme, 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 $\text{rmod } H \subseteq \text{lmod } H$. Symetrický argument dokazuje obrácenou implikaci.

(5) Opět se budeme věnovat jen ekvivalenci $\text{rmod } H$. Použijeme definici rozkladové třídy:

$$\begin{aligned} [a]_{\text{rmod } H} &= \{b \in G \mid (a, b) \in \text{rmod } H\} = \{b \in G \mid \exists h \in H : a \cdot b^{-1} = h\} = \\ &= \{b \in G \mid \exists h \in H : b = h^{-1} \cdot a\} = \{b \in G \mid \exists h' \in H : b = h' \cdot a\} = Ha. \end{aligned}$$

(6) Definujme zobrazení $b : H \rightarrow Ha$ (resp. $H \rightarrow aH$) 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). \square

Definice. Bud' H podgrupa grupy $G(\cdot)$. Potom číslu $[G : H] = |G/\text{rmod } H|$ ($= |G/\text{lmod } H|$ podle 1.11) budeme říkat *index podgrupy H* v grupě G a velikosti $|G|$ množiny G budeme říkat *řád grupy G* .

Věta 1.12 (Lagrange). *Je-li H podgrupa grupy $G(\cdot)$, pak $|G| = [G : H] \cdot |H|$.*

Důkaz. Podle 1.11(1) je $\text{rmod } H$ ekvivalence, proto $G = \dot{\bigcup}_{A \in G/\text{rmod } H} A$, kde sjednocujeme disjunktní množiny. Využijeme-li dále poznatek 1.11(6), který říká, že všechny ekvivalenční třídy mají počet prvků stejný jako množina H , pak dostáváme

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

□

Důsledek 1.13. *Je-li $G(\cdot)$ konečná grupa, potom řád každé její podgrupy dělí řád grupy G .*

Příklad 1.14. Z předchozího důsledku okamžitě plynou následující pozorování:

- (1) Grupa prvočíselného řádu obsahuje jen triviální podgrupy, tedy G a $\{1\}$.
- (2) Protože $|S_{10}| = 10!$ a 11 nedělí $10!$, permutační grupa řádu $S_{10}(\circ)$ neobsahuje žádnou podgrupu řádu 11.
- (3) Jsou-li H a K dvě konečné podgrupy nějaké grupy $G(\cdot)$ a platí-li, že jsou řády H a K nesoudělné, pak $H \cap K = \{1\}$.

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 $\rho = \text{rmod } H$ ($= \text{lmod } H$).*

Důkaz. (\Rightarrow) Nejprve předpokládejme, že je ρ ekvivalence slučitelná s operací \cdot . Protože je ρ reflexivní relace, leží 1 v třídě $[1]_\rho$. 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 1.11(4) $\text{rmod } [1]_\rho = \text{lmod } [1]_\rho$.

Nyní bychom měli dokázat, že $(a, b) \in \rho$, právě když $(a, b) \in \text{lmod } [1]_\rho$. 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 ekvivalence slučitelná s \cdot , tedy $(a, b) \in \text{lmod } [1]_\rho$. Naopak, zvolíme-li $(a, b) \in \text{lmod } [1]_\rho$, 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 $\text{rmod } H$ (tj. $(a, b) \in \rho \Leftrightarrow a \cdot b^{-1} \in H$). Podle 1.11(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 . □

Všimněme si, že kongruence $\equiv (\text{mod } n)$ na množině $\mathbf{Z}(+)$ popsaná v Příkladu 0.5 je právě ekvivalencí $\text{rmod } n\mathbf{Z} = \text{lmod } n\mathbf{Z}$.

Vezmeme-li si například pro grupu $H = \{\text{id}, (12)\}$ grupy permutací $S_3(\circ)$, která podle 1.10(2) není normální, ekvivalence $\text{rmod}H$ podle předchozí věty není slučitelná s operací \circ a podle 1.11(4) platí $\text{rmod}H \neq \text{lmod}H$.

Definice. Zobrazení $f : G \rightarrow H$ grup $G(\cdot)$ a $H(\cdot)$ slučitelné s jejich binárními operacemi se nazývá (grupový) *homomorfismus*. Bijektivní homomorfismus budeme nazývat *izomorfismus*. Podmnožině $\text{Ker}f = \{g \in G \mid f(g) = 1\}$ i relaci $\text{ker}f = \{(g_1, g_2) \in G \times G \mid f(g_1) = f(g_2)\}$ 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 1.16. *Nechť $G_1(\cdot)$, $G_2(\cdot)$ a $G_3(\cdot)$ jsou grupy a $f : G_1 \rightarrow G_2$ a $g : G_2 \rightarrow G_3$ jsou homomorfismy.*

- (1) $f(1) = 1$ a $f(a^{-1}) = (f(a))^{-1}$ pro každé $a \in G$
- (2) gf je homomorfismus,
- (3) je-li f bijekce, pak f^{-1} je izomorfismus,
- (4) obraz $g(H)$ je podgrupa $G_3(\cdot)$ a úplný vzor $f^{-1}(H)$ je podgrupa $G_1(\cdot)$ pro každou podgrupu H grupy $G_2(\cdot)$,
- (5) $\text{Ker}f$ je normální podgrupa $G_1(\cdot)$ a $\text{ker}f = \text{rmod} \text{Ker}f = \text{lmod} \text{Ker}f$ je ekvivalence slučitelná s operací \cdot na G_1 ,
- (6) f je prostý homomorfismus, právě když $\text{Ker}f = \{1\}$ a to nastává, právě když $\text{ker}f = \text{id}$.

Důkaz. (1) 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 $1 = f(1) = f(a^{-1} \cdot a) = f(a^{-1}) \cdot f(a)$ a podobně $1 = f(a) \cdot f(a^{-1})$, proto $f(a^{-1}) = (f(a))^{-1}$.

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

(3) 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 $f^{-1}(c) \cdot f^{-1}(d) = f^{-1}(c \cdot d)$.

(4) Nejprve ukážeme, že je $g(H)$ podgrupa $G_3(\cdot)$. Podle 1.16(1) je $1 = g(1) \in g(H)$. Vezmeme $u, v \in g(H)$, 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(1).

Poznamenejme, že $1 \in f^{-1}(H)$ 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 $a \cdot b, a^{-1} \in f^{-1}(H)$, proto je $f^{-1}(H)$ podgrupa.

(5) Protože $\{1\}$ je podgrupa $G_2(\cdot)$ a $\text{Ker}f = f^{-1}(\{1\})$, je $\text{Ker}f$ podgrupa podle (3). Vezmeme-li libovolné $g \in G_1$ a $h \in \text{Ker}f$, 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 $g \cdot h \cdot g^{-1} \in \text{Ker}f$. Zbývá si uvědomit, že $f(a) = f(b) \Leftrightarrow f(a) \cdot f(b)^{-1} = 1 \Leftrightarrow f(a \cdot b^{-1}) = 1 \Leftrightarrow a \cdot b^{-1} \in \text{Ker}f$. Konečně $\text{ker}f = \text{rmod} \text{Ker}f = \text{lmod} \text{Ker}f$ je ekvivalence podle 1.15.

(6) Je-li f prosté, pak existuje jediný vzor jednotky, tedy $\text{Ker}f = \{1\}$ a jestliže $\text{ker}f = \text{id}$, pak je zřejmě f prosté. Konečně, jestliže $\text{Ker}f = \{1\}$, potom $\text{ker}f = \text{rmod} \text{Ker}f = \text{rmod} \{1\} = \text{id}$ podle (4). \square

Příklad 1.17. (1) V rámci kurzu lineární algebry bylo dokázáno, že znaménko součinu permutací je rovno součinu jejich znamének, tedy, že $\text{sgn} : S_n \rightarrow \{1, -1\}$ je

homomorfismus grup permutací na n prvcích a grupy $\{1, -1\}(\cdot)$. Snadno nahlédneme, $\text{Ker sgn} = A_n$, což je podle 1.16 normální podgrupa grupy S_n .

(2) Rovněž v lineární algebře se dokazuje, že determinant \det je homomorfismus z grupy regulárních matice $n \times n$ nad tělesem T do multiplikativní grupy tělesa $T \setminus \{0\}(\cdot)$ je homomorfismus a tedy $\text{Ker } \det$ je díky 1.16 normální podgrupa matice s determinátem 1.

(3) Jsou-li U a V dva vektorové prostory nad týmž tělesem a $f : U \rightarrow V$ je lineární zobrazení, pak je f homomorfismus grup $U(+)$ a $V(+)$, kde je $+$ sčítáním vektorů.

