

UNIVERZITA PALACKÉHO V OLOMOUCI
PŘÍRODOVĚDECKÁ FAKULTA

Předmětová

Učební text je určen pro studijní obory Biostatistika, program Matematika (ve studijních oborech Diskrétní matematika, Matematické aplikace a Matematika v počítačovém modelování) a Informatika na Přírodovědecké fakultě Palackého v Olomouci. Učebním textem je možnost použití v ANTONINKA AČKOVÝ semestru, a to zejména pro řešení některých cvičení.

Oblastí aktivity jsou binární relace (hlavní ekvivalence) a teorií algoritmů (algoritmy, výpočetní možnosti, výpočetní komplexita). Pojďme se s definicemi některých pojmů týkajících se výpočetního algoritmu, které výpočetní algoritmus v prvním semestru, jistě všechny pojmy znova připomenut, takže algoritam tvoří v podstatě samostatný celek.

Probíhající lektka je ilustrována na konkrétních příkladech a při řešení cvičení uvedených za každou kapitolou si čtenec může ověřit své závědnutí.

GRUPY A OKRUHY

Olomouc, prosinec 2004

Autorka

Tiskovna Univerzity Palackého v Olomouci
IČ 251 67 000
ISBN 80-210-3800-8
8 8 0 80

Olomouc
2005

© Univerzita Palackého 2005
ISBN 80-210-3800-8

Obsah

Binární relace na množinách

Předmluva

3

1 Binární relace na množinách	7
1.1 Algebra binárních relací	8
1.2 Relace ekvivalence	13
2 Grupoidy, pologrupy, grupy	21
2.1 Grupoidy a pologrupy	21
2.2 Základní vlastnosti grup	27
2.3 Podgrupy a normální podgrupy grup	29
2.4 Věty o izomorfismu grup	39
2.5 Kongruence grup	43
2.6 Cyklické a permutační grupy	46
2.7 Automorfismy grup	49
2.8 Direktní součiny grup	51
3 Okruhy, obory integrity, tělesa	61
3.1 Základní vlastnosti okruhů	61
3.2 Ideály a homomorfismy okruhů	65
3.3 Charakteristiky okruhů a prvookruhy okruhů	70
3.4 Podílová tělesa oborů integrity	76
4 Dělitelnost v oborech integrity	83
4.1 Základní vlastnosti dělitelů prvků	83
4.2 Existence největších společných dělitelů	89
4.3 Eukleidovské obory integrity	91
4.4 Gaussovy obory integrity	95
Literatura	103

Kapitola 1

Binární relace na množinách

V této úvodní kapitole prohloubíme některé znalosti týkající se binárních relací na množinách.

Připomeňme, že *kartézským součinem* množin A_1, A_2, \dots, A_n ($n \geq 1$) rozumíme množinu

$$\prod_{i=1}^n A_i = A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n); a_i \in A_i, i = 1, 2, \dots, n\},$$

tedy množinu všech uspořádaných n -tic, jejichž i -té složky jsou prvky z A_i ($i = 1, 2, \dots, n$).

Jestliže $A_1 = A_2 = \dots = A_n = A$, pak kartézský součin

$$\prod_{i=1}^n A_i = A \times A \times \dots \times A$$

nazýváme také n -tá *kartézská mocnina množiny* A a značíme ji symbolem A^n .

Pro $n = 0$ klademe $A^0 = \{\emptyset\}$.

Dalším dobré známým pojmem je pojem n -árni relace:

Jestliže A_1, A_2, \dots, A_n ($n \geq 1$) jsou množiny, pak n -árni relaci mezi těmito množinami rozumíme libovolnou podmnožinu ϱ kartézského součinu $A_1 \times A_2 \times \dots \times A_n$. Přitom n -árni relaci na množině A nazýváme každou podmnožinu ϱ kartézské mocniny A^n .

Pro potřeby tohoto textu budeme dále pracovat jen s relacemi na množině.

V případě malých n se často používá zvláštních názvů pro n -árni relace.

1-árni relace se nazývá *unární*. Je zřejmé, že unární relace na A je vlastně podmnožina množiny A .

2-árni relace se nazývá *binární*. Jestliže ϱ je binární relace na A , $a, b \in A$ a platí-li, že uspořádaná dvojice (a, b) patří do ϱ , pak místo $(a, b) \in \varrho$ budeme většinou tento vztah zapisovat $a \varrho b$.

3-árni relace se nazývá *ternární*. S těmito typy relací se můžeme často setkat v geometrii. Ternární relaci je např. vztah vyjádřený predikátem „*Bod X leží mezi body A a B*“ pro uspořádané trojice bodů na dané přímce.

Pro 4-árni relaci se také užívá název *kvaternární*.

1.1 Algebra binárních relací

Nechť A je množina a nechť ϱ a σ jsou binární relace na A . Víme, že složením relací ϱ a σ je binární relace $\varrho \circ \sigma$ na A taková, že

$$\forall a, b \in A; a \varrho \circ \sigma b \iff \exists c \in A; a \varrho c \wedge c \sigma b,$$

a že inverzní relaci k relaci ϱ je binární relace ϱ^{-1} na A taková, že

$$\forall a, b \in A; a \varrho^{-1} b \iff b \varrho a.$$

Proto skládání relací můžeme uvažovat jako binární operaci a vytváření inverzní relace jako unární operaci na množině všech binárních relací na A . Je zřejmé, že také sjednocení a průnik binárních relací jsou binárními operacemi na této množině všech binárních relací.

Ukážeme si některé vlastnosti uvedených operací s relacemi.

Věta 1.1.1 Jestliže ϱ, σ, τ a ϱ_i ($i \in I$) jsou binární relace na množině A , pak platí:

a) $\varrho \circ (\sigma \circ \tau) = (\varrho \circ \sigma) \circ \tau;$

b) $\left(\bigcup_{i \in I} \varrho_i \right) \circ \sigma = \bigcup_{i \in I} (\varrho_i \circ \sigma), \quad \tau \circ \left(\bigcup_{i \in I} \varrho_i \right) = \bigcup_{i \in I} (\tau \circ \varrho_i);$

c) $\left(\bigcap_{i \in I} \varrho_i \right) \circ \sigma \subseteq \bigcap_{i \in I} (\varrho_i \circ \sigma), \quad \tau \circ \left(\bigcap_{i \in I} \varrho_i \right) \subseteq \bigcap_{i \in I} (\tau \circ \varrho_i);$

d) $\varrho \subseteq \sigma \implies \varrho \circ \tau \subseteq \sigma \circ \tau, \quad \tau \circ \varrho \subseteq \tau \circ \sigma.$

Důkaz. a) Tvrzení a) je zvláštním případem již známé skutečnosti, že skládání binárních relací mezi libovolnými množinami je asociativní.

