ALGEBRA I PRO INFORMATIKY

Obsah

1. Předmět(y) zkoumání

Pod názvem algebra se po dlouhou 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* úpravu odpovídající přičtení výrazu k oběma 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 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*

Date: 8. ledna 2019.

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.

V souladu se značením zavedeným na kurzu lineární algebry položme $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ pro nějaké celé číslo $n > 1$.

Poznámka 1.2. *Pro každé a celé a b kladné existují jednoznačně určená čísla $q \in \mathbb{Z}$ a $r \in \mathbb{Z}_b$, pro která $a = qb + r$.*

Důkaz. Pro $a \geq 0$ existenci $q \in \mathbb{Z}$ a $r \in \mathbb{Z}_b$ dokazuje školský algoritmus dělení se zbytkem (opírající se o fakt, že každé celé číslo lze zapsat v dekadickém zápisu). Pro $a < 0$ najdeme algoritmem $p \in \mathbb{Z}$ a $z \in \mathbb{Z}_b$, pro která $-a = pb + z$ $-a$ a b. Hledaným podílem je $-q$ a zbytkem 0, pokud $z = 0$, nebo podíl je $-q - 1$ a zbytek $b - r$, pokud $z > 0$.

Nechť $a = qb + r = q'b + r'$ pro $q, q' \in \mathbb{Z}$ a $r, r' \in \mathbb{Z}_b$ a předpokládejme, že například $r \geq r'$. Pak $0 \leq r - r' = (q' - q)b < b$, proto $q = q'$ a tudíž $r = r'$, čímž jsme dokázali jednoznačnost volby $q \in \mathbb{Z}$ a $r \in \mathbb{Z}_b$. □

Nadále budeme používat značení $(a)\mathrm{div}\ b$ pro celočíselný podíl a $(a)\mathrm{mod}\ b$ pro zbytek, tj. pro hodnoty jednoznačně zajištěné předchozí poznámkou.

Příklad 1.3. Zaveďme na množině $\mathbb{Z}_n$ operace $+$ a $\cdot$ předpisem $a+b = (a+b)\mathrm{mod}\ n$ a $a \cdot b = (a \cdot b)\mathrm{mod}\ n$, kde mod n znamená zbytek po celočíselném dělení hodnotou n a v závorce uvažujeme vždy obvyklé sčítání a násobení celých čísel. Konečně definujme zobrazení $F_n : \mathbb{Z} \to \mathbb{Z}_n$ předpisem $F_n(k) = (k)\mathrm{mod}\ n$. 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 1.3 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 1.4. (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.

2. Základy elementární teorie čísel

V této kapitole připomeneme a korektně dokážeme několik jednoduchých poznatků z teorie čísel, konkrétně Eukleidův algoritmus, Základní větu aritmetiky a Čínskou větu o zbytcích. Poslouží nám nejen jako motivace zkoumání obecných algebraických vlastností (slučitelnost ekvivalence s operací), nýbrž i jako užitečný nástroj, jenž budeme potřebovat v následujících kapitolách.

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 *nejmenší společný násobek* 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 pro $a, b \in \mathbb{N}$ najde největší společný dělitel a pro $x, y \in \mathbb{Z}$ 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 vztahů $a_{i-1} = a_{i+1} + q_i \cdot a_i$ a $a_{i+1} = a_{i-1} - q_i \cdot a_i$:

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

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 na výstupu Eukleidova algoritmu se nazývají *Bezoutovy koeficienty* a že není těžké dokázat omezení na jejich velikost $|x| \leq \frac{b}{2}$ a $|y| \leq \frac{b}{2}$, pokud $a, b > 1$.

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) Předpokládejme, že $p/a \cdot b$ a p nedělí a. Protože p má pouze dělitele ± 1 a $\pm p$, vidíme, že $\mathrm{GCD}(p, a) = 1$, a proto podle 2.1 existují taková celá x a y, že $1 = a \cdot x + p \cdot y$. Přenásobením této rovnosti hodnotou b dostaneme $b = abx + pby$, a protože p dělí oba sčítance vpravo, platí také, že p/b.

(2) Dokážeme indukcí podle k. Pro $k = 1$ je tvrzení triviální. Předpokládáme-li, že $p/a_1 a_2 \ldots a_k = a_1 \cdot (a_2 \ldots a_k)$, pak podle (1) buď p/a_1 a jsme hotovi nebo $p/a_2 a_3 \ldots a_k$ a závěr plyne z indukčního předpokladu.

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 každá přirozená a, b existuje 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 jsou stejné. □

Nyní si všimneme, že počítání v množině $\mathbb{Z}_n$ s operacemi modulo n lze „algebraicky"přesně reprezentovat pomocí počítání v menších množinách $\mathbb{Z}_{n_i}$, což je pozorování významné pro výpočty pracující s velkými celými čísly.

Nejprve zavedeme součinové operace. Pro kladná celá čísla $n_1, \ldots, n_k$, definujme na kartézském součinu $\prod_{i=1}^k \mathbb{Z}_{n_i}$ po složkách (součinové) operace $+$, $-$ a $\cdot$:

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

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

kde odčítání ve složkách definujeme rovněž modulo n_i.

Příklad 2.4. Uvažujme kladná celá čísla $n_1, \ldots, n_k$, položme $n = n_1 \cdot \cdots \cdot n_k$ a definujme zobrazení

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

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

Ve výše zavedené notaci vyslovíme klasické tvrzení:

Věta 2.5 (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 2.4 slučitelné s operacemi $+$ a $\cdot$. Navíc H je bijekce, právě když jsou čísla $n_1, n_2, \ldots, n_k$ po dvou nesoudělná.*

Důkaz. V Příkladu 2.4 jsme si uvědomili, že je f zobrazení slučitelné s oběma operacemi. Zbývá dokázat ekvivalenci.

Nejprve dokážeme zpětnou implikaci. Nechť jsou čísla $n_1, n_2, \ldots, n_k$ po dvou nesoudělná. Ukážeme, že je H bijekce. 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 není konstruktivní, tedy nám neposkytuje algoritmus k nalezení vzoru nějakého prvku v zobrazení H. Zavedeme proto relaci kongruence, která nám spolu Eukleidovým algoritmem umožní efektivně počítat vzory zobrazení H.

Relací na množině A rozumíme libovolnou podmnožinu ρ množiny $A \times A$ a označme $\equiv \pmod n$ relaci *kongruence* na množině celých čísel $\mathbb{Z}$ danou předpisem $a \equiv b \pmod n \leftrightarrow n / (a - b)$.

Dále připomeňme, že obecná relace ρ je

- *reflexivní*, jestliže $(a, a) \in \rho$ pro každé $a \in A$,

- *symetrická*, platí-li pro každé $a, b \in A$ implikace $(a, b) \in \rho \Rightarrow (b, a) \in \rho$,
- *tranzitivní*, platí-li pro každé $a, b, c \in A$ implikace $(a, b), (b, c) \in \rho \Rightarrow (a, c) \in \rho$,
- *ekvivalence*, je-li reflexivní, symetrická a tranzitivní relace.

Připomeňme, že na každé množině A máme k dispozici dvě tzv. *triviální* ekvivalence $\mathrm{id} = \{(a, a) \mid a \in A\}$, $A \times A$ je tzv. *triviální*, navíc zobrazení $f : A \to B$ určuje ekvivalenci $\ker f = \{(x, y) \in A \times A |\ f(x) = f(y)\}$ (tzv. *jádro zobrazení*).

Dříve než začneme používat termín kongruence v mnohem obecnějším významu, všimněme si některých jejich (zjevně algebraických) vlastností:

Poznámka 2.6. *Nechť $k, n \in \mathbb{N}$ a $n > 1$. Pak je $\equiv \pmod n$ ekvivalence na $\mathbb{Z}$ a pro každé $a, b, c, d \in \mathbb{Z}$ 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. $\equiv \pmod n$ tvoří ekvivalenci například proto, že jde o ekvivalenci $\ker F_n$ pro F_n z 1.3.