Je-li G množina a ρ ekvivalence na G , pak *přirozenou projekci* na faktorovou množinu G/ρ rozumíme zobrazení $\pi_\rho : G \rightarrow G/\rho$ dané podmínkou $\pi_\rho(g) = [g]_\rho$, kde $g \in G$. Všimněme si, že $\ker \pi_\rho = \rho$.

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, musíme 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. \square

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 $H = [1]_\rho$, nám umožňuje faktorovou množinu zapisovat ve tvaru G/H , tedy $G/H := G/\text{rmod} H$.

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 $[a]_H = aH = Ha$ (poslední rovnosti platí podle 1.11(4) a (5)).

Příklad 1.19. Uvážíme-li na grupě $\mathbf{Z}(+)$ ekvivalenci $\equiv (\text{mod } n)$ zavedenou v Příkladu 0.5, jedná se o ekvivalenci slučitelnou s operací $+$ a $[0]_{\equiv (\text{mod } n)} = n\mathbf{Z}$, tedy $\equiv (\text{mod } n) = \text{rmod } n\mathbf{Z}$ a na faktorové množině $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}/(\equiv (\text{mod } n))$ máme dobře zavedenu strukturu grupy $\mathbf{Z}/n\mathbf{Z}(+)$ předpisem $[a]_{\equiv (\text{mod } n)} + [b]_{\equiv (\text{mod } n)} = [a + b]_{\equiv (\text{mod } n)}$.

Věta 1.20. *Nechť $f : G_1 \rightarrow G_2$ je homomorfismus grup $G_1(\cdot)$ a $G_2(\cdot)$.*

(1) (Věta o homomorfismu) *Je-li H normální podgrupa $G_1(\cdot)$, pak existuje homomorfismus $g : G_1/H \rightarrow G_2$ splňující podmínku $g\pi_H = f$ právě tehdy, když $H \subseteq \text{Ker } f$ (tj. $\text{rmod} H \subseteq \text{rmod } \text{Ker } f$). Navíc, jestliže g existuje, je g izomorfismus, právě když f je na $\text{Ker } f = H$.*

(2) (1. věta o izomorfismu) *$f(G_1)$ je podgrupa G_2 (tedy opět grupa) a $G_1/\text{Ker } f(\cdot)$ je izomorfní $f(G_1)(\cdot)$.*

Důkaz. (1) Nejprve předpokládejme, že existuje homomorfismus $g : G_1/H \rightarrow G_2$ 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(1). Tedy $a \in \text{Ker } f$, čímž jsme ověřili, že $H \subseteq \text{Ker } f$.

Naopak, nechť $H \subseteq \text{Ker } f$. Musíme ověřit, že jediná možná definice g daná předpisem $g([a]_H) = f(a)$ je korektní. Vezměme proto $[a]_H = [b]_H$. Potom $a \cdot b^{-1} \in H \subseteq \text{Ker } f$, tedy $1 = f(a \cdot b^{-1}) = f(a) \cdot f(b)^{-1}$ podle 1.16(1), 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 $a \in \text{Ker } f$. 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 $\text{Ker } f \subseteq H$, a protože už víme, že $H \subseteq \text{Ker } f$, máme rovnost $H = \text{Ker } f$. Konečně předpokládejme, že $g([a]_H) = g([b]_H)$. Potom $f(a) = f(b)$ a $a \cdot b^{-1} \in \text{Ker } f = H$. Tudíž $(a, b) \in \text{rmod } H$ a $[a]_H = [b]_H$, čímž jsme ověřili, že je g prosté.

(2) Z 1.16(5) dostáváme, že $f(G_1)$ je podgrupa G_2 . Omezíme-li obor hodnot zobrazení f , můžeme ho chápat jako homomorfismus $f : G_1 \rightarrow f(G_1)$. Nyní aplikujeme (1) pro $H = \text{Ker } f$ a dostaneme přímo požadovaný izomorfismus $g : G_1/\text{Ker } f \rightarrow f(G_1)$. \square

Příklad 1.21. Mějme homomorfismus $f_n : \mathbf{Z} \rightarrow \mathbf{Z}_n$ grupy $\mathbf{Z}(+)$ do grupy $\mathbf{Z}_n(+)$ s počítáním modulo n daný předpisem $f_n(k) = (k) \bmod n$. Pak máme podle 1.20(2) izomorfismus $\mathbf{Z}/\text{Ker } f_n \cong \mathbf{Z}_n(+)$, navíc je zjevně $(a, b) \in \text{ker } f_n$, právě když $n \mid (a - b)$, a $\text{Ker } f_n = n\mathbf{Z}$.

Věta 1.22 (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. Nejprve použijeme 1.20(1) pro homomorfismy $\pi_K : G \rightarrow G/K$ (jako f z 1.20(1)) a $\pi_H : G \rightarrow G/H$ (jako π_H z 1.20(1)). Protože podle předpokladu $H \subseteq K = \text{Ker } \pi_K$, dává nám 1.20(1) homomorfismus $g : G/H \rightarrow G/K$ splňující vztah $g([a]_H) = [a]_K$. Všimněme si, že je g zjevně na. Nyní přímočaře spočítáme $\text{Ker } g = \{[a]_H \in G/H \mid g([a]_H) = [a]_K = [1]_K\} = K/H$. Poznamenejme, že je $\text{Ker } g = K/H$ normální podgrupa $G/H(\cdot)$ podle 1.16(5). Nyní pro homomorfismus g využijeme 1.20(2), abychom dostali $G/K = g(G/H) \cong (G/H)/\text{Ker } g = (G/H)/(K/H)$. \square

2. CYKlickÉ GRUPY

Připomeňme, že podle 1.9(2) 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 $\{g\}$, je-li $g \in G$.

Definice. Bud' $G(\cdot)$ 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 $\langle g \rangle = G$.

Příklad 2.1. (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 $\text{NSD}(a, n) = 1$.

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

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

Poznámka 2.2. Nechť $G(\cdot)$ je grupa a $a \in G$. Zobrazení $\phi : \mathbf{Z} \rightarrow G$ dané předpisem $\phi(n) = a^n$ je homomorfismus grupy $\mathbf{Z}(+)$ do grupy $G(\cdot)$ a $\phi(\mathbf{Z}) = \langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$.

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 $\phi(\mathbf{Z}) = \{a^n \mid n \in \mathbf{Z}\}$, a proto se jedná o nejmenší podgrupu $G(\cdot)$ obsahující a . \square

Důsledek 2.3. Nechť $G(\cdot)$ je grupa a $a \in G$. Potom pro každé $n, m \in \mathbf{Z}$ platí, že $a^{-n} = (a^n)^{-1}$ a $(a^n)^m = a^{nm}$.

Věta 2.4. Bud' $G(\cdot)$ 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 $\phi : \mathbf{Z} \rightarrow G$ dané předpisem $\phi(n) = g^n$. Podle 2.2 jde o homomorfismus a $\phi(\mathbf{Z}) = \langle g \rangle = G$, tedy ϕ je zobrazení na. Nyní podle 1.20(2) je $\mathbf{Z}/\text{Ker}\phi(+) \cong G(\cdot)$. Zbývá si rozmyslet, jak vypadá $\mathbf{Z}/\text{Ker}\phi$. Z 1.10(4) víme, že $\text{Ker}\phi = n\mathbf{Z}$ pro vhodné nezáporné celé n . V případě, že $n = 0$, pak $\mathbf{Z}/\text{Ker}\phi = \mathbf{Z}/\{0\} \cong \mathbf{Z}$, a v případě kladného n je $\mathbf{Z}/\text{Ker}\phi = \mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$ podle 1.21. \square

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(4) 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 $f_n : \mathbf{Z} \rightarrow \mathbf{Z}_n$ z 1.21. Zvolíme-li podgrupu H grupy $\mathbf{Z}_n(+)$, pak $f_n^{-1}(H)$ je podle předchozí úvahy a 1.16(5) cyklická podgrupa \mathbf{Z} , tedy $H = f_n(f_n^{-1}(H))$ je cyklická podgrupa $\mathbf{Z}_n(+)$. \square

Připomeňme, že pro každé přirozené k značíme $k\mathbf{Z} = \langle k \rangle = \{kz \mid z \in \mathbf{Z}\}$. Podobně budeme pro každé $k \in \mathbf{Z}_n$ označovat $k\mathbf{Z}_n = \langle k \rangle = \{k \cdot z \mid z \in \mathbf{Z}_n\}$.