b) Nechť $a, b \in A$. Pak:

$$\begin{aligned} a \left(\bigcup_{i \in I} \varrho_i \right) \circ \sigma b &\iff \exists c \in A; a \left(\bigcup_{i \in I} \varrho_i \right) c \wedge c \sigma b \iff \\ &\iff \exists c \in A \exists i_0 \in I; a \varrho_{i_0} c \wedge c \sigma b \iff \exists i_0 \in I; a \varrho_{i_0} \circ \sigma b \iff \\ &\iff a \left(\bigcup_{i \in I} \varrho_i \circ \sigma \right) b. \end{aligned}$$

c) Pro libovolné $a, b \in A$ platí:

$$\begin{aligned} a \left(\bigcap_{i \in I} \varrho_i \right) \circ \sigma b &\iff \exists c \in A; a \left(\bigcap_{i \in I} \varrho_i \right) c \wedge c \sigma b \iff \\ &\iff \exists c \in A \forall i \in I; a \varrho_i c \wedge c \sigma b \implies \forall i \in I; a \varrho_i \circ \sigma b \iff \\ &\iff a \left(\bigcap_{i \in I} \varrho_i \circ \sigma \right) b. \end{aligned}$$

d) Nechť $\varrho \subseteq \sigma$, $a, b \in A$. Pak platí:

$$\begin{aligned} a \varrho \circ \tau b &\implies \exists c \in A; a \varrho c \wedge c \tau b \implies \\ &\implies \exists c \in A; a \sigma c \wedge c \tau b \implies a \sigma \circ \tau b. \end{aligned}$$

Podobně se dokáže druhá implikace. \square

Poznámka 1.1.2 1. Již z dřívějška je známé, že skládání binárních relací na A obecně není komutativní.

2. V části c) právě dokázané věty obecně neplatí rovnost.

Příklad 1.1.3 Položme

$$A = \{a, b, c, d, e\}, \quad \varrho_1 = \{(a, c), (a, d), (b, e), (c, b)\}, \quad \varrho_2 = \{(b, a), (c, d), (a, d)\}, \\ \sigma = \{(c, e), (d, a), (b, a)\}.$$

Pak:

$$\varrho_1 \cap \varrho_2 = \{(a, d)\}, \quad (\varrho_1 \cap \varrho_2) \circ \sigma = \{(a, a)\}, \quad \varrho_1 \circ \sigma = \{(a, e), (a, a), (c, a)\},$$

$$\varrho_2 \circ \sigma = \{(c, a), (a, a)\}, \quad (\varrho_1 \circ \sigma) \cap (\varrho_2 \circ \sigma) = \{(a, a), (c, a)\},$$

a tedy

$$(\varrho_1 \cap \varrho_2) \circ \sigma \subset (\varrho_1 \circ \sigma) \cap (\varrho_2 \circ \sigma).$$

Věta 1.1.4 Pro libovolné binární relace ϱ, σ a ϱ_i ($i \in I$) na množině A platí:

$$a) \quad (\varrho^{-1})^{-1} = \varrho;$$

$$b) \quad \varrho \subseteq \sigma \implies \varrho^{-1} \subseteq \sigma^{-1};$$

$$c) \quad \left(\bigcap_{i \in I} \varrho_i \right)^{-1} = \bigcap_{i \in I} \varrho_i^{-1};$$

$$d) \quad \left(\bigcup_{i \in I} \varrho_i \right)^{-1} = \bigcup_{i \in I} \varrho_i^{-1};$$

$$e) \quad (\varrho \circ \sigma)^{-1} = \sigma^{-1} \circ \varrho^{-1};$$

$$f) \quad \text{id}_A \circ \varrho = \varrho \circ \text{id}_A = \varrho, \quad \text{kde id}_A \text{ je identická relace na } A.$$

Důkaz. Pravdivost tvrzení a) a e) jsme již ověřili v prvním semestru a tvrzení b) a f) jsou zřejmá přímo z definic operací s binárními relacemi.

c) Nechť $a, b \in A$. Pak

$$\begin{aligned} a \left(\bigcap_{i \in I} \varrho_i \right)^{-1} b &\iff b \left(\bigcap_{i \in I} \varrho_i \right) a \iff \forall i \in I; b \varrho_i a \iff \\ &\iff \forall i \in I; a \varrho_i^{-1} b \iff a \left(\bigcap_{i \in I} \varrho_i^{-1} \right) b. \end{aligned}$$

d) Dokáže se analogicky využitím definice sjednocení. □

Mezi binární relace, které se nejčastěji vyskytují a kterých budeme i v tomto textu používat, patří relace ekvivalence a uspořádání. V definicích těchto typů relací se používají podmínky z následující definice.

Definice. Binární relace ϱ na množině A se nazývá

a) *reflexivní*, jestliže

$$\forall a \in A; a \varrho a;$$

b) *symetrická*, jestliže

$$\forall a, b \in A; a \varrho b \implies b \varrho a;$$

c) *antisymetrická*, jestliže

$$\forall a, b \in A; a \varrho b \wedge b \varrho a \implies a = b;$$

d) *tranzitivní*, jestliže

$$\forall a, b, c \in A; a \varrho b \wedge b \varrho c \implies a \varrho c.$$

Poznámka 1.1.5 Uvedené vlastnosti jsme mohli také ekvivalentně definovat využitím operací s relacemi a inkluze mezi relacemi. Čtenář se totiž může snadno přesvědčit, že platí:

- a) ϱ je reflexivní, právě když $\text{id}_A \subseteq \varrho$.
- b) ϱ je symetrická, právě když $\varrho^{-1} = \varrho$.
- c) ϱ je antisymetrická, právě když $\varrho \cap \varrho^{-1} \subseteq \text{id}_A$.
- d) ϱ je tranzitivní, právě když $\varrho \circ \varrho \subseteq \varrho$.

V dalším textu budeme těchto skutečností často používat.

Definice. Nechť ϱ je binární relace na množině A a nechť $B \subseteq A$. Pak *restrikcí relace ϱ na podmnožinu B* budeme rozumět binární relaci ϱ_B na B takovou, že $\varrho_B = \varrho \cap (B \times B)$. (To znamená, že $\forall a, b \in B; a \varrho_B b \iff a \varrho b$.)

