ALGEBRA I PRO INFORMATIKY

Obsah

1. Předmět(y) zkoumání

Pod názvem algebra se dlouho dobu rozuměla nauka o řešení rovnic, což dosvědčuje i etymologie tohoto slova; termínem al-džabr označuje Muhammad Ibn Músá al-Chórezmí (kolem 780 – kolem 850) ve svém *Algebraickém traktátu* přičtení výrazu k obou stranám rovnice. Ač je al-Chórezmí často nazýván Otcem algebry a stal se neplánovaným autorem pojmenování celé matematické disciplíny (a také pojmu algoritmus skrze přízvisko al-Chorézmí, které označuje jeho rodiště Chorézm, dnešní uzbeckou Chívu), algebraické úvahy a postupy jsou mnohem staršího data. Zmiňme alespoň teorii čísel, pěstovanou už v antickém starověku, například Eukleidův algoritmus je stále velmi užitečný nástroj, jehož algebraická povaha je mimo vší pochybnost.

V současném pojetí algebry už netvoří otázka řešení polynomiálních rovnic, jak bychom měli předmět starověké, středověké a raně novověké algebry upřesnit, centrální roli. Přesto lze mnoho algebraických problémů rovnicovým jazykem vyjádřit a například otázka obtížnosti nalezení řešení kvadratických či kubických rovnic je

Date: 5. dubna 2017.

zajímavá nejen pro současnou algebru, nýbrž i pro kryptologii. V algebře se podobně jako v celé matematice zásadně změnil jazyk. Symbolický zápis umožňuje přesnější a jasnější formulace starých otázek a přirozeně nabízí otázky nové. Obdobně se zásadně změnila míra abstrakce algebraických úvah. Zatímco v *klasické algebře* se matematici zabývali vždy zcela konkrétní algebraickou strukturou, jakou představují přirozená čísla se sčítáním a násobením, celá či racionální čísla se sčítáním, násobením, odčítáním, popřípadě dělením nebo reálná či komplexní čísla v kontextu otázek vyjádřených obvyklými operacemi, v takzvané *moderní algebře* už v centru pozornosti stojí obecný, obvykle axiomaticky popsaný algebraický objekt. My se budeme pochopitelně věnovat základním konceptům moderní algebry s přihlédnutím k historickým souvislostem a postoji studenta informatiky, pro nějž je realitou jen velmi omezený sortiment konkrétních algebraických struktur, což je postoj přirozeně blízký klasické algebře.

Velmi zhruba vyjádřeno se tedy moderní algebra věnuje zkoumání množin opatřených jistým systémem operací. Předmětem zájmu jsou ovšem nejen strukturní vlastnosti takové množiny popsané podmínkami, které pomocí operací umíme vyjádřit, nýbrž i vlastnostmi „vyšších řádů", například vlastnosti systémů různých množin s podobnými systémy operací či tříd takových množin. Tento text si přitom klade za cíl seznámit studenty informatiky s nejzákladnějšími 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. Jak už bylo zmíněno, 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 nepominutelný považujeme přístup, který můžeme nepříliš přesně označit jako kontextuální, a jímž míníme seznámení studenta s terminologickými a historickými kontexty současné algebry.

Dříve než se začneme systematicky zabývat abstraktními úvahami o algebraických objektech, uvedeme několik motivačních příkladů, které by nám pomohly usnadnit porozumění důvodům (ať už praktickým tak historickým), proč právě tu či onu vlastnost sledujeme.

Nejprve se domluvme, že *binární operací* na neprázdné množině A budeme rozumět libovolné zobrazení $A^2 = A \times A \to A$ (obvykle ji budeme zapisovat centrálně), *unární operace* na A bude jakékoli zobrazení $A \to A$ a *nulární operace* bude zobrazení kartézské mocniny A^0, která sestává právě z jediné prázdné posloupnosti, do množiny A, můžeme ji proto chápat jako vybrání prvku z množiny A, právě toho, na nějž se zobrazí jednoprvková množina A^0 (obvykle se nulární operace s tímto vyznačeným prvkem ztotožňuje).

Můžeme si poněkud předčasně dovolit i zcela obecnou definici operace:

Definice. Pro každé celé $n \geq 0$ nazveme *n-ární operací na množině A* každé zobrazení $A^n \to A$ (číslo n budeme nazývat *aritou* nebo *četností* operace).

Příklad 1.1. Uvažujme množinu celých čísel $\mathbb{Z}$ a na ní obvyklé operace sčítání $+$ a násobení $\cdot$. Pro libovolné přirozené číslo n položme $n\mathbb{Z} = \{n \cdot z |\ z \in \mathbb{Z}\}$. Nyní si můžeme všimnout, že je množina $n\mathbb{Z}$ „uzavřená" na obě uvažované operace, tj. pro každou dvojici $a, b \in n\mathbb{Z}$ platí, že $a + b, a \cdot b \in n\mathbb{Z}$, tedy operace $+$ a $\cdot$ můžeme uvažovat také omezeně na množině $n\mathbb{Z}$. Ačkoli pro žádné $n > 1$ množiny $n\mathbb{Z}$ a $\mathbb{Z}$ nesplývají, nelze pomocí vlastností operace $+$ obě množiny odlišit (tj. mají stejné

„algebraické" vlastnosti vzhledem ke sčítání), což ozřejmíme, zavedeme-li zobrazení $f_n : \mathbb{Z} \to n\mathbb{Z}$ předpisem $f_n(k) = kn$. Zjevně se jedná o bijekci, která navíc splňuje podmínku $f_n(a+b) = f_n(a) + f_n(b)$.

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

Příklad 1.2. V souladu se značením zavedeným na kurzu lineární algebry položme $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ pro nějaké celé číslo $n > 1$. Zaveďme na $\mathbb{Z}_n$ operace $+$ a $\cdot$ předpisem $a + b = (a+b) \bmod n$ a $a \cdot b = (a \cdot b) \bmod n$, kde mod n znamená zbytek po celočíselném dělení hodnotou n a v závorce uvažujeme vždy obvyklé sčítání a násobení celých čísel. Konečně definujme zobrazení $F_n : \mathbb{Z} \to \mathbb{Z}_n$ 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 $f : A \to B$ nazveme *slučitelné* s operacemi $*$ a $\circ$ je-li pro všechna $x, y \in A$ splněna rovnost $f(x * y) = f(x) \circ f(y)$.

Všimněme si, že zobrazení f_n z 1.1 je slučitelné s operacemi $+$ a není slučitelné s operacemi $\cdot$, zatímco zobrazení F_n z 1.2 je slučitelné s oběma páry operací $+$ i $\cdot$. Navíc množina $n\mathbb{Z}$ je uzavřená na operace $+$ i $\cdot$.

Na dvou známých příkladech si ilustrujme, že jsou uvedené pojmy základním stavebním kamenem algebry:

Příklad 1.3. (1) Podprostor vektorového prostoru je zjevně podmnožinou uzavřenou na (vektorové) sčítání a lineární zobrazení jsou se sčítáním slučitelná. Navíc uvažujeme-li násobení skalárem pro každý skalár a jako unární operaci, pak je podprostor uzavřený na všechny takto definované unární operace.

(2) Uvážíme na množině $\{0,1\}$ Booleovské operace $\wedge$, $\vee$ a XOR, zapsat si je můžeme tabulkami:

$\wedge$	**0**	**1**
0	0	0
1	0	1

$\vee$	**0**	**1**
0	0	1
1	1	1

XOR	**0**	**1**
0	0	1
1	1	0

Vezmeme-li bijekci $b(0) = 1, b(1) = 0$, pak z tabulky operací vidíme, že je b slučitelná s operacemi $\wedge$ a $\vee$ v obou možných pořadí operací, nikoli ovšem s operacemi $\wedge$ a $\wedge$ respektive $\vee$ a $\vee$. Podobně z tabulky operace XOR nahlédneme, že b s operacemi $\wedge$ a XOR ani $\vee$ a XOR (v žádném pořadí) slučitelná není.

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),
- $\rho^{+} = \{(a,b) \mid \exists a = a_0, a_1, \ldots, a_{n-1}, a_n = b \in A; (a_i, a_{i+1}) \in \rho\}$ (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 $\rho^{+} \subseteq \rho$.

Ekvivalencí budeme nazývat každou symetrickou, reflexivní a tranzitivní relaci.

Příklad 1.4. Pro libovolné množiny A a B a zobrazení $f : A \to B$ množin tvoří ekvivalenci relace

(1) $\mathrm{id} = \{(a, a) \mid a \in A\}$,
(2) $A \times A$,
(3) $\ker f = \{(x, y) \in A \times A |\ f(x) = f(y)\}$ (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 $A/\rho = \{[a]_\rho |\ a \in A\}$, kde $[a]_\rho = \{b \in A |\ (a, b) \in \rho\}$ jsou rozkladové třídy (kosety), tedy A/ρ tvoří rozklad množiny A.

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

2. Základy elementární teorie čísel

Nyní připomeňme několik nejzákladnějších poznatků z teorie čísel, které nám poslouží nejen jako motivace zkoumání obecných algebraických vlastností (slučitelnost ekvivalence s operací), nýbrž i jako užitečný nástroj, jenž využijeme v následujících kapitolách, konkrétně Eukleidův algoritmus a Čínskou větu o zbytcích.

Jsou-li a, b dvě celá čísla, budeme fakt, že číslo a dělí b, značit a/b a symbolem $\mathrm{GCD}(a, b)$ budeme rozumět *největší společný dělitel* čísel a a b, tedy nezáporné číslo d, které je společným dělitelem čísel a a b ($d/a, b$) a které je děleno všemi společnými děliteli čísel a a b ($c/a, b \Rightarrow c/d$). Podobně $\mathrm{lcm}(a, b)$ bude označovat *největší společný dělitel* čísel a a b, tedy nezáporné číslo n, které je společným násobkem čísel a a b ($a, b/n$) a které je děleno všemi společnými děliteli čísel a a b ($a, b/m \Rightarrow n/m$).

Konečně přirozené číslo p nazveme prvočíslem, jestliže pro každá celá a, b platí implikace $p = a \cdot b \Rightarrow a = \pm 1$ nebo $b = \pm 1$.

Připomeňme nejprve rozšířený Eukleidův algoritmus hledání největšího společného dělitele čísel a a a:

VSTUP: $a, b \in \mathbb{N}$, $a \geq b$
VÝSTUP: $\mathrm{GCD}(a, b), x, y \in \mathbb{Z}$, pro které $\mathrm{GCD}(a, b) = x \cdot a + y \cdot b$
0. $i := 1$, $(a_0, a_1) := (a, b)$; $(x_0, x_1) := (1, 0)$; $(y_0, y_1) := (0, 1)$;
1. while$(a_i > 0)$ do
$\{a_{i+1} := (a_{i-1}) \mathrm{mod}\ a_i$; $q_i := (a_{i-1}) \mathrm{div}\ a_i$; %tj. $a_{i-1} = q_i a_i + a_{i+1}$
$x_{i+1} := x_{i-1} - x_i \cdot q_i$; $y_{i+1} := y_{i-1} - y_i \cdot q_i$; $i := i + 1;\}$
2. return $a_{i-1}, x_{i-1}, y_{i-1}$.

Poznámka 2.1. *Eukleidův algoritmus pracuje správně, tedy najde největší společný dělitel a pro x, y na jeho výstupu platí, že* $\mathrm{GCD}(a, b) = x \cdot a + y \cdot b$.

Důkaz. Využijeme značení algoritmu a poznamenejme, že vypočítaná hodnota a_{i+1} je vždy menší než předchozí a_i, proto while-cyklus v algoritmu skončí.

Nyní zvolíme index n tak, že $a_n > 0$ a $a_{n+1} = 0$. Všimněme si, že $a_n = \mathrm{GCD}(a_{n-1}, a_n)$, protože a_n / a_{n-1}.

Označíme $\mathcal{D}(u,v) = \{c \in \mathbb{Z} |\ c/u, c/v\}$ pro každé u, v množinu všech jejich společných dělitelů a ukážeme pro každé $i = 1, \ldots, n-1$, že množina všech dělitelů dvojice a_i, a_{i+1} je stejná jako množina všech dělitelů dvojice a_{i-1}, a_i, tedy že

$$\mathcal{D}(a_i, a_{i+1}) = \mathcal{D}(a_{i-1}, a_i).$$

Využijeme při tom vztahu $a_{i-1} = a_{i-1} + q_i \cdot a_i$ hodnot a_{i-1}, a_i a a_{i+1}:

$$c/a_{i-1}, a_i \Rightarrow c/a_{i+1} = a_{i-1} - q_i \cdot a_i$$

a podobně

$$d/a_i, a_{i+1} \Rightarrow d/a_{i-1} = a_{i-1} + q_i \cdot a_i.$$

Protože a_n je největší společný dělitel prvků a_n a a_{n-1} a

$$\mathcal{D}(a_{n-1}, a_n) = \mathcal{D}(a_{n-2}, a_{n-1}) = \cdots = \mathcal{D}(a_0, a_1),$$

platí, že $a_n \in \mathcal{D}(a_{i-1}, a_i)$ a navíc d/a_n pro každé $d \in \mathcal{D}(a_{i-1}, a_i)$, tedy

$$a_n = \mathrm{GCD}(a_n, a_{n-1}) = \mathrm{GCD}(a_{n-1}, a_{n-2}) = \cdots = \mathrm{GCD}(a_0, a_1).$$

Nakonec ověříme indukcí podle i platnost tvrzení $a_i = x_i \cdot a_0 + y_i \cdot a_1$, které potřebujeme dokázat pro $i = n$. Zřejmě tvrzení platí pro $i = 0$ a $i = 1$ a předpokládejme, že tvrzení platí pro i a $i-1$, tedy $a_i = x_i \cdot a_0 + y_i \cdot a_1$ a $a_{i-1} = x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1$. Dokážeme rovnost pro $i+1$ dosazením za a_i a a_{i-1} do vztahu:

$$a_{i+1} = a_{i-1} - a_i \cdot q_i = (x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1) - (x_i \cdot a_0 + y_i \cdot a_1) \cdot q_i =$$
$$= (x_{i-1} - x_i \cdot q_i) \cdot a_0 + (y_{i-1} - y_i \cdot q_i) \cdot a_1 = x_{i+1} \cdot a_0 + y_{i+1} \cdot a_1,$$

čímž jsme dokončili důkaz. □

Poznamenejme, že čísla x a y se obvykle nazývají Bezoutovy koeficienty.

Nyní už je snadné dokázat jednoznačnost prvočíselného rozkladu.

Věta 2.2 (Základní věta aritmetiky)**.** *Každé přirozené číslo větší než jedna lze až na pořadí jednoznačně rozložit na součin prvočísel.*

Důkaz. Nejprve si uvědomíme, že lze každé přirozené číslo $n > 1$ napsat jako součin prvočísel, což můžeme snadno dokázat indukcí podle n. Číslo 2 je zřejmě prvočíslo. Pokud n není prvočíslo, existují taková přirozená čísla k, $l < n$, že $n = k \cdot l$. Obě jsou samozřejmě větší než jedna a podle indukčního předpokladu máme prvočíselný rozklad čísel $k = p_1 \cdot \ldots \cdot p_r$ a $l = q_1 \cdot \ldots \cdot q_s$. Tedy číslo n je součinem prvočísel $p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s$.

Dříve než ověříme jednoznačnost prvočíselného rozkladu, dokážeme technické

Lemma. Nechť p je prvočíslo a $a, b, a_1, a_2, \ldots, a_k \in \mathbb{N}$. Pak platí

(1) $p/a \cdot b \Rightarrow p/a$ nebo p/b,
(2) $p/a_1 a_2 \ldots a_k \Rightarrow \exists i$, že p/a_i.

(1) Protože $\mathrm{GCD}(p, a) = 1$ (p má pouze dělitele ± 1 a $\pm p$), existují podle 2.1 taková celá x a y, že $1 = a \cdot x + p \cdot y$, tudíž $b = abx + pby$. Protože p dělí abx i pby, platí také, že p/b.

(2) Indukční rozšíření (1).

Nyní indukcí provedeme důkaz jednoznačnosti prvočíselného rozkladu čísla n. Indukčním předpokladem zde bude tvrzení, že je prvočíselný rozklad určen jednoznačně až na pořadí pro všechna čísla menší než n.

Je-li n prvočíslo (speciálně $n = 2$), obsahuje prvočíselný rozklad jediné prvočíslo a je tedy zřejmě určen jednoznačně. Platí-li tvrzení pro všechna $k < n$ a $n =$

$p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot p_s$ jsou dva prvočíselné rozklady, potom podle tvrzení Lemmatu existuje takové j, že p_1/q_j. Bez újmy na obecnosti můžeme předpokládat, že $j = 1$. Protože p_1 i q_1 jsou prvočísla, máme $p_1 = q_1$. Nyní stačí použít indukční předpoklad pro $p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot p_s < n$. □

Důsledek 2.3. *Pro každé $a, b \in \mathbb{Z}$ existuje až na znaménko jednoznačně určený* $\mathrm{GCD}(a,b)$ *a* $\mathrm{lcm}(a,b)$ *a platí, že* $\mathrm{lcm}(a,b) = \frac{a \cdot b}{\mathrm{GCD}(a,b)}$.