Poznámka 2.6. *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 $\text{NSD}(a, n) = k$.*

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 $(a \cdot x) \bmod n = k$. Proto také existuje takové celé y , že $a \cdot x + n \cdot y = k$. Odtud plyne, že $\text{NSD}(a, n)/k$. 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 $k/\text{NSD}(a, n)$, tudíž $\text{NSD}(a, n) = k$.

Nyní předpokládejme, že $\text{NSD}(a, n) = k$. Potom díky Euklidovu algoritmu existují $x \in \mathbf{Z}_n$ a celé y , pro něž $a \cdot x + n \cdot y = k$. Proto $(a \cdot x) \bmod n = k$, 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 $k\mathbf{Z}_n = a\mathbf{Z}_n$. \square

Uvědomíme-li si, že speciálním případem předchozí poznámky pro $k = 1$ je tvrzení, že $a\mathbf{Z}_n = \mathbf{Z}_n$ (tj. a generuje grupu $\mathbf{Z}_n(+)$), právě když $\text{NSD}(a, n) = 1$, okamžitě dostáváme:

Důsledek 2.7. *Je-li $n \in \mathbf{N}$, pak číslo $\varphi(n)$ udává počet prvků, které generují grupu $\mathbf{Z}_n(+)$ a počet invertibilních prvků monoidu $\mathbf{Z}_n(\cdot)$.*

Poznámka 2.8. *Bud' $G(\cdot)$ 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 1.12 $n/|G|$, tedy $g^{|G|} = (g^n)^{\frac{|G|}{n}} = 1^{\frac{|G|}{n}} = 1$, kde 1. rovnost plyne z 2.3. \square

Věta 2.9. *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 $\langle \frac{n}{k} \rangle = \{0, \frac{n}{k}, 2\frac{n}{k}, \dots, (k-1)\frac{n}{k}\}$ je podgrupa a $|\langle \frac{n}{k} \rangle| = k$.

Mějme nyní nějakou podgrupu H grupy $\mathbf{Z}_n(+)$ řádu k . Pak je H podle 2.5 cyklická, a tedy existuje $h \in H$, pro $H = \langle h \rangle$. Z 2.8 plyne, že $(k \cdot h) \bmod n = 0$, a 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. \square

Následující tvrzení je pro prvočíselné n známo také jako Malá Fermatova věta:

Věta 2.10 (Eulerova věta). *Pro nesoudělná kladná celá čísla $a, n > 1$ je*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Důkaz. Díky Poznámce 0.6 tvrzení stačí dokázat pro kladné $a < n$. Použijeme k tomu Poznámku 2.8, kde jako grupu G vezmeme grupu invertibilních prvků $\mathbf{Z}_n^*(\cdot)$ monoidu $\mathbf{Z}_n(\cdot)$ tj. prvků nesoudělných s n podle 2.7. Protože $a \in \mathbf{Z}_n^*$, je $(a^{\varphi(n)}) \bmod n = (a^{|\mathbf{Z}_n^*|}) \bmod n = 1$ díky 2.8 a 2.7. \square

Příklad 2.11. (1) Uvažujme konečnou cyklickou grupu $G(\cdot)$. Potom nám 2.7 říká, že $G(\cdot)$ obsahuje právě $\varphi(|G|)$ generátorů. Protože díky Lagrangeově větě řád podgrupy vždy dělí řád grupy podle 2.9 $G(\cdot)$ pro každý dělitel řádu cyklické grupy existuje právě jedna podgrupa daného řádu, obsahuje $G(\cdot)$ právě tolik podgrup,

kolik existuje dělitelů jejího řádu. Máme-li $n = \prod_{i=1}^k p_i^{r_i}$, kde $p_1 < p_2 < \dots < p_k$ jsou prvočísla a $r_i \in \mathbf{N}$, pak děliteli n jsou právě čísla $\prod_{i=1}^k p_i^{s_i}$, kde $0 \leq s_i \leq r_i$, tedy $G(\cdot)$ obsahuje právě $\prod_{i=1}^k (r_i + 1)$ podgrup a podle 0.11 právě $\prod_{i=1}^k (p_i - 1)p_i^{r_i - 1}$ generátorů.

(2) Konkrétně, vezmeme-li cyklickou grupu $\mathbf{Z}_{50}(+)$. Protože $50 = 2 \cdot 5^2$, dostáváme z bodu (1), že $\mathbf{Z}_{50}(+)$ obsahuje $\varphi(50) = 20$ generátorů a právě $6 = 2 \cdot 3$ 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 2.6 víme, že $\langle 42 \rangle = \langle \text{NSD}(42, 50) \rangle = \langle 2 \rangle = 2\mathbf{Z}_{50}$, a jedná se tedy o podgrupu řádu $25 = \frac{50}{2}$.

Příklad 2.12 (Rivest, Shamir, Adleman). Zvolíme p a q dvě různá lichá prvočísla a položíme $m = \text{nsn}(p - 1, q - 1)$. Nejprve dokážeme drobný důsledek 2.10 a 0.8:

Lemma. Pro každé $a \in \mathbf{Z}_{pq}$ a $u \in \mathbf{N}$ platí, že $(a^{mu+1}) \bmod pq = a$.

Důkaz lemmatu: Nejprve ukážeme, že $(a^{m+1}) \bmod pq = a$.

Podle Věty 2.10 $(x^m) \bmod p = 1$ a $(y^m) \bmod q = 1$ pro ta x , která nejsou násobkem p a ta y , která nejsou násobkem q . Dále zřejmě platí $((up)^{m+1}) \bmod p = 0$, a proto i $(x^{m+1}) \bmod p = (x) \bmod p$ a $(y^{m+1}) \bmod q = (y) \bmod q$ pro každé nezáporné celé x a y . Vezměme nyní $a \in \mathbf{Z}_{pq}$. Z předchozího pozorování plyne, že $((a) \bmod p, (a) \bmod q) = ((a^{m+1}) \bmod p, (a^{m+1}) \bmod q)$, a díky Větě 0.8 použité pro bijekci $\mathbf{Z}_{pq} \rightarrow \mathbf{Z}_p \times \mathbf{Z}_q$ dostáváme, že shodné jsou i vzory prvků $((a) \bmod p, (a) \bmod q)$ a $((a^{m+1}) \bmod p, (a^{m+1}) \bmod q)$, tedy, že $(a^{m+1}) \bmod pq = a$.

Nyní indukcí díky 2.3 dostáváme, 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 $a \in \mathbf{Z}_{pq}$. \square

Vezměme $e < m$ nesoudělné s m a pak (například pomocí Euklidova algoritmu) najdeme takové $d < m$, že $(ed) \bmod m = 1$.

Nyní podle lemmatu 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 vlastností 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 dvojice čísel (n, e) a soukromý klíč tvoří *tajný exponent* d . Chceme-li informaci vyjádřenou posloupností hodnot $a_1, \dots, a_k \in \mathbf{Z}_n$ adresovat majiteli soukromého klíče, stačí ji zašifrovat pomocí mocnění veřejně známou hodnotou e v monoidu $\mathbf{Z}_n(\cdot)$, tj. odeslat zprávu $(a_1^e) \bmod pq, \dots, (a_k^e) \bmod pq$. K jejímu rozluštění stačí umocnit v $\mathbf{Z}_n(\cdot)$ pomocí tajného exponentu, protože $(a_i^e)^d = a_i^{ed} = a_i$. Naopak, zveřejnění-li majitel soukromého klíče zašifrovanou zprávu $(a_1^d) \bmod n, \dots, (a_k^d) \bmod n$, mohou si příjemci zprávy stejným způsobem (tj. umocněním na veřejně známý exponent e : $((a_1^d)^e) \bmod n, \dots, ((a_k^d)^e) \bmod n = a_1, \dots, a_k$) ověřit, že odesílatel zprávy opravdu zná tajný exponent (vlastnictví soukromého klíče tedy garantuje pravost elektronického podpisu).

Poznamenejme, že je ze znalosti $n = pq$ 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.

3. UNIVERZÁLNÍ POHLED: POJEM ALGEBRY

Definice. Pro každé celé $n \geq 0$ nazveme n -ární operací na množině A každé zobrazení $A^n \rightarrow A$ (číslo n budeme nazývat *aritou* nebo *četností* operace). Je-li I množina, budeme říkat zobrazení $\Omega : I \rightarrow \mathbf{N}_0 = \mathbf{N} \cup \{0\}$ *typ*. Řekneme, že $A(\alpha_i | i \in I)$ je *algebra typu* Ω , je-li A neprázdná a pro každé $i \in I$ je α_i právě $\Omega(i)$ -ární operací na A .