(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 $n/(a - b)$ díky Větě 2.2. □

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

Příklad 2.7. 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 2.6 budeme kongruenci upravovat ekvivalentními úpravami:

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

Poznamenejme, že jsme v posledním kroku využili toho, že umíme (obecně díky Eukleidovu algoritmu) najít „inverz modulo 7"k číslu 5, jímž je 3). Hledaným řešením je tedy $x = 5 \cdot 3 + 2 = 17$.

3. Asociativní binární operace

Zkusíme se nyní oprostit od konkrétní algebraické struktury a uvážíme sice obecnou avšak velmi jednoduchou situaci množiny opatřené asociativní binární operací. Hlavním výsledkem této kapitoly bude kromě příkladů řady struktur, které takovou podmínku splňují, především pozorování, že množina s asociativní operací je jistým způsobem velmi blízko mnohem silnějšímu pojmu grupa (Poznámka 3.4), který jako jeden ze základních pojmů moderní algebry také zavedeme.

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

Všimněme si, že v jedné množině nemohou být pro stejnou operaci dva různé neutrální prvky:

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

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

Než se omezíme na zkoumání asociativních operací, učiníme zcela obecné pozorování o neutrálních prvcích.

Definice. Nechť $\cdot$ je binární operace na množině S a e je její neutrální prvek. Řekneme, že prvek $s \in S$ je *invertibilní*, jestliže existuje takový prvek $s^{-1} \in S$, pro který $s^{-1} \cdot s = s \cdot s^{-1} = e$. Prvek s^{-1} nazveme *inverzním prvkem* k prvku s.

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*, tj. pro všechna $x, y, z \in G$ platí rovnost $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- *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*, tj. pro všechna $x, y \in G$ platí rovnost $x \cdot y = y \cdot x$.

V Příkladu 1.1 jsme připomněli asociativní a komutativní operace $+$ a $\cdot$ na množině celých čísel (a v Příkladech 1.3 a 2.4 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 3.2. Nechť $n > 1$ je přirozené číslo, X neprázdná množina.

(1) Definujeme na X binární operaci $*$ předpisem $x * y = x$, je operace $*$ asociativní, tedy $X(*)$ je pologrupa. Je-li X aspoň dvouprvková, pak X neobsahuje žádný neutrální prvek, tudíž nejde o monoid, přestože každý prvek X splňuje první z rovností, kterou je neutrální prvek definován. V definici neutrálního prvku se tedy nemůžeme omezit jen na jednu ze dvou rovností.

(2) Nechť $M(X)$ je množina všech slov, tj. všech konečných posloupností písmen z množiny X, uvažujme 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 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.

(3) Označme $T(X)$ množinu všech zobrazení množiny X do sebe. Potom $T(X)(\circ)$ tvoří (s operací skládání $\circ$) (tzv. *transformační*) monoid, kde identické zobrazení Id představuje neutrální prvek.

Uvažíme-li v transformačním monoidu $T(\mathbb{Z})$ transformace α, β dané předpisy $\alpha(k) = 2k$ a $\beta(k) = [\frac{k}{2}]$, pak platí, že $\beta\alpha = \mathrm{Id}$ a $\alpha\beta \neq \mathrm{Id}$. Prvky α a β tedy splňují právě jednu z definitorických rovností invertibilního prvku, ačkoli se zjevně o invertibilní prvky nejedná. Snadno nahlédneme, že invertibilní transformace jsou právě bijekce.

(4) Čtvercové matice $M_n(T)$ nad tělesem T stupně n spolu s násobením tvoří monoid $M_n(T)(\cdot)$ s neutrálním prvkem tvořeným jednotkovou maticí.

(5) $\mathbb{Z}_n(\cdot)$ je konečný komutativní monoid s neutrálním prvkem 1.

Do konce této kapitoly budeme nadále označovat neutrální prvek obecné binární operace $\cdot$ symbolem e. 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).

Následující dvě tvrzení známe z kontextu počítání se čtvercovými maticemi.

Poznámka 3.3. *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. □

Nyní víme, že je inverz k invertibilnímu prvku a v monoidu určen jednoznačně, budeme ho tedy značit a^{-1}. Množinu všech invertibilních prvků monoidu $S(\cdot)$ označíme S^*.

Poznámka 3.4. *Nechť $S(\cdot)$ je monoid. Jestliže $s, t \in S^*$, pak $s \cdot t$ a s^{-1} jsou také invertibilní prvky S a platí, že $(s \cdot t)^{-1} = t^{-1} \cdot s^{-1}$ a $(s^{-1})^{-1} = s$. Označíme-li $\cdot_{S^*}$ restrikci $\cdot|_{S^* \times S^*}$ operace $\cdot$ na množinu $S^* \times S^*$, pak $S^*(\cdot_{S^*})$ je grupa.*

Důkaz. Protože $s \cdot s^{-1} = s^{-1} \cdot s = e$, je zřejmě s^{-1} invertibilní a díky 3.3 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

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

Dokázali jsme, že je množina S^* uzavřená na operaci $\cdot$ i na inverzní prvky, protože $e \cdot e = e$, vidíme, že $e \in S^*$, tedy $S^*(\cdot)$ je grupa. □

Grupu invertibilních prvků monoidu $S(\cdot)$ z Poznámky 3.4 budeme značit $S^*(\cdot)$.

Podívejme se na grupy invertibilních prvků monoidů z Příkladu 3.2:

Příklad 3.5. Nechť $n > 1$ je přirozené číslo a X neprázdná množina a T těleso.

(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). Poznamenejme, že grupa permutací na množině $\{1, \ldots, n\}$ se obvykle značí $S_n(\circ)$.

(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 $\mathbb{Z}_n^*(\cdot) = \{a \in \mathbb{Z}_n \mid \text{GCD}(a,n) = 1\}$. 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 $\text{GCD}(a,n) = 1$. Nechť naopak $\text{GCD}(a,n) = 1$, potom díky Euklidovu algoritmu existují $x \in \mathbb{Z}$ a $y \in \mathbb{Z}$, pro které $ax + ny = 1$, proto $a^{-1} = x \text{mod } n$. To znamená, že $a \in \mathbb{Z}_n^*$.

4. Grupy, podgrupy a homomorfismy

Nyní zaměříme svou pozornost na obecné grupy. Nejprve učiníme soubor obecných pozorování o jejich algebraicky významných podmnožinách, kterým budeme říkat podgrupy a algebraicky významných zobrazeních mezi grupami, jež budeme nazývat homomorfismy. Poté si prohlédneme ekvivalence na obecných grupách, které zcela přímočaře zobecňují pojem kongruence na celých číslech. Jako důsledek souboru elementárních technických pozorování o těchto ekvivalencích dostaneme pro úvahy o podgrupách velmi užitečnou Lagrangeovu větu, která svazuje dělitelností velikost grupy a její podgrupy.

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 $h \in H$. Je-li H podgrupa $G(\cdot)$, definujme na G relace rmod H a lmod H:

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

Protože podle 3.4 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.*
(5) rmod H *i* lmod H *jsou ekvivalence na G,*
(6) rmod $H =$ lmod H, *právě když je H normální podgrupa $G(\cdot)$,*
(7) *je-li H normální, pak je* rmod H *slučitelná s operací $\cdot$.*

Důkaz. (1) Plyne okamžitě z definice podgrupy a vlastností operace $\cdot$ na G (srovnej s důkazem 3.4).

(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 $g \cdot h \cdot g^{-1} = g \cdot g^{-1} \cdot h = h \in H$.

(5) Dokážeme jen, že je rmod H ekvivalence, 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 3.3 a 3.4), 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.

(6) 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.