Věta 1.1.6 Pro každé ϱ , $\varrho_i \subseteq A \times A$ ($i \in I$) a pro každou $B \subseteq A$ platí:

a) $(\varrho_B)^{-1} = (\varrho^{-1})_B$;

b) $\left(\bigcap_{i \in I} \varrho_i \right)_B = \bigcap_{i \in I} (\varrho_i)_B$;

$$c) \quad \left(\bigcup_{i \in I} \varrho_i \right)_B = \bigcup_{i \in I} (\varrho_i)_B.$$

Důkaz.

a)

$$(\varrho_B)^{-1} = (\varrho \cap (B \times B))^{-1} = \varrho^{-1} \cap (B \times B)^{-1} = \varrho^{-1} \cap (B \times B) = (\varrho^{-1})_B.$$

b)

$$\left(\bigcap_{i \in I} \varrho_i \right)_B = \left(\bigcap_{i \in I} \varrho_i \right) \cap (B \times B) = \bigcap_{i \in I} (\varrho_i \cap (B \times B)) = \bigcap_{i \in I} (\varrho_i)_B.$$

c) Analogicky jako pro b). □

Při studiu množin uvažovaných spolu s relacemi (např. uspořádaných množin) je důležité znát také vlastnosti relací, které jsou z původních relací odvozeny. Některé z těchto vlastností se mohou přenášet, jak je to vidět např. v následující větě.

Věta 1.1.7 Nechť $\varrho \subseteq A \times A$ a $B \subseteq A$. Jestliže relace ϱ je reflexivní (resp. symetrická, antisymetrická, tranzitivní), pak také relace ϱ^{-1} a ϱ_B jsou reflexivní (resp. symetrické, antisymetrické, tranzitivní).

Důkaz. 1. Nejdříve ukážeme, že uvedené vlastnosti se přenáší při vytváření inverzní relace. Využijeme k tomu výsledků z věty 1.1.4.

a) Jestliže ϱ je reflexivní, pak $\text{id}_A \subseteq \varrho$, a tedy $\text{id}_A = \text{id}_A^{-1} \subseteq \varrho^{-1}$.

b) Nechť ϱ je symetrická, tzn. $\varrho^{-1} = \varrho$. Pak $(\varrho^{-1})^{-1} = \varrho = \varrho^{-1}$, tedy ϱ^{-1} je také symetrická.

c) Jestliže ϱ je antisymetrická, pak z $\varrho \cap \varrho^{-1} \subseteq \text{id}_A$ dostaneme

$$\varrho^{-1} \cap (\varrho^{-1})^{-1} = \varrho^{-1} \cap \varrho \subseteq \text{id}_A,$$

proto ϱ^{-1} je antisymetrická.

d) Jestliže $\varrho \circ \varrho \subseteq \varrho$, pak $(\varrho \circ \varrho)^{-1} \subseteq \varrho^{-1}$, a tedy $\varrho^{-1} \circ \varrho^{-1} \subseteq \varrho^{-1}$.

2. Nyní odvodíme vlastnosti relace ϱ_B . Budeme k tomu navíc používat výsledky z věty 1.1.6:

a) Označme id_A (resp. id_B) identickou relaci na A (resp. na B). Jestliže $\text{id}_A \subseteq \varrho$, pak

$$\text{id}_B = \text{id}_A \cap (B \times B) \subseteq \varrho \cap (B \times B),$$

proto $\text{id}_B \subseteq \varrho_B$.

b) Jestliže $\varrho^{-1} = \varrho$, pak $(\varrho_B)^{-1} = (\varrho^{-1})_B = \varrho_B$, tedy symetričnost relace se přenáší.

c) Nechť $\varrho \cap \varrho^{-1} \subseteq \text{id}_A$. Pak

$$\begin{aligned} \varrho_B \cap (\varrho_B)^{-1} &= \varrho_B \cap (\varrho^{-1})_B = (\varrho \cap \varrho^{-1})_B = \\ &= (\varrho \cap \varrho^{-1}) \cap (B \times B) \subseteq \text{id}_A \cap (B \times B) = \text{id}_B. \end{aligned}$$

d) Nechť ϱ je tranzitivní, $a, b, c \in B$. Pak platí:

$$\begin{aligned} a \varrho_B b \wedge b \varrho_B c &\implies a(\varrho \cap (B \times B)) b \wedge b(\varrho \cap (B \times B)) c \implies \\ &\implies a \varrho b \wedge a(B \times B) b \wedge b \varrho c \wedge b(B \times B) c \implies \\ &\implies a \varrho b \wedge b \varrho c \wedge a, b, c \in B \implies a \varrho c \wedge a, c \in B \implies a \varrho_B c, \end{aligned}$$

proto ϱ_B je tranzitivní. \square

Je samozřejmé, že ne každá binární relace na množině je tranzitivní. Přesto bude často nutné vytvořit k dané relaci tranzitivní relaci, která je s původní relací ve velice úzkém vztahu. Konstrukce této tranzitivní relace je popsána v následující větě.

Věta 1.1.8 Jestliže ϱ je binární relace na množině A , pak pro binární relaci $\hat{\varrho}$ na A takovou, že

$\forall a, b \in A; a \hat{\varrho} b \iff \exists a_0, a_1, \dots, a_n \in A; a_0 = a, a_n = b, a_i \varrho a_{i+1}, i = 0, 1, \dots, n - 1$, platí:

a) $\hat{\varrho}$ je tranzitivní relace na A a $\varrho \subseteq \hat{\varrho}$;

b) jestliže σ je tranzitivní binární relace na A a $\varrho \subseteq \sigma$, pak $\hat{\varrho} \subseteq \sigma$.

(Tj., $\hat{\varrho}$ je nejmenší tranzitivní binární relace na A obsahující ϱ .)

Důkaz. a) Nechť $a, b, c \in A$, $a \hat{\varrho} b, b \hat{\varrho} c$. Pak v A existují prvky

$$a = a_0, a_1, \dots, a_n = b, b = b_0, b_1, \dots, b_m = c$$

takové, že $a_i \varrho a_{i+1}, b_j \varrho b_{j+1}$ pro každé $i = 0, 1, \dots, n - 1, j = 0, 1, \dots, m - 1$. Tedy platí také, že $a \hat{\varrho} c$. Přitom je zřejmé, že $\varrho \subseteq \hat{\varrho}$.

b) Nechť $\sigma \subseteq A \times A$ je tranzitivní a nechť $\varrho \subseteq \sigma$. Jestliže $a, b \in A$ a $a \hat{\varrho} b$, pak existují $a = a_0, a_1, \dots, a_n = b$ v A takové, že $a_i \varrho a_{i+1}$ pro každé $i = 0, 1, \dots, n - 1$. Pak ale platí také $a_i \sigma a_{i+1}$ pro každé $i = 0, 1, \dots, n - 1$, a proto z tranzitivnosti relace σ dostáváme $a \sigma b$. Tedy $\hat{\varrho} \subseteq \sigma$. \square

Definice. Nechť ϱ je binární relace na A . Pak relaci $\hat{\varrho}$ z věty 1.1.8 nazveme *tranzitivní uzávěr* (nebo také *tranzitivní obal*) relace ϱ .