1-ární operace se obvykle nazývají unárními operacemi, 2-árními operacím se říká binární operace a 3-ární se nazývají ternárními operacemi.

Všimněme si, že množina A^0 sestává právě z prázdné posloupnosti, tedy je jednoprvková. Nulární operace tudíž vyznačuje v algebře jeden její prvek, a proto ji můžeme s tímto vyznačeným prvkem ztotožnit.

Příklad 3.1. (1) Uvážíme grupu $G(\cdot)$ s unární operací inverzního prvku $^{-1}$ a nulární operací 1. Pak $G(\cdot)$, $G(\cdot, ^{-1})$, $G(\cdot, ^{-1}, 1)$ tvoří (nejen formálně) různé algebry.

(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 $V(+, \cdot | t \in \mathbf{T})$ nebo $V(+, 0, \cdot | t \in \mathbf{T})$. Všimněme si, že pro nekonečné těleso potřebujeme uvažovat nekonečně mnoho unárních operací.

Definice. Bud' 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 , $i \in I$.

Příklad 3.2. Nahlédneme, jak v jednotlivých případech algeber z Příkladu 3.1 vypadají podalgebry.

(1) Pro grup $G(\cdot)$ máme:

- Podalgebry $G(\cdot, ^{-1}, 1)$ jsou právě podmnožiny G uzavřené na 1 (tj. obsahující prvek 1), na inverzy a součiny, což jsou podle definice právě podgrupy grupy $G(\cdot)$.
- Je-li H neprázdná podalgebra $G(\cdot, ^{-1})$, pak existuje $h \in H$, a proto $1 = h \cdot h^{-1} \in H$. Tedy neprázdné podalgebry $G(\cdot, ^{-1})$ jsou právě podgrupy $G(\cdot)$, navíc prázdná množina je v souladu s definicí také podalgebra.
- Podalgeber algebry $G(\cdot)$ je obecně mnohem víc než podgrup grupy $G(\cdot)$. Například pro každé $g \in G$ a $n \in \mathbf{N}$ tvoří množina $\{g^k | k \geq n\}$ podalgebry $G(\cdot)$. V případě $G(\cdot) = \mathbf{Z}(+)$ to znamená, že množiny $\{ak | k \geq n\}$ jsou podalgebry, speciálně množina všech přirozených čísel, která podgrupou $\mathbf{Z}(+)$ určitě není.

(2) Podalgebrou algebry $V(+, 0, \cdot | t \in \mathbf{T})$ jsou právě podprostory tohoto vektorového prostoru a podalgebry algebry $V(+, \cdot | t \in \mathbf{T})$ jsou právě podprostory a prázdná množina.

Označíme-li $\beta_i = \alpha_i|_{B^n}$ omezení n -ární operace α_i na B^n , potom pro podalgebry 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 $f : A \rightarrow B$ je *slučitelné s operací* α , jestliže $f(\alpha(a_1, \dots, a_n)) = \alpha(f(a_1), \dots, f(a_n))$. Zobrazení $f : A \rightarrow B$ mezi dvěma algebrami $A(\alpha_i | i \in I)$ a $B(\alpha_i | i \in I)$ stejného typu Ω budeme říkat *homomorfismus*, je-li slučitelné se

všemi operacemi α_i , $i \in I$. Bijektivní homomorfismus budeme nazývat *izomorfismus*. Jestliže mezi dvěma algebry $A(\alpha_i | i \in I)$ a $B(\alpha_i | i \in I)$ existuje izomorfismus, říkáme, že A a B jsou *izomorfní* a píšeme $A(\alpha_i | i \in I) \cong B(\alpha_i | i \in I)$ nebo zjednodušeně $A \cong B$.

Příklad 3.3. (1) Bud' $G_i(\cdot)$ pro $i = 1, 2$ grupy s unární operací inverzního prvku $^{-1}$ a nulární operací 1 . Pak každý homomorfismus grup $G_1(\cdot)$ a $G_2(\cdot)$ je podle 1.16(1) 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) Necht' U a V jsou dva vektorové prostory nad tělesem T . Potom každé lineární zobrazení (homomorfismus) vektorových prostorů je homomorfismem algeber $U(+, \cdot | t \in T)$ a $V(+, \cdot | t \in T)$.

Definice. Necht' ρ je ekvivalence 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 3.4. (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 $f : A \rightarrow B$ zobrazení, rozumíme jeho *jádrem* $\ker f$ relací danou předpisem: $(a, b) \in \ker f \Leftrightarrow f(a) = f(b)$. Nyní jsme připraveni vyslovit obdobu Poznámky 1.16 pro obecné algebry:

Poznámka 3.5. Necht' $A_1(\alpha_i | i \in I)$, $A_2(\alpha_i | i \in I)$ a $A_3(\alpha_i | i \in I)$ jsou algebry stejného typu, $f : A_1 \rightarrow A_2$ a $g : A_2 \rightarrow A_3$ 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 1.16.

(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) Necht' je opět α_i libovolná n -ární operace na A_2 i A_3 . Vezmeme 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) Vezmeme 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. \square

Poznámka 3.6. *Nechť $A(\alpha_i \mid i \in I)$ je algebra a A_j jsou podalgebry A a ρ_j kongruence na A pro každé $j \in J$.*

- (1) $\bigcap_{j \in J} A_j$ je podalgebra A ,
- (2) $\bigcap_{j \in J} \rho_j$ je kongruence na A .

Důkaz. (1) Obdoba Poznámky 1.9(2). 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 $A(\alpha_i \mid i \in I)$ 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) Fakt, že je průnik ekvivalencí je ekvivalence je snadné cvičení.

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 $(\alpha_i(a_1, \dots, a_n), \alpha_i(b_1, \dots, b_n)) \in \bigcap_{j \in J} \rho_j$. \square

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

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.

Poznámka 3.7. *Je-li ρ kongruence na algebře A , pak je definice algebry A/ρ korektní, jde o algebru stejného typu jako A a přirozená projekce $\pi_\rho : A \rightarrow A/\rho$ je homomorfismus.*

Důkaz. Vezměme libovolnou n -ární operaci α algebry A a nechť $[a_j]_\rho = [b_j]_\rho$, kde $j = 1, \dots, n$. 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. \square

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 3.8. *Bud' 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 . \square

Nyní už můžeme vyslovit obecné verze Věty o homomorfismu a Vět o izomorfismu:

Věta 3.9. *Nechť $f : A \rightarrow B$ je homomorfismus dvou algeber stejného typu.*

(1) (Věta o homomorfismu) *Je-li ρ kongruence na algebře A , pak existuje homomorfismus $g : A/\rho \rightarrow B$ 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 $\ker f = \rho$.*

(2) (1. věta o izomorfismu) *$f(A)$ je podalgebra B (tedy algebra stejného typu) a $A/\ker f$ je izomorfní $f(A)$.*

Důkaz. Tvrzení dokážeme stejně jako Větu o homomorfismu a 1. věta o izomorfismu pro grupy (1.20).

(1) Nejprve předpokládejme, že existuje homomorfismus $g : A/\rho \rightarrow B$ 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 dokažme závěrečnou ekvivalenci. Protože $g(G_1/\rho) = f(G_1)$, 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.

(2) Rozmyslíme si, že podle 3.5(3) je $f(A)$ podalgebra B a poté stejně jako v důkazu 1.20(2) použijeme Větu o homomorfismu (1) na $\rho = \ker f$. \square

Věta 3.10 (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 1.22: nejprve použijeme 3.9(1) pro homomorfismy $\pi_\sigma : A \rightarrow A/\sigma$ a $\pi_\rho : A \rightarrow A/\rho$, která nám dává homomorfismus $g : A/\rho \rightarrow A/\sigma$ splňující vztah $g([a]_\rho) = [a]_\sigma$. Zbývá spočítat $\ker g = \sigma/\rho$ a použít 3.9(2). \square

Nyní zobecníme definici ze začátku 2.kapitoly.

Definice. Bud' 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 $\langle X \rangle$).

Příklad 3.11. (1) Uvažujme algebra $\mathbf{Z}(+)$. Pak sice $\langle \{1\} \rangle = \mathbf{N}$, ale nejmenší podalgebra $\mathbf{Z}(+)$ obsahující množinu $\{-1, 1\}$ je už rovna celému \mathbf{Z} tj. $\langle \{-1, 1\} \rangle = \mathbf{Z}$.

(2) Uvažujme-li nyní algebra $\mathbf{Z}(+, -)$, pak $\langle 1 \rangle = \mathbf{Z}$.