Důkaz. Snadno díky jednoznačnosti prvočíselného rozkladu zaručeného Větou 2.2 ověříme bezprostředně z definice, že pro $a = \prod p_i^{\alpha_i}$, $b = \prod p_i^{\beta_i}$

$$\mathrm{GCD}(a,b) = \prod p_i^{\min(\alpha_i,\beta_i)} \text{ a } \mathrm{lcm}(a,b) = \prod p_i^{\max(\alpha_i,\beta_i)}.$$

Navíc každé dva $\mathrm{GCD}(a,b)$ (respektive $\mathrm{lcm}(a,b)$) se podle definice vzájemně dělí, tedy se mohou lišit jen znaménkem. □

Připomeňme užitečný příklad číselně teoretické ekvivalence.

Příklad 2.4. Vezměme přirozené číslo $n \geq 2$ a označme $\equiv \pmod n$ relaci na množině celých čísel $\mathbb{Z}$ danou předpisem: $a \equiv b \pmod n \leftrightarrow n/(a-b)$. Není těžké si uvědomit, že se jedná o ekvivalenci (obvykle se jí říká kongruence na $\mathbb{Z}$). Navíc si můžeme všimnout jejího těsného vztahu k zobrazení F_n z 1.2, 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 $\ker F_n$.

Dříve než začneme používat termín kongruence v mnohem obecnější situaci, připomeňme si několik jednoduchých vlastností, které kongruence na celých číslech má:

Poznámka 2.5. *Pro každé $a, b, c, d \in \mathbb{Z}$ a $k, n \in \mathbb{N}$, 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* $\mathrm{GCD}(c,n) = 1$, *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 $n/(a-b)$. □

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 2.5 jsme tedy zjistili, že je kongruence $\equiv \pmod n$ slučitelná s přirozenými operacemi $+$, $-$ a $\cdot$ na celých číslech.

Příklad 2.6. Mějme kladná celá čísla $n_1, \ldots, n_k$ a položme $n = n_1 \cdot \cdots \cdot n_k$. Zaveďme nyní na kartézském součinu $\prod_{i=1}^{k} \mathbb{Z}_{n_i}$ po složkách operace $+$, $-$ a $\cdot$:

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

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

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

kde odčítání ve složkách definujeme rovněž modulo n_i. Definujme dále zobrazení

$$G : \mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}_{n_i} \quad \text{předpisem} \quad G(a) = ((a) \bmod n_1, \ldots, (a) \bmod n_k)$$

a stejným předpisem zavedeme i zobrazení $H : \mathbb{Z}_n \to \prod_{i=1}^{k} \mathbb{Z}_{n_i}$. Obě zobrazení jsou opět slučitelná s operacemi $+$, operacemi $-$ i operacemi $\cdot$.

V následující poznámce budeme uvažovat operace na kartézských součinech zavedené v Příkladu 2.6.

Věta 2.7 (Čínská věta o zbytcích)**.** *Nechť $n_1, n_2, \ldots, n_k$ jsou kladná celá čísla a $n = n_1 \cdot n_2 \cdot \cdots \cdot n_k$. Potom je zobrazení H z 2.6 slučitelné s operacemi $+$, $-$ a $\cdot$. Navíc H je bijekce, právě když jsou čísla $n_1, n_2, \ldots, n_k$ po dvou nesoudělná.*

Důkaz. Nejprve dokážeme zpětnou implikaci. V Příkladu 2.6 jsme si uvědomili, že je f zobrazení slučitelné s oběma operacemi. Zbývá nahlédnout, že jde o bijekci. Protože jsou $\mathbb{Z}_n$ a $\prod_{i=1}^{k} \mathbb{Z}_{n_i}$ stejně velké konečné množiny, stačí ověřit, že je f prosté. Nechť pro $a \leq b \in \mathbb{Z}_n$ platí, že $H(a) = H(b)$. Potom $H(b - a) = 0$, tedy $n_i / b - a$ pro všechna $i = 1, \ldots, k$. Protože jsou n_i po dvou nesoudělná dostáváme z Věty 2.2 $n / b - a$. Protože ovšem $0 \leq b - a \leq n - 1$, máme $b = a$.

Přímou implikaci dokážeme nepřímo. Nechť existují indexy $i \neq j$, pro něž $c = \mathrm{GCD}(n_i, n_j) > 1$. Potom $\frac{n}{c} \in \mathbb{Z}_n \setminus \{0\}$ a pro všechna $r = 1, \ldots, k$ platí, že $n_r / \frac{n}{c}$. To znamená, že $H(0) = (0, \ldots, 0) = H(\frac{n}{c})$, tedy H není prosté. □

Uvedený důkaz Čínské věty o zbytcích sice není konstruktivní, tedy nám neposkytuje algoritmus k nalezení vzoru nějakého prvku v zobrazení H. Následující příklad ukazuje, že hledat vzory zobrazení H není díky početním pravidlům 2.5 těžké.

Příklad 2.8. Podle Čínské věty o zbytcích existuje právě jedno $x \in \mathbb{Z}_{35}$ splňující kongruence $x \equiv 2 \pmod 5$ a $x \equiv 3 \pmod 7$, pokusíme se ho spočítat. Nejprve si všimneme, že z první kongruence plyne, že $x = 5y + 2$ pro vhodná $y \in \mathbb{Z}$ a toto vyjádření dosadíme do druhé kongruence a pomocí Poznámky 2.5 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 „inverz modulo 7"k číslu 5 jímž je 3). Hledaným řešením je tedy $x = 5 \cdot 3 + 2 = 17$.

Na závěr zdůrazněme, že Čínská věta o zbytcích má praktické význam pro počítání s velkými celými čísly, neboť nám umožňuje „algebraicky"přesně reprezentovat větší množinu $\mathbb{Z}_n$ pomocí počítání v menších množinách $\mathbb{Z}_{n_i}$.

3. Asociativní binární operace

Zkusíme se nyní oprostit od konkrétní algebraické struktury a uvážíme sice obecnou ale velmi jednoduchou situaci množiny opatřené asociativní binární operací. Hlavním výsledkem této kapitoly bude kromě příkladů řady struktur, které takovou podmínku splňují, především pozorování (Důsledek 3.7), že množina s asociativní operací je jistým způsobem velmi blízko mnohem silnějšímu pojmu grupa, který zde jako jeden ze základních pojmů moderní algebry zavedeme. Na závěr kapitoly se na chvíli vrátíme k teorii čísel a jako aplikaci předchozího aparátu dokážeme užitečný vzoreček na výpočet Eulerova funkce.

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

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

Poznámka 3.1. *Každá binární operace má nejvýše jeden neutrální prvek.*

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

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

Příklad 3.2. 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 e je její neutrální prvek. Řekneme, že prvek $s \in S$ je *invertibilní*, existuje-li takový prvek $s^{-1} \in S$, že $s^{-1} \cdot s = s \cdot s^{-1} = e$. Prvek s^{-1} nazveme *inverzním prvkem* k prvku s.

Příklad 3.3. Uvažujme $T(\mathbb{N})$ množinu všech zobrazení přirozených čísel do sebe s operací skládání $\circ$ a nechť $\alpha(k) = 2k$ a $\beta(k) = [\frac{k}{2}]$. 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 1.1 a 2.4 jsme připomněli asociativní a komutativní operace $+$ a $\cdot$ na množině celých čísel (a v Příkladech 1.2 a 2.6 jsme si uvědomili, že asociativitu i komutativitu splňují jimi indukované operace na množinách $\mathbb{Z}_n$). 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 3.4. 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) $\mathbb{Z}_n(\cdot)$ je konečný komutativní monoid, který není grupou, protože prvek 0 není invertibilní.

Do konce této kapitoly budeme v následujícím e označovat neutrální prvek obecné binární operace $\cdot$. Zároveň poznamenejme, že je obvyklé značit neutrální prvek multiplikativní operace (tj. $\cdot$) symbolem 1 a neutrální prvek aditivní operace (tj. $+$) symbolem 0 (a my se tohoto úzu budeme později také držet).

Poznámka 3.5. *Buď $S(\cdot)$ monoid a $a, b, c \in S$. Platí-li, že $a \cdot b = c \cdot a = e$, potom $b = c$ je jednoznačně určený inverzní prvek k prvku a.*

Důkaz. S využitím asociativity spočítejme:

$$c = c \cdot e = c \cdot (a \cdot b) = (c \cdot a) \cdot b = e \cdot b = b,$$

odkud vidíme nejen rovnost $b = c$, ale i jednoznačnost, neboť dva prvky inverzní k a splňují podmínku předpokladu. □

Poznámka 3.6. *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 $s \cdot s^{-1} = s^{-1} \cdot s = e$, je zřejmě s^{-1} invertibilní a díky 3.5 máme $(s^{-1})^{-1} = s$. Nyní stačí dokázat, že je prvek $t^{-1} \cdot s^{-1}$ inverzní k $s \cdot t$:

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

a symetricky

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

□

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 $e \in S^*$, protože $e \cdot e = e$, dostáváme díky předchozí poznámce následující pozorování:

Důsledek 3.7. *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 3.8. 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 $\mathbb{Z}_n^*(\cdot) = \{a \in \mathbb{Z}_n \mid \mathrm{GCD}(a,n) = 1\}$. Jestliže $a \in \mathbb{Z}_n^*$, existují $x \in \mathbb{Z}_n$ a $y \in \mathbb{Z}$, pro něž $ax + by = 1$. Je-li s společný dělitel čísel a, n, pak $s/(ax + ny) = 1$, proto $\mathrm{GCD}(a,n) = 1$. Nechť naopak $\mathrm{GCD}(a,n) = 1$, potom díky Euklidovu algoritmu existují $x \in \mathbb{Z}_n$ a $y \in \mathbb{Z}$, pro které $ax + ny = 1$, proto $a^{-1} = x \bmod n$, tudíž $a \in \mathbb{Z}_n^*$.

Na závěr se podívejme poněkud podrobněji na grupu $\mathbb{Z}_n^*(\cdot)$ jejíž prvky jsme charakterizovali v předchozím příkladu.

Definice. *Eulerovou funkcí* nazveme zobrazení $\varphi : \mathbb{N} \to \mathbb{N}$ dané předpisem

$$\varphi(n) = |\,\mathbb{Z}_n^*\,| = |\{k \in \mathbb{Z}_n \mid \mathrm{GCD}(k,n) = 1\}|.$$

S využitím Čínské věty o zbytcích a prvočíselného rozkladu čísla n budeme umět spočítat hodnotu $\varphi(n)$:

Věta 3.9. *Buď $p_1 < p_2 < \cdots < p_k$ prvočísla a $r_1, r_2, \ldots, r_k$ kladná celá čísla. Potom $\varphi(\prod_{i=1}^k p_i^{r_i}) = \prod_{i=1}^k \varphi(p_i^{r_i}) = \prod_{i=1}^k (p_i - 1)p_i^{r_i - 1}$.*

Důkaz. Nejprve pro libovolné prvočíslo p a kladné celé číslo r spočítáme, že $\varphi(p^k) = (p-1) \cdot p^{k-1}$. Číslo menší než p^k je soudělné s p^k právě tehdy, když je násobkem čísla p. Protože nezáporných násobků čísla p menších než p^k je zřejmě právě p^{k-1}, dostáváme, že kladných čísel nesoudělných s p^k máme

$$\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}.$$

Dále položme $n_i = p_i^{r_i}$ a $n = \prod_{i=1}^k n_i$ a uvažujme zobrazení $H : \mathbb{Z}_n \to \prod_{i=1}^k \mathbb{Z}_{n_i}$ z Věty 2.7. Všimněme si, že $\prod_{i=1}^k \mathbb{Z}_{n_i}(\cdot)$ s operací z Příkladu 2.6 tvoří monoid s neutrálním prvkem $H(1) = (1, \ldots, 1)$, a proto platí ekvivalence

$$(a_1, \ldots, a_k) \in (\prod_{i=1}^k \mathbb{Z}_{n_i})^* \Leftrightarrow \forall i = 1, \ldots, n \exists b_i : a_i \cdot b_i = 1 \Leftrightarrow (a_1, \ldots, a_k) \in \prod_{i=1}^k \mathbb{Z}_{n_i}^*.$$

Protože jsou $n_1, \ldots, n_k$ nesoudělné, je H podle 2.7 bijekce, a proto platí

$$a \in \mathbb{Z}_n^* \Leftrightarrow \exists b \in \mathbb{Z}_n : a \cdot b = 1 \Leftrightarrow \exists c \in \prod_{i=1}^k \mathbb{Z}_{n_i} : H(a) \cdot c = H(1) \Leftrightarrow H(a) \in (\prod_{i=1}^k \mathbb{Z}_{n_i})^*.$$

Spojíme-li obě pozorování dostáváme rovnost $H(\mathbb{Z}_n^*) = \prod_{i=1}^k \mathbb{Z}_{n_i}^*$. Odtud a z výše dokázaného faktu $\varphi(n_i) = (p_i - 1) \cdot p_i^{k-1}$ plyne dokazovaná rovnost

$$\varphi(n) = |\,\mathbb{Z}_n^*\,| = |H(\mathbb{Z}_n^*)| = |\prod_{i=1}^k \mathbb{Z}_{n_i}^*\,| = \prod_{i=1}^k \varphi(n_i) = \prod_{i=1}^k (p_i - 1) \cdot p_i^{k-1} \qquad \square$$

4. Podgrupy

Nyní si pozorně prohlédneme ekvivalence na obecných grupách, které zcela přímočaře zobecňují kongruence na celých číslech. Jako důsledek souboru elementárních technických pozorování těchto ekvivalencí dostaneme dvě velmi důležitá tvrzení o struktuře grup: Lagrangeovu větu, která svazuje dělitelností velikost grupy a její podgrupy, a větu charakterizující všechny ekvivalence slučitelné s grupovou operací pomocí pojmu normální podgrupa.

Podobně jako v předchozí kapitole budeme neutrální prvek obecné multiplikativně zapsané grupy $G(\cdot)$ označovat symbolem e a inverzní prvek k prvku g symbolem g^{-1}.

Definice. *Podgrupou* grupy $G(\cdot)$ budeme rozumět každou podmnožinu H množiny G, která je uzavřená na $\cdot$, obsahuje prvek e 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 3.6 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 4.1. *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 3.6).

(2) $e \in H_i$ pro všechna $i \in I$ podle, tedy $e \in \bigcap_{i\in I} H_i$. 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 $g \cdot h \cdot g^{-1} = g \cdot g^{-1} \cdot h = h \in H$. □

Příklad 4.2. (1) Všimněme si, že v každé grupě $G(\cdot)$ tvoří množiny $\{e\}$ a G (tzv. *triviální*) příklady normálních podgrup.

(2) Uvažujme grupu permutací na množině $\{1, \dots, n\}$, obvykle se značí $S_n(\circ)$ (viz také 3.8(2)). Přímočaře spočítáme, 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 $\{\mathrm{Id}\}$, S_n a A_n (v případě S_4 se vyskytuje ještě jedna tzv. Kleinova normální podgrupa $K = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$). Uveďme alespoň příklad zjevné podgrupy $T = \{\mathrm{Id}, (12)\}$ 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) Uvažujeme-li komutativní grupu celých čísel $\mathbb{Z}(+)$ (s neutrálním prvkem 0 a inverzními prvky značenými standardně symbolem $-$), potom množiny tvaru $n\mathbb{Z} = \{n \cdot z \mid z \in \mathbb{Z}\}$ jsou pro každé nezáporné celé n podgrupou grupy $\mathbb{Z}(+)$ (viz 1.1). Naopak, uvažujme libovolnou nenulovou podgrupu P grupy $\mathbb{Z}(+)$. 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 $P = n\mathbb{Z}$. 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 $n\mathbb{Z} \subseteq P$. Nyní zvolme libovolně $a \in P$. Potom vydělíme se zbytkem číslo a číslem n, t.j. najdeme celé q a nezáporné celé $z < n$, pro která $a = qn + z$. Z uzavřenosti P na $+$ použité pro prvky $a, -qn \in P$ plyne, že $z = a + (-qn) \in P$, a z minimality volby n dostáváme, že $z = 0$, tedy $n\mathbb{Z} = P$.

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

Příklad 4.3. (1) Mějme dvě normální podgrupy H a K grupy $G(\cdot)$. Pak pro každé $h_0 \in H$ a $k \in K$ existuje $h_1 \in H$, pro které $k \cdot h_0 \cdot k^{-1} = h_1$, tedy $k \cdot h_0 = h_1 \cdot k$ a $KH \subseteq HK$. Symetrický argument dokazuje i obrácenou inkluzi, proto $KH = HK$. Nyní snadno nahlédneme, že je součin HK rovněž podgrupou $G(\cdot)$: zřejmě $e = e \cdot e \in HK$ a zvolíme-li $h_0, h_1 \in H$ a $k_0, k_1 \in K$, potom $(h_0 \cdot k_0)^{-1} = k_0^{-1} \cdot h_0^{-1} \in KH = HK$ a dále existuje takové $h_2 \in H$, že $k_0 \cdot h_1 = h_2 \cdot k_0$, proto $h_0 \cdot k_0 \cdot h_1 \cdot k_1 = h_0 \cdot h_2 \cdot k_0 \cdot k_1 \in HK$. Konečně vezmeme-li libovolné prvky $g \in G$, $h \in H$ a $k \in K$, pak platí $g \cdot h \cdot k \cdot g^{-1} = (g \cdot h \cdot g^{-1}) \cdot (g \cdot k \cdot g^{-1}) \in HK$ díky předpokládané normalitě obou podgrup. Vidíme, že „součin"normálních podgrup (například tedy součin libovolných podgrup komutativní grupy) dává opět normální podgrupu. Poznamenejme, že součin podgrup, které normální nejsou, vůbec nemusí být podgrupou (stačí uvážit například podgrupy $H = \{Id, (12)\}$ a $K = \{Id, (13)\}$ grupy S_3).