Asociativnost skládání binárních relací umožňuje zavést pojem přirozené mocniny binární relace. Jestliže totiž $\varrho \subseteq A \times A$, pak můžeme její mocninu definovat matematickou indukcí takto:

$$\varrho^1 = \varrho, \quad \varrho^{n+1} = \varrho^n \circ \varrho.$$

Věta 1.1.9 Pro libovolnou binární relaci ϱ na A platí

$$\hat{\varrho} = \bigcup_{n=1}^{\infty} \varrho^n.$$

Důkaz. Podle předchozí věty víme, že $\varrho \subseteq \hat{\varrho}$. Proto podle věty 1.1.1d) platí $\varrho^n \subseteq \hat{\varrho}^n$. Z tranzitivnosti $\hat{\varrho}$ tedy dostáváme $\varrho^n \subseteq \hat{\varrho}^n \subseteq \hat{\varrho}$ pro každé $n = 1, 2, \dots$, proto platí

$$\bigcup_{n=1}^{\infty} \varrho^n \subseteq \hat{\varrho}.$$

b) Obráceně, nechť $a, b \in A$, $a \hat{\varrho} b$. Pak existují prvky $a = a_0, a_1, \dots, a_n = b$ z A takové, že $a_i \varrho a_{i+1}$, $i = 0, 1, \dots, n-1$, což znamená, že $a \varrho^n b$ pro některé přirozené číslo n . Proto

$$\hat{\varrho} \subseteq \bigcup_{n=1}^{\infty} \varrho^n.$$

□

Příklad 1.1.10 Sestrojíme tranzitivní uzávěr relace $\varrho = \{(1, 3), (2, 1), (2, 4), (3, 3), (4, 3)\}$ na množině $A = \{1, 2, 3, 4\}$. Platí

$$\varrho^2 = \{(1, 3), (2, 3), (3, 3), (4, 3)\},$$

$$\varrho^3 = \varrho^2,$$

$$\text{a tedy } \hat{\varrho} = \varrho \cup \varrho^2 = \{(1, 3), (2, 1), (2, 4), (3, 3), (4, 3), (2, 3)\}.$$

(Zde jsme užili zřejmého faktu, že existuje-li $m \in \mathbb{N}$ takové, že $\varrho^m = \varrho^{m+1}$, pak

$$\hat{\varrho} = \bigcup_{i=1}^m \varrho^i.)$$

Věta 1.1.11 Nechť ϱ je binární relace na A . Pak platí:

- a) jestliže ϱ je reflexivní, pak $\hat{\varrho}$ je také reflexivní;
- b) jestliže ϱ je symetrická, pak $\hat{\varrho}$ je také symetrická.

Důkaz. a) Je zřejmé, že z předpokladu reflexivnosti ϱ dostaneme $\text{id}_A \subseteq \varrho \subseteq \hat{\varrho}$.

b) Nechť $a, b \in A$, $a \hat{\varrho} b$. Pak existují prvky $a = a_0, a_1, \dots, a_n = b$ z A , pro které

$a_i \varrho a_{i+1}$, $i = 0, 1, \dots, n-1$. Ze symetričnosti ϱ pak dostáváme $a_{i+1} \varrho a_i$ pro každé $i = 0, 1, \dots, n-1$, tedy $b = a_n \varrho a_{n-1}, \dots, a_1 \varrho a_0 = a$, a proto platí $b \hat{\varrho} a$. □

1.2 Relace ekvivalence

V této části se budeme věnovat relacím ekvivalence a jejich vztahu k rozkladům množin. Později poznáme význam tohoto typu relací také pro vytváření faktorových algebraických struktur.

Definice. Relací ekvivalence (stručně také *ekvivalenci*) na množině A rozumíme každou binární relaci $\theta \subseteq A \times A$, která je reflexivní, symetrická a tranzitivní.

Poznámka 1.2.1 Relace ekvivalence se vyskytují a využívají ve všech oblastech matematiky. Např. každá z následujících binárních relací je ekvivalencí na příslušné množině:

- Kongruence na \mathbb{Z} podle libovolného přirozeného modulu n . (Tj. pro libovolná celá čísla a, b platí $a \equiv b \pmod{n} \iff n|(b-a)$.)
- Rovnoběžnost přímek v rovině.
- Podobnost trojúhelníků v rovině.
- Rovnost matic typu $m \times n$ nad číselným tělesem T .
- Relace ϱ na množině $M_n(T)$ všech čtvercových matic stupně n taková, že $A \varrho B \iff \det A = \det B$.
- Relace σ na množině všech funkcí jedné reálné proměnné definovaných na intervalu $\langle a, b \rangle$ taková, že

$$f \sigma g \iff \exists c \in \mathbb{R} \forall x \in \langle a, b \rangle; f(x) = g(x) + c.$$

Věta 1.2.2 Jestliže ϱ_i ($i \in I$) jsou ekvivalence na množině A , pak jejich průnik $\bigcap_{i \in I} \varrho_i$ je také ekvivalencí na A .

Důkaz. Označme $\varrho = \bigcap_{i \in I} \varrho_i$.

- Reflexivita: Podle předpokladu $\text{id}_A \subseteq \varrho_i$ pro každé $i \in I$, proto také $\text{id}_A \subseteq \bigcap_{i \in I} \varrho_i = \varrho$.
- Symetrie: Podle předpokladu $\varrho_i^{-1} = \varrho_i$ pro každé $i \in I$. Proto

$$\varrho^{-1} = \left(\bigcap_{i \in I} \varrho_i \right)^{-1} = \bigcap_{i \in I} \varrho_i^{-1} = \bigcap_{i \in I} \varrho_i = \varrho.$$

- Tranzitivita: Využitím věty 1.1.1c) a předpokladu, že všechny relace ϱ_i jsou tranzitivní, dostaneme

$$\begin{aligned} \varrho \circ \varrho &= \varrho \circ \left(\bigcap_{i \in I} \varrho_i \right) \subseteq \bigcap_{i \in I} (\varrho \circ \varrho_i) = \bigcap_{i \in I} \left(\left(\bigcap_{j \in I} \varrho_j \right) \circ \varrho_i \right) \subseteq \\ &\subseteq \bigcap_{i \in I} \left(\bigcap_{j \in I} (\varrho_j \circ \varrho_i) \right) \subseteq \bigcap_{i \in I} (\varrho_i \circ \varrho_i) \subseteq \bigcap_{i \in I} \varrho_i = \varrho. \end{aligned}$$

□

Poznámka 1.2.3 Z předchozí věty je vidět, že pro každou binární relaci ϱ na A existuje nejmenší ekvivalence na A obsahující ϱ . Tuto ekvivalencí je průnik všech ekvivalencí na A obsahujících ϱ . (Mezi ekvivalence na A , které obsahují ϱ , vždy patří $A \times A$.)

Věta 1.2.4 Nechť ϱ je binární relace na A a $\sigma = \text{id}_A \cup \varrho \cup \varrho^{-1}$. Pak nejmenší ekvivalence na A obsahující ϱ je tranzitivní uzávěr $\hat{\sigma}$ relace σ .