Zobecníme princip dobře známý z lineární algebry, který říká, že je homomorfismus určen hodnotami na množině generátorů:

Poznámka 3.12. *Bud' $f, g : A \rightarrow B$ dva homomorfismy algeber stejného typu a necht' $X \subseteq A$ generuje algebra A . Jestliže $f(x) = g(x)$ pro všechna $x \in X$, potom $f = g$.*

Důkaz. Nejprve ukážeme, že je množina $C = \{a \in A \mid f(a) = g(a)\}$ podalgebrou algebry A . Vezměme n -ární operaci α algebry A a necht' $a_1, \dots, a_n \in C$. 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. \square

Velmi důležitým a užitečným faktem obecné algebry, který jsme už bez velkých komentářů několikrát použili, je pozorování, že dvě izomorfní algebry jsou z hlediska algebry nerozlišitelné, mají všechny vlastnosti stejné a platí o nich tudíž stejná tvrzení. Důvod platnosti takového pozorování je v podstatě velmi elementární: u vlastností izomorfních algeber nezáleží na tom jak konkrétně vypadají jejich prvky (a „překlad“ zajišťuje bijekce určená izomorfismem), podstatné je, že operace jsou na odpovídajících prvcích stejné, což právě zajišťuje slučitelnost operace s homomorfismem. Samotná přesná formalizace uvedené myšlenky vyžaduje pečlivou práci s formální logikou a my ji pouze pro informaci alespoň naznačíme na závěr této sekce.

Připomeňme, že term je jakákoli proměnná a jsou-li t_1, \dots, t_n termy a α funkční symboly (operace) četnosti n , pak i $\alpha(t_1, \dots, t_n)$, je term, dále je-li P predikát četnosti n a t_1, \dots, t_n jsou termy, pak je výraz $P(t_1, \dots, t_n)$ atomickou formulí a a jsou-li φ a ψ dvě formule, pak výrazy $(\varphi \rightarrow \psi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $\neg\varphi$, $\forall\varphi$ a $\exists\varphi$ jsou rovněž formule. Jazykem predikátové logiky (prvního řádu) potom rozumíme všechny formule, které vyniknou z daného systémem funkčních a predikátových symbolů.

Dále připomeňme, že formule φ platí ve struktuře \mathbf{A} (tedy například v algebře s daným systémem operací, které se v jazyce algeber daného typu objeví jako funkční symboly), právě když je φ splněna každým ohodnocením proměnných nosné množiny A struktury \mathbf{A} . Uzavřenou formulí rozumíme formuli, která neobsahuje žádnou volnou proměnnou. V našich úvahách se pro jednoduchost omezíme na jazyk s jediným predikátovým symbolem $=$ a proměnnými jako prvky algebry.

Poznámka 3.13. *Necht' $A(\alpha_i \mid i \in I)$ a $B(\alpha_i \mid i \in I)$ jsou dvě izomorfní algebry (stejného typu). Potom uzavřená formule φ jazyka algeber platí v algebře $A(\alpha_i \mid i \in I)$, právě když platí v algebře $B(\alpha_i \mid i \in I)$.*

Důkaz. Necht' $f : A \rightarrow B$ je nějaký izomorfismus algeber $\mathbf{A} = A(\alpha_i \mid i \in I)$ a $\mathbf{B} = B(\alpha_i \mid i \in I)$, φ formule. Vezmeme-li nějaké ohodnocení e formule φ v A , označíme fe , které hodnotě $e(x)$ nějaké proměnné v A přiřadí hodnotu $fe(x)$ téže proměnné v B . Je-li E množina všech ohodnocení formule φ v A , vidíme, že množina $\{fe \mid e \in E\}$ tvoří právě množinu všech ohodnocení formule φ v B , neboť f je bijekce. Dále snadno nahlédneme, že a pro každou uzavřenou formulí φ platí, že buď $\mathbf{A} \models \varphi$ nebo $\mathbf{A} \models \neg\varphi$, a protože f je izomorfismus algeber \mathbf{A} a \mathbf{B} , stačí indukci podle počtu kroků, jimiž je φ odvozena z atomický formulí a jimiž jsou v nich vytvořeny zúčastněné termy, dokázat $\mathbf{A} \models \varphi$ implikuje $\mathbf{B} \models \varphi$.

Nejprve uvážíme jedinou atomickou formulí $t = s$, kde $t = t(x_1, \dots, x_n)$ a $s = s(x_1, \dots, x_n)$ jsou termy v proměnných x_1, \dots, x_n . Mějme realizaci nějaké funkčního symbolu na obou algebrách, tedy právě n -ární operaci α_i pro nějaké $i \in I$ a předpokládáme například, že $t = \alpha_i(t_1, \dots, t_n)$, kde t_1, \dots, t_n jsou termy a necht' e je nějaké ohodnocení formule $t = s$. Protože $e(\alpha_i(t_1, \dots, t_n)) = \alpha_i(e(t_1), \dots, e(t_n))$ a z indukčního předpokladu užitého pro termy t_1, \dots, t_n víme, že $f(e(t_i)) = fe(t_i)$

(t.j. obraz izomorfismem f termu t_i ohodnoceného v algebře A pomocí e je týž jako ohodnocení termu t_i ohodnocený v algebře B ohodnocením fe). Protože je f homomorfismus, vidíme, že

$$\begin{aligned} f(e(\alpha_i(t_1, \dots, t_n))) &= f(\alpha_i(e(t_1), \dots, e(t_n))) = \\ &= \alpha_i(fe(t_1), \dots, fe(t_n)) = fe(\alpha_i(t_1, \dots, t_n)). \end{aligned}$$

Tím jsme ověřili, že platnost $e(t) = e(s)$ implikuje platnost $fe(t) = fe(s)$.

Zbytek důkazu už je jen přímočaré indukční ověření platnosti formule na \mathbf{B} vzniklé použitím pravidel $(\varphi \rightarrow \psi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $\neg\varphi$, $(\forall x)\varphi$ a $(\exists x)\varphi$ z kratších formulí φ a ψ za předpokladu, že daná dlouhá formule platí na \mathbf{A} . \square

Závěrem poznamenejme, že ve skutečnosti na izomorfních algebrách ekvivalence platí i pro výroky vyřčené v mnohem bohatším jazyce (například tvrzení, které se vyslovuje o struktuře podalgeber nějaké algebry).

4. OKRUHY, IDEÁLY A TĚLESA

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.

Prvek okruhu $R(+, \cdot, -, 0, 1)$ se nazývá *invertibilní*, jedná-li se o invertibilní prvek monoidu $R(\cdot)$ a o (komutativní) okruhu řekneme, že je (komutativní) *těleso*, jsou-li všechny prvky množiny $R \setminus \{0\}$ invertibilní a $0 \neq 1$.

Příklad 4.1. (1) Je-li T těleso ve smyslu definice z lineární algebry, pak je algebra $T(+, \cdot, -, 0, 1)$ komutativním tělesem.

(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.

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

Poznámka 4.2. *Nechť $R(+, \cdot, -, 0, 1)$ je okruh. Pak pro každé $a, b \in R$ platí:*

- (1) $0 \cdot a = a \cdot 0 = 0$,
- (2) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$, $(-1) \cdot a = a \cdot (-1) = -a$,
- (3) 1 je různé od 0 , právě když $|R| > 1$ (tj. R je netriviální okruh).

Důkaz. U bodů (1) a (2) 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).

Poslední rovnost dostáváme přímo z (2) pro $b = 1$.

(3) 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). \square

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 homomorfismus (izomorfismus) příslušných algeber.

Příklad 4.3. (1) $\{0\}$ a R jsou (tzv. *triviálními*) ideály každého okruhu R .

(2) Podle 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 .

(3) Množiny $aR = \{a \cdot r \mid r \in R\}$ (resp. $Ra = \{r \cdot a \mid r \in R\}$) 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 4.2(2). Dále $0 = a0 \in aR$ díky 4.2(1) a $(ar)x = a(rx) \in aR$ díky asociativitě pro libovolné $x \in R$.

Definice. O (levém, pravém) ideálu I okruhu $R(+, \cdot, -, 0, 1)$ řekneme, že je *vlastní*, jestliže $I \neq \{0\}$ a $I \neq R$ a, že je *maximální*, jestliže $I \neq R$ a neexistuje žádný (levý, pravý) ideál J splňující $I \subset J \subset R$ a $I \neq J \neq R$.

Poznámka 4.4. 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. \square

Věta 4.5. 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 4.4.