(2) Uvažujeme-li komutativní grupu $A(+)$ a H, K její podgrupy, pak $H + K = \{h + k |\ h \in H,\ k \in K\}$ je podle předchozího pozorování opět podgrupa. Speciálně, vezmeme-li grupu celých čísel $\mathbb{Z}(+)$, pak $30\,\mathbb{Z} + 54\,\mathbb{Z} = \{30x + 54y |\ x, y \in \mathbb{Z}\} = \mathrm{GCD}(30, 54)\,\mathbb{Z} = 6\,\mathbb{Z}$. Všimněme si také, že $30\,\mathbb{Z} \cap 54\,\mathbb{Z} = \{z \in \mathbb{Z} |\ 30/z, 54/z\} = \mathrm{lcm}(30, 54)\,\mathbb{Z} = 270\,\mathbb{Z}$.

Definice. Je-li $G(\cdot)$ grupa $H \subseteq G$, definujme na G relace rmod H a lmod H:

$$(a, b) \in \text{rmod } H \Leftrightarrow a \cdot b^{-1} \in H$$

$$(a, b) \in \text{lmod } H \Leftrightarrow a^{-1} \cdot b \in H$$

Poznámka 4.4. *Nechť $G(\cdot)$ je grupa a H její podgrupa. Potom platí:*

(1) rmod H *i* 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) rmod $H =$ lmod H, *právě když je* H *normální podgrupa* $G(\cdot)$,
(5) $[a]_{\text{rmod } H} = Ha$ *a* $[a]_{\text{lmod } H} = aH$ *pro každé* $a \in G$,
(6) $|[a]_{\text{rmod } H}| = |[a]_{\text{lmod } H}| = |H|$ *pro každé* $a \in G$.

Důkaz. (1) Tvrzení dokážeme jen o rmod H, pro lmod H bude důkaz symetrický. Podgrupa H obsahuje neutrální prvek e, proto pro každé $a \in G$ máme $a \cdot a^{-1} = e \in H$, 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 3.5 a 3.6), tudíž $(b, a) \in \text{rmod } H$. Nyní předpokládejme, že $(a, b), (b, c) \in \text{rmod } H$, což podle definice naší relace znamená, že $a \cdot b^{-1}, b \cdot c^{-1} \in H$. Z uzavřenosti H na binární operaci plyne, že $(a \cdot b^{-1}) \cdot (b \cdot c^{-1}) \in H$, tedy $a \cdot c^{-1} = a \cdot b^{-1} \cdot b \cdot c^{-1} \in H$ a $(a, c) \in \text{rmod } H$. Tím jsme ověřili, že je relace rmod H reflexivní, symetrická a tranzitivní.

(2) Díky 3.6 máme rovnost $a \cdot b^{-1} = (a^{-1})^{-1} \cdot b^{-1}$, proto $a \cdot b^{-1} \in H \Leftrightarrow (a^{-1})^{-1} \cdot b^{-1} \in H$, čímž jsme dokončili důkaz.

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

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

Nyní 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 rmod $H \subseteq$ lmod H. Symetrický argument dokazuje obrácenou implikaci.

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

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

$$= \{b \in G |\ \exists h \in H :\ b = h^{-1} \cdot a\} = \{b \in G |\ \exists h' \in H :\ b = h' \cdot a\} = Ha.$$

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

Definice. Buď H podgrupa grupy $G(\cdot)$. Potom číslu $[G : H] = |G/\text{rmod } H|$ (= $|G/\text{lmod } H|$ podle 4.4) budeme říkat *index podgrupy* H v grupě G a velikosti $|G|$ množiny G budeme říkat *řád grupy* G.

Věta 4.5 (Lagrange)**.** *Je-li H podgrupa grupy $G(\cdot)$, pak $|G| = [G : H] \cdot |H|$.*

Důkaz. Podle 4.4(1) je rmod H ekvivalence, proto $G = \dot{\bigcup}_{A \in G/\text{rmod } H} A$, kde sjednocujeme disjunktní množiny. Využijeme-li dále poznatek 4.4(6), který říká, že všechny ekvivalenční třídy mají počet prvků stejný jako množina H, pak dostáváme

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

□

Důsledek 4.6. *Je-li $G(\cdot)$ konečná grupa, potom řád každé její podgrupy dělí řád grupy G.*

Příklad 4.7. Z předchozího důsledku okamžitě plynou následující pozorování:

(1) Grupa prvočíselného řádu obsahuje jen triviální podgrupy, tedy G a $\{e\}$.

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

Důkaz. ($\Rightarrow$) Nejprve předpokládejme, že je ρ je ekvivalence slučitelná s operací $\cdot$. Protože je ρ reflexivní relace, leží e v třídě $[e]_\rho$. Zvolme $a, b \in [e]_\rho$ a $g \in G$. Vidíme, že $(e,a),(e,b) \in \rho$, 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 $(e\cdot e, a\cdot b) \in \rho$, dále že $(e\cdot a^{-1}, a\cdot a^{-1}) \in \rho$ a $(g\cdot e\cdot g^{-1}, g\cdot a\cdot g^{-1}) \in \rho$. Využijeme-li vlastností neutrálního prvku a symetrie ρ, vidíme, že $(e, a\cdot b),(e,a^{-1}),(e, g\cdot a\cdot g^{-1}) \in \rho$, tedy $a\cdot b$, a^{-1}, $g\cdot a\cdot g^{-1} \in [e]_\rho$, čímž máme ověřeno, že je $[e]_\rho$ normální podgrupa $G(\cdot)$. Připomeňme, že podle 4.4(4) $\operatorname{rmod}[e]_\rho = \operatorname{lmod}[e]_\rho$.

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

($\Leftarrow$) Předpokládejme, že je H normální podgrupa $G(\cdot)$ a definujme relaci ρ jako $\operatorname{rmod} H$ (tj. $(a,b) \in \rho \leftrightarrow a\cdot b^{-1} \in H$). Podle 4.4(1) je ρ ekvivalence a přímým výpočtem zjistíme, že $[e]_\rho = H$. 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 $\equiv \pmod n$ na množině $\mathbb{Z}(+)$ popsaná v Příkladu 2.4 je právě ekvivalencí $\operatorname{rmod} n\,\mathbb{Z} = \operatorname{lmod} n\,\mathbb{Z}$.

Vezmeme-li si například pro grupu $H = \{\mathrm{id}, (12)\}$ grupy permutací $S_3(\circ)$, která podle 4.2(2) není normální, ekvivalence $\operatorname{rmod} H$ podle předchozí věty není slučitelná s operací $\circ$ a podle 4.4(4) platí $\operatorname{rmod} H \neq \operatorname{lmod} H$.

5. Faktorové grupy a izomorfismy grup

V této kapitole se seznámíme s homomorfismy, tedy se zobrazeními grup, které budou s to přenášet některé jejich vlastnosti. Mimořádné místo mezi homomorfismy zaujímají bijektivní homomorfismy, jimž budeme říkat izomorfismy. Nahlédneme, že na faktorizaci nosné množiny grupy, která umožňuje opětovné zavedení odpovídající grupové struktury, lze přirozeně nahlížet prostřednictvím homomorfismů . Hlavním výsledkem kapitoly budou dvě věty o izomorfismu, které nabízejí technicky velmi příjemné uchopení faktorizace.

Definice. Zobrazení $\varphi : G \to H$ grup $G(\cdot)$ a $H(\cdot)$ slučitelné s jejich binárními operacemi se nazývá (grupový) *homomorfismus*. Bijektivní homomorfismus budeme nazývat *izomorfismus*. Podmnožině $\operatorname{Ker}\varphi = \{g \in G |\ \varphi(g) = e\}$ i relaci $\ker\varphi = \{(g_1,g_2) \in G\times G |\ \varphi(g_1) = \varphi(g_2)\}$ 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 $G_1 \cong G_2$.

Je-li $\varphi : G \to H$ zobrazení, $A \subseteq G$ a , připomeňme, že obrazem $\varphi(A)$ podmnožiny $A \subseteq G$ rozumíme podmnožinu $\{\varphi(a) \mid a \in A\}$ množiny H a úplným vzorem $\varphi^{-1}(B)$ podmnožiny $B \subseteq H$ rozumíme podmnožinu $\{g \in G |\ \exists b \in B : \varphi(g) = b\}$ množiny H. Všimněme si, že symbol $\varphi^{-1}(B)$ má dobrý význam i v případě, že zobrazení φ není bijekce, a tedy nemáme k dispozici inverzní zobrazení. Je-li $\varphi : G \to H$ grupový homomorfismus, pak si dále všimneme, že $\varphi^{-1}(\{e\}) = \operatorname{Ker}\varphi$ a že $\varphi(\operatorname{Ker}\varphi) = \{e\}$.

Poznámka 5.1. *Nechť $G_1(\cdot)$, $G_2(\cdot)$ a $G_3(\cdot)$ jsou grupy a $\varphi : G_1 \to G_2$ a $\psi : G_2 \to G_3$ jsou homomorfismy.*

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

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

(2) Je-li $a, b \in G_1$, pak $\psi\varphi(a \cdot b) = \psi(\varphi(a) \cdot \varphi(b)) = \psi(\varphi(a)) \cdot \psi(\varphi(b))$.

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

(4) Nejprve ukážeme, že je $\psi(H)$ podgrupa $G_3(\cdot)$. Podle 5.1(1) je $e = \psi(e) \in \psi(H)$. Vezměme $u, v \in \psi(H)$, tj. existují $c, d \in H$, pro která $\psi(c) = u$ a $\psi(d) = v$. Protože $c\cdot d$, $c^{-1} \in H$, dostáváme přímo z definice, že $u \cdot v = \psi(c) \cdot \psi(d) = \psi(c\cdot d) \in \psi(H)$, a $u^{-1} = \psi(c)^{-1} = \psi(c^{-1}) \in \psi(H)$ podle 5.1(1).

Poznamenejme, že $e \in \varphi^{-1}(H)$ a zvolme $a, b \in \varphi^{-1}(H)$, tj. $\varphi(a), \varphi(b) \in H$. Potom opět $\varphi(a) \cdot \varphi(b) = \varphi(a \cdot b) \in H$, a $\varphi(a^{-1}) = \varphi(a)^{-1} \in H$, tedy $a \cdot b$, $a^{-1} \in \varphi^{-1}(H)$, proto je $\varphi^{-1}(H)$ podgrupa.

(5) Protože $\{e\}$ je podgrupa $G_2(\cdot)$ a $\mathrm{Ker}\varphi = \varphi^{-1}(\{e\})$, je $\mathrm{Ker}\varphi$ podgrupa podle (3). Vezmeme-li libovolné $g \in G_1$ a $h \in \mathrm{Ker}\varphi$, potom

$$\varphi(g \cdot h \cdot g^{-1}) = \varphi(g) \cdot \varphi(h) \cdot \varphi(g^{-1}) = \varphi(g) \cdot e \cdot \varphi(g)^{-1} = e,$$

tedy $g \cdot h \cdot g^{-1} \in \mathrm{Ker}\varphi$. Zbývá si uvědomit, že $\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a) \cdot \varphi(b)^{-1} = e \Leftrightarrow \varphi(a \cdot b^{-1}) = e \Leftrightarrow a \cdot b^{-1} \in \mathrm{Ker}\varphi$. Konečně $\ker\varphi = \mathrm{rmod}\ \mathrm{Ker}\varphi = \mathrm{lmod}\ \mathrm{Ker}\varphi$ je ekvivalence slučitelná s operací $\cdot$ podle 4.8.

(6) Je-li φ prosté, pak existuje jediný vzor jednotky, tedy $\mathrm{Ker}\varphi = \{e\}$ a jestliže $\ker\varphi = \mathrm{id}$, pak je zřejmě φ prosté. Konečně, jestliže $\mathrm{Ker}\varphi = \{e\}$, potom $\ker\varphi = \mathrm{rmod}\ \mathrm{Ker}\varphi = \mathrm{rmod}\ \{e\} = \mathrm{id}$ podle (4). □

Příklad 5.2. (1) Jsou-li U a V dva vektorové prostory nad týmž tělesem a $\varphi : U \to V$ je lineární zobrazení, pak je φ homomorfismus grup $U(+)$ a $V(+)$, kde je $+$ sčítáním vektorů.

(2) V rámci kurzu lineární algebry bylo dokázáno, že znaménko součinu permutací je rovno součinu jejich znamének, tedy, že $\mathrm{sgn} : S_n \to \{1, -1\}$ je homomorfismus grup permutací na n prvcích a grupy $\{1, -1\}(\cdot)$. Snadno nahlédneme, $\mathrm{Ker}\ \mathrm{sgn} = A_n$, což je podle 5.1 normální podgrupa grupy S_n.

(3) 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 $\mathrm{Ker}\ \det$ je díky 5.1 normální podgrupa matice s determinantem 1 .

Připomeňme, že pro ekvivalenci ρ na množině G rozumíme *přirozenou projekci* na faktorovou množinu G/ρ zobrazení $\pi_\rho : G \to G/\rho$ dané podmínkou $\pi_\rho(g) = [g]_\rho$, kde $g \in G$. Všimněme si, že $\ker \pi_\rho = \rho$.

Věta 5.3. *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 $[e]_\rho$ a inverzním prvkem k prvku $[a]_\rho$ právě prvek $[a^{-1}]_\rho$, dostaneme přímým výpočtem. Konečně $\pi_\rho(a \cdot b) = [a \cdot b]_\rho = [a]_\rho \odot [b]_\rho = \pi_\rho(a) \odot \pi_\rho(b)$ z definice. □

Grupu zavedenou na faktorové množině budeme nazývat *faktorovou grupou*. Věta 4.8, která říká, že každé ekvivalenci ρ slučitelné s binární operací na grupě jednoznačně odpovídá normální podgrupa $H = [e]_\rho$, nám umožňuje faktorovou množinu zapisovat ve tvaru G/H, tedy $G/H := G/\mathrm{rmod} H$.

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 $H = [e]_\rho$ 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 4.4(4) a (5)).

Příklad 5.4. Uvážíme-li na grupě $\mathbb{Z}(+)$ ekvivalenci $\equiv \pmod n$ zavedenou v Příkladu 2.4, jedná se o ekvivalenci slučitelnou s operací $+$ a $[0]_{\equiv(\mathrm{mod}\ n)} = n\mathbf{Z}$, tedy $\equiv \pmod n = \mathrm{rmod}\ n\mathbf{Z}$ a na faktorové množině $\mathbb{Z}/n\mathbf{Z} = \mathbb{Z}/(\equiv \pmod n)$ máme dobře zavedenu strukturu grupy $\mathbb{Z}/n\mathbf{Z}(+)$ předpisem $[a]_{\equiv(\mathrm{mod}\ n)} + [b]_{\equiv(\mathrm{mod}\ n)} = [a + b]_{\equiv(\mathrm{mod}\ n)}$.

Věta 5.5. *Nechť $\varphi : G_1 \to G_2$ 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 $\psi : G_1/H \to G_2$ splňující podmínku $\psi\pi_H = \varphi$ právě tehdy, když $H \subseteq \mathrm{Ker}\varphi$ (tj. $\mathrm{rmod} H \subseteq \mathrm{rmod}\ \mathrm{Ker}\varphi$). Navíc, jestliže ψ existuje, je ψ izomorfismus, právě když φ je na a $\mathrm{Ker}\varphi = H$.*

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

Důkaz. (1) Nejprve předpokládejme, že existuje homomorfismus $\psi : G_1/H \to G_2$ splňující $\psi\pi_H = \varphi$, tedy $\psi([a]_H) = \varphi(a)$. Zvolme $a \in H$. Pak $[a]_H = H = [e]_H$ je neutrální prvek grupy $G_1/H(\cdot)$, a proto $\varphi(a) = \psi([a]_H) = e$ podle 5.1(1). Tedy $a \in \mathrm{Ker}\varphi$, čímž jsme ověřili, že $H \subseteq \mathrm{Ker}\varphi$.

Naopak, nechť $H \subseteq \mathrm{Ker}\varphi$. Musíme ověřit, že jediná možná definice ψ daná předpisem $\psi([a]_H) = \varphi(a)$ je korektní. Vezměme proto $[a]_H = [b]_H$. Potom $a \cdot b^{-1} \in H \subseteq \mathrm{Ker}\varphi$, tedy $e = \varphi(a \cdot b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1}$ podle 5.1(1), a proto $\varphi(a) = \varphi(b)$. Konečně

$$\psi([a]_H \cdot [b]_H) = \psi([a \cdot b]_H) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \psi([a]_H) \cdot \psi([b]_H),$$

tedy ψ je homomorfismus.