Důkaz. Je zřejmé, že $\text{id}_A \subseteq \varrho \subseteq \sigma$ a $\sigma^{-1} = \sigma$, tedy σ je reflexivní a symetrická. Proto na základě vět 1.1.8 a 1.1.11 platí, že $\hat{\sigma}$ je ekvivalence na A . Přitom samozřejmě $\varrho \subseteq \hat{\sigma}$.

Nechť τ je ekvivalence na A , $\varrho \subseteq \tau$, $a, b \in A$, $a \hat{\sigma} b$. Pak v A existují prvky $a = a_0, a_1, \dots, a_n = b$ takové, že $a_i \sigma a_{i+1}$ pro každé $i = 0, 1, \dots, n-1$. Tedy pro každé $i = 0, 1, \dots, n-1$ musí platit buď $a_i = a_{i+1}$ nebo $a_i \tau a_{i+1}$ nebo $a_i \varrho^{-1} a_{i+1}$. Protože $\varrho^{-1} \subseteq \tau^{-1} = \tau$, platí ve všech případech $a_i \tau a_{i+1}$, a tedy $a \tau b$. To však znamená, že $\hat{\sigma} \subseteq \tau$. \square

Poznámka 1.2.5 Na rozdíl od průniků nemusí být sjednocení ekvivalence také ekvivalence.

Příklad 1.2.6 Označme $A = \{a, b, c\}$, $\varrho_1 = \text{id}_A \cup \{(a, b), (b, a)\}$, $\varrho_2 = \text{id}_A \cup \{(a, c), (c, a)\}$. Zřejmě ϱ_1 a ϱ_2 jsou ekvivalence na A . Platí však $(b, a) \in \varrho_1 \cup \varrho_2$, $(a, c) \in \varrho_1 \cup \varrho_2$, ale $(b, c) \notin \varrho_1 \cup \varrho_2$, tedy relace $\varrho_1 \cup \varrho_2$ není ekvivalence.

Definice. Nechť ϱ_i ($i \in I$) jsou ekvivalence na A , $\sigma = \bigcup_{i \in I} \varrho_i$. Potom ekvivalence $\hat{\sigma}$ nazveme spojením ekvivalence ϱ_i ($i \in I$) a označíme ji $\bigvee_{i \in I} \varrho_i$.

Spojení $\varrho \vee \sigma = \widehat{\varrho \cup \sigma}$ dvou ekvivalence můžeme chápout jako výsledek binární operace „ \vee “ na množině všech ekvivalence na A . Ukážeme si, jaké jsou vztahy mezi operacemi „ \cup “, „ \circ “ a „ \vee “.

Věta 1.2.7 Pro libovolné ekvivalence ϱ a σ na A platí

$$\varrho \cup \sigma \subseteq \varrho \circ \sigma \subseteq \varrho \vee \sigma.$$

Důkaz. Je zřejmé, že platí (podle vět 1.1.4f) a 1.1.1d))

$$\varrho = \varrho \circ \text{id}_A \subseteq \varrho \circ \sigma, \quad \sigma = \text{id}_A \circ \sigma \subseteq \varrho \circ \sigma,$$

tedy

$$\varrho \cup \sigma \subseteq \varrho \circ \sigma.$$

Nechť $a, b \in A$, $a(\varrho \circ \sigma)b$. Pak existuje prvek $c \in A$ takový, že $a \varrho c \wedge c \sigma b$, tedy také $a(\varrho \cup \sigma)c \wedge c(\varrho \cup \sigma)b$. Z definice spojení ekvivalence proto dostáváme $a(\varrho \vee \sigma)b$, tedy $\varrho \circ \sigma \subseteq \varrho \vee \sigma$. \square

Připomeňme si, že relace ϱ a σ na A se nazývají zaměnitelné, platí-li $\varrho \circ \sigma = \sigma \circ \varrho$. V případě zaměnitelných ekvivalence je konstrukce jejich spojení podstatně jednodušší než v obecném případě:

Věta 1.2.8 Nechť ϱ a σ jsou ekvivalence na A . Pak $\varrho \circ \sigma$ je ekvivalencí na A právě tehdy, když ϱ a σ jsou zaměnitelné. V takovém případě navíc platí, že $\varrho \circ \sigma = \varrho \vee \sigma$.

Důkaz. a) Nechť $\varrho \circ \sigma$ je ekvivalence na A . Pak ze symetričnosti relací $\varrho \circ \sigma$, ϱ a σ dostaneme

$$\varrho \circ \sigma = (\varrho \circ \sigma)^{-1} = \sigma^{-1} \circ \varrho^{-1} = \sigma \circ \varrho.$$

b) Protože $\text{id}_A = \text{id}_A \circ \text{id}_A \subseteq \text{id}_A \circ \sigma \subseteq \varrho \circ \sigma$, je $\varrho \circ \sigma$ reflexivní pro kterékoliv dvě (i nezaměnitelné) ekvivalence. Předpokládejme dále, že $\varrho \circ \sigma = \sigma \circ \varrho$. Pak $(\varrho \circ \sigma)^{-1} = \sigma^{-1} \circ \varrho^{-1} = \sigma \circ \varrho = \varrho \circ \sigma$, tedy $\varrho \circ \sigma$ je symetrická.

Platí také $(\varrho \circ \sigma) \circ (\varrho \circ \sigma) = \varrho \circ (\sigma \circ \varrho) \circ \sigma = \varrho \circ (\varrho \circ \sigma) \circ \sigma = (\varrho \circ \varrho) \circ (\sigma \circ \sigma) \subseteq \varrho \circ \sigma$, a proto $\varrho \circ \sigma$ je rovněž tranzitivní.

c) Zbývá dokázat, že pro zaměnitelné ekvivalence ϱ a σ splývají jejich složení a spojení.

Víme, že za daného předpokladu je $\varrho \circ \sigma$ ekvivalencí a že platí $\varrho \subseteq \varrho \circ \sigma$, $\sigma \subseteq \varrho \circ \sigma$. Přitom ale $\varrho \vee \sigma$ je nejmenší ekvivalence obsahující $\varrho \cup \sigma$. Tedy $\varrho \vee \sigma \subseteq \varrho \circ \sigma$.

Obrácená inkluze platí podle věty 1.2.7. □

Příklad 1.2.9 Nechť

$$A = \{0, 1, 2, 3, 4, 5\},$$

$$\varrho = \text{id}_A \cup \{(0, 3), (3, 0), (1, 4), (4, 1), (2, 5), (5, 2)\},$$

$$\sigma = \text{id}_A \cup \{(0, 2), (2, 0), (0, 4), (4, 0), (2, 4), (4, 2), (1, 3), (3, 1), (1, 5), (5, 1), (3, 5), (5, 3)\}.$$

Pak $\varrho \circ \sigma = \sigma \circ \varrho = A \times A$, tedy $\varrho \vee \sigma = \varrho \circ \sigma = A \times A$.