(7) Zvolme $(a_0, b_0), (a_1, b_1) \in \text{rmod } H$, 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 ekvivalence rmod H s s operací $\cdot$. □

Vedle obecných příkladů největší a nejmenší podgrupy nejprve nahlédneme, jak vypadají všechny podgrupy grupy celých čísel.

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

(2) Uvažujeme-li komutativní grupu celých čísel $\mathbb{Z}(+)$ (s neutrálním prvkem 0 a inverzními prvky značenými standardně symbolem $-$), potom množiny tvaru $n\mathbb{Z} = \{n \cdot z |\ z \in \mathbb{Z}\}$ 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 $2n = n + n \in P$, $3n \in P$, ..., $kn \in P$, ..., 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 $n\mathbb{Z} = P$.

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 $\text{Ker}\varphi = \{g \in G |\ \varphi(g) = e\}$ 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 $\varphi^{-1}(\{e\}) = \mathrm{Ker}\varphi$ a že $\varphi(\mathrm{Ker}\varphi) = \{e\}$.

Poznámka 4.3. *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 $\ker\varphi = \mathrm{rmod}\ \mathrm{Ker}\varphi = \mathrm{lmod}\ \mathrm{Ker}\varphi$,*
(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

$$\varphi(\varphi^{-1}(c) \cdot \varphi^{-1}(d)) = c \cdot d, \quad \text{proto} \quad \varphi^{-1}(c) \cdot \varphi^{-1}(d) = \varphi^{-1}(c \cdot d).$$

(4) Nejprve ukážeme, že je $\psi(H)$ podgrupa $G_3(\cdot)$. Podle (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 (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 (4). 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 $\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a) \cdot \varphi(b)^{-1} = e \Leftrightarrow \varphi(a \cdot b^{-1}) = e \Leftrightarrow a \cdot b^{-1} \in \mathrm{Ker}\varphi$.

(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 (5). □

Příklad 4.4. (1) Identita na libovolné grupě $G(\cdot)$ a zobrazení, které jakémukoli prvku grupy přiřadí neutrální prvek jiné grupy, představují triviální příklady homomorfismů.

(2) Je-li $\varphi : U \to V$ lineární zobrazení dvou vektorových prostorů nad týmž tělesem se sčítáním vektorů označeným symbolem $+$, pak je φ homomorfismus aditivních grup $U(+)$ a $V(+)$.

(3) V rámci kurzu lineární algebry bylo dokázáno, že znaménko součinu permutací je rovno součinu jejich znamének, tedy, že $\operatorname{sgn} : S_n \to \{1, -1\}$ je homomorfismus grupy permutací $S_n(\circ)$ do dvouprvkové grupy $\{1, -1\}(\cdot)$. Podle 4.3(5) je $\operatorname{Ker}\ \operatorname{sgn} = A_n$ je normální podgrupa grupy $S_n(\circ)$. 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 $K = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$). Všimneme si, že například podgrupy $T = \{\mathrm{Id}, (12)\}$ grupy S_3 není normální ($(13) \circ (12) \circ (13)^{-1} = (23) \notin T$).

(4) V lineární algebře se dále dokazuje, že determinant det je homomorfismus z grupy regulárních matice $n \times n$ nad tělesem T do multiplikativní grupy tělesa $T \setminus \{0\}(\cdot)$, snadno nahlédneme, že i druhá mocnina determinantu $\det^2$ je homomorfismus stejných grup, tedy $\operatorname{Ker}\ \det = \{\mathbf{A} \in GL_n(T) \mid \det(\mathbf{A}) = 1\}$ a $\operatorname{Ker}\ \det^2 = \{\mathbf{A} \in GL_n(T) \mid \det(\mathbf{A}) = \pm 1\}$ jsou díky 4.3(5) normální podgrupy grupy $GL_n(T)(\cdot)$.

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 $H \cdot K$.

Poznámka 4.5. *Nechť $G(\cdot)$ je grupa a H její podgrupa. Potom platí:*

(1) $(a, b) \in \operatorname{rmod} H \Leftrightarrow (a^{-1}, b^{-1}) \in \operatorname{lmod} H$ *pro každé* $a, b \in G$,
(2) $|G/\operatorname{rmod} H| = |G/\operatorname{lmod} H|$,
(3) $[a]_{\operatorname{rmod} H} = Ha$ *a* $[a]_{\operatorname{lmod} H} = aH$ *pro každé* $a \in G$,
(4) $|[a]_{\operatorname{rmod} H}| = |[a]_{\operatorname{lmod} H}| = |H|$ *pro každé* $a \in G$.

Důkaz. (1) Díky 3.4 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.

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

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

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

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

(4) 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 (3). □

Definice. Buď H podgrupa grupy $G(\cdot)$. Potom číslu $[G : H] = |G/\operatorname{rmod} H|$ ($= |G/\operatorname{lmod} H|$ podle 4.5) budeme říkat *index podgrupy* H v grupě G a velikosti $|G|$ množiny G budeme říkat *řád grupy* G.

Věta 4.6 (Lagrange)**.** *Je-li H podgrupa grupy $G(\cdot)$, pak $|G| = [G : H] \cdot |H|$.*

Důkaz. Podle 4.1(5) je rmod H ekvivalence, proto $G = \dot{\bigcup}_{A\in G/\mathrm{rmod}\ H} A$, kde sjednocujeme disjunktní množiny. Využijeme-li dále poznatek 4.5(4), který říká, že všechny ekvivalenční třídy mají počet prvků stejný jako množina H, pak dostáváme

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

□

Důsledek 4.7. *Je-li $G(\cdot)$ konečná grupa, potom řád každé její podgrupy dělí řád grupy G.*

Příklad 4.8. 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 $H \cap K = \{1\}$.

5. Klasifikace cyklických grup

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 5.1. (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 $(a\cdot x)\mathrm{mod}\ n = 1$, 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 $n < 0$.

Poznamenejme, že pro „aditivně"zapsané grupy $A(+)$ označujeme neutrální prvek 0. Proto pro $a \in G$ značíme $-a$ opačný prvek a dále $0 \cdot a = 0$, $n \cdot a = (n-1) \cdot a + a$ pro $n > 0$ a $n \cdot a = |n| \cdot (-a)$ pro $n < 0$.

Poznámka 5.2. *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 5.3. *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 $(a^n)^m = a^{nm}$.*

Pro práci s jednotlivými prvky grupy je užitečné zavést následující terminologii.

Definice. *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 $g^n = 1$.

Z Důsledky 4.7 okamžitě dostáváme pozorování, že v konečné grupě řád prvku dělí řád grupy. Následující popis řádu prvku využijeme v následující klasifikaci obecných cyklických grup.

Poznámka 5.4. *Řád prvku g grupy $G(\cdot)$ je nejmenší kladné číslo k, pro něž $g^k = e$ nebo ∞ v případě, že takové k neexistuje. Navíc, je-li řád g konečný, pak dělí každý exponent g.*

Důkaz. Nechť existuje kladné číslo k, pro něž $g^k = e$. Označíme-li $q := (n)\mathrm{div}\ k$ a $r := (n)\mathrm{div}\ k$ pro libovolné celé n, pak z 5.2 a 5.3 dostáváme

$$g^n = g^{qk+r} = (g^k)^q \cdot g^r = e^q \cdot g^r = g^r,$$

a proto $\langle g \rangle = \{g^i |\ i \in \mathbb{Z}_k\}$. Zvolíme-li k minimální možné, pak pro $0 \leq 0i < j < k$ platí, že $g^i \neq g^j$, neboť $g^{j-i} \neq e$. To znamená, že $|\langle g \rangle| = k$ a nejmenší kladný exponent je dělitelem ostatních exponentů.