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

(2) Z 5.1(5) dostáváme, že $\varphi(G_1)$ je podgrupa G_2. Omezíme-li obor hodnot zobrazení φ, můžeme ho chápat jako homomorfismus $\varphi : G_1 \to \varphi(G_1)$. Nyní aplikujeme (1) pro $H = \mathrm{Ker}\varphi$ a dostaneme přímo požadovaný izomorfismus $\psi : G_1/\mathrm{Ker}\varphi \to \varphi(G_1)$. □

Věta 5.6 (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 5.5(1) pro homomorfismy $\pi_K : G \to G/K$ (jako φ z 5.5(1)) a $\pi_H : G \to G/H$ (jako π_H z 5.5(1)). Protože podle předpokladu $H \subseteq K = \mathrm{Ker}\pi_K$, dává nám 5.5(1) homomorfismus $\psi : G/H \to G/K$ splňující vztah $\psi([a]_H) = [a]_K$. Všimněme si, že je ψ zjevně na. Nyní přímočaře spočítáme $\mathrm{Ker}\psi = \{[a]_H \in G/H |\ \psi([a]_H) = [a]_K = [e]_K\} = K/H$. Poznamenejme, že je $\mathrm{Ker}\psi = K/H$ normální podgrupa $G/H(\cdot)$ podle 5.1(5). Nyní pro homomorfismus ψ využijeme 5.5(2), abychom dostali $G/K = \psi(G/H) \cong (G/H)/\mathrm{Ker}\psi = (G/H)/(K/H)$. □

Máme-li tedy homomorfismus $F_n : \mathbb{Z} \to \mathbf{Z}_n$ grupy $\mathbb{Z}(+)$ do grupy $\mathbf{Z}_n(+)$ s počítáním modulo n daný předpisem $F_n(k) = (k) mod\ n$, potom 5.5(2) zajišťuje izomorfismus $\mathbb{Z}/\mathrm{Ker}\ F_n(+) \cong \mathbf{Z}_n(+)$. Navíc je zjevně $(a, b) \in ker\ F_n$, právě když $n/(a - b)$, a $\mathrm{Ker}\ F_n = n\mathbf{Z}$.

6. Cyklické grupy

V následující kapitole omezíme záběr našeho zkoumání na grupy, které jsou určeny jediným prvkem a obvykle se nazývají *cyklické*. Nejen, že záhy nahlédneme, že jsou nutně komutativní, ale ukážeme, že jich je málo a že je všechny už známe, konkrétně, že jsou izomorfní některé z grup $\mathbb{Z}(+)$ a $\mathbb{Z}_n(+)$ pro $n \in \mathbb{N}$. S využitím dělitelnosti se proto ukáže, že víme dost o jejich struktuře.

Nejprve ovšem připomeňme, že podle 4.1(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 $\langle \{g\} \rangle$, je-li $g \in G$.

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

Příklad 6.1. (1) $\mathbb{Z}(+)$ je cyklická grupa, kde $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

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

$1 \in \langle a \rangle$, a proto existuje $x \in \mathbb{N}$, pro které $a \cdot x \equiv 1 \pmod{n}$. To znamená, že $a \cdot x + n \cdot y = 1$ pro vhodné celé y, a protože $\mathrm{GCD}(a, n)$ dělí levou stranu rovnosti, musí dělit i jedničku a proto $\mathrm{GCD}(a, n) = 1$.

Naopak, předpokládáme-li, že $\mathrm{GCD}(a, n) = 1$, potom díky Eukleidovu algoritmu (2.1) existují $x \in \mathbb{Z}_n$ a celé y, pro něž $a \cdot x + n \cdot y = 1$. Proto $(a \cdot x) \bmod n = 1$, tudíž $1 \in a\,\mathbb{Z}_n$ a $\mathbb{Z}_n = \langle a \rangle$.

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

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

Poznámka 6.2. *Nechť $G(\cdot)$ je grupa a $a \in G$. Zobrazení $\phi : \mathbb{Z} \to G$ dané předpisem $\phi(n) = a^n$ je homomorfismus grup $\mathbb{Z}(+)$ a $G(\cdot)$ a $\phi(\mathbb{Z}) = \langle a \rangle = \{a^n |\ n \in \mathbb{Z}\}$.*

Důkaz. Potřebujeme pro každou dvojici $m, n \in \mathbb{Z}$ 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 $\phi(\mathbb{Z})$ je právě tvaru $\phi(\mathbb{Z}) = \{a^n |\ n \in \mathbb{Z}\}$, a proto se jedná o nejmenší podgrupu $G(\cdot)$ obsahující a. □

V následujícím pozorování shrňme užitečné početní vlastnosti exponentů.

Důsledek 6.3. *Nechť $G(\cdot)$ je grupa a $a \in G$. Potom pro každé $n, m \in \mathbb{Z}$ platí, že $a^{-n} = (a^n)^{-1}$ a $(a^n)^m = a^{nm}$.*

Využijeme-li První větu o izomorfismus na homomorfismus z Poznámky 6.2, který popisuje cyklickou grupu pomocí exponentů generátoru, dostaneme charakterizaci cyklických grup:

Věta 6.4. *Buď $G(\cdot)$ cyklická grupa.*

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

Důkaz. Vezměme nějaký generátor g cyklické grupy $G(\cdot)$, tedy $\langle g \rangle = G$ a definujme zobrazení $\phi : \mathbb{Z} \to G$ dané předpisem $\phi(n) = g^n$. Podle 6.2 jde o homomorfismus a $\phi(\mathbb{Z}) = \langle g \rangle = G$, tedy ϕ je zobrazení na. Nyní podle 5.5(2) je $\mathbb{Z}/\mathrm{Ker}\phi(+) \cong G(\cdot)$.

Zbývá si rozmyslet, jak vypadá $\mathbb{Z}/\mathrm{Ker}\phi$. Z 4.2(4) víme, že $\mathrm{Ker}\phi = n\,\mathbb{Z}$ pro vhodné nezáporné celé n. V případě, že $n = 0$, pak $\mathbb{Z}/\mathrm{Ker}\phi = \mathbb{Z}/\{0\} \cong \mathbb{Z}$, a v případě kladného n je $\mathbb{Z}/\mathrm{Ker}\phi = \mathbb{Z}/n\,\mathbb{Z} \cong \mathbb{Z}_n$ podle 5.5(2). □

Předchozí kritérium nám usnadní důkaz následující vlastnosti cyklických grup.

Poznámka 6.5. *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 6.4 stačí tvrzení o podgrupách dokázat pro grupy $\mathbb{Z}(+)$ a $\mathbb{Z}_n(+)$. Nejprve ho dokažme pro grupu $\mathbb{Z}(+)$. V 4.2(4) jsme ověřili, že $\mathbb{Z}(+)$ jiné podgrupy než podgrupy tvaru $n\,\mathbb{Z}$ neobsahuje. Přitom $\langle n \rangle = n\,\mathbb{Z}$ je cyklická grupa, čímž je tvrzení ověřeno.

Nyní využijeme homomorfismu $F_n : \mathbb{Z} \to \mathbf{Z}_n$ z 1.1. Zvolíme-li podgrupu H grupy $\mathbf{Z}_n(+)$, pak $F_n^{-1}(H)$ je podle předchozí úvahy a 5.1(5) cyklická podgrupa $\mathbb{Z}$, tedy $H = F_n(F_n^{-1}(H))$ je cyklická podgrupa $\mathbf{Z}_n(+)$. □

Na závěr si všimněme, že pro každé přirozené k značíme $k\,\mathbb{Z} = \{kz|\ z \in \mathbb{Z}\}$, a proto jde podle Poznámky 6.2 o nejmenší podgrupu grupy $\mathbb{Z}(+)$, obsahující k, tedy $\langle k\rangle = k\,\mathbb{Z}$. Podobně pro každé $k \in \mathbb{Z}_n$ platí, že $k\,\mathbb{Z}_n = \langle k\rangle = \{k \cdot z|\ z \in \mathbb{Z}_n\}$.

7. Kryptografické aplikace cyklických grup

Teorie prezentovaná v předchozích kapitolách má několik užitečných kryptografických aplikací založených na jednoduchém pozorování, že je obvykle mnohem snazší v grupě mocnit, než ze známé mocniny určovat její základ či exponent. Dříve než se k popisu protokolu založeného na obtížnosti odmocňování (RSA v Příkladu 7.7) a protokolů, které se opírají o obtížnost diskrétního logaritmu (Příkladu 7.9) dostaneme, učiníme pozorování o struktuře uspořádané množiny podgrup konečné cyklické grupy (Věta 7.2) a o řádu prvků, které je známo pod názvem Eulerova věta (Věta 7.5).

Poznámka 7.1. *Je-li $n \in \mathbb{N}$, $a, d \in \mathbb{Z}_n \setminus \{0\}$ a $d = \mathrm{GCD}(a, n)$, pak $\langle a\rangle = \langle d\rangle$.*

Důkaz. Podobně jako v Příkladu 6.1(2) vidíme, že díky Eukleidovu algoritmu existují $x \in \mathbb{Z}_n$ a celé y, pro něž $a \cdot x + n \cdot y = d$. To znamená, že $(a \cdot x) \bmod n = d$, tudíž $d \in a\,\mathbb{Z}_n = \langle a\rangle =$ a $\langle d\rangle \subseteq \langle a\rangle$.

Naopak, protože d/a, dostáváme, že $a \in d\,\mathbb{Z}_n = \langle d\rangle$, a proto $\langle a\rangle \subseteq \langle d\rangle$. Tím jsme ověřili rovnost množin $\langle a\rangle = \langle d\rangle$. □

Speciálním případem předchozí poznámky je tvrzení Příklad 6.1(2), jehož důsledkem je pozorování, že hodnota Eulerovy funkce $\varphi(n)$ udává počet generátorů cyklické grupy řádu n.

Věta 7.2. *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 6.4, díky němuž stačí tvrzení dokázat pro (izomorfní) grupu $\mathbb{Z}_n(+)$. Jestliže $k = 1$, je tvrzení triviální, předpokládejme tedy, že $k > 1$. Potom snadno nahlédneme, že množina $\langle \frac{n}{k}\rangle = \{0, \frac{n}{k}, 2\frac{n}{k}, \ldots, (k-1)\frac{n}{k}\}$ je podgrupa a $|\langle \frac{n}{k}\rangle| = k$.

Mějme nyní nějakou podgrupu H grupy $\mathbb{Z}_n(+)$ řádu k, pak podle Lagrangeovy věty k/n. Navíc H je podle 6.5 cyklická, a tedy existuje $h \in H$, pro $H = \langle h\rangle$. Označíme-li $d = \mathrm{GCD}(h, n)$, potom z 7.1 plyne, že $\langle h\rangle = \langle d\rangle$. Z první části důkazu dostáváme, že je řád podgrupy $\langle d\rangle$ roven $\frac{n}{d}$, proto $k = \frac{n}{d}$, a tedy $\langle h\rangle = \langle d\rangle = \langle \frac{n}{k}\rangle$ □

Příklad 7.3. (1) Uvažujme konečnou cyklickou grupu $G(\cdot)$. Potom nám 7.1 říká, že $G(\cdot)$ obsahuje právě $\varphi(|G|)$ generátorů. Protože díky Lagrangeově větě řád podgrupy vždy dělí řád grupy, podle 7.2 $G(\cdot)$ 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 $p_1 < p_2 < \cdots < p_k$ jsou prvočísla a $r_i \in \mathbb{N}$, pak děliteli n jsou právě čísla $\prod_{i=1}^{k} p_i^{s_i}$, kde $0 \le s_i \le r_i$, tedy $G(\cdot)$ obsahuje právě $\prod_{i=1}^{k}(r_i+1)$ podgrup a podle 3.9 právě $\prod_{i=1}^{k}(p_i-1)p_i^{r_i-1}$ generátorů.

(2) Konkrétně, vezmeme cyklickou grupu $\mathbb{Z}_{50}(+)$. Protože $50 = 2 \cdot 5^2$, dostáváme z bodu (1), že $\mathbb{Z}_{50}(+)$ obsahuje $\varphi(50) = 20$ generátorů a právě $6 = 2 \cdot 3$ podgrup. Vezmeme-li například podgrupu $\langle 42 \rangle$ grupy $\mathbb{Z}_{50}(+)$ (a jiné než cyklické podgrupy tato grupa podle 6.5 neobsahuje), pak díky 7.1 víme, že $\langle 42 \rangle = \langle \mathrm{GCD}(42, 50) \rangle = \langle 2 \rangle = 2\,\mathbb{Z}_{50}$, a jedná se tedy o podgrupu řádu $25 = \frac{50}{2}$.

Poznámka 7.4. *Buď $G(\cdot)$ konečná grupa. Potom $g^{|G|} = 1$ pro každý prvek $g \in G$.*

Důkaz. $\langle g \rangle$ je cyklická grupa řádu n, tedy je podle 6.4 izomorfní $\mathbb{Z}_n(+)$, proto $g^n = 1$. Podle 4.5 $n/|G|$, tedy $g^{|G|} = (g^n)^{\frac{|G|}{n}} = 1^{\frac{|G|}{n}} = 1$, kde 1. rovnost plyne z 6.3. □

Poznamenejme, že *řádem prvku* g grupy $G(\cdot)$ rozumíme právě řád cyklické podgrupy $\langle g \rangle$ a *exponentem prvku* g rozumíme každé přirozené číslo n, pro které platí $g^n = 1$. Předchozí poznámka tedy říká, že řád konečné grupy je exponentem každého jejího prvku. Toto pozorování využije následující důsledek, který je pro prvočíselné n znám také jako Malá Fermatova věta:

Věta 7.5 (Eulerova věta)**.** *Pro nesoudělná kladná celá čísla $a, n > 1$ je*

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

Důkaz. Díky Poznámce 2.5 tvrzení stačí dokázat pro nenulové $a \in \mathbb{Z}_n$. Použijeme k tomu Poznámku 7.4, kde jako grupu G vezmeme grupu invertibilních prvků $\mathbb{Z}_n^*(\cdot)$ monoidu $\mathbb{Z}_n(\cdot)$ tj. prvků nesoudělných s n. Protože $a \in \mathbb{Z}_n^*$, je $(a^{\varphi(n)})\mathrm{mod}\ n = (a^{|\mathbb{Z}_n^*|})\mathrm{mod}\ n = 1$ díky 7.4. □

Než obrátíme pozornost k aplikacím předchozích pozorování, vyslovme pozorování, které slouží jako technický nástroj níže popsaného protokolu RSA.

Poznámka 7.6. *Buď p a q dvě různá lichá prvočísla a $m = \mathrm{lcm}(p-1, q-1)$. Potom pro každé $a \in \mathbb{Z}_{pq}$ a $u \in \mathbb{N}$ platí, že* $(a^{mu+1})\mathrm{mod\ pq} = \mathrm{a}$.

Důkaz. Nejprve ukážeme, že $(a^{m+1})\mathrm{mod\ pq} = \mathrm{a}$.

Podle Věty 7.5 $(x^m)\mathrm{mod\ p} = 1$ a $(y^m)\mathrm{mod\ q} = 1$ pro ta x, která nejsou násobkem p a ta y, která nejsou násobkem q. Dále zřejmě platí $((up)^{m+1})\mathrm{mod}\ p = 0$, a proto i $(x^{m+1})\mathrm{mod}\ p = (x)\mathrm{mod}\ p$ a $(y^{m+1})\mathrm{mod}\ q = (y)\mathrm{mod}\ q$ pro každé nezáporné celé x a y. Vezměme nyní $a \in \mathbb{Z}_{pq}$. Z předchozího pozorování plyne, že

$$((a)\mathrm{mod}\ p, (a)\mathrm{mod}\ q) = ((a^{m+1})\mathrm{mod}\ p, (a^{m+1})\mathrm{mod}\ q),$$

a díky Větě 2.7 použité pro bijekci $\mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$ dostáváme, že shodné jsou i vzory prvků $((a)\mathrm{mod}\ p, (a)\mathrm{mod}\ q)$ a $((a^{m+1})\mathrm{mod}\ p, (a^{m+1})\mathrm{mod}\ q)$, proto

$$(a^{m+1})\mathrm{mod\ pq} = \mathrm{a}.$$

Nyní indukcí díky 6.3 dostáváme, že $a^{um+1} = a^{(u-1)m} \cdot a^{m+1} = a^{(u-1)m+1} = a$ pro každé $u \in \mathbb{N}$ a $a \in \mathbb{Z}_{pq}$. □

Příklad 7.7 (Rivest, Shamir, Adleman)**.** Nejprve zvolíme p a q dvě různá lichá prvočísla a položme $m = \mathrm{lcm}(p-1, q-1)$.

Vezměme $e < m$ nesoudělné s m a pak (například pomocí Eukleidova algoritmu) najdeme takové $d < m$, že $(ed)\mathrm{mod}\ m = 1$. Nyní podle 7.6 pro každé $a \in \mathbb{Z}_{pq}$ platí, že $(a^e)^d = a^{ed} = a^{um+1} = a$ (počítáno v $\mathbb{Z}_{pq}$, tedy modulo pq).