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 4.2(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 1.5 a b je tedy inverzní k a . \square

Poznamenejme, že existují okruhy (říká se jim *jednoduché*), které neobsahují žádné vlastní (oboustranné) ideály, a zároveň se nejedná o tělesa. Typickým příkladem jsou maticové okruhy $M_n(T)$, kde $n > 1$ a T je komutativní těleso.

Uvážíme-li ideál I okruhu $R(+, \cdot, -, 0, 1)$, pak je I podgrupa grupy $R(+)$, tedy můžeme pracovat s ekvivalencí $\text{rmod } I$ danou podmínkou $(a, b) \in \text{rmod } I \Leftrightarrow a - b = a + (-b) \in I$.

Nyní budeme aplikovat Větu 1.15 na aditivní grupu okruhu:

Věta 4.6. Je-li $R(+, \cdot, -, 0, 1)$ okruh, pak zobrazení $I \mapsto \text{rmod } I$ a $\rho \mapsto [0]_\rho$ jsou vzájemně inverzní zobrazení mezi množinou všech ideálů grupy $R(+, -, 0)$ a množinou všech kongruencí okruhu.

Důkaz. Podle Větu 1.15 jsou $H \mapsto \text{rmod } H$ a $\rho \mapsto [0]_\rho$ vzájemně inverzní zobrazení mezi množinou všech podgrup grupy $R(+, -, 0)$ a množinou všech jejích grupových kongruencí. Ukážeme, že jde (po zúžení) o vzájemně inverzní zobrazení

mezi množinou všech ideálů okruhu \mathcal{R} a množinou všech okruhových kongruencí tohoto okruhu.

Ať je nejprve H ideál okruhu \mathcal{R} . Předpokládejme, že $(a, b), (c, d) \in \text{rmod } H$, čili $a-b, c-d \in H$. Potom ovšem i $(a-b)c+b(c-d) = ac-bd \in H$, tj. $(ac, bd) \in \text{rmod } H$ a $\text{rmod } H$ je tedy okruhová kongruence.

Opačně mějme dány okruhovou kongruenci ρ a $r \in R$ buď libovolný prvek. Triviálně máme $(r, r) \in \rho$. Je-li dále $(a, 0) \in \rho$, potom $(ra, r0) = (ra, 0) \in \rho$ a také $(ar, 0r) = (ar, 0) \in \rho$. Jinými slovy: $a \in [0]_\rho$ implikuje jak $ra \in [0]_\rho$, tak $ar \in [0]_\rho$, a tedy $[0]_\rho$ je ideál okruhu \mathcal{R} . \square

Můžeme analogicky modifikovat pro okruhy i Poznámky 1.18 a 1.16. Je-li I ideál (resp. ρ jemu odpovídající kongruence), potom lze na množině $R/I = R/\text{rmod } I$ definovat obvyklým způsobem definovat kromě operace $+$ (tj. aplikace Poznámky 1.18 na grupu $R(+, -, 0)$) i operaci \cdot vztahem $(a+I) \cdot (b+I) = ab+I$ (resp. $[a]_\rho \cdot [b]_\rho = [ab]_\rho$).

Poznámka 4.7. Je-li I ideál okruhu $R(+, \cdot, -, 0, 1)$, potom je faktorová algebra $R/I(+, \cdot, -, [0]_I, [1]_I)$ rovněž okruh a $\text{Ker}\varphi$ je ideál pro každý homomorfismus okruhu $R(+, \cdot, -, 0, 1)$ do okruhu $S(+, \cdot, -, 0, 1)$.

Důkaz. Tom že je $R/I(+, \cdot, -, I, 1+I)$ okruh se snadno přímočaře ověří z definice.

$\text{Ker}\varphi$ je určitě normální podgrupa a zbývá nahlédnout, že pro každé $r \in R$ a $k \in \text{Ker}\varphi$ je

$$\varphi(r \cdot k) = \varphi(r) \cdot \varphi(k) = \varphi(r) \cdot 0 = 0 = 0 \cdot \varphi(r) = \varphi(k) \cdot \varphi(r) = \varphi(k \cdot r),$$

tedy $r \cdot k, k \cdot r \in \text{Ker}\varphi$. \square

Takto zavedenému okruhu říkáme *faktorový okruh* (nebo krátce *faktorokruh*) okruhu R podle ideálu I .

Věta 4.8. Ať $R(+, \cdot, -, 0, 1)$ je komutativní okruh a I jeho ideál. Potom R/I je těleso právě tehdy, když I je maximální ideál.

Důkaz. Ať R/I je těleso a buď $J \supsetneq I$ ideál v R . Potom je $\pi_I(J)$ ideál v R/I , přičemž $\pi_I(J) \neq \{I\}$, tj. nejde o triviální (nulový) ideál. Podle Věty 4.5 musí být již $\pi_I(J) = R/I$. Musí tedy existovat $r \in J$ tak, že $r+I = 1+I$, tj. $1-r \in I$, z čehož ihned plyne $1 = r + (1-r) \in J$, a proto $J = R$. Dokázali jsme, že I je maximální ideál.

Je-li naopak I maximální ideál a $a \in R \setminus I$ (tj. $a+I \neq I$ v okruhu R/I), potom z maximality I (je totiž nutně $aR+I = R$) dostáváme existenci takového $r \in R$ a $i \in I$, že $ar+i = 1$ (a tedy $1-ar \in I$). Jinak řečeno $(a+I)(r+I) = ar+I = 1+I$ v okruhu R/I , což znamená, že $r+I$ je inverz v okruhu R/I k nenulovému prvku $a+I$. Ověřili jsme, že R/I je těleso. \square

Definice. Buď okruh. Položme $R[x] = \{p : \mathbf{N}_0 \rightarrow R \mid \{n \mid p(n) \neq 0\} \text{ je konečné}\}$. 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 $q = \sum_{n \in \mathbf{N}_0} q_n x^n$:

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

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

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 $\text{st } p$.

Je velmi snadné (a přenecháme to čtenáři) ověřit, že

Poznámka 4.9. $R(+[x], \cdot, -, \mathbf{0}, \mathbf{1})$ tvoří s výše zavedenými operacemi okruh pro každý okruh $R(+, \cdot, -, \mathbf{0}, \mathbf{1})$.

Je-li T komutativní těleso, ukážeme, jak poznat maximální ideály v okruhu $T[x]$, tj. okruhu polynomů v jedné neurčité (značené x) s koeficienty v T .

Definice. O polynomu $f \in T[x]$ stupně alespoň jedna řekneme, že je *ireducibilní*, pokud neexistují polynomy $g, h \in T[x]$ takové, že $f = gh$ a současně $\text{deg } g, \text{deg } h < \text{deg } f$.

Poznámka 4.10. Bud' T komutativní těleso a I ideál okruhu $T[x]$ a $g \in T[x]$.

- (1) existuje $f \in T[x]$ takové, že $I = fT[x]$,
- (2) I je maximální právě tehdy, když existuje ireducibilní polynom $f \in T[x]$ takový, že $I = fT[x]$

Důkaz. (1) Je-li $I = \{0\}$, položme $f = 0$. Jinak vezměme nenulové $f \in I$ nejmenšího možného stupně. Ukážeme, že $I = fT[x]$.

Bud' $g \in I$ libovolné. Vydělme g polynomem f se zbytkem: existují tedy $q, r \in T[x]$ tak, že $g = qf + r$ a $\text{deg } r < \text{deg } f$. Jelikož $f, g \in I$ a I je ideál, máme rovněž $r = g - qf \in I$, a tedy $r = 0$ vzhledem k minimalitě stupně f . Jelikož g bylo libovolné, ukázali jsme, že $I \subseteq fT[x]$. Druhá inkluze je triviální.

(2) Z Poznámky 4.10 víme, že existuje $f \in T[x]$ takový, že $I = fT[x]$. Dále stačí využít vztahu z Příkladu 4.3(4): pro ideál $gT[x]$ máme $fT[x] \subsetneq gT[x] \subsetneq T[x] \Leftrightarrow g|f$ a současně $g \nmid 1$ a $f \nmid g$; pravá strana ekvivalence neříká nic jiného, než $g|f$ a $0 < \text{deg } g < \text{deg } f$, tj. f není ireducibilní. \square

Kapitolu zakončíme konstrukcí konečných (komutativních) těles, přičemž budeme následující výsledek brát jako fakt (bez důkazu).

Tvrzení. Pro každé prvočíslo p a $n \in \mathbf{N}$ existuje ireducibilní polynom $f \in \mathbf{Z}_p[x]$ stupně n . Navíc v $\mathbf{Z}_p[x]$ platí $f|(x^{p^n} - x)$.