Definice. Nechť A je neprázdná množina. *Rozkladem množiny A na třídy* nazýváme libovolný systém $\mathcal{R} = (A_i, i \in I)$ jejích neprázdných podmnožin takový, že

$$1. \bigcup_{i \in I} A_i = A;$$

$$2. \forall i, j \in I; A_i \neq A_j \implies A_i \cap A_j = \emptyset.$$

Poznámka. Pojem „systém“ použitý v definici znamená, že v \mathcal{R} mohou existovat prvky systému s různými indexy, které se sobě rovnají. (Na rozdíl od *množiny*, v níž je každý její prvek právě jednou.)

Věta 1.2.10 Nechť $\mathcal{R} = (A_i, i \in I)$ je rozklad na množině A . Pak binární relace ϱ na A taková, že $\forall a, b \in A; a \varrho b \iff \exists i \in I; a, b \in A_i$, je ekvivalencí na A .

Důkaz. Reflexivita: Protože $A = \bigcup_{i \in I} A_i$, musí ke každému prvku $a \in A$ existovat třída $A_{i_0} \in \mathcal{R}$ taková, že $a \in A_{i_0}$. Tedy $a \varrho a$.

Symetrie je zřejmá.

Tranzitivita: Jestliže $a, b, c \in A$, $a \varrho b$, $b \varrho c$, pak existují $i_1, i_2 \in I$ takové, že $a, b \in A_{i_1}$, $b, c \in A_{i_2}$. To znamená, že $b \in A_{i_1} \cap A_{i_2}$, a proto $A_{i_1} = A_{i_2}$, tedy $a \varrho c$. □

Definice. Řekneme, že ekvivalence ϱ z věty 1.2.10 je *indukovaná rozkladem \mathcal{R}* .

Definice. Nechť ϱ je ekvivalence na množině A , $a \in A$. Pak množinu

$$[a]_{\varrho} = \{x \in A; x \varrho a\}$$

nazýváme *třída množiny A podle ekvivalence ϱ určená prvkem a* .

(Bude-li z kontextu zřejmé, kterou ekvivalenci uvažujeme, budeme místo $[a]_{\varrho}$ psát také stručněji $[a]$.)

Věta 1.2.11 Jestliže ϱ je ekvivalence na množině A , pak systém \mathcal{R} všech tříd $[a]_{\varrho}$, kde $a \in A$, tvoří rozklad na A .

Důkaz. 1. Protože pro každý $a \in A$ platí, že $a \in [a]_{\varrho}$, je zřejmé, že každá třída $[a]_{\varrho}$ je neprázdná a že $A = \bigcup_{a \in A} [a]_{\varrho}$.

2. Nechť $a, b \in A$, $[a]_{\varrho} \cap [b]_{\varrho} \neq \emptyset$ a nechť $c \in [a]_{\varrho} \cap [b]_{\varrho}$. Nechť $x \in [a]_{\varrho}$. Pak $x \varrho a$, $a \varrho c$, $c \varrho b$, tedy $x \varrho b$, což znamená, že $x \in [b]_{\varrho}$. Proto platí $[a]_{\varrho} \subseteq [b]_{\varrho}$. Inkluze $[b]_{\varrho} \subseteq [a]_{\varrho}$ se dokáže analogicky. \square

Definice. Rozklad \mathcal{R} na množině A z věty 1.2.11 se nazývá *rozklad indukovaný ekvivalence ϱ* .

Poznámka 1.2.12 Věty 1.2.10 a 1.2.11 ukazují, že existuje vzájemně jednoznačná korespondence mezi rozklady a ekvivalencemi na dané množině A . Platí totiž, že každý rozklad na A určuje ekvivalence na A a obráceně. Přitom je zřejmé, že vyjdeme-li z rozkladu, vytvoříme-li k tomuto rozkladu indukovanou ekvivalence a k ní pak indukovaný rozklad, pak původní a výsledný rozklad splývají. Podobně, když k dané ekvivalence vytvoříme indukovaný rozklad a k němu indukovanou ekvivalence, pak opět původní a výsledná ekvivalence splývají.

V dalším textu budeme proto tohoto vzájemně jednoznačného vztahu mezi rozklady a ekvivalencemi s výhodou často používat.

Definice. a) Množina všech navzájem různých tříd množiny A vzhledem k ekvivalence ϱ se nazývá *faktorová množina množiny A podle ϱ* (a značí se A/ϱ).

b) Zobrazení $\nu : A \rightarrow A/\varrho$ takové, že $\forall a \in A; \nu(a) = [a]_{\varrho}$, se nazývá *přirozené zobrazení A na A/ϱ* .

Poznámka 1.2.13 Je zřejmé, že prvky faktorové množiny A/ϱ jsou vlastně třídy rozkladu na A indukovaného ekvivalence ϱ .



Věta 1.2.14 Nechť f je zobrazení množiny A do množiny B . Pak relace ϱ na A taková, že

$$\forall a, b \in A; a \varrho b \iff f(a) = f(b),$$

je ekvivalencí na A .

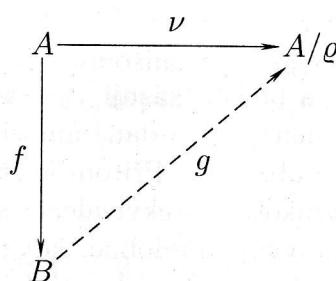
Důkaz. Je zřejmý. □

Definice. Řekneme, že ekvivalence ϱ z věty 1.2.14 je *indukovaná zobrazením* f .

Definice. Jestliže C a D jsou množiny, pak řekneme, že jsou *ekvivalentní*, existuje-li bijektivní zobrazení množiny C na množinu D (a také obráceně).

Věta 1.2.15 Jestliže f je surjektivní zobrazení množiny A na množinu B a ϱ je relace ekvivalence na A indukovaná zobrazením f , pak množiny B a A/ϱ jsou ekvivalentní a existuje právě jedno bijektivní zobrazení g množiny B na faktorovou množinu A/ϱ takové, že $f \circ g$ je přirozené zobrazení množiny A na A/ϱ .

Vztah mezi zobrazeními f , ν a g je možno zobrazit diagramem



Důkaz. Nechť b je libovolný prvek z B . Protože f je surjektivní, existuje $a \in A$ takový, že $f(a) = b$. Položme $g(b) = [a]_\varrho$. Ukažme, že jsme takto korektně definovali zobrazení B do A/ϱ . Jestliže $f(a) = f(a_1) = b$, pak platí $a \varrho a_1$, tzn. $[a]_\varrho = [a_1]_\varrho$. Proto ke každému prvku $b \in B$ existuje právě jedna třída z A/ϱ , na kterou se b zobrazí. (Je určena libovolným prvkem zobrazujícím se v f na prvek b .)