Pomocí vlastnosti čísel p, q, m, d, e můžeme nyní popsat protokol asymetrického šifrování známý pod zkratkou RSA. Položíme-li $n = p \cdot q$, je veřejným klíčem dvojice

čísel (n, e) a soukromý klíč tvoří *tajný exponent* d. Chceme-li zprávu $a \in \mathbb{Z}_n$ adresovat majiteli soukromého klíče, stačí ji zašifrovat pomocí mocnění veřejně známou hodnotou e v monoidu $\mathbb{Z}_n(\cdot)$ a odeslat hodnotu $x = (a^e) \bmod pq$. K jejímu rozluštění stačí umocnit v $\mathbb{Z}_n(\cdot)$ pomocí tajného exponentu, protože $x^d = (a_i^e)^d = a_i^{ed} = a_i$.

Naopak, zveřejnění-li majitel soukromého klíče zašifrovanou zprávu

$$(a_1^d) \bmod \ n, \ldots, (a_k^d) \bmod \ n,$$

mohou si příjemci zprávy stejným způsobem (tj. umocněním na veřejně známý exponent e: $((a_1^d)^e) mod\ n, \ldots, ((a_k^d)^e) mod\ n = (a_1, \ldots, a_k)$) ověřit, že odesilatel 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 časové složitosti vzhledem k bitové délce), zatímco mocnění čísel v $\mathbb{Z}_{pq}$ je (i pro velké exponenty a velké pq) velmi snadné a rychlé.

Důkaz následujícího tvrzení o cyklických grupách je elegantnější, využijeme-li jistých znalostí z teorie polynomů nad obecným tělesem, proto ho provedeme později:

Věta 7.8. *Nechť T je komutativní těleso s operacemi $+$ a $\cdot$ a nechť G je konečná podgrupa multiplikativní grupy $T \setminus \{0\}(\cdot)$. Potom G je cyklická grupa.*

Zatímco je protokol RSA založen na diskrétním odmocňování, následující dvě aplikace využívají tak zvaný problém *diskrétního logaritmu*, tedy obtížnost nalezení přirozeného n pro známé prvky g, h vhodné grupy pro něž $h = g^n$.

Příklad 7.9 (Diffieho–Hellmanův protokol výměny klíčů)**.** Otázku domluvy tajného klíče veřejným kanálem lze s použitím cyklické grupy, například multiplikativní grupy $\mathbb{Z}_p^*(\cdot)$ pro p (dostatečně velké) prvočíslo následovně: Veřejným klíčem bude kromě prvočísla p ještě generátor g grupy $\mathbb{Z}_p^*(\cdot)$, tedy prvek splňující podmínku $\langle g \rangle = \mathbb{Z}_p^*$, který existuje díky Větě 7.8. Každá strana komunikace zvolí svou tajnou hodnotu čísla m a n ze $\mathbb{Z}_p^*$ a vzájemně si pošlou hodnotu $x = g^m$ a $y = g^n$. Poté co obě strany umocní přijatou hodnotu na svůj tajný exponent, získají obě společný tajný klíč

$$s = x^n = g^{mn} = y^m.$$

Bez rychlého výpočtu diskrétního logaritmu (který v grupě $\mathbb{Z}_p^*(\cdot)$ není k dispozici) nelze ze znalosti hodnot x a y zjistit hodnotu s.

Příklad 7.10 (ElGamal)**.** Tentokrát využijeme problém diskrétního logaritmu pro stejnou úlohu, kterou řeší 7.7. Opět zvolíme cyklickou grupu $\mathcal{G} = G(\cdot)$, její generátor g a náhodné číslo $k \in \mathbb{Z}_{|G|}$ a spočítáme $b = a^k$ (bohužel nemůžeme už vzít například grupu $\mathbb{Z}_p^*(\cdot)$ pro p prvočíslo, protože je pro ni je znám útok, který popisovaný protokol prolomí, místo toho se obvykle volí grupa definovaná pomocí eliptických křivek). Veřejný klíč je potom trojice $\mathcal{G}, a, b$ a tajným klíčem hodnota k. Chceme-li zašifrovat zprávu $x \in G$, náhodně zvolíme $r \in \mathbb{Z}_{|G|}$ a spočítáme $c_1 = a^r$ a $c_2 = x \cdot b^r$. Posílanou zprávou je dvojice (c_1, c_2), kterou příjemce znalý tajného klíče snadno rozšifruje výpočtem

$$c_2 \cdot c_1^{-k} = x \cdot b^r \cdot (a^r)^{-k} = x \cdot a^{kr} \cdot a^{-kr} = x.$$

I tentokrát bez schopnosti rychlého výpočtu diskrétního logaritmu nelze ze znalosti veřejného klíče a hodnot dvojice (c_1, c_2) zprávu x rozšifrovat.

8. Obecný pohled: základy univerzální algebry

Smyslem této kapitoly je nahlédnout, že některé výsledky, které jsme formulovali pro grupy platí v téměř nezměněné podobě i v mnohem obecnějším kontextu a lze jich tak využít i pro algebraické objekty, které s grupami mají strukturně jen málo společného. Konkrétně si na příkladech všimneme pojmů algebra, podalgebra, homomorfismus a kongruence, které zobecňují pojmy grupa, podgrupa, grupový homomorfismus a ekvivalence slučitelná s operací zkoumané v předchozích kapitolách. Příklady koncepty, které lze zcela přímočaře přeložit do obecného kontextu shrnuje Poznámka 8.5.

Připomeňme, že každé zobrazení $A^n \to A$ pro celé $n \geq 0$ se nazývá *n-ární operací na množině A*, kde n budeme nazývat *arita* neboli *četnost* operace. Zaveďme nyní pojem obecné algebry:

Definice. Je-li I množina, budeme říkat zobrazení $\Omega : I \to \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ *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.

Je-li indexová množina I konečná, můžeme předpokládat, že je dobře uspořádaná, a tedy typ lze chápat jako konečnou posloupnost arit jednotlivých operací a místo $A(\alpha_i |\ i \in I)$ budeme psát $A(\alpha_1, \ldots, \alpha_{|I|})$.

Příklad 8.1. (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 $V(+,\cdot t | t \in \mathbf{T})$ nebo $V(+,0,\cdot t | t \in \mathbf{T})$. Všimněme si, že pro nekonečné těleso potřebujeme uvažovat nekonečně mnoho unárních operací.

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

Příklad 8.2. Nahlédneme, jak v jednotlivých případech algeber z Příkladu 8.1 vypadají podalgebry.

(1) Pro grupu $G(\cdot)$ máme:

(a) 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 $G(\cdot)$.

(b) 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.

(c) Podalgeber algebry $G(\cdot)$ je obecně mnohem víc než podgrup grupy $G(\cdot)$. Například pro každé $g \in G$ a $n \in \mathbb{N}$ tvoří množina $\{g^k |\ k \geq n\}$ podalgebru $G(\cdot)$. V případě $G(\cdot) = \mathbb{Z}(+)$ to znamená, že množiny $\{ak |\ k \geq n\}$ jsou podalgebry, speciálně množina všech přirozených čísel, která podgrupou $\mathbb{Z}(+)$ určitě není.

(2) Podalgebrou algebry $V(+,0,\cdot t | t \in \mathbf{T})$ jsou právě podprostory tohoto vektorového prostoru a podalgebry algebry $V(+,\cdot t | t \in \mathbf{T})$ 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 podalgebru B leží všechny hodnoty zobrazení β_i opět v B. Zobrazení β_i tedy můžeme chápat jako operace na množině B a tak dostáváme strukturu algebry $B(\beta_i|\ i \in I)$ na každé podalgebře B.

Definice. Nechť symbol α označuje n-ární operaci na množině A a β je n-ární operace na množině B. Řekneme, že zobrazení $f : A \to B$ je *slučitelné s operacemi* α *a* β, jestliže $f(\alpha(a_1, \dots, a_n)) = \alpha(f(a_1), \dots, f(a_n))$. Zobrazení $f : A \to B$ mezi dvěma algebrami $\mathcal{A} = A(\alpha_i|\ i \in I)$ a $\mathcal{B} = B(\beta_i|\ i \in I)$ stejného typu Ω budeme říkat *homomorfismus*, je-li slučitelné s operacemi α_i a β_i, pro všechna $i \in I$. Bijektivní homomorfismus budeme nazývat *izomorfismus*. Jestliže mezi dvěma algebrami $\mathcal{A}$ a $\mathcal{B}$ existuje izomorfismus, říkáme, že $\mathcal{A}$ a $\mathcal{B}$ jsou *izomorfní* a píšeme $\mathcal{A} \cong \mathcal{B}$ nebo zkráceně $A \cong B$.

Poznamenejme, že budeme obvykle odpovídající operace dvou algeber stejného typu označovat stejně, tedy $A(\alpha_i|\ i \in I)$ a $B(\alpha_i|\ i \in I)$. V takovém případě slučitelnosti s operací α_i pro nějaké (nebo všechna) $i \in I$.

Příklad 8.3. (1) Buď $G_i(\cdot)$ 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 5.1(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) Nechť U a V jsou dva vektorové prostory nad tělesem T. Potom každé lineární zobrazení (homomorfismus) vektorových prostorů je homomorfismem algeber $U(+, \cdot t|t \in T)$ a $V(+, \cdot t|t \in T)$.

Definice. Nechť 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 8.4. (1) id a $A \times A$ jsou kongruence na libovolné algebře $A(\alpha_i|\ i \in I)$.

(2) Každá ekvivalence je slučitelná s libovolnou nulární operací, protože dvojice (α, α) je ekvivalentní díky reflexivitě ekvivalence pro každou nulární operaci α

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

Díky (2) si stačí uvědomit, že pro $(a, b) \in \rho$ platí, že $(a^{-1}, b^{-1}) \in \rho$. To dostaneme aplikací slučitelnosti ρ s operací $\cdot$ na ekvivalentní dvojice

$$(a, b), (a^{-1}, a^{-1}), (b^{-1}, b^{-1}) \in \rho,$$

neboť $(a^{-1}, b^{-1}) = (a^{-1} \cdot ab^{-1}, a^{-1}ab^{-1})$.

Připomeňme, že je-li $f : A \to B$ zobrazení, rozumíme jeho *jádrem* $\ker f$ relaci danou předpisem: $(a, b) \in ker\ f \Leftrightarrow f(a) = f(b)$. Nyní jsme připraveni vyslovit obdobu Poznámky 5.1 pro obecné algebry:

Poznámka 8.5. *Nechť* $A_1(\alpha_i|\ i \in I)$, $A_2(\alpha_i|\ i \in I)$ *a* $A_3(\alpha_i|\ i \in I)$ *jsou algebry stejného typu,* $f : A_1 \to A_2$ *a* $g : A_2 \to A_3$ *jsou homomorfismy a* B *je podalgebra algebry* $A_2(\cdot)$.

(1) gf *je také homomorfismus,*

(2) *je-li* f *izomorfismus, 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 5.1.

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

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

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

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

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

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

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

Poznámka 8.6. *Nechť* $\mathcal{A} = A(\alpha_i|\ i \in I)$ *je algebra a* A_j *jsou podalgebry* $\mathcal{A}$ *a* ρ_j *kongruence na* $\mathcal{A}$ *pro každé* $j \in J$.

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

Důkaz. (1) Obdoba Poznámky 4.1(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 $A(\alpha_i|\ i \in I)$ máme $\alpha_i(a_1, \dots a_n) \in A_k$, tedy $\alpha_i(a_1, \dots a_n) \in \bigcap_{j\in J} A_j$.

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

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

9. Izomorfismy algeber

V návaznosti na předchozí kapitolu vyslovíme obecnou verzi Věty o homomorfismus a Vět o izomorfismus. a pozorněji než v grupovém případě prozkoumáme

otázku, proč dvě izomorfní algebry chápeme jako stejné. Nejprve ovšem musíme zobecnit princip faktorizace pro obecné algebry (Věta 9.1). Zatímco je zavedení faktorové algebry zcela přímočarým zobecněním definice faktorové grupy, vyslovení Druhé věty o izomorfismu vyžaduje nový pojem faktorové ekvivalence.

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 $A(\alpha_i |\ i \in I)$, pak tímto způsobem definujeme na A/ρ strukturu algebry stejného typu.

Následující tvrzení je obecnou variantou grupové Věty 5.3.

Věta 9.1. *Je-li ρ kongruence na algebře $\mathcal{A} = A(\alpha_i |\ i \in I)$, pak je definice algebry A/ρ korektní, jde o algebru stejného typu jako $\mathcal{A}$ a přirozená projekce $\pi_\rho : A \to A/\rho$ je homomorfismus.*

Důkaz. Vezměme libovolnou n-ární operaci α algebry A a nechť $[a_j]_\rho = [b_j]_\rho$, 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. □

Algebru $A/\rho(\alpha_i |\ i \in I)$ z předchozí věty budeme nazývat *faktorovou algebrou* algebry $\mathcal{A}$ a budeme ji značit $\mathcal{A}/\rho$.

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 9.2. *Buď ρ kongruence na algebře $\mathcal{A} = A(\alpha_i |\ i \in I)$.*

(1) *Je-li σ kongruence na $\mathcal{A}$ obsahující ρ, je σ/ρ dobře definovaná kongruence na algebře $\mathcal{A}/\rho$.*

(2) *Je-li η kongruence na algebře $\mathcal{A}/\rho$, potom existuje právě jedna kongruence σ na algebře $\mathcal{A}$ 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. □

Věta 9.3. *Nechť $f : A \to B$ je homomorfismus dvou algeber $\mathcal{A} = A(\alpha_i |\ i \in I)$ a $\mathcal{B} = B(\alpha_i |\ i \in I)$ stejného typu.*

(1) (Věta o homomorfismu) *Je-li ρ kongruence na algebře $\mathcal{A}$, pak existuje homomorfismus $g : A/\rho \to B$ splňující podmínku $g\pi_\rho = f$ právě tehdy, když $\rho \subseteq \ker f$. Navíc, pokud g existuje, je g izomorfismus, právě když f je na a $\ker f = \rho$.*

(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 stejným postupem jako Větu o homomorfismu a 1. věta o izomorfismu pro grupy (5.5).

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

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

Konečně 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 8.5(3) je $f(A)$ je podalgebra B a poté stejně jako v důkazu 5.5(2) použijeme Větu o homomorfismu (1) na $\rho = \ker f$. □

Věta 9.4. *[2. věta o izomorfismu] Nechť $\rho \subseteq \sigma$ jsou dvě kongruence na algebře $\mathcal{A}$. Pak algebra $\mathcal{A}/\sigma$ je izomorfní algebře $(\mathcal{A}/\rho)/(\sigma/\rho)$.*

Důkaz. I tentokrát postupujeme stejně jako v důkazu Věty o izomorfismu pro grupy 5.6: nejprve použijeme 9.3(1) pro homomorfismy $\pi_\sigma : A \to A/\sigma$ a $\pi_\rho : A \to A/\rho$, která nám dává homomorfismus $g : A/\rho \to A/\sigma$ splňující vztah $g([a]_\rho) = [a]_\sigma$. Zbývá spočítat $\ker g = \sigma/\rho$ a použít 9.3(2). □

Nyní zobecníme definici ze začátku 6.kapitoly.

Definice. Buď $\mathcal{A} = A(\alpha_i |\ i \in I)$algebra a $X \subseteq A$. Potom podalgebru $\langle X \rangle$ algebry $\mathcal{A}$, kterou dostaneme jako průnik všech podalgeber $\mathcal{A}$ obsahujících množinu X, což je podle 8.6 podalgebra, nazveme podalgebrou *generovanou* X (nebo budeme říkat, že X *generuje* podalgebru $\langle X \rangle$). Řekneme, že X *generuje* $\mathcal{A}$, jestliže $\langle X \rangle = A$.

Příklad 9.5. (1) Uvažujme algebru $\mathbb{Z}(+)$. Pak sice $\langle \{1\} \rangle = \mathbf{N}$, ale nejmenší podalgebra $\mathbb{Z}(+)$ obsahující množinu $\{-1, 1\}$ je už rovna celému $\mathbb{Z}$ tj. $\langle \{-1, 1\} \rangle = \mathbb{Z}$.

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

(3) Algebru $\mathbb{Z}(+, -, 1)$ dokonce generuje prázdná množina, tedy $\langle \emptyset \rangle = \mathbb{Z}$.

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

Poznámka 9.6. *Buď $f, g : A \to B$ dva homomorfismy algeber stejného typu a nechť $X \subseteq A$ generuje algebru $\mathcal{A}$. Jestliže $f(x) = g(x)$ pro všechna $x \in X$, potom $f = g$.*

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

Příklad 9.7. (1) Uvažujme grupu celých čísel $\mathbb{Z}(+)$ a $G(+)$ nějaký grupoid, tedy algebru s jednou binární operací $+$. Nechť $f, g : \mathbb{Z} \to G$ je homomorfismus. Uvědomme si, že nejmenší podalgebra $\mathbb{Z}(+)$ obsahující množinu $\{-1, 1\}$ je už rovna

celému $\mathbb{Z}$ tj. $\langle\{-1,1\}\rangle = \mathbb{Z}$. Podle předchozí poznámky jsou tedy f a g shodné, jestliže $f(1) = g(1)$ a $f(-1) = g(-1)$.

(2) Uvažujme-li nyní dva homomorfismy $f, g : \mathbb{Z} \to G$ na algebře celých čísel $\mathbb{Z}(+,-)$ a obecné algebře $G(+,-)$ s jednou binární operací $+$ a jednou unární operací $-$. Nechť $f, g : \mathbb{Z} \to G$ je homomorfismus. Potom $\langle 1\rangle = \mathbb{Z}$, a podle 9.6 jsou f a g shodné, jestliže $f(1) = g(1)$.