Větu o konečných tělesech zformulujeme v klasickém znění. Důkaz bodů (2) a (3) ovšem uvádíme jen informativně.

Věta 4.11. (1) Pro každé prvočíslo p a $n \in \mathbf{N}$ existuje komutativní těleso o p^n prvcích.

(2) Je-li \mathbb{F} konečné těleso, pak $|\mathbb{F}| = p^n$ pro p prvočíslo a $n \in \mathbf{N}$.

(3) Libovolná dvě konečná komutativní tělesa o téže počtu prvků jsou izomorfní.

Důkaz. (1) Z faktu výše máme existenci ireducibilního polynomu $f \in \mathbf{Z}_p[x]$ stupně n . Definujme $\mathbb{F}_{p^n} = \mathbf{Z}_p[x]/f\mathbf{Z}_p[x]$. Potom z Poznámky 4.10(2) a Věty 4.8 plyne, že \mathbb{F}_{p^n} je komutativní těleso. Označíme-li $I = f\mathbf{Z}_p[x]$, v tomto tělese (pro $g, h \in \mathbf{Z}_p[x]$) platí $g + I = h + I$ právě tehdy, když f dělí $g - h$; mj. tedy $g + I = (g \bmod f) + I$. Jako zbytky po dělení f figurují právě všechny polynomy nad \mathbf{Z}_p stupně $< n$, těch je p^n , což je následně i počet prvků \mathbb{F}_{p^n} .

(2) Buď \mathbb{F} konečné těleso. Uvažujme cyklickou podgrupu $\langle 1 \rangle$ grupy $\mathbb{F}(+, -, 0)$. Ta musí být konečná, a tedy $\mathbf{Z}_p(+)$ $\cong \langle 1 \rangle(+)$ pro nějaké $p \in \mathbf{N}$. Uvažujme izomorfismus, který posílá prvek $k \in \mathbf{Z}_p$ na prvek $\underbrace{1 + 1 + \dots + 1}_{k \times}$ tělesa \mathbb{F} , a jak je

v podobných případech zvykem, pro další úvahy ztotožníme prvky tělesa \mathbb{F} tvaru $\underbrace{1 + 1 + \dots + 1}_{k \times}$, kde $0 \leq k < p$, a prvky množiny \mathbf{Z}_p . Z grupy \mathbf{Z}_p tímto ztotožněním

uděláme podgrupu grupy $\mathbb{F}(+, -, 0)$.

Jelikož z distributivity máme $\underbrace{(1 + 1 + \dots + 1)}_{k \times} \underbrace{(1 + 1 + \dots + 1)}_{m \times} = \underbrace{1 + 1 + \dots + 1}_{km \times} = \underbrace{1 + 1 + \dots + 1}_{(km \bmod p) \times}$, tvoří \mathbf{Z}_p dokonce podokruh tělesa \mathbb{F} .

Dále, p musí být prvočíslo. Jinak by existovaly $0 \neq k, m \in \mathbf{Z}_p$ tak, že $km = 0$, což v žádném tělese (tedy ani v \mathbb{F}) není možné.

Nyní je již snadné si uvědomit, že \mathbb{F} tvoří vektorový prostor nad svým podtělesem \mathbf{Z}_p , a tedy $\dim_{\mathbf{Z}_p} \mathbb{F} = n \in \mathbf{N}$. V důsledku toho jest $|\mathbb{F}| = p^n$.

(3) Ukážeme, že je-li \mathbb{F} konečné komutativní těleso o p^n prvcích, potom $\mathbb{F} \cong \mathbb{F}_{p^n}$ (z části (1) důkazu). Tak jako v bodu (2) budeme BÚNO předpokládat, že \mathbf{Z}_p je přímo podtělesem tělesa \mathbb{F} (nikoliv pouze izomorfní podtělesu generovanému prvkem 1).

Nejprve nahlédneme, že každý prvek tělesa \mathbb{F} je kořenem polynomu $x^{p^n} - x \in \mathbf{Z}_p[x]$. To pro 0 zřejmě platí a pro nenulové prvky to plyne aplikací Poznámky 2.8 na grupu $\mathbb{F}^*(\cdot, ^{-1}, 1)$, která má $p^n - 1$ prvků.

Z faktu výše plyne, že ireducibilní polynom $f \in \mathbf{Z}_p[x]$ použitý ke konstrukci tělesa \mathbb{F}_{p^n} , dělí v $\mathbf{Z}_p[x]$ polynom $x^{p^n} - x$. To ovšem znamená, že ho dělí i v jeho nadokruhu $\mathbb{F}[x]$. Máme tedy nějaký polynom g takový, že $fg = x^{p^n} - x$. Dosadíme-li nyní libovolný prvek $a \in \mathbb{F}$, máme $f(a)g(a) = 0$, což znamená, že a je kořen jednoho ze dvou těchto polynomů. Jelikož polynom g má menší stupeň než p^n (a tedy méně než p^n kořenů), musí existovat nějaké $a \in \mathbb{F}$, které je kořenem polynomu f .

Pro toto a uvažujme (dosazovací) homomorfismus $d_a : \mathbf{Z}_p[x] \rightarrow \mathbb{F}$ definovaný vztahem $d_a(h) = h(a)$. Výše jsme dokázali, že $f\mathbf{Z}_p[x] \subseteq \text{Ker}(d_a)$. Můžeme proto užít Větu o homomorfismu pro okruhy, která nám dá (jediný) okruhový homomorfismus $\psi : \mathbf{Z}_p[x]/f\mathbf{Z}_p[x] \rightarrow \mathbb{F}$, pro nějž $d_a = \psi \pi_{f\mathbf{Z}_p[x]}$. Jelikož $d_a(1) = 1 \neq 0$, je ψ nenulový homomorfismus. Víme, že $\text{Ker}(\psi)$ musí být ideál tělesa \mathbb{F}_{p^n} , a tedy nutně $\text{Ker}(\psi)$ je triviální (jednoprvkový) ideál (užíváme Větu 4.5). To ovšem znamená, že ψ je prosté, a tedy musí být i na, jelikož jde o zobrazení mezi dvěma stejně velkými konečnými množinami. Tudíž ψ je hledaný izomorfismus těles \mathbb{F}_{p^n} a \mathbb{F} . \square

Wedderburnova věta říká, že všechna konečná tělesa jsou komutativní. Důkaz ale není nikterak triviální. V důkazu části (3) jsme využili komutativitu tělesa \mathbb{F} , abychom mohli argumentovat, že polynom g nemá v \mathbb{F} více kořenů, než je jeho stupeň; to ovšem nad nekomutativními tělesy neplatí! Stačí uvážit polynom $x^2 + 1$ nad tělesem kvaternionů. Ten má za kořeny $i, j, k, -i, -j, -k$.

Důkaz následujícího důležitého tvrzení o konečných multiplikativních grupách vyžaduje jisté znalosti z teorie polynomů nad obecným tělesem, proto ho provedeme až v příštím semestru:

Věta 4.12. *Nechť $T(+, \cdot)$ je komutativní těleso a necht' G je konečná podgrupa multiplikativní grupy $T \setminus \{0\}(\cdot)$. Potom G je cyklická grupa.*

Příklad 4.13. (1) Je-li p prvočíslo, pak \mathbf{Z}_p je se sčítáním a násobením modulo p těleso, proto je podle předchozí věty $\mathbf{Z}_p^*(\cdot)$ cyklická grupa řádu $p - 1$. Je-li $p - 1 = \prod_{i=1}^k p_i^{s_i}$ prvočíselný rozklad, kde $p_1 < p_2 < \dots < p_k$ a $r_i > 0$, pak můžeme generátory a podgrupy grupy $\mathbf{Z}_p^*(\cdot)$ počítat postupem Příkladu 2.11. Tedy $\mathbf{Z}_p^*(\cdot)$ obsahuje právě $\prod_{i=1}^k (p_i - 1)p_i^{r_i - 1}$ generátorů a $\prod_{i=1}^k (r_i + 1)$ podgrup.

(2) Z předchozí úvahy plyne, že $\mathbf{Z}_{53}^*(\cdot)$ je cyklická grupa řádu $52 = 2^2 \cdot 13$, proto $\mathbf{Z}_{53}^*(\cdot)$ obsahuje právě $2 \cdot 12 = 24$ generátorů a $3 \cdot 2 = 6$ podgrup.

5. SVAZY

Připomeňme, že 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). Dvojice (M, \leq) se obvykle nazývá uspořádaná množina.