Zbývá dokázat, že g je bijekce B na A/ϱ . Pro každou třídu $[a]_\varrho \in A/\varrho$ platí, že $[a]_\varrho = g(f(a))$, tedy g je surjektivní. Nechť $b, b_1 \in B$, $g(b) = g(b_1)$, a nechť a, a_1 jsou takové prvky z A , že $b = f(a)$, $b_1 = f(a_1)$. Pak $[a]_\varrho = [a_1]_\varrho$, tj. $a \varrho a_1$, a tedy $b = f(a) = f(a_1) = b_1$. To znamená, že g je také injektivní, a proto bijektivní. (Dokázali jsme tak, mj., že množiny B a A/ϱ jsou ekvivalentní.)

Fakt, že g je jediná bijekce B na A/ϱ , pro kterou platí $f \circ g = \nu$, je zřejmý. □

Cvičení

1. Zjistěte, které z následujících binárních relací jsou relacemi ekvivalence:

- relace dělitelnosti na \mathbb{N} ;
- relace kongruence podle přirozeného modulu n na \mathbb{Z}
 $(x, y \in \mathbb{Z}, n \in \mathbb{N}; x \equiv y \iff \exists z \in \mathbb{Z}; y - x = nz);$
- relace podobnosti geometrických útvarů v rovině;
- relace kolmosti přímkov v rovině;
- relace rovnoběžnosti přímkov v rovině;
- relace množinové inkluze na potenční množině $\mathcal{P}(A)$ množiny A .

V kladném případě popište třídy odpovídajícího rozkladu.

2. Dokažte, že binární relace „ \sim “ na kartézském součinu $\mathbb{Z} \times \mathbb{Z}$ taková, že

$$\forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}; (a, b) \sim (c, d) \iff ad = bc,$$

je relací ekvivalence.

3. Nechť $M_n(\mathcal{T})$ je množina všech čtvercových matic stupně n na číselném tělesem \mathcal{T} . Jsou-li $\mathbf{A}, \mathbf{B} \in M_n(\mathcal{T})$, pak řekneme, že matice \mathbf{B} je podobná matici \mathbf{A} , existuje-li regulární matice $\mathbf{C} \in M_n(\mathcal{T})$ taková, že $\mathbf{B} = \mathbf{C}^{-1} \mathbf{A} \mathbf{C}$. Dokažte, že relace podobnosti matic je relací ekvivalence na $M_n(\mathcal{T})$.

4. Nechť $\varrho = \{(a, b), (a, c), (b, d), (e, f), (a, e), (c, f), (d, e), (e, c)\}$ je relace na množině $A = \{a, b, c, d, e, f\}$.

- Určete tranzitivní uzávěr $\hat{\varrho}$ relace ϱ .
- Určete nejmenší ekvivalenci na A obsahující ϱ .

5. Uvažujme množinu $B = \{0, 1, 2, 3, 4, 5, 6, 7\}$ a relace τ, χ na B takové, že

$$\begin{aligned}\tau &= \{(x, y) \in B^2; |x - y| \in \{0, 4\}\}, \\ \chi &= \{(u, v) \in B^2; |u - v| \in \{0, 2, 4, 6\}\}.\end{aligned}$$

Ověřte, že relace τ a χ jsou ekvivalence na B , a určete jejich spojení.

6. Pro libovolná komplexní čísla α, β položíme $\alpha \approx \beta$ právě tehdy, když $|\alpha| = |\beta|$.

- Dokažte, že relace „ \approx “ je ekvivalencí na množině všech komplexních čísel \mathbb{C} .
- Určete faktorovou množinu \mathbb{C}/\approx .
- Sestrojte přirozené zobrazení $\nu : \mathbb{C} \longrightarrow \mathbb{C}/\approx$.

7. Nechť $n \in \mathbb{N}$. Uvažujme zobrazení $\varphi : M_n(\mathcal{R}) \longrightarrow \mathbb{R}$ takové, že

$$\forall \mathbf{B} \in M_n(\mathcal{R}); \quad \varphi : \mathbf{B} \longmapsto \det \mathbf{B}.$$

- a) Ověřte, že φ je surjekce.
- b) Určete ekvivalenci σ na $M_n(\mathcal{R})$ takovou, že
- $$\forall \mathbf{B}, \mathbf{C} \in M_n(\mathcal{R}); \mathbf{B} \sigma \mathbf{C} \iff \varphi(\mathbf{B}) = \varphi(\mathbf{C}).$$
- c) Najděte bijekci $\psi : \mathbb{R} \longrightarrow M_n(\mathcal{R})/\sigma$ takovou, že $\varphi \circ \psi$ se rovná přirozenému zobrazení $M_n(\mathcal{R})$ na $M_n(\mathcal{R})/\sigma$.

Kapitola 2

Grupoidy, pologrupy, grupy

2.1 Grupoidy a pologrupy

Nejdříve si připomeneme pojmy operace na množině a algebraické struktury.

Definice. Jestliže $G \neq \emptyset$ je množina a $n \in \mathbb{N} \cup \{0\}$, pak n -ární operací na G rozumíme každé zobrazení $f : G^n \rightarrow G$.

Podle této definice platí, že operace f přiřazuje libovolné uspořádané n -tici (a_1, \dots, a_n) prvků z G jednoznačně určený prvek $f(a_1, \dots, a_n)$ z G , který nazýváme výsledek operace f provedené na tyto prvky.

Pro $n = 0$ vidíme (protože $G^0 = \{\emptyset\}$), že nulární operace $f : G^0 \rightarrow G$ vyznačuje v G jeden prvek.

Pro $n = 1$ je unární operace $f : G^1 \rightarrow G$ vlastně zobrazením G do G . Pro binární operace budeme pro výsledek operace místo zápisu $f(a_1, a_2)$ používat raději zápisu ve tvaru $a_1 f a_2$.

Definice. Neprázdná množina G spolu s neprázdnou množinou $\{f_\alpha; \alpha \in I\}$ operací na G se nazývá algebraická struktura (nebo stručněji algebra). Označení: $\mathcal{G} = (G; f_\alpha, \alpha \in I)$.