Pokud neexistuje žádný kladný exponent, pak pro každou dvojici $i < j$ ze stejného důvodu platí, že $g^i \neq g^j$, tudíž je řád prvku g nekonečný. □

Věta 5.5. *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 $\langle g \rangle = G$. Je-li řád $|G| = |\langle g \rangle|$ nekonečný, definujme zobrazení $\phi : \mathbb{Z} \to G$ předpisem $\phi(j) = g^j$. Potom jde podle 5.2 o homomorfismus na celé G, pro který $\mathrm{Ker}\phi = \{0\}$ díky Poznámce 5.4 a tudíž je podle Poznámky 4.3(6) ϕ prostý.

Nechť $n = |G| = |\langle g\rangle|$ je konečný řád. Pak je zobrazení $\phi : \mathbb{Z}_n \to G$ dané předpisem $\phi(j) = g^j$ bijekce a platí, že

$$\phi((x+y)\text{mod } n) = g^{(x+y)\text{mod } n} = g^{(x+y)\text{mod } n} \cdot g^{n(x+y)\text{div } n} = g^x \cdot g^y = \phi(x) \cdot \phi(y),$$

tedy jde o homomorfismus. □

Předchozí kritérium nám usnadní důkaz následující vlastnosti cyklických grup.

Důsledek 5.6. *Každá podgrupa cyklické grupy je opět cyklická.*

Důkaz. Díky 5.5 stačí tvrzení o podgrupách dokázat pro grupy $\mathbb{Z}(+)$ a $\mathbb{Z}_n(+)$. Nejprve ho dokažme pro grupu $\mathbb{Z}(+)$. V 4.2(2) 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 $F_n : \mathbb{Z} \to \mathbb{Z}_n$ z 1.1. Zvolíme-li podgrupu H grupy $\mathbf{Z}_n(+)$, pak $F_n^{-1}(H)$ je podle předchozí úvahy a 4.3(5) cyklická podgrupa $\mathbb{Z}$, tedy $H = F_n(F_n^{-1}(H))$ je cyklická podgrupa $\mathbb{Z}_n(+)$. □

Na závěr si všimněme, že pro každé přirozené k značíme $k\,\mathbb{Z} = \{kz|\ z \in \mathbb{Z}\}$, a proto jde podle Poznámky 5.2 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 $k\,\mathbb{Z}_n = \langle k\rangle = \{k \cdot z|\ z \in \mathbb{Z}_n\}$.

6. Cyklické grupy v kryptografii

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 6.7) a protokolů, které se opírají o obtížnost diskrétního logaritmu (Příkladu 6.9) dostaneme, učiníme pozorování o struktuře uspořádané množiny podgrup konečné cyklické grupy (Poznámka 6.1), počtu generátorů cyklické grupy pomocí Eulerovy funkce (Věta 6.2) a o řádu prvků obecné grupy, které je známo pod názvem Eulerova věta (Věta 6.5).

Poznámka 6.1. *Nechť k, n jsou taková přirozená čísla, že $k > 1$ a k/n. Pak $\langle \frac{n}{k}\rangle$ je jediná podgrupa grupy $\mathbb{Z}_n(+)$ řádu k a pro každé $a \in \mathbb{Z}_n \setminus\{0\}$ platí, že $\langle a\rangle = \langle \frac{n}{k}\rangle$, právě když $\frac{n}{k} = \text{GCD}(a, n)$.*

Důkaz. Nejprve zvolme libovolný dělitel d čísla n menší než n. Pak snadno nahlédneme, že $\langle d\rangle = \{0, d, 2d, \ldots, (\frac{n}{d} - 1)d\}$ je podgrupa řádu $\frac{n}{d}$. Pro volbu $d = \frac{n}{k}$ je podgrupa $\langle \frac{n}{k}\rangle$ řádu k.

Položíme-li $d := \text{GCD}(a, n)$ pro nějaké $a \in \mathbb{Z}_n \setminus\{0\}$, pak je d dělitel n a ukážeme, že $\langle a\rangle = \langle d\rangle$. Eukleidův algoritmus nám zaručuje existenci čísla $x \in \mathbb{Z}_n$ a celého y, pro něž $a \cdot x + n \cdot y = d$, z čehož plyne, že $(a \cdot x)\text{mod } n = d$. Proto $d \in \langle a\rangle =$, a tudíž $\langle d\rangle \subseteq \langle a\rangle$. Naopak, protože d/a, dostáváme, že $a \in \langle d\rangle$, proto $\langle a\rangle \subseteq \langle d\rangle$, čímž jsme dokončili důkaz rovnosti $\langle a\rangle = \langle d\rangle$.

Dokázali jsme, že pro každý dělitel k čísla n větší než 1 máme jedinou podgrupu tvaru $\langle \frac{n}{k}\rangle$ a pro $a \in \mathbb{Z}_n \setminus\{0\}$ máme $\langle a\rangle = \langle \text{GCD}(a, n)\rangle$. Ze zřejmého faktu, že $\text{GCD}(a, n)$ dělí n, plyne platnost závěrečné ekvivalence. □

Poznamenejme, že $\langle 0\rangle = \{0\}$ je jediná podgrupa grupy $\mathbb{Z}_n(+)$ řádu 1, a s využitím klasifikační Věty 5.5 vidíme, že pro každý dělitel k řádu konečné cyklické

grupy, existuje právě jedna její podgrupa grupy řádu k. Protože podle Lagrangeovy věty řád podgrupy dělí řád grupy, máme kompletně popsánu strukturu podgrup konečných cyklických grup.

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

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

Rovnost v definici jsme nahlédli v Příkladu 3.5(4) a v Příkladu 5.1(2) jsme ukázali, že hodnota Eulerovy funkce $\varphi(n)$ udává počet generátorů cyklické grupy řádu n. Následují věta nám nám při znalosti prvočíselného rozkladu čísla n umožní spočítat hodnotu $\varphi(n)$, tedy počet generátorů jakékoli cyklické grupy řádu n.

Věta 6.2. *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 2.5. Všimněme si, že $\prod_{i=1}^k \mathbb{Z}_{n_i}(\cdot)$ s operací z Příkladu 2.4 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 2.5 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

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

Příklad 6.3. (1) Uvažujme cyklickou grupu $G(\cdot)$ řádu $n := |G|$. Potom $G(\cdot)$ obsahuje právě $\varphi(n)$ generátorů. Protože díky Lagrangeově větě řád podgrupy vždy dělí řád grupy, podle 6.1 $G(\cdot)$ 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 6.2 právě $\prod_{i=1}^k (p_i - 1)p_i^{r_i - 1}$ generátorů.

Konečně si všimněme, že pro k, které nedělí n nemáme žádný prvek G řádu k, zatímco pro k/n existuje právě $\varphi(k)$ generátorů jediné cyklické podgrupy řádu k, tedy právě $\varphi(k)$ prvků G řádu k. Toto pozorování můžeme shrnout do vzorce uvažujícího všech n prvků grupy $G(\cdot)$, z nichž každý má určitý řád dělící n:

$$n = \sum_{k/n} \varphi(k).$$

(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 5.6 neobsahuje), pak díky 6.1 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 $25 = \frac{50}{2}$ a tudíž je prvek 42 řádu 25 a naopak prvků řádu 25 najdeme v $\mathbb{Z}_{50}(+)$ právě $\varphi(25) = 20$.