Definice. Necht' \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 $\{n \in M \mid \forall a \in A : a \leq n\}$ (resp. největší prvek množiny $\{n \in M \mid \forall a \in A : n \leq a\}$), 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 5.1. Připomeňme známé příklady uspořádání a svazů:

- (1) Relace dělení $/$ je uspořádání na množině všech přirozených čísel \mathbf{N} , navíc $\sup_{/}(n, m) = nsn(n, m)$ a $\inf_{/}(a, b) = NSD(n, m)$, proto je $(\mathbf{N}, /)$ svaz.
- (2) Přirozené uspořádání \leq indukuje na množině všech celých (reálných, racionálních) čísel \mathbf{Z} (\mathbf{R} , \mathbf{Q}) strukturu (dokonce lineárně uspořádaného) svazu, kde $\sup_{\leq}(a, b) = \max(a, b)$ a $\inf_{\leq}(a, b) = \min(a, b)$.
- (3) Inkluze tvoří na množině všech podmnožin $\mathcal{P}(X)$ množiny X uspořádání a $(\mathcal{P}(X), \subseteq)$ úplný svaz kde $\sup_{\subseteq}(\mathcal{B}) = \bigcup \mathcal{B}$ a $\inf_{\subseteq}(\mathcal{B}) = \bigcap \mathcal{B}$ pro každou podmnožinu $\mathcal{B} \subseteq \mathcal{P}(X)$.
- (4) Je-li \mathcal{C} množina všech podalgeber nebo všech kongruencí na nějaké algebře, ukážeme, že (\mathcal{C}, \subseteq) tvoří úplný svaz, kde $\sup_{\subseteq}(\mathcal{B}) = \bigcap \{C \in \mathcal{C} \mid \bigcup \mathcal{B} \subseteq C\}$ a $\inf_{\subseteq}(\mathcal{B}) = \bigcap \mathcal{B}$ pro každé $\mathcal{B} \subseteq \mathcal{C}$.
 \subseteq je uspořádání a $\bigcap \mathcal{B}$ je zjevně infimem. Protože je množina \mathcal{C} dle 3.6 uzavřená na průniky, vidíme, že $\bigcap \{X \in \mathcal{C} \mid \bigcup \mathcal{B} \subseteq X\}$ tvoří nejmenší prvkem \mathcal{C} obsahujícím všechna $B \in \mathcal{B}$, což je podle definice právě supremum vzhledem k inkluzi.
- (5) id je na libovolné neprázdné množině M uspořádání, ovšem pro $|M| > 1$ se jistě nejedná o svaz.

Je-li (M, \leq) svaz, budeme pro každé dva prvky $m, n \in M$ značit $m \vee n = \sup_{\leq}(m, n)$ a $m \wedge n = \inf_{\leq}(m, n)$. Zavedené binární operace \vee nazveme *spojení* a \wedge *průsek*.

Věta 5.2. (1) Je-li (M, \leq) svaz, pak pro všechna $a, b, c \in M$ platí:

$$(S1) \quad a \vee b = b \vee a, \quad a \wedge b = b \wedge a,$$

- (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) $a \vee (b \wedge a) = a = a \wedge (b \vee a)$.

(2) *Nechť $M(\wedge, \vee)$ je algebra s dvěma binárními operacemi, které splňují podmínky (S1) – (S4) a definujeme na M relaci \leq předpisem: $a \leq b \Leftrightarrow b = a \vee b$. Pak platí $a \leq b \Leftrightarrow a = a \wedge b$, dále (M, \leq) je svaz a $\sup_{\leq}(a, b) = a \vee b$ a $\inf_{\leq}(a, b) = a \wedge b$.*

Důkaz. (1) 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 .

(2) 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 (S1), 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 symetricky 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 $\sup_{\leq}(a, b) = a \vee b$. \square

Dokázané tvrzení poskytuje dva ekvivalentní pohledy na svaz: buď jako na uspořádanou množinu se supremy a infimy nebo algebra splňující čtveřici axiomů (S1)–(S4).

Příklad 5.3. U příkladů svazů uvedených v 5.1 máme tedy dva způsoby jak na svaz nahlížet:

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

Definice. O svazu $S(\wedge, \vee)$ řekneme, že 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 5.4. *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 5.2 upravovat: $(a \wedge b) \vee (a \wedge c) = ((a \wedge b) \vee a) \wedge ((a \wedge b) \vee c) = a \wedge (a \vee c) \wedge (b \vee c) = a \wedge (b \vee c)$, kde druhá rovnost plyne z (S4) a třetí rovnost plyne z (S1) a (S4) a \square

Příklad 5.5. (1) Svaz $\mathcal{P}(X)(\cap, \cup)$, kde $\mathcal{P}(X)$ je množina všech podmnožin množiny X , je distributivní.

(2) 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. (říká se mu obvykle diamant).

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

Poznámka 5.6. *Homomorfismus svazů je monotónní zobrazení.*

Důkaz. Je-li $f : A \rightarrow B$ 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 $f(a_1) \leq f(a_2)$. \square

Věta 5.7. *Bijekce svazů f je izomorfismus, právě když jsou f i f^{-1} monotónní zobrazení.*

Důkaz. Díky 5.6 stačí dokázat zpětnou implikaci. Ověříme sloučitelnost f například s \vee . Mějme $f : A \rightarrow B$ 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 monotónii f , dostaneme $f(a \vee b) \leq f(f^{-1}(f(a) \vee f(b))) = f(a) \vee f(b)$. Ze slabé antisymetrie \leq , potom plyne, že $f(a \vee b) = f(a) \vee f(b)$. \square

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

Konečné uspořádané množiny je často výhodné znázornit Hasseovým diagramem, připomeňme jeho definici:

Definice. Nechť (M, \leq) je uspořádaná množina a $a, b, c \in M$. Řekneme, že prvek b *pokrývá* prvek a (píšeme $a < \cdot b$), jestliže $a \leq b$, a není b a $a \leq c \leq b \Rightarrow c = a$ nebo $c = b$. *Hasseovým diagramem* uspořádané množiny (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 .

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 homomorfismus (izomorfismus) algeber v obvyklém smyslu.

Příklad 5.9. Necht' $\mathcal{P}(X)$ 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 5.10. Necht' $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ 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 5.8 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 $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = \mathbf{1} \vee \mathbf{1} = \mathbf{1}$. \square

Věta 5.11. Bud' $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ konečná Booleova algebra a A bud' množina všech atomů svazu S . Potom zobrazení $\phi : \mathcal{P}(A) \rightarrow S$ dané předpisem $\phi(B) = \sup B$ je izomorfismus Booleových algeber $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ a $\mathcal{P}(A)(\cup, \cap, \emptyset, X, ')$.

Důkaz. Pro každé $M = \{m_1, \dots, m_n\} \subseteq S$ značme $\bigwedge M = m_1 \wedge m_2 \wedge \dots \wedge m_n$ a $\bigvee M = m_1 \vee m_2 \vee \dots \vee m_n$, dále $\bigwedge \emptyset = \mathbf{1}$ a $\bigvee \emptyset = \mathbf{0}$

Definujme nejprve zobrazení $\psi : S \rightarrow \mathcal{P}(A)$ předpisem $\psi(s) = \{a \in A \mid a \leq s\}$. 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 5.7 tedy zbývá ověřit, že $\phi \circ \psi = \text{Id}_S$ i $\psi \circ \phi = \text{Id}_{\mathcal{P}(A)}$, tedy že ϕ je bijekce a $\phi^{-1} = \psi$.

Položme $t = \phi\psi(s) = \bigvee\{a \in A \mid a \leq s\}$. Potom $t = \bigvee\{a \in A \mid a \leq s\} \leq s$. 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 $C = \psi\phi(B) = \{a \in A \mid a \leq \bigvee B\}$. 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 $\mathbf{0} \neq c = c \wedge \bigvee B = \bigvee\{c \wedge b \mid b \in B\}$ 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 $B = C$. \square

Příklad 5.12. (1) Je-li $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ Booleova algebra o $64 = 2^6$ prvcích, pak je podle předchozí věty izomorfní Booleově algebře $\mathcal{P}(X)(\cup, \cap, \emptyset, , ')$ pro $X = \{1, 2, 3, 4, 5, 6\}$.

(2) Neexistuje žádná patnáctiprvková Booleova algebra, protože podle Věty 5.11 musí být každá Booleova algebra izomorfní potenční Booleově algebře, tedy musí mít 2^n prvků, kde n je počet atomů.