(3) Z algebry $\mathbb{Z}(+,-,1)$ do obecné algebry $G(+,-,1)$ existuje nejvýše jeden homomorfismus.

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 izomorfismem. Samotná přesná formalizace uvedené myšlenky, která je tvrzením o metajazyku algebry, vyžaduje pečlivou práci s formální logikou a my ji zde pouze pro informaci alespoň naznačíme.

Připomeňme, že term je jakákoli proměnná a jsou-li $t_1, \ldots, t_n$ termy a α funkční symboly (operace) četnosti n, pak i $\alpha(t_1, \ldots, t_n)$, je term, dále je-li P predikát četnosti n a $t_1, \ldots, t_n$ jsou termy, pak je výraz $P(t_1, \ldots, t_n)$ atomickou formulí a a jsou-li φ a ψ dvě formule, pak výrazy $(\varphi \to \psi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $\neg\varphi$, $\forall\varphi$ 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.

Věta 9.8. *Nechť $A(\alpha_i|\ i \in I)$ a $B(\alpha_i|\ i \in I)$ jsou dvě izomorfní algebry stejného typu. Potom uzavřená formule φ jazyka algeber platí v algebře $A(\alpha_i|\ i \in I)$, právě když platí v algebře $B(\alpha_i|\ i \in I)$.*

Důkaz. Nechť $f : A \to B$ je nějaký izomorfismus algeber $\mathcal{A} = A(\alpha_i|\ i \in I)$ a $\mathcal{B} = B(\alpha_i|\ i \in I)$, φ formule. Vezmeme-li nějaké ohodnocení e formule φ v A, označíme fe zobrazení, 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 $\{fe|\ e \in E\}$ tvoří právě množinu všech ohodnocení formule φ v B, neboť f je bijekce. Dále snadno nahlédneme, že pro každou uzavřenou formuli φ platí, že buď $\mathcal{A} \models \varphi$ nebo $\mathcal{A} \models \neg\varphi$, a protože f je izomorfismus algeber $\mathcal{A}$ a $\mathcal{B}$, stačí indukcí podle počtu kroků, jimiž je φ odvozena z atomický formulí a jimiž jsou v nich vytvořeny zúčastněné termy, dokázat $\mathcal{A} \models \varphi$ implikuje $B \models \varphi$.

Nejprve uvážíme jedinou atomickou formuli $t = s$, kde $t = t(x_1, \ldots, x_n)$ a $s = s(x_1, \ldots, x_n)$ jsou termy v proměnných $x_1, \ldots, x_n$. Mějme realizaci nějaké funkčního symbolu na obou algebrách, tedy právě n-ární operaci α_i pro nějaké $i \in I$ a

předpokládáme například, že $t = \alpha_i(t_1, \ldots, t_n)$, kde $t_1, \ldots, t_n$ jsou termy a nechť e je nějaké ohodnocení formule $t = s$. Protože $e(\alpha_i(t_1, \ldots, t_n) = \alpha_i(e(t_1), \ldots, e(t_n))$ a z indukčního předpokladu užitého pro termy $t_1, \ldots, t_n$ 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

$$f(e(\alpha_i(t_1, \ldots, t_n))) = f(\alpha_i(e(t_1), \ldots, e(t_n))) =$$

$$= \alpha_i(fe(t_1), \ldots, fe(t_n)) = fe(\alpha_i(t_1, \ldots, t_n)).$$

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 $\mathcal{B}$ vzniklé použitím pravidel $(\varphi \to \psi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $\neg\varphi$, $(\forall x)\varphi$ a $(\exists x)\varphi$ z kratších formulí φ a ψ za předpokladu, že daná dlouhá formule platí na $\mathcal{A}$. □

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).

10. Okruhy a ideály

Nyní obrátíme svou pozornost k další důležité třídě algebraických objektů, jimiž jsou okruhy. Protože je naším hlavním cílem konstrukce a algoritmické uchopení (především konečných) těles, zaměříme se na obecný popis těles (Věta 10.5) a charakterizaci těch faktorů komutativních okruhů, které tvoří těleso (Věta 10.8).

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 $(a+b) \cdot c = a \cdot c + b \cdot c$. Prvek okruhu $R(+, \cdot, -, 0, 1)$ se nazývá *invertibilní*, jedná-li se o invertibilní prvek monoidu $R(\cdot)$.

Řekneme, že je okruh

- *komutativní*, je-li operace $\cdot$ komutativní,
- *obor*, jestliže pro každé $a, b \in R$ platí implikace $a \cdot b = 0 \Rightarrow a = 0$ nebo $b = 0$,
- *těleso*, jsou-li všechny prvky množiny $R \setminus \{0\}$ invertibilní a $0 \neq 1$ a
- *komutativní těleso*, je-li to komutativní okruh a zároveň těleso.

Příklad 10.1. (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) $\mathbb{Z}(+, \cdot, -, 0, 1)$ a $\mathbb{Z}_n(+, \cdot, -, 0, 1)$ pro každé přirozené $n > 1$ jsou komutativní okruhy.

Poznámka 10.2. *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). □

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.

Příklad 10.3. (1) $\{0\}$ a R jsou ideály každého okruhu R.

(2) Podle 6.5 jsou ideály okruhu celých čísel $\mathbb{Z}(+,\cdot,-,0,1)$ právě tvaru $k\,\mathbb{Z}$ a ideály okruhu $\mathbb{Z}_n(+,\cdot,-,0,1)$ tvaru $k\,\mathbb{Z}_n$, kde $k < n$ je 0 nebo dělitel čísla n.

(3) Množiny $aR = \{a\cdot r |\ r \in R\}$ (resp. $Ra = \{r\cdot a |\ r \in R\}$) jsou (tzv. *hlavní*) pravé (resp. levé) ideály okruhu R pro každé $a \in R$. Ověříme to například pro aR. Je-li $ar, as \in aR$, pak díky distributivitě $ar + as = a(r+s) \in aR$ a $-ar = a(-r) \in aR$ podle 10.2(2). Dále $0 = a0 \in aR$ díky 10.2(1) a $(ar)x = a(rx) \in aR$ díky asociativitě pro libovolné $x \in R$.

Nechť $R(+,\cdot,-,0,1)$ je okruh. Poznamenejme, že se ideálům $\{0\}$ a R říká *triviálními* ideály a (levý, pravý) netriviální ideál I okruhu $R(+,\cdot,-,0,1)$ (tj. platí-li, že $\{0\} \neq I \neq R$) se nazývá *vlastní*. Pravé (levé) ideály tvaru aR (Ra) popsané v Příkladu 10.3(3) jsou takzvané *hlavní* pravé (levé) ideály. Konečně alespoň dvouprvkovému okruhu se říká *netriviální okruh*.

Nyní dokážeme elementární poznámku, která nám umožní charakterizovat tělesa pomocí pojmu pravý (levý ideál).

Poznámka 10.4. *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. □

Věta 10.5. *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 10.4.

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 10.2(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 3.5 a b je tedy inverzní k a. □

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.

Připomeňme, že *Homomorfismus* (*izomorfismus*) okruhů bude homomorfismus (izomorfismus) příslušných algeber. Uvážíme-li ideál I okruhu $R(+,\cdot,-,0,1)$, pak je I podgrupa grupy $R(+)$, tedy můžeme pracovat s ekvivalencí rmod I danou podmínkou $(a,b) \in \text{rmod } I \Leftrightarrow a-b = a+(-b) \in I$. *Podokruhem* okruhu $R(+,\cdot,-,0,1)$ budeme rozumět každou podalgebru algebry $R(+,\cdot,-,0,1)$.

Poznámka 10.6. *Nechť $\mathcal{R} = R(+,\cdot,-,0,1)$ a $\mathcal{S} = S(+,\cdot,-,0,1)$ jsou okruhy, I ideál okruhu $\mathcal{R}$ a $\varphi : R \to S$ okruhový homomorfismus.*

(1) rmod I *je kongruence okruhu $\mathcal{R}$. Označíme-li $R/I := R/\text{rmod } I$, pak je faktorová algebra $R/I(+,\cdot,-,[0]_I,[1]_I)$ rovněž okruh a přirozená projekce $\pi_I : R \to R/I$ okruhový homomorfismus.*

(2) Kerφ *je ideál okruhu $\mathcal{R}$.*

Důkaz. (1) Podle 8.4(1),(3) je rmod I ekvivalence slučitelná s operacemi $+$, $-$, 0 a 1. Zbývá ukázat slučitelnost s násobením. Zvolme $(a,b),(c,d) \in \text{rmod } I$. Pak $a-b, c-d, (a-b)c, b(c-d) \in I$, a tudíž $ac-bd = (a-b)c + b(c-d) \in I$. Proto i $(a\cdot c, b\cdot d) \in \rho$, čímž jsme ověřili, že je rmod I kongruence na $R(+,\cdot,-,0,1)$.

Tom že je $R/I(+,\cdot,-,I,1+I)$ okruh se snadno přímočaře ověří z definice a fakt, že je π_I homomorfismus plyne okamžitě z 9.1.

(2) Kerφ je jistě 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 $r\cdot k, k\cdot r \in \text{Ker}\varphi$. □

Právě zavedenému okruhu říkáme *faktorový okruh* (nebo krátce *faktorokruh*) okruhu R podle ideálu I . V následujícím tvrzení si uvědomíme vztah množiny ideálů faktorového a původního okruhu.

Poznámka 10.7. *Nechť $\mathcal{R} = R(+,\cdot,-,0,1)$ je okruh, I jeho ideál a $\pi_I : R \to R/I$ přirozená projekce. Označme $\mathcal{I}_I^R$ množinu všech ideálů okruhu $\mathcal{R}$ obsahujících ideál I a $\mathcal{I}_0^{R/I}$ množinu všech ideálů okruhu $R/I(+,\cdot,-,[0]_I,[1]_I)$. Pak jsou zobrazení*

$$J \to \pi(J) \quad \text{a} \quad \widetilde{J} \to \pi^{-1}(\widetilde{J})$$

vzájemně inverzní bijekce mezi množinami $\mathcal{I}_I^R$ a $\mathcal{I}_{[0]}^{R/I}$.

Důkaz. Protože je π grupový homomorfismus, jsou pro ideál J okruhu $\mathcal{R}$ a ideál $\widetilde{J}$ okruhu $\mathcal{R}/I$ obraz $\pi(J)$ i úplný vzor $\pi^{-1}(\widetilde{J})$ podgrupy, navíc platí, že $I \subseteq \pi^{-1}(\widetilde{J})$. Dále potřebujeme nahlédnout, že se jedná opravdu o ideály. Zvolíme-li $r \in R$ a $j \in J$, pak

$$\pi_I(r)\cdot\pi_I(j) = \pi_I(rj) \in \pi_I(J), \quad \pi_I(j)\cdot\pi_I(r) = \pi_I(jr) \in \pi_I(J)$$

a podobně pro pro $r \in R$ a $j \in \pi^{-1}(\widetilde{J})$

$$\pi_I(rj) = \pi_I(r)\cdot\pi_I(j) \in \widetilde{J}, \quad \pi_I(jr) = \pi_I(j)\cdot\pi_I(r) \in \widetilde{J},$$

tedy obě uvažovaná zobrazení jsou dobře definovaná zobrazení mezi množinami $\mathcal{I}_I^R$ a $\mathcal{I}_{[0]}^{R/I}$. Protože $\pi\pi^{-1}(\widetilde{J}) = \widetilde{J}$ a $\pi^{-1}\pi(J) = J$, jedná se vzájemně inverzní bijekce. □

Nyní zformulujeme důsledek předchozích tvrzení, který nám řekne, kdy je faktor komutativního okruhu těleso. Toto tvrzení bude hrát zásadní roli v konstrukci konečných těles, jíž se budeme zabývat v následující kapitole.

Definice. Řekneme, že ideál I komutativního okruhu $\mathcal{R} = R(+, \cdot, -, 0, 1)$ je *maximální*, pokud $I \neq R$ a pro každý ideál J, že $I \subseteq J$, platí buď $J = I$ nebo $J = R$.

Všimněme si, že v tělese je maximálním ideálem právě nulový ideál.

Věta 10.8. *Nechť $R(+, \cdot, -, 0, 1)$ je komutativní okruh a I jeho ideál. Potom je $R/I(+, \cdot, -, [0]_I, [1]_I)$ komutativní těleso právě tehdy, když I je maximální ideál.*

Důkaz. Využívejme značení Poznámky 10.7.

Podle Věty 10.5 je $R/I(+, \cdot, -, [0]_I, [1]_I)$ komutativní těleso právě tehdy, když $\mathcal{I}_0^{R/I}$ obsahuje pouze triviální ideály, což je podle Poznámky 10.7 ekvivalentní podmínce, že $\mathcal{I}_I^R$ obsahuje právě dva ideály, což právě znamená, že je I I je maximální ideál. □

11. Okruhy polynomů a konstrukce těles

V následující kapitole ukážeme dvě cesty, jak najít další přirozené (a občas i užitečné) příklady těles. Zatímco druhá z nich zobecňuje známou konstrukci zlomků, která z celých čísel vytváří těleso racionálních čísel (Věta 11.10), v první konstrukci využijeme faktorizace okruhů polynomů nad tělesy $\mathbb{Z}_p$, kde p je prvočíslo, abychom dostali libovolné konečné těleso (Věta 11.8). Nejprve ovšem zavedeme polynomy nad obecnými okruhy a uvědomíme si, že známý školský algoritmus dělení se zbytkem funguje v mnohem obecnější situaci než jsme zvyklí.

11.1. **Konečná tělesa.**

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

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

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

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 $\deg p$.

Poznámka 11.1. *Nechť $R(+, \cdot, -, 0, 1)$ je okruh a $p,\ q \in R[x]$.*

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

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

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

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

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

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

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

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

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

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

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

kde $\mathbf{1} = \sum_n \mathbf{1}_n x^n$, tedy $\mathbf{1}_0 = 1$ a $\mathbf{1}_n = 0$ pro všechna $n > 0$. Bezprostředně z konstrukce okruhu $R[x]$ vidíme, že zobrazení $\nu : R \to R[x]$ dané vztahem $\nu(r) = rx^0$ je prostý okruhový homomorfismus, proto díky 9.3(2) dostáváme izomorfismus okruhu $R(+, \cdot, -, 0, 1)$ s podokruhem $\nu(R) = \{sx^0 |\ s \in R\}$.

(2) Nerovnost $\deg p + q \leq \max(\deg p,\ \deg q)$ plyne z inkluze

$$\{n \mid p_n + q_n \neq 0\} \subseteq \{n \mid p_n \neq 0\} \cup \{n \mid q_n \neq 0\}.$$

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

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

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

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

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

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

Věta 11.2 (O dělení se zbytkem)**.** *Nechť $R(+, \cdot, -, 0, 1)$ je obor, $a,\ b \in R[x]$, kde $b = \sum b_n x^n$. Předpokládejme, že $m = \deg b \geq 0$ a b_m je invertibilní v R. Pak existují takové jednoznačně určené polynomy $q,\ r \in R[x]$, že $a = b \cdot q + r$ a $\deg r < \deg b$.*

Důkaz. Existenční část tvrzení dokážeme pomocí algoritmu:

`VSTUP:` $a,\ b \in R[x]$, `kde` $b_{\deg b}$ `invertibilní`

`VÝSTUP:` $q,\ r \in R[x]$, `pro které` $a = q \cdot b + r,\ \deg r < \deg b$

`0.` $m := \deg b;\ n := \deg a - m;$

`1. if` $n < 0$ `then return` $0, a$ `else` $r := a;$

`2. for` $i := n$ `downto` 0 `do` $\{q_i := r_{i+m} b_m^{-1}; r := r - q_i x^i b;\}$

`3. return` $\sum_i q_i x^i,\ r.$

Indukcí podle i ve for-cyklu snadno nahlédneme, že algoritmus pracuje správně.

Zbývá ukázat jednoznačnost. Předpokládejme, že $a = b \cdot q' + r'$ a $\deg r' < \deg b$. Potom $b \cdot (q - q') = r' - r$ a podle 11.1(3) a protože $\deg(r' - r) < \deg b$, dostáváme $r' - r = 0$, a proto $q - q' = 0$ □

Důsledek 11.3. *Nechť $T(+, \cdot, -, 0, 1)$ je komutativní těleso. Pak je každý ideál okruhu $T[x](+, \cdot, -, \mathbf{0}, \mathbf{1})$ hlavní.*

Důkaz. Vezměme libovolný nenulový ideál I a v ideálu I zvolme nenulový polynom p nejmenšího možného stupně. Zřejmě $pT[x] \subseteq I$. Nechť $i \in I$. Pak podle 11.2 existují takové polynomy $q, r \in T[x]$, že $i = p \cdot q + r$ a $\deg(r) < \deg(p)$. Protože $r = i - p \cdot q \in I$ a $\deg(p)$ byl minimální, je nutně $r = 0$ a $pT[x] = I$. □

Definice. Nechť $\mathcal{R} = R(+, \cdot, -, 0, 1)$ je komutativní okruh a $a, b \in R$. Řekneme, že *a dělí b*, $a|b$, existuje-li $c \in R$, pro které $a \cdot c = b$. O neinvertibilním nenulovém prvku $p \in R$ řekneme, že je *ireducibilní*, pokud pro každý rozklad $p = a \cdot b$ platí že je a nebo b invertibilní.