Poznámka 6.4. *Buď $G(\cdot)$ konečná grupa. Potom $g^{|G|} = e$ pro každý prvek $g \in G$.*

Důkaz. Z Poznámky 5.4 plyne, že $g^n = e$ a podle Věty 4.6 $n/|G|$, proto

$$g^{|G|} = (g^n)^{\frac{|G|}{n}} = e^{\frac{|G|}{n}} = e,$$

kde první rovnost plyne z 5.3. □

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

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

Důkaz. Díky Poznámce 2.6 tvrzení stačí dokázat pro hodnoty $a \in \mathbb{Z}_n$. Použijeme k tomu Poznámku 6.4, kde jako grupu G můžeme díky 3.4 vzít grupu invertibilních prvků $\mathbb{Z}_n^*(\cdot)$ monoidu $\mathbb{Z}_n(\cdot)$ tj. prvků nesoudělných s n, která má podle definice Eulerovy funkce právě $\varphi(n)$ prvků. Protože $a \in \mathbb{Z}_n^*$, dostáváme pomocí 6.4

$$(a^{\varphi(n)})\mathrm{mod}\ n = (a^{|\,\mathbb{Z}_n^*\,|})\mathrm{mod}\ n = 1.$$

□

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

Poznámka 6.6. *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 6.5 $(x^m)\mathrm{mod\ p} = 1$ 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 2.5 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 5.3 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 6.7 (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 6.6 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 $x = (a^e) \mathrm{mod}\ pq$. 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

$$(a_1^d) \mathrm{mod}\ \ n, \ldots, (a_k^d) \mathrm{mod}\ \ n,$$

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:

Fakt 6.8. *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 6.9 (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 6.8. 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 6.10 (ElGamal)**.** Tentokrát využijeme problém diskrétního logaritmu pro stejnou úlohu, kterou řeší 6.7. Opět zvolíme cyklickou grupu $\mathcal{G} = G(\cdot)$, její generátor a 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 $w \in G$, náhodně zvolíme $r \in \mathbb{Z}_{|G|}$ a spočítáme $x = a^r$ a $y = w \cdot b^r$. Posílanou zprávou je dvojice (x, y), kterou příjemce znalý tajného klíče snadno rozšifruje výpočtem

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

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

7. Základy univerzální algebry

Smyslem této kapitoly je nahlédnout, že některé výsledky, které jsme formulovali pro grupy, lze v téměř nezměněné podobě formulovat i v mnohem obecnějším kontextu a lze jich tak využít i pro další algebraické objekty. Ačkoli tvrzení, která (znovu) dokážeme v obecné situaci, platí i pro algebraické objekty, již s grupami mají jen málo společného, my jich využijeme především při práci s pojmem okruhu, kde strukturu Abelovy grupy zatížíme dalšími podmínkami.

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. Koncepty, které lze zcela přímočaře přeložit do obecného kontextu shrnují Poznámka 7.4 a 7.5.

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 pojmy obecné algebry a podalgebry:

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.

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, $i \in I$.

Je-li indexová množina I konečná, můžeme předpokládat, že je dobře uspořádaná $I = \{i_1, \ldots, i_k\}$, a tedy typ lze chápat jako konečnou posloupnost arit jednotlivých operací, místo $A(\alpha_i |\ i \in I)$ budeme psát $A(\alpha_{i_1}, \ldots, \alpha_{i_k})$ a typ Ω budeme zapisovat jako vektor $(\Omega(i_1), \ldots . \Omega(i_k))$.

Příklad 7.1. (1) Uvážíme grupu $G(\cdot)$ s unární operací inverzního prvku $^{-1}$ a nulární operací 1. Pak $G(\cdot)$, $G(\cdot, ^{-1})$ a $G(\cdot, ^{-1}, 1)$ představují různé algebry.

(a) Podalgebry algebry $G(\cdot, ^{-1}, 1)$ typu $(2, 1, 0)$ 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 algebry $G(\cdot, ^{-1})$ typu $(2, 1)$, 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 $G(\cdot)$ typu (2) 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) 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. 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.

(3) Je-li $\mathcal{A} = A(\alpha_i |\ i \in I)$ obecná *algebra typu* Ω, je A jistě její triviální podalgebrou. Pokud $\mathcal{A}$ neobsahuje žádné nulární operace, je prázdná množina triviální podalgebrou.

(4) Každá podalgebra algebry $\mathbb{Z}(+, -, 0, 1)$ typu $(2, 1, 0, 0)$ je podalgebrou algebry $\mathbb{Z}(+, -, 0)$, tedy podgrupou a nutně obsahuje prvek 1, proto $\mathbb{Z}(+, -, 0, 1)$ obsahuje jedinou podalgebru $\mathbb{Z}$.

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 $f(\alpha(a_1, \ldots, a_n)) = \beta(f(a_1), \ldots, f(a_n))$. 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 7.2. (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 4.3(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 $V(+, \cdot t | t \in T)$.

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

Definice. Nechť ρ je ekvivalence a α je n-ární operace na množině A. Řekneme, že ρ je *slučitelná s* α, jestliže pro každý systém prvků $a_1, \ldots, a_n, b_1 \ldots, b_n \in A$, pro které $(a_i, b_i) \in \rho$, $i = 1, \ldots, n$, platí, že $(\alpha(a_1, \ldots, a_n), \alpha(b_1, \ldots, b_n)) \in \rho$. 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 7.3. (1) Ekvivalence $\equiv \pmod n$ tvoří podle Poznámky 2.6 kongruenci na algebře $\mathbb{Z}(+, -, 0, \cdot)$.

(2) id a $A \times A$ jsou kongruence na libovolné algebře $A(\alpha_i |\ i \in I)$.

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

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 4.3 pro obecné algebry:

Poznámka 7.4. *Nechť $A_1(\alpha_i|\ i \in I)$, $A_2(\alpha_i|\ i \in I)$ a $A_3(\alpha_i|\ i \in I)$ jsou algebry stejného typu, $f : A_1 \to A_2$ a $g : A_2 \to A_3$ jsou homomorfismy a B je podalgebra algebry $A_2(\cdot)$.*

(1) *gf je také homomorfismus,*
(2) *je-li f 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 4.3.

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

8. Homomorfismy, izomorfismy a rozklad algeber

V návaznosti na předchozí kapitolu nahlédneme, že na faktorizaci nosné množiny algebry, která umožňuje opětovné zavedení struktury algebry stejného typu, lze přirozeně nahlížet prostřednictvím homomorfismů. Ve speciálním případě grup zjistíme, že kongruence jsou právě ekvivalence rmod H pro normální podgrupy H. Hlavním výsledkem kapitoly budou dvě věty o izomorfismu, které nabízejí technicky velmi příjemné uchopení faktorizace.

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 $\ker \pi_\rho = \rho$.

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 $A/\rho = \{B_i |\ i \in I\}$. Zobrazení $\pi_\rho : A \to A/\rho$ dané podmínkou $\pi_\rho(a) = [a]_\rho$, kde $a \in A$ se nazývá *přirozená projekce* .

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.

Poznámka 8.1. *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. Označme $\Omega : I \to \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ typ algebry $\mathcal{A}$ a zvolme libovolné $i \in I$. Jestliže $[a_j]_\rho = [b_j]_\rho \in A/\rho$, kde $j = 1, \dots \Omega(i)$, potom $(a_j, b_j) \in \rho$ pro všechna $j = 1, \dots \Omega(i)$, proto $[\alpha_i(a_1, \dots, a_{\Omega(i)})]_\rho = [\alpha_i(b_1, \dots, b_{\Omega(i)})]_\rho$, tedy definice operací na A/ρ je korektní.

Podobně pro $a_1, \dots, a_{\Omega(i)} \in A$ platí, že $\alpha_i(\pi(a_1), \dots, \pi(a_{\Omega(i)})) =$

$$= \alpha_i([a_1]_\rho, \dots, [a_{\Omega(i)}]_\rho) = [\alpha_i(a_1, \dots, a_{\Omega(i)})]_\rho = \pi(\alpha_i(a_1, \dots, a_{\Omega(i)})),$$

což znamená, že je π opravdu homomorfismus. □

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

Nyní si uvědomíme, že kongruence na grupě jsou právě ekvivalence rmod H = lmod H pro normální podgrupy H.

Věta 8.2. *Pro grupu $G(\cdot)$ a relaci ρ jsou následující podmínky ekvivalentní:*

(1) *ρ je kongruence na algebře $G(\cdot)$,*
(2) *ρ je kongruence na algebře $G(\cdot, ^{-1}, 1)$,*
(3) *$H = [e]_\rho$ je normální podgrupa $G(\cdot)$ a $\rho =$ rmod H (= lmod H).*

Důkaz. (1)⇒(2) V Příkladu 7.3(3) jsme si uvědomili, že je každá ekvivalence slučitelná s nulární operací 1. Nechť dále $(a,b) \in \rho$ a dokážeme, že rovněž $(a^{-1}, b^{-1}) \in \rho$. Z reflexivity ρ plyne, že $(a^{-1}, a^{-1}), (b^{-1}, b^{-1}) \in \rho$ a díky symetrii ρ platí, že $(b,a) \in \rho$. Využijeme-li dvakrát slučitelnosti ρ s operací $\cdot$ dostáváme, že

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

a tudíž $(a^{-1}, b^{-1}) = (a^{-1} \cdot b \cdot b^{-1}, 1 \cdot b^{-1}) \in \rho$.

(2)⇒(3) Protože je ρ ekvivalence, tedy reflexivní relace, leží 1 v třídě $[1]_\rho$. Zvolme $a, b \in [1]_\rho$ a $g \in G$. Potom $(1, a), (1, b) \in \rho$ a využijeme-li slučitelnosti ρ s operacemi $\cdot$ a $^{-1}$, dostáváme, že $(1, a \cdot b) = (1 \cdot 1, a \cdot b) \in \rho$, že $(1, a^{-1}) = (1^{-1}, a^{-1}) \in \rho$ a že $(1, g \cdot a \cdot g^{-1})(g \cdot 1 \cdot g^{-1}, g \cdot a \cdot g^{-1}) \in \rho$. Proto $a \cdot b, a^{-1}, g \cdot a \cdot g^{-1} \in [1]_\rho$, čímž jsme ověřili, že je $[1]_\rho$ normální podgrupa $G(\cdot)$.

Zbývá dokázat, že $(a, b) \in \rho$, právě když $(a, b) \in \operatorname{lmod}[1]_\rho$. Jestliže nejprve $(a, b) \in \rho$, potom $(1, a^{-1} \cdot b) = (a^{-1} \cdot a, a^{-1} \cdot b) \in \rho$, protože je ρ ekvivalence slučitelná s $\cdot$, tedy $(a, b) \in \operatorname{lmod}[1]_\rho$. Naopak, zvolíme-li $(a, b) \in \operatorname{lmod}[1]_\rho$, pak $(a, b) = (a \cdot 1, a \cdot a^{-1} \cdot b) \in \rho$. Konečně podle 4.5(4) platí, že $\operatorname{rmod}[1]_\rho = \operatorname{lmod}[1]_\rho$.

(3)⇒(1) 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 4.1(5) a (7) je ρ ekvivalence slučitelná s s operací $\cdot$ a přímým výpočtem zjistíme, že $[1]_\rho = H$. □

Věta 8.2, která říká, že kongruenci ρ na grupě jednoznačně odpovídá normální podgrupa $H = [e]_\rho$, nám umožňuje faktorovou množinu zapisovat ve tvaru $G/H := G/\rho = G/\operatorname{rmod} H$. Obvyklý zápis faktorové grupy $G/\rho(\odot)$ tedy bude tvaru $G/H(\cdot)$, kde $H = [e]_\rho$ s prvky $[a]_H = [a]_\rho = aH = Ha$ z nichž $[e]_\rho = H$ je neutrální a operacemi

$$[a]_H \cdot [b]_H = aH \cdot bH = [a \cdot b]_H = (a \cdot b)H, \qquad [a]_H^{-1} = [a^{-1}]_H = a^{-1}H$$

Podobně budeme přirozenou projekci G na G/H označovat symbolem π_H, tedy $\pi_H(a) = [a]_H = aH$.

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 8.3. *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 definice σ/ρ korektní. Zbytek plyne bezprostředně z definic relace 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 8.4. *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 $\mathcal{B}$ (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 (8.7).

(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 $[a_1]_\rho = [a_2]_\rho$, 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 $g(A/\rho) = f(A)$, 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 7.4(3) je $f(A)$ podalgebra algebry $\mathcal{B}$, omezíme-li tedy obor hodnot zobrazení f, můžeme ho chápat jako homomorfismus $f : A \to f(A)$. Nyní aplikujeme (1) pro $\rho = \ker\ f$ a dostaneme přímo požadovaný izomorfismus $\psi : A/\ker\ f \to f(A)$. □

Věta 8.5 (2. věta o izomorfismu)**.** *Nechť $\rho \subseteq \sigma$ jsou dvě kongruence na algebře $\mathcal{A}$. Pak je algebra $\mathcal{A}/\sigma$ izomorfní algebře $(\mathcal{A}/\rho)/(\sigma/\rho)$.*

Důkaz. Nejprve použijeme 8.4(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 $g([a]_\rho) = [a]_\sigma$. Nyní přímočaře spočítáme $\ker g = \{([a]_\rho, [b]_\rho) |\ (a, b) \in \sigma\} = \sigma/\rho$ a použijeme Větu 8.4(2), která nám dá izomorfimus $\mathcal{A}/\sigma \cong (\mathcal{A}/\rho)/\ker g = (\mathcal{A}/\rho)/(\sigma/\rho)$. □

Příklad 8.6. Máme-li homomorfismus $F_n : \mathbb{Z} \to \mathbb{Z}_n$ grupy $\mathbb{Z}(+)$ do grupy $\mathbb{Z}_n(+)$ s počítáním modulo n daný předpisem $F_n(k) = (k) mod\ n$, potom 8.7(2) zajišťuje izomorfismus $\mathbb{Z}/\mathrm{Ker}\ F_n(+) \cong \mathbb{Z}_n(+)$. Navíc je zjevně $(a, b) \in ker\ F_n$, právě když $n/(a - b)$, tedy $\ker\ F_n = (\equiv\ (\mathrm{mod}\ n)$ a $\mathrm{Ker}\ F_n = n\,\mathbb{Z}$.

Všimněme si, že na faktorové množině $\mathbb{Z}/n\,\mathbb{Z} = \mathbb{Z}/(\equiv\ (\mathrm{mod}\ n))$ máme dobře zavedenu strukturu grupy $\mathbb{Z}/n\,\mathbb{Z}(+)$ předpisem

$$[a]_{\equiv(\mathrm{mod}\ n)} + [b]_{\equiv(\mathrm{mod}\ n)} = [a + b]_{\equiv(\mathrm{mod}\ n)}$$

Nakonec s využitím Věty 8.2 přeformulujeme obecné věty o homomorfismu a izomorfismu pro grupy:

Důsledek 8.7. *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.* rmod$H \subseteq$ 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 $\varphi(G_1)(\cdot)$.*

Důsledek 8.8 (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 $(G/H)/(K/H)(\cdot)$.*

9. Okruhy a ideály

Nyní obrátíme svou pozornost k další důležité třídě algebraických objektů, jimiž jsou okruhy, tedy komutativní aditivní grupa disponující navíc asociatívním násobením, které je pomocí distributivity svázáno se sčítáním. Jedná se o společné uchopení známých struktur těles a celých čísel s opreacemi sčítání a násobení.

Protože je naším hlavním cílem konstrukce a algoritmické uchopení (především konečných) těles, zaměříme se na obecný popis těles (Věta 9.5) a charakterizaci těch faktorů komutativních okruhů, které tvoří těleso (Věta 9.7).

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 9.1. (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) $\mathbb{Z}(+,\cdot,-,0,1)$ je obor a $\mathbb{Z}_n(+,\cdot,-,0,1)$ jsou pro každé přirozené $n > 1$ jsou komutativní okruhy. Z lineární algebry víme, že je $\mathbb{Z}_n(+,\cdot,-,0,1)$ komutativní těleso, právě když je n prvočíslo.