Příklad 11.4. (1) Prvočísla jsou právě ireducibilní prvky oboru celých čísel. Navíc je-li p prvočíslo a $n\mathbb{Z}$ ideál okruhu celých čísel, pro který $p\mathbb{Z} \subseteq n\mathbb{Z}$, pak $n|p$, tedy buď $n\mathbb{Z} = p\mathbb{Z}$ nebo $n\mathbb{Z} = \mathbb{Z}$, což znamená, že $p\mathbb{Z}$ je maximální ideál.

(2) Ireducibilní prvky v okruhu polynomů nad tělesem jsou právě ireducibilní polynomy.

Všimněme si, že přímo z definice dostáváme charakterizaci relace dělitelnosti pomocí inkluze hlavních ideálů:

Poznámka 11.5. *Nechť $R(+, \cdot, -, 0, 1)$ komutativní okruh a $a, b \in R$. Pak*

$$a/b \Leftrightarrow b \in aR \Leftrightarrow bR \subseteq aR.$$

Smyslem následujícího tvrzení je pozorování, že nám faktorizace okruhu polynomů nad tělesem podle ideálu generovaného ireducibilním polynomem dá těleso.

Poznámka 11.6. *Je-li $T(+, \cdot, -, 0, 1)$ komutativní těleso a I ideál okruhu polynomů $T[x](+, \cdot, -, 0, 1)$, pak je I maximální právě tehdy, když existuje ireducibilní polynom $f \in T[x]$ takový, že $I = fT[x]$*

Důkaz. Z 11.3 víme, že existuje $f \in T[x]$ takový, že $I = fT[x]$. Dále si stačí všimnout, že pro ideál $gT[x]$ máme $fT[x] \subsetneq gT[x] \subsetneq T[x] \Leftrightarrow g|f$ a současně $g \not| 1$ a $f \not| g$; pravá strana ekvivalence neříká nic jiného, než $g|f$ a $0 < \text{def } g < \deg f$, tj. f není ireducibilní. □

Nyní zkonstruujeme konečná (komutativní) tělesa, přičemž budeme následující výsledek brát jako fakt, který dokážeme až příští semestr.

Poznámka 11.7. *Pro každé prvočíslo p a $n \in \mathbb{N}$ existuje ireducibilní polynom $f \in \mathbb{Z}_p[x]$ stupně n. Navíc v $\mathbb{Z}_p[x]$ platí $f|(x^{p^n} - x)$.*

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

Věta 11.8. (1) *Je-li p prvočíslo a $n \in \mathbb{N}$, existuje komutativní těleso o p^n prvcích.*
(2) *Je-li $\mathbb{F}$ konečné těleso, pak $|\mathbb{F}| = p^n$ pro p prvočíslo a $n \in \mathbb{N}$.*
(3) *Libovolná dvě konečná komutativní tělesa o témže počtu prvků jsou izomorfní.*

Důkaz. (1) Díky 11.7 existuje ireducibilní polynom $u \in \mathbb{Z}_p[x]$ stupně n. Definujme $\mathbb{F}_{p^n} = \mathbb{Z}_p[x]/u\,\mathbb{Z}_p[x]$. Potom z Poznámky 11.6 a Věty 10.8 plyne, že $\mathbb{F}_{p^n}$ je komutativní těleso. Označíme-li $I = u\,\mathbb{Z}_p[x]$, v tomto tělese (pro $g, h \in \mathbb{Z}_p[x]$) platí $g + I = h + I$ právě tehdy, když u dělí $g - h$; mj. tedy $g + I = (g \bmod u) + I$. Jako zbytky po dělení u figurují právě všechny polynomy nad $\mathbb{Z}_p$ stupně menšího než n, těch je p^n, což je následně i počet prvků $\mathbb{F}_{p^n}$.

(2) Mějme konečné těleso $\mathbb{F}$. Uvažujme cyklickou podgrupu $\langle 1\rangle$ grupy $\mathbb{F}(+,-,0)$. Ta musí být konečná, a tedy $\mathbb{Z}_p(+) \cong \langle 1\rangle(+)$ pro nějaké $p \in \mathbb{N}$. Uvažujme dále izomorfismus, který posílá prvek $k \in \mathbb{Z}_p$ na prvek $\underbrace{1+1+\ldots+1}_{k\times}$ tělesa $\mathbb{F}$, a jak je v podobných případech zvykem, pro další úvahy ztotožníme prvky tělesa $\mathbb{F}$ tvaru $\underbrace{1+1+\ldots+1}_{k\times}$, kde $0 \le k < p$, a prvky množiny $\mathbb{Z}_p$. Z grupy $\mathbb{Z}_p$ tímto ztotožněním uděláme podgrupu grupy $\mathbb{F}(+,-,0)$. Jelikož z distributivity máme

$$(\underbrace{1+1+\ldots+1}_{k\times})(\underbrace{1+1+\ldots+1}_{m\times}) = \underbrace{1+1+\ldots+1}_{km\times} = \underbrace{1+1+\ldots+1}_{(km \bmod p)\times},$$

tvoří $\mathbb{Z}_p$ dokonce podokruh tělesa $\mathbb{F}$. Dále p musí být prvočíslo, jinak by existovaly $0 \neq k, m \in \mathbb{Z}_p$ 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 $\mathbb{Z}_p$, a položíme-li $n := \dim_{\mathbb{Z}_p} \mathbb{F}$, pak $|\mathbb{F}| = p^n$.

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

Nejprve nahlédneme, že každý prvek tělesa $\mathbb{F}$ je kořenem polynomu $x^{p^n} - x \in \mathbb{Z}_p[x]$. To pro 0 zřejmě platí a pro nenulové prvky to plyne aplikací Poznámky 7.4 na grupu $\mathbb{F}^*(.)$, která má $p^n - 1$ prvků. Z 11.7 navíc plyne, že ireducibilní polynom $u \in \mathbb{Z}_p[x]$ použitý ke konstrukci tělesa $\mathbb{F}_{p^n}$, dělí v $\mathbb{Z}_p[x]$ 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 $ug = x^{p^n} - x$. Dosadíme-li nyní libovolný prvek $a \in \mathbb{F}$, máme $u(a)g(a) = 0$, 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 u.

Pro toto a uvažujme dosazovací zobrazení $\Omega_a : \mathbb{Z}_p[x] \to \mathbb{F}$ definované vztahem $\Omega_a(h) = h(a)$. Snadno nahlédneme, že $\Omega_a(h+k) = \Omega_a(h) + \Omega_a(k)$, $\Omega_a(h \cdot k) = \Omega_a(h) \cdot \Omega_a(k)$ a $\Omega_a(1) = \Omega_a(1)$, což znamená, že jde o (takzvaný dosazovací) homomorfismus. Výše jsme dokázali, že $u\,\mathbb{Z}_p[x] \subseteq \mathrm{Ker}(\Omega_a)$, můžeme proto užít 9.3, která nám dá (jediný) okruhový homomorfismus $\psi : \mathbb{Z}_p[x]/u\,\mathbb{Z}_p[x] \to \mathbb{F}$, pro nějž $\Omega_a = \psi\pi_{u\,\mathbb{Z}_p[x]}$. Jelikož $\Omega_a(1) = 1 \neq 0$, je ψ nenulový homomorfismus. Víme, že $\mathrm{Ker}(\psi)$ musí být ideál tělesa $\mathbb{F}_{p^n}$, a tedy nutně $\mathrm{Ker}(\psi)$ je triviální (jednoprvkový) ideál (užíváme Větu 10.5). 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 $\mathbb{F}$. □

Příklad 11.9. (1) Postupem důkazu bodu (1) Věty 11.8 zkonstruujeme konečné těleso o $8 = 2^3$ prvcích. Zvolme ireducibilní polynom $f = x^3 + x + 1$ (rozložitelnost polynomu stupně 3 implikuje, že má kořen, což zde neplatí) a dostaneme těleso $\mathbb{F}_8 = \{a + bx + cx^2 + f\,\mathbb{Z}_2[x] \mid a, b, c \in \mathbb{Z}_2\} = \{a + b\alpha + c\alpha^2 |\ a, b, c \in \mathbb{Z}_2\}$, kde $\alpha := x + f\,\mathbb{Z}_2[x]$.

(2) Pokud bychom chtěli zkonstruovat těleso, které má právě 2^{13} prvků, potřebovali bychom najít nad tělesem $\mathbb{Z}_2$ ireducibilní polynom stupně 13. Poznámka 11.7 nám říká, že ho lze najít mezi děliteli polynomu $x^{2^{13}} - x$, navíc poznamenejme, že není příliš těžké ověřit silnější tvrzení, že ireducibilní polynom $g \in \mathbb{Z}_p[x]$ stupně k dělí polynom $x^{p^n} - x$, právě když k/n. Protože je 13 prvočíslo, obsahuje ireducibilní rozklad polynomu $x^{2^{13}} - x$ právě všechny ireducibilní polynomy stupně 13 a 1. Zřejmě právě polynomy x a $x+1$ jsou jediné dva ireducibilní polynomy stupně 1 nad $\mathbb{Z}_2$, proto snadnou úvahou o stupních zjistíme, že se polynom $\frac{x^{2^{13}} - x}{x(x+1)} = \sum_{i=0}^{2^{13}-2} x^i$ rozkládá právě na $\frac{2^{13}-2}{13} = 630$ ireducibilních polynomů stupně 13. Ireducibilní polynom stupně stupně 13 je tvaru $\sum_{i=0}^{13} a_i x^i$, kde $a_{13} = 1$ a dále $a_0 = 1$, neboť 0 není kořenem a $\sum_{i=0}^{13} a_i = 1$, neboť ani 1 není kořenem. To znamená, že při náhodné volbě máme 630 příznivých možností ze 2^{11}, tedy více než třicetiprocentní pravděpodobnost úspěchu. To, zda je náhodný polynom dělitel polynomu $x^{2^{13}} - x$ přitom můžeme otestovat (v tomto případě ještě) rychlým algoritmem dělení se zbytkem.

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 $i, j, k, -i, -j, -k$.

11.2. **Podílová tělesa.** Následující tvrzení zobecňuje dobře známou konstrukci zlomků pro všechny obory integrity. Jejím důsledkem je fakt, že každý obor integrity lze chápat jako podokruh nějakého tělesa (konkrétně svého podílového tělesa).

Uvažujme obor $R(+, \cdot, -, 0, 1)$, a definujme algebru $F(+, \cdot, -, \mathbf{0}, \mathbf{1})$, kde $F = R \times (R \setminus \{0\})$ s operacemi:

$$(a, b) \cdot (c, d) = (a \cdot c, b \cdot d), \quad (a, b) + (c, d) = (a \cdot d + b \cdot c, b \cdot d), \quad -(a, b) = (-a, b),$$

$\mathbf{0} = (0, 1)$ a $\mathbf{1} = (1, 1)$. Na množině F konečně definujme relaci $\sim$ předpisem $(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c$.

Věta 11.10. *Pro algebru $F(+, \cdot, -, \mathbf{0}, \mathbf{1})$ platí:*

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

Důkaz. Vezměme $(a, b), (c, d), (e, f) \in F$.

(1) Postupujeme zcela přímočaře podle definice.

$$(a, b) + ((c, d) + (e, f)) = (a, b) + ((cf + de, df)) = ((adf + b(cf + de), bdf)) =$$
$$= ((adf + bcf + bde, bdf)) = (((ad + bc)f + bde, bdf)) = ((a, b) + (c, d)) + (e, f),$$
$$(a, b) + (c, d) = (ad + bc, bd) = (cb + ad, bd) = (c, d) + (a, b).$$

Ověřili jsme, že je operace + asociativní a komutativní. Uvážíme-li, že $(a,b)+(0,1)=(a,b)$, máme dokázáno, že $F(+)$ je komutativní monoid. Totéž provedeme pro násobení:

$$(a,b)\cdot((c,d)\cdot(e,f))=(a,b)\cdot((ce,df))=(ace,bdf))=((a,b)\cdot(c,d))\cdot(e,f),$$

dále $(a,b)\cdot(c,d)=(c,d)\cdot(a,b)$ a $(a,b)\cdot(1,1)=(a,b)$, proto i $F(\cdot)$ je komutativní monoid.

(2) Předně uvažme, že je relace $\sim$ reflexivní a symetrická a předpokládejme, že $(a,b)\sim(c,d)$ a $(c,d)\sim(e,f)$, tedy $ad=bc$ a $cf=de$. Potom $adf=bcf=bde$, a proto $(af-be)d=0$. Jelikož $d\neq 0$, dostáváme z definice oboru integrity, že $af-be=0$, a tudíž $(a,b)\sim(e,f)$. Díky pozorování Příkladu 3.3 z minulého semestru zbývá ověřit slučitelnost $\sim$ s operacemi $+$, $\cdot$ a $-$. Předpokládejme, že $(a_i,b_i)\sim(c_i,d_i)$ tedy $a_id_i=c_ib_i$ pro $i=1,2$. Proto $(a_1b_2+b_1a_2)d_1d_2=a_1d_1\cdot b_2d_2+a_2d_2\cdot b_1d_1=c_1b_1\cdot b_2d_2+c_2b_2\cdot b_1d_1=(c_1d_2+d_1c_2)b_1b_2$, tedy $(a_1,b_1)+(a_2,b_2)\sim(c_1,d_1)+(c_2,d_2)$. Dále $a_1a_2d_1d_2=c_1c_2b_1b_2$, tudíž $(a_1,b_1)\cdot(a_2,b_2)\sim(c_1,d_1)\cdot(c_2,d_2)$ a konečně $(-a_1,b_1)\sim(-c_1,d_1)$ podle 5.2(2). Vztahy $(0,a)\sim\mathbf{0}$ a $(a,a)\sim\mathbf{1}$ plynou okamžitě z definice $\sim$.

(3) Díky (1), (2) a 3.10 už víme, že $F/\sim(+)$ a $F/\sim(\cdot)$ jsou komutativní monoidy. Zbývá tedy dokázat existenci opačných prvků monoidu $F/\sim(+)$ a distributivitu. Označme $\frac{a}{b}$ rozkladové třídy $[(a,b)]_\sim$. Všimněme si, že $\frac{ad}{bd}=\frac{ac}{bc}$ pro každé nenulové $b,d\in R$, protože $(ad,bd)\sim(ac,bc)$. Nyní snadno spočítáme, že

$$\frac{a}{b}+\frac{-a}{b}=\frac{a+(-a)}{bb}=\frac{0}{bb}=\mathbf{0},$$

$$\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}=\frac{acbf+bdae}{bdbf}=\frac{acf+ade}{bdf}=\frac{a}{b}\cdot\frac{cf+de}{df}=\frac{a}{b}\cdot(\frac{c}{d}+\frac{e}{f}).$$

Konečně, zvolíme-li $\frac{a}{b}\neq\mathbf{0}$, pak $(a,b)\not\sim(0,1)$, tedy $a\neq 0$, a proto $\frac{b}{a}\in F$ a $\frac{a}{b}\cdot\frac{b}{a}=\mathbf{1}$. Tím jsme dokázali, že každý nenulový prvek F je invertibilní, a proto je $F/\sim$ komutativní těleso.

(4) Okamžitě vidíme, že je $\frac{a}{1}\cdot\frac{b}{1}=\frac{a\cdot b}{1}$, $\frac{a}{1}+\frac{b}{1}=\frac{a+b}{1}$ a $\sigma(1)=\mathbf{1}$, proto je σ homomorfismus. Konečně, je-li $\sigma(a)=\sigma(b)$, pak $a=b$, tedy jde o prostý homomorfismus. □

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

Příklad 11.11. (1) Těleso racionálních čísel $\mathbb{Q}(+,\cdot,-,0,1)$ je podílovým tělesem oboru celých čísel $\mathbb{Z}(+,\cdot,-,0,1)$.

(2) Těleso racionálních lomených funkcí je podílovým tělesem oboru reálných polynomů $\mathbb{R}[x](+,\cdot,-,0,1)$.

(3) Podílové těleso oboru polynomů $\mathbb{Z}_2[x](+,\cdot,-,0,1)$ je příkladem nekonečného tělesa charakteristiky 2.

12. Svazy

Následující dvě kapitoly kurzu věnujeme algebraickému popisu uspořádaných množin. Nejprve si rozmyslíme, jak třídu takzvaných svazů uchopit jako algebry. Algebraický pohled nám umožní pracovat se všemi standardními univerzálně algebraickými pojmy.

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

Příklad 12.1. Připomeňme známé příklady uspořádání a svazů:

(1) Relace dělení / je uspořádání na množině všech přirozených čísel $\mathbb{N}$, navíc $\sup_{/}(n, m) = \mathrm{lcm}(n, m)$ a $\inf_{/}(a, b) = \mathrm{GCD}(n, m)$, proto je $(\mathbb{N}, /)$ svaz.