Poznámka 9.2. *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 9.3. (1) $\{0\}$ a R jsou ideály každého okruhu R.

(2) Podle 5.6 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 9.2(2). Dále $0 = a0 \in aR$ díky 9.2(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 *triviální* 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 9.3(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 9.4. *Je-li $R(+, \cdot, -, 0, 1)$ okruh a I jeho pravý nebo levý ideál, pak $I = R$, právě když $1 \in I$.*

Důkaz. Protože $1 \in R$, je přímá implikace triviální. Jestliže I pravý (levý) ideál, který obsahuje prvek 1 a vezmeme libovolné $r \in R$, potom $r = 1 \cdot r = (r \cdot 1) \in I$, tedy $I = R$. □

Věta 9.5. *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 9.4.

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 9.2(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 3.3 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 9.6. *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 7.3(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 $R(+,\cdot,-,0,1)$.

To, 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 8.1.

(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 .

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.

Nyní zformulujeme tvrzení, které charakterizuje, kdy je faktor komutativního okruhu těleso. Toto tvrzení bude hrát zásadní roli v konstrukci konečných těles, jíž se budeme zabývat v následující kapitole.

Věta 9.7. *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. Označme $\mathcal{I}_I^R$ množinu všech ideálů okruhu $\mathcal{R}$ obsahujících ideál I a $\mathcal{I}_0^{R/I}$ množinu všech ideálů okruhu $R/I(+,\cdot,-,[0]_I,[1]_I)$. Nejprve dokážeme obecnější pozorování, v němž si uvědomíme vztah množiny ideálů faktorového a původního okruhu.

Lemma. Je-li $\pi_I : R \to R/I$ přirozená projekce, 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 $\mathcal{I}_{[0]}^{R/I}$.

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, čímž máme Lemma dokázáno.

Nyní si stačí všimnout, že je $R/I(+,\cdot,-,[0]_I,[1]_I)$ podle Věty 9.5 komutativní těleso právě tehdy, když $\mathcal{I}_0^{R/I}$ obsahuje pouze triviální ideály, což je díky Lemmatu ekvivalentní podmínce, že $\mathcal{I}_I^R$ obsahuje právě dva ideály, tedy právě když je I je maximální ideál. □

10. 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 10.10), v první konstrukci využijeme faktorizace okruhů polynomů nad tělesy $\mathbb{Z}_p$, kde p je prvočíslo, abychom dostali libovolné konečné těleso (Věta 10.8). 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.

10.1. **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 $q = \sum_{n\in\mathbf{N}_0} q_n x^n$:

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

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

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

Poznámka 10.1. *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 $\mathbf{1}=\sum_n\mathbf{1}_nx^n$, 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 8.4(2) dostáváme izomorfismus okruhu $R(+,\cdot,-,0,1)$ s podokruhem $\nu(R)=\{sx^0|\ s\in R\}$.

(2) Nerovnost $\deg p+q\le\max(\deg p,\ \deg q)$ 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 $\deg p\cdot q\le\nu+\mu$.

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, pak snadno nahlédneme, že je násobení polynomů komutativní a pro každé $p,q\neq\mathbf{0}$, máme podle (3) $\deg p\cdot q=\deg p+\deg q\ge 0$, proto $p\cdot q\neq 0$. Navíc 44 □

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

Věta 10.2 (O dělení se zbytkem)**.** *Nechť $R(+,\cdot,-,0,1)$ je obor, $a,\ b\in R[x]$, kde $b=\sum b_nx^n$. Předpokládejme, že $m=\deg b\ge 0$ 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` $\{q_i:=r_{i+m}b_m^{-1};r:=r-q_ix^ib;\}$
`3.` `return` $\sum_i q_ix^i,\ r$`.`

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 10.1(3) a protože $\deg(r'-r)<\deg b$, dostáváme $r'-r=0$, a proto $q-q'=0$ □

Důsledek 10.3. *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 10.2 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 10.4. (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 10.5. *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 10.6. *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 10.3 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 $g \nmid 1$ a $f \nmid g$; pravá strana ekvivalence neříká nic jiného, než $g|f$ a $0 <$ 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.

Fakt 10.7. *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 bodu (2) a (3) ovšem uvádíme jen informativně.

Věta 10.8. (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 10.7 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 10.6 a Faktu 9.7 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 $0 \leq k < p$, 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 6.4 na grupu $\mathbb{F}^*(.)$, která má $p^n - 1$ prvků. Z 10.7 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 8.4, 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 9.5). 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 10.9. (1) Postupem důkazu bodu (1) Věty 10.8 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 10.7 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 $i, j, k, -i, -j, -k$.

10.2. **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 10.10. *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 $(a, b) \sim (e, f)$. Protože je každá ekvivalence slučitelná s každou nulární operací, zbývá ověřit slučitelnost $\sim$ s operacemi $+$, $\cdot$ a $-$.

Předpokládejme, že $(a_i, b_i) \sim (c_i, d_i)$ tedy $a_i d_i = c_i b_i$ pro $i = 1, 2$. Proto $(a_1 b_2 + b_1 a_2) d_1 d_2 = a_1 d_1 \cdot b_2 d_2 + a_2 d_2 \cdot b_1 d_1 = c_1 b_1 \cdot b_2 d_2 + c_2 b_2 \cdot b_1 d_1 = (c_1 d_2 + d_1 c_2) b_1 b_2$, tedy $(a_1, b_1) + (a_2, b_2) \sim (c_1, d_1) + (c_2, d_2)$. Dále $a_1 a_2 d_1 d_2 = c_1 c_2 b_1 b_2$, 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* oboru R a jeho prvky budeme značit $\frac{a}{b} = [(a, b)]_\sim$.

Příklad 10.11. (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 $\mathbb{R}[x](+, \cdot, -, 0, 1)$.

11. Svazy a Booleovy algebry

Závěrečnou kapitoly kurzu věnujeme algebraickému popisu uspořádaných množin. Nejprve si rozmyslíme, že jistou třídu uspořádaných množin lze nahlížet jako algebry s dvojicí binárních operací. Algebraický pohled nám umožní pracovat se všemi standardními univerzálně algebraickými pojmy. Na závěr se budeme zabývat pojmem obecné Booleovy algebry jako distributivního svazu s komplementy a ukažáženeme, že konečné Booleovy algebry nejsou (až na izomorfismus) ničím jiným než systémy všech podmnožin nějaké množiny.

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.

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*.

Vidímme, že svaz $(M, \leq)$ určuje na množině M strukturu algebry $M(\wedge, \vee)$ typu $(2, 2)$.

Snadno si uvědomíme, že id tvoří na libovolné neprázdné množině M uspořádání, ovšem pro $|M| > 1$ se jistě nejedná o svaz.

Příklad 11.1. Uveďme známé příklady uspořádání a svazů:

(1) Relace / dělitelnosti na množině všech přirozených čísel $\mathbb{N}$ (tj. daná podmínkou $a/b \equiv \exists c : b = a \cdot c$) je uspořádání na $\mathbb{N}$, navíc $\sup_{/}(n, m) = \mathrm{lcm}(n, m)$ a $\inf_{/}(a, b) = \mathrm{GCD}(n, m)$, proto je $(\mathbb{N}, /)$ svaz, který určuje algebru $\mathbb{N}(\mathrm{GCD}, \mathrm{lcm})$.
(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 $\inf_{\leq}(a, b) = \min(a, b)$. Tyto svazy určují algebry $\mathbb{Z}(\min, \max)$ (respektive $\mathbb{R}(\min, \max)$, $\mathbb{Q}(\min, \max)$).
(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 $\mathcal{B} \subseteq \mathcal{P}(X)$. Úplný svaz $(\mathcal{P}(X), \subseteq)$ určuje algebru $\mathcal{P}(X)(\cap, \cup)$.
(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 7.5 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.

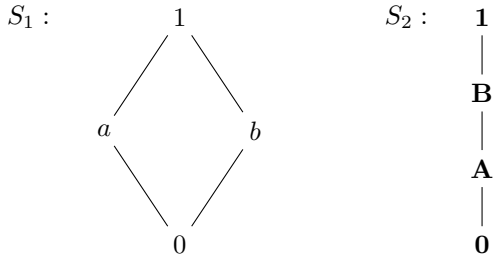
Konečné uspořádané množiny je často výhodné znázornit Hasseovým diagramem, připomeňme jeho definici:

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 $c = b$.

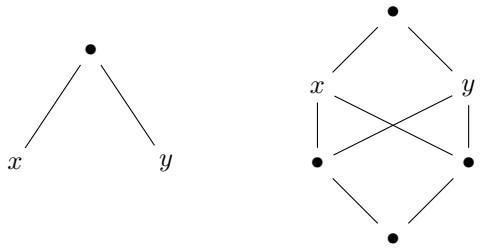
Hasseovým diagramem uspořádané množiny $(M, \leq)$ rozumíme orientovaný graf, jehož vrcholy tvoří prvky množiny M a a je s b spojen takovou hranou, že b se nachází výše než a, právě když b pokrývá a.

Příklad 11.2. Uveďme uspořádané množiny popsané Hasseovými diagramy:

(1) Uvažujme svazy $(S_1, \leq)$ a $(S_2, \leq)$, kde $S_1 = \{0, 1, a, b\}$ je dán relacemi:$0 <\cdot\, a <\cdot\, 1$ a $S_2 = \{\mathbf{0}, \mathbf{1}, \mathbf{A}, \mathbf{B}\}$ popisuje $0 <\cdot\, b <\cdot\, 1$ a $\mathbf{0} <\cdot\, \mathbf{A} <\cdot\, \mathbf{B} <\cdot\, \mathbf{1}$. Pak je jsou jejich Hasseovy diagramy následující:



(2) Žádný z následujících Hasseových diagramů uspořádaných množin neurčuje svaz, protože pro prvky x a y neexistuje infimum:



Nyní si rozmyslíme, že algebra určená svazem tomuto svazu odpovídá jednoznačně:

Věta 11.3. (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 $(M, \leq)$ se supremy a infimy nebo algebru $M(\wedge, \vee)$ splňující čtveřici axiomů (S1)–(S4). V následujícím textu budeme v závislosti na kontextu pracovat s oběma pohledy na svaz.

Nyní popíšeme izomorfismy svazů chápaných jako algebry pomocí pojmu monotónní zobrazení.

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 $A(\wedge, \vee)$.

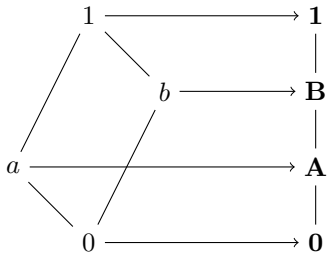
Poznámka 11.4. *Homomorfismus svazů je monotónní zobrazení.*

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

Důkaz. Díky 11.4 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 $f(a \vee b) = f(a) \vee f(b)$. □

Příklad 11.6. Pro svazy z Příkladu 11.2(1) uvažujme zobrazení $f(0) = \mathbf{0}$, $f(1) = \mathbf{1}$, $f(a) = \mathbf{A}$, $f(b) = \mathbf{B}$:



Zřejmě jde o monotónní zobrazení, ale nejedná se o homomorfismus svazů, protože $f(a \wedge b) = f(0) = \mathbf{0} \neq \mathbf{A} = f(a) \wedge f(b)$.

Nyní budeme zkoumat svazy splňující některé další přirozené identity.

Definice. Uvažujme svaz $S(\wedge, \vee)$ (chápaný jako algebra).

Řekneme, že je $S(\wedge, \vee)$ *distributivní* svaz, platí-li pro každé $a, b, c \in S$ rovnost $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Nechť svaz $S(\wedge,\vee)$ obsahuje nejmenší prvek $\mathbf{0}$ a největší prvek $\mathbf{1}$ (vzhledem k uspořádání $\leq$ danému podmínkou $a \leq b \Leftrightarrow b = a \vee b$). 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 11.7. (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.*

(2) *Každý prvek distributivního svazu má nejvýše jeden komplement.*

Důkaz. (1) Ze symetrie vlastností operací plyne, že stačí dokázat pouze jednu implikaci. Nechť je svaz distributivní. Budeme s využitím definice distributivity a 11.3 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).

(2) 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 11.8. Nechť $\mathcal{P}(X)$ je množina všech podmnožin množiny X a pro každou podmnožinu $Y \subseteq X$ definujme $Y' = X \setminus Y$. Pak je svaz $\mathcal{P}(X)(\cap,\cup)$ distributivní a $\mathcal{P}(X)(\cup,\cap,\emptyset,X,\ ')$ je Booleova algebra.

Poznámka 11.9. *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) $(a \vee b)' = a' \wedge b'$, $(a \wedge b)' = a' \vee b'$.

Důkaz. (1) a (2) plyne přímo z definice a 11.7(2).

(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 $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = \mathbf{1} \vee \mathbf{1} = \mathbf{1}$.

Důkaz druhé rovnosti je symetrický. □

Věta 11.10. *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 $M = \{m_1,\ldots,m_n\} \subseteq S$ 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 11.5 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 11.10 musí být každá Booleova algebra izomorfní potenční Booleově algebře, tedy musí mít 2^n prvků, kde n je počet atomů.

12. Shrnutí

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

12.1. **Teorie čísel a okruhy.** 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 10.5.

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).
- 2.5 Čínská věta o zbytcích pro celá čísla. I toto tvrzení lze zobecnit a využít například pro rychlé násobení polynomů.
- 9.7 Tvrzení, že tělesem jsou právě faktory komutativního okruhu podle maximálního ideálu, spolu
- 10.2 s algoritmickou větou o dělení se zbytkem, nám umožňuje
- 10.8 konstruovat konečná tělesa (ta jsou posléze základním stavebním kamenem algebraické teorie kódů).

12.2. **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 existují-li, jsou určeny jednoznačně. Navíc v každém monoidu, jak množinu s asociativní binární operací a neutrálním prvkem nazýváme, vždy najdeme kanonickou grupu invertibilních prvků (3.4).

Co důležitého se nám podařilo nahlédnout:

6.2 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.
4.6 Lagrangeova věta popisující vztah počtu prvků grupy a její podgrupy je důsledek zkoumání vlastností kongruencí rmod a lmod, jejichž dalšími důsledky jsou
8.2 popis kongruencí grupy pomocí pojmu normální podgrupa.
5.5 Snadný popis struktury cyklických grup umožňuje
6.1 zesílit tvrzení Lagrangeovy věty pro cyklické grupy a formulovat
6.5 Eulerovu větu, která je základním nástrojem několika kryptografických aplikací (protokoly RSA, Diffie–Hellman, ElGamal).

12.3. **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 porozumět inkluzí uspořádaným systémům podalgeber a kongruencí algeber, což jsou základní nástroje zkoumání obecných algeber, je pojem svazu, který představuje algebraicky uchopené uspořádané množiny.

Co důležitého se nám podařilo nahlédnout:

8.1 Uvědomili jsme si, že faktorizovat algebry lze právě podle kongruencí a že přirozená projekce na faktorovou algebru je právě homomorfismus.
8.4 1.věta o izomorfismu jako důsledek Věty o homomorfismu umožňuje překládat problémy týkající se faktorových algeber do podalgeber známých algeber,
8.5 zatímco 2.věta o izomorfismu ukazuje, že faktor faktorové algebry lze vždy izomorfně přeložit na faktor původní algebry.
11.5 Tvrzení, že izomorfismy svazů lze popsat jazykem monotónie, využívá důkaz
11.10 izomorfního popisu konečných Booleových algeber jako potenční Booleovy algebry.