(2) Přirozené uspořádání $\leq$ indukuje na množině všech celých (reálných, racionálních) čísel $\mathbb{Z}$ ($\mathbb{R}$, $\mathbb{Q}$) 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 $(\mathcal{C}, \subset)$ tvoří úplný svaz, kde $\sup_{\subseteq}(\mathcal{B}) = \bigcap\{C \in \mathcal{C} | \bigcup \mathcal{B} \subseteq C\}$ a $\inf_{\subseteq}(\mathcal{B}) = \bigcap \mathcal{B}$ pro každé $\mathcal{B} \subseteq \mathcal{C}$.

$\subseteq$ je uspořádání a $\bigcap \mathcal{B}$ je zjevně infimem. Protože je množina $\mathcal{C}$ dle 8.6 uzavřená na průniky, vidíme, že $\bigcap\{X \in \mathcal{C} | \bigcup \mathcal{B} \subseteq X\}$ tvoří nejmenší prvek $\mathcal{C}$ 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 $\vee$ a $\wedge$ nazveme *spojení* a *průsek*.

Věta 12.2. (1) *Je-li $(M, \leq)$ svaz, pak pro všechna $a, b, c \in M$ platí:*

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

(S2) $a \vee a = a = a \wedge a$,

(S3) $a \vee (b \vee c) = (a \vee b) \vee c$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$,

(S4) $a \vee (b \wedge a) = a = a \wedge (b \vee a)$.

(2) *Nechť $M(\wedge, \vee)$ je algebra s dvěma binárními operacemi, které splňují podmínky* (S1) – (S4) *a definujme 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 $\sup_{\leq}(a,b) = a \vee b$. □

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

Příklad 12.3. U příkladů svazů uvedených v 12.1 máme tedy dva způsoby jak na svaz nahlížet:

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

Definice. Nechť $f : A \to B$ je zobrazení a $(A, \leq)$ a $(B, \leq)$ jsou svazy. Řekneme, že je f *homomorfismus* (*izomorfismus*) jde-li o 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 12.4. *Homomorfismus svazů je monotónní zobrazení.*

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

Věta 12.5. *Bijekce svazů f je izomorfismus, právě když jsou f i f^{-1} monotónní zobrazení.*

Důkaz. Díky 12.4 stačí dokázat zpětnou implikaci. Ověříme slučitelnost f například s $\vee$. Mějme $f : A \to B$ takovou bijekci svazů, že f i f^{-1} jsou monotónní, a zvolme $a, b \in A$. Protože $a, b \leq a \vee b$, je $f(a), f(b) \leq f(a \vee b)$, tudíž $f(a) \vee f(b) \leq f(a \vee b)$. Podobně $f(a), f(b) \leq f(a) \vee f(b)$, proto $a, b \leq f^{-1}(f(a) \vee f(b))$ a $a \vee b \leq f^{-1}(f(a) \vee f(b))$. Použijeme-li na poslední vztah znovu monotonii f, dostaneme $f(a \vee b) \leq f(a) \vee f(b)$. Ze slabé antisymetrie $\leq$, potom plyne, že $f(a \vee b) = f(a) \vee f(b)$. □

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

Je-li $(M, \leq)$ 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.

Příklad 12.6. Uvažujme svazy $(S_1, \leq)$ a $(S_2, \leq)$, kde $S_1 = \{0, 1, a, b\}$, $S_2 = \{\mathbf{0}, \mathbf{1}, \mathbf{A}, \mathbf{B}\}$ a daný relacemi:$0 <\cdot\, a <\cdot\, 1$, $0 <\cdot\, b <\cdot\, 1$ a $\mathbf{0} <\cdot\, \mathbf{A} <\cdot\, \mathbf{B} <\cdot\, \mathbf{1}$. Potom zobrazení $f(0) = \mathbf{0}$, $f(1) = \mathbf{1}$, $f(a) = \mathbf{A}$, $f(b) = \mathbf{B}$ je monotónní, ale není to homomorfismus svazů, protože $f(a \wedge b) = f(0) = \mathbf{0} \neq \mathbf{A} = f(a) \wedge f(b)$.

13. Kde se berou svazy?

V závěrečné kapitole se budeme věnovat izomorfnímu popisu dvou zajímavých tříd svazů: konečným Booleovým algebrám a svazu kongruencí grupy a okruhu. K tomu účelu zavedeme pojmy obecné Booleovy algebry jako distributivního svazu s komplementy a uzávěrového systému. Izomorfismu svazů tak využijeme pro důkaz tvrzení, že konečné Booleovy algebry nejsou (až na izomorfismus) ničím jiným než systémy všech podmnožin nějaké množiny, a pro lepší porozumění vztahu kongruencí a normálních podgrup pro grupy a vztahu kongruencí a ideálů pro okruhy.

13.1. **Booleovy algebry.**

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 13.1. *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 12.2 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 □

Příklad 13.2. (1) Svaz $\mathcal{P}(X)(\cap, \cup)$, kde $\mathcal{P}(X)$ je množina všech podmnožin nějaké 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 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 13.3. *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 $b_i = b_i \wedge 1 = b_i \wedge (a \vee b_j) = (b_i \wedge a) \vee (b_i \wedge b_j) = \mathbf{0} \vee (b_i \wedge b_j) = b_i \wedge b_j$, tedy $b_i \leq b_j$ pro všechna $i, j \in \{1, 2\}$, což znamená, že $b_1 = b_2$. □

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

Poznámka 13.5. *Nechť $S(\vee,\wedge,\mathbf{0},\mathbf{1},\ ')$ je Booleova algebra. Pak pro každé $a,b \in S$ platí:*

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

Důkaz. (1) a (2) plyne přímo z definice a 13.3 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 $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = \mathbf{1} \vee \mathbf{1} = \mathbf{1}$. □

Věta 13.6. *Buď $S(\vee,\wedge,\mathbf{0},\mathbf{1},\ ')$ konečná Booleova algebra a A buď množina všech atomů svazu S. Potom zobrazení $\phi : \mathcal{P}(A) \to S$ dané předpisem $\phi(B) = \sup B$ je izomorfismus Booleových algeber $S(\vee,\wedge,\mathbf{0},\mathbf{1},\ ')$ a $P(A)(\cup,\cap,\emptyset,A,\ ')$.*

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

Definujme nejprve zobrazení $\psi : S \to \mathcal{P}(A)$ předpisem $\psi(s) = \{a \in A |\ a \leq s\}$. Okamžitě vidíme, že zobrazení ϕ i ψ jsou monotónní vzhledem k inkluzi a $\phi(\emptyset) = \mathbf{0}$. Ukážeme-li navíc, že je ϕ bijekce slučitelná s průsekem a spojením, pak nutně $\phi(A) = \mathbf{1}$ a $\phi(B') = \phi(B)'$ pro každé $B \in \mathcal{P}(A)$. Podle 12.5 tedy zbývá ověřit, že $\phi \circ \psi = \mathrm{Id}_S$ i $\psi \circ \phi = \mathrm{Id}_{\mathcal{P}(A)}$, tedy že ϕ je bijekce a $\phi^{-1} = \psi$.

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

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

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

Z téhož důvodu neexistuje žádná patnáctiprvková Booleova algebra, protože podle Věty 13.6 musí být každá Booleova algebra izomorfní potenční Booleově algebře, tedy musí mít 2^n prvků, kde n je počet atomů.

13.2. **Svazy kongruencí.**

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

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

Všimněme si, že každý uzávěrový systém tvoří úplný svaz:

Poznámka 13.7. (1) *Je-li $\mathcal{C}$ uzávěrový systém, pak $(\mathcal{C}, \subseteq)$ tvoří úplný svaz, kde* $\sup_{\subseteq}(\mathcal{B}) = \bigcap\{C \in \mathcal{C} | \bigcup \mathcal{B} \subseteq C\}$ *a* $\inf_{\subseteq}(\mathcal{B}) = \bigcap \mathcal{B}$ *pro každé $\mathcal{B} \subseteq \mathcal{C}$.*

(2) *Systém všech podalgeber i systém všech kongruencí na algebře spolu s inkluzí je uzávěrový systém a tedy úplný svaz.*

Důkaz. (1) $\subseteq$ je uspořádání a $\bigcap \mathcal{B}$ je zjevně infimem. Protože je $\mathcal{C}$ uzavřené na průniky, je $\bigcap\{X \in \mathcal{C} | \bigcup \mathcal{B} \subseteq X\}$ nejmenším prvkem $\mathcal{C}$ obsahujícím všechna $B \in \mathcal{B}$, což je podle definice právě supremum vzhledem k inkluzi.

(2) Stejná úvaha jako v 12.1(4). □

Věta 13.8. (1) *Všechny normální podgrupy libovolné grupy $G(\cdot)$ tvoří spolu s inkluzí svaz a zobrazení $\rho \to [1]_\rho$ je izomorfismus svazu všech kongruencí na grupě $G(\cdot)$ svazu všech normálních podgrup.*

(2) *Všechny kongruence a všechny ideály okruhu $R(+, \cdot, -, 0, 1)$ tvoří spolu s inkluzí svazy a zobrazení $\rho \to [0]_\rho$ je izomorfismus svazu všech kongruencí na svazu všech ideálů okruhu R.*

Důkaz. Nejprve dokážeme technické lemma:

Lemma. Buď $\mathcal{C}$ uzávěrový systém obsažený v systému všech ekvivalencí na množině A. Nechť pro $\mathcal{N} \subseteq \mathcal{P}(A)$ a $e \in A$ platí:

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

Pak $\mathcal{N}$ je uzávěrový systém na A a tedy podle 13.7 svaz a zobrazení $\varphi : \mathcal{C} \to \mathcal{N}$ dané předpisem $\varphi(\rho) = [e]_\rho$ je izomorfismus svazů.

Důkaz lemmatu. Nejprve ukážeme, že je $\mathcal{N}$ uzávěrový systém. Protože $A \times A \in \mathcal{C}$, máme $A = [e]_{A\times A} \in \mathcal{N}$ díky (a). Vezmeme-li $N_i \in \mathcal{N}$, $i \in I$, pak podle (b) existuje pro každé $i \in I$ taková ekvivalence $\rho_i \in \mathcal{C}$, že $N_i = [e]_{\rho_i}$. Protože je $\mathcal{C}$ uzávěrový systém, tedy $\bigcap_{i\in I} \rho_i \in \mathcal{C}$, dostáváme $\bigcap_{i\in I} N_i = \bigcap_{i\in I} [e]_{\rho_i} = [e]_{\bigcap_{i\in I} \rho_i} \in \mathcal{N}$ opět díky (a).

Nyní stačí podle 12.5 ověřit, že je φ dobře definovaná bijekce a že φ i φ^{-1} jsou monotónní vzhledem k inkluzi. Korektnost definice přitom zaručuje podmínka (a), podmínka (b) říká, že je φ na $\mathcal{N}$, a z podmínky (c) plyne, že jde o prosté zobrazení. Konečně, je-li $\rho \subseteq \eta$, pak $[e]_\rho \subseteq [e]_\eta$ pro každou dvojici ekvivalencí ρ a η, což zaručuje monotónii φ, a monotónie φ^{-1} je přímo obsahem podmínky (c). □

(1) Označme symbolem $\mathcal{C}$ množinu všech kongruencí na $G(\cdot)$, tj. ekvivalencí slučitelných s operací $\cdot$ (viz 8.4(3)), symbolem $\mathcal{N}$ množinu všech normálních podgrup $G(\cdot)$ a symbolem e neutrální prvek $G(\cdot)$. Z 13.7 plyne, že je $\mathcal{C}$ uzávěrový systém a 4.8 zaručuje, že jsou splněny předpoklady (a), (b), (c) Lemmatu, odkud plyne závěr.

(2) Nejprve dokážeme, že ekvivalence ρ je kongruence na $R(+,\cdot,-,0,1)$, právě když $[0]_\rho$ je ideál a $\rho = \mathrm{Ker}[0]_\rho$. V 10.6(1) jsme dokázali zpětnou implikaci. Je-li naopak ρ je kongruence na okruhu R, pak jde také o kongruenci grupy $R(+)$, proto je $[0]_\rho$ podle 4.8 podgrupou $R(+)$ a $(a,b) \in \rho \Leftrightarrow a-b \in [0]_\rho$. Zbývá ověřit, že jde o ideál. Zvolme $i \in [0]_\rho$ a $r \in R$, tedy $(i,0) \in \rho$ a $(r,r) \in \rho$, proto $(ir,0) = (ir,0r) \in \rho$ a $(ri,0) = (ri,r0) \in \rho$, tedy $ir, ri \in I$.

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

Příklad 13.9. Podle předchozí věty a 7.2 tvoří svaz všech kongruencí na dvanáctiprvkové cyklické grupě právě šestiprvková množina kongruencí $\mathrm{rmod}\langle i\rangle$ pro $i \in \{0,1,2,3,4,6,\}$ s inkluzí a tento svaz je stejný jako svaz kongruencí na okruhu $\mathbb{Z}_{12}(+,\cdot,-,0,1)$.

14. Shrnutí

Na závěr kurzu si uvědomme jakými algebraickými prostředky disponujeme, jaké je jejich místo v kontextu matematiky a k jakým účelům se dají využít.

14.1. **Teorie čísel a okruhy.** Uvědomme si, že otázky teorie čísel lze formulovat právě jazykem teorie okruhů, tedy jazykem pracujícím se dvěma distributivitou svázanými asociativními binárními operacemi. Samotná teorie čísel fakticky pracuje s konkrétním okruhem celých čísel, ovšem mnohá její tvrzení lze vyslovit a dokázat v obecnějším kontextu teorie okruhů a naopak mnohé poznatky a postupy teorie okruhů poskytují užitečný aparát v teorii čísel. Klíčem k pochopení tohoto vztahu je vyjádření dělitelnosti (tedy základnímu výrazovému prostředku teorie čísel) pomocí inkluze ideálů, jež je formulováno ($a/b \Leftrightarrow bR \subseteq aR$) v elementárním pozorování 11.5.

Co důležitého se nám podařilo nahlédnout:

- 2.2 Základní věta aritmetiky. Obdobu tohoto tvrzení lze dokázat i pro další třídy okruhů (například pro okruhy jednoho či více proměnných nad tělesem).
- 2.7 Čínská věta o zbytcích pro celá čísla. I toto tvrzení lze zobecnit a využít například pro rychlé násobení polynomů.
- 10.8 Tvrzení, že tělesem jsou právě faktory komutativního okruhu podle maximálního ideálu, spolu
- 11.2 s algoritmickou větou o dělení se zbytkem, nám umožňuje
- 11.8 konstruovat konečná tělesa (ta jsou posléze základním stavebním kamenem algebraické teorie kódů).

14.2. **Grupy.** Základnějším, ačkoli možná méně přirozeným objektem našeho zkoumání byly jednotlivé binární operace. Omezíme-li se na množiny s jedinou asociativní binární operací, pak neutrální prvek ani invertibilní prvky obecně nemusí být k dispozici, ovšem existujíc-li, jsou určeny jednoznačně. Navíc v každém monoidu, jak množinu s asociativní binární operací a neutrálním prvkem nazýváme, vždy najdeme kanonickou grupu invertibilních prvků (3.6).

Co důležitého se nám podařilo nahlédnout:

3.9 Vzorec pro výpočet Eulerovy funkce, tedy počtu invertibilních prvků monoidu $\mathbb{Z}_n(\cdot)$ získaný pomocí Čínské věty o zbytcích je užitečný v kontextu teorie čísel.

4.5 Lagrangeova věta popisující vztah počtu prvků grupy a její podgrupy je důsledek zkoumání vlastností kongruencí rmod a lmod, jejichž dalšími důsledky jsou

4.8 popis kongruencí grupy pomocí pojmu normální podgrupa a posléze

13.8 jednoznačná korespondence svazů normálních podgrup (resp. ideálů) a kongruencí grup (resp. okruhů).

6.4 Snadný popis struktury cyklických grup umožňuje

7.2 zesílit tvrzení Lagrangeovy věty pro cyklické grupy a formulovat

7.5 Eulerovu větu, která je základním nástrojem několika kryptografických aplikací (protokoly RSA, Diffie–Hellman, ElGamal).

14.3. **Univerzální algebra.** Mnoho základních úvah o konkrétních algebraických objektech, jaké tvoří například grupy nebo okruhu, má stejnou podstatu, a proto je možné učinit je velmi obecně pro abstraktní algebry opatřené systémem blíže nespecifikovaných operací. Velmi užitečný prostředek, jak uspořádání inkluzí na systémech podalgeber a kongruencí algeber, což jsou základní nástroje zkoumání obecných algeber, porozumět, je pojem svazu, který představuje algebraicky uchopené uspořádané množiny.

Co důležitého se nám podařilo nahlédnout:

9.1 Jako zobecnění pozorování 5.3 pro grupy jsme si uvědomili, že faktorizovat algebry lze právě podle kongruencí a že přirozená projekce na faktorovou algebru je právě homomorfismus.

9.3 1.věta o izomorfismu jako důsledek Věty o homomorfismu, kterou jsme nejprve dokázali v jednodušším případě grup 5.5, umožňuje překládat problémy týkající se faktorových grup do podgrup známých grup,

9.4 zatímco 2.věta o izomorfismu ukazuje, že faktor faktorové algebry lze vždy izomorfně přeložit na faktor původní algebry.

12.5 Tvrzení, že izomorfismy svazů lze popsat jazykem monotónie, využívá důkaz

13.6 izomorfního popisu konečných Booleových algeber jako potenční Booleovy algebry.