Definice. a) Algebraická struktura $\mathcal{G} = (G; \cdot)$, kde „ \cdot “ je binární operace na $G \neq \emptyset$, se nazývá grupoid.

b) Grupoid \mathcal{G} se nazývá komutativní, platí-li

$$\forall a, b \in G; a \cdot b = b \cdot a.$$

c) Grupoid \mathcal{G} se nazývá pologrupa, je-li jeho operace asociativní, tj. platí-li

$$\forall a, b, c \in G; a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

d) Řekneme, že grupoid \mathcal{G} má jednotkový prvek, platí-li

$$\exists e \in G \forall a \in G; a \cdot e = a = e \cdot a.$$

Poznámka 2.1.1 a) Podobně jako v předchozí definici budeme pro grupoidy nejčastěji používat multiplikativní symboliku. Výsledek operace $a \cdot b$ budeme zpravidla zapisovat ve tvaru ab .

b) Už z dřívějška je známo, že v grupoidu existuje nejvýše jeden jednotkový prvek. Jednotkový prvek budeme v multiplikativním zápisu označovat e .

Jestliže grupoid \mathcal{G} není pologrupou, pak existují prvky $a_1, a_2, a_3 \in G$ takové, že $a_1(a_2a_3) \neq (a_1a_2)a_3$. Podobně mohou existovat $a_1, a_2, a_3, a_4 \in G$, pro něž jsou navzájem různé některé z prvků $(a_1a_2)(a_3a_4)$, $a_1((a_2a_3)a_4)$, $a_1(a_2(a_3a_4))$, ...

Příklad 2.1.2 Uvažujme grupoid $\mathcal{G} = (G; \cdot)$, kde $G = \{a, b, c\}$ a násobení je zadáno Cayleyovou tabulkou:

	a	b	c
a	b	a	c
b	c	c	b
c	b	c	a

Platí např.: $a(bc) = ab = a$, $(ab)c = ac = c$, a tedy $a(bc) \neq (ab)c$.

Podobně: $(ab)(ac) = ac = c$, $a((ba)c) = a(cc) = aa = b$, $a(b(ac)) = a(bc) = ab = a$, ...

V pologrupě ale předpokládáme, že pro libovolné její prvky a_1, a_2, a_3 platí $a_1(a_2a_3) = (a_1a_2)a_3$. Ukážeme, že tento předpoklad asociativnosti už postačuje k platnosti obecného zákona asociativnosti použitelného pro libovolnou uspořádanou n -tici prvků pologrupy.

Věta 2.1.3 Jestliže $\mathcal{G} = (G; \cdot)$ je pologrupa, $a_1, a_2, \dots, a_n \in G$ ($n \geq 3$), pak pro všechna uzávorkování při násobení těchto prvků zapsaných v daném pořadí dostaneme stejný výsledný prvek.

Důkaz. Jestliže $a_1, a_2, \dots, a_n \in G$, označíme standardně

$$a_1a_2 \dots a_n = (\dots (((a_1a_2)a_3)a_4) \dots)a_n.$$

Ukážeme, že pro každé uzávorkování je výsledný prvek roven $a_1a_2 \dots a_n$. Důkaz provedeme matematickou indukcí pro $n \geq 3$.

Pro $n = 3$ je tvrzení pravdivé přímo z definice pologrupy.

Nechť $n > 3$. Předpokládejme, že tvrzení platí pro každé $m \in \mathbb{N}$ takové, že $3 \leq m < n$. Nechť daný součin prvků $a_1, a_2, \dots, a_n \in G$ je tvaru $w = w_1 \cdot w_2$.

a) Jestliže $w_2 = a_n$, pak podle indukčního předpokladu platí $w_1 = a_1a_2 \dots a_{n-1}$, tedy

$$w = (a_1a_2 \dots a_{n-1}) \cdot a_n = a_1a_2 \dots a_{n-1}a_n.$$

b) Nechť w_2 vznikne vynásobením alespoň dvou prvků. Pak podle indukčního předpokladu platí

$$w_1 = a_1a_2 \dots a_k, \quad w_2 = a_{k+1} \dots a_n, \quad \text{kde } 1 \leq k \leq n-2.$$

Proto

$$\begin{aligned} w &= (a_1 a_2 \cdots a_k) \cdot (a_{k+1} \cdots a_{n-1} a_n) = (a_1 a_2 \cdots a_k) \cdot ((a_{k+1} \cdots a_{n-1}) a_n) = \\ &= ((a_1 a_2 \cdots a_k)(a_{k+1} \cdots a_{n-1})) a_n = (a_1 a_2 \cdots a_{n-1}) \cdot a_n = a_1 a_2 \cdots a_{n-1} a_n. \end{aligned}$$

To tedy znamená, že součin prvků a_1, a_2, \dots, a_n při dodržení zvoleného pořadí těchto prvků nezávisí na uzávorkování. \square

Poznámka 2.1.4 Při násobení prvků v libovolné pologrupě proto nemusíme používat závorky.

Definice. Nechť $\mathcal{G} = (G; \cdot)$ je pologrupa, $a \in G$. Pak n -tou přirozenou mocninou ($n \in \mathbb{N}$) prvku a rozumíme prvek $a^n \in G$ takový, že

$$a^1 = a, \quad a^{n+1} = a^n \cdot a.$$

Pokud použijeme aditivní zápis, budeme místo o n -té přirozené mocnině hovořit o n -té přirozeném násobku $n \times a$ prvku a , který je pak definován následovně:

$$1 \times a = a, \quad (n+1) \times a = (n \times a) + a.$$

Poznámka 2.1.5 V případě grupoidu, který není pologrupou, nemůžeme obecně zavést jednoznačně určenou n -tou mocninu prvku. Např. v grupoidu \mathcal{G} z příkladu 2.1.2 platí:

$$(aa)a = ba = c, \quad a(aa) = ab = a.$$

Věta 2.1.6 Jsou-li a, b prvky pologrupy \mathcal{G} a $m, n \in \mathbb{N}$, pak platí:

- a) $a^m \cdot a^n = a^{m+n}$;
- b) $(a^m)^n = a^{mn}$;
- c) jestliže $ab = ba$, pak $(ab)^n = a^n b^n$.

Důkaz. Budeme dokazovat matematickou indukcí.

- a) Nechť m je libovolné přirozené číslo. Pro $n = 1$ pak platí $a^m \cdot a^1 = a^m \cdot a = a^{m+1}$. Nechť $n > 1$ a nechť pro každé $m \in \mathbb{N}$ platí $a^m \cdot a^{n-1} = a^{m+(n-1)}$. Pak

$$a^m \cdot a^n = a^m \cdot (a \cdot a^{n-1}) = (a^m \cdot a) \cdot a^{n-1} = a^{m+1} \cdot a^{n-1} = a^{m+1+n-1} = a^{m+n}.$$
- b) Nechť $m \in \mathbb{N}$ je libovolné. Jestliže $n = 1$, pak $(a^m)^1 = a^m = a^{m \cdot 1}$. Nechť $n > 1$ a nechť platí $(a^m)^{n-1} = a^{m(n-1)}$. Pak

$$(a^m)^n = (a^m)^{(n-1)+1} = (a^m)^{n-1} \cdot (a^m)^1 = a^{m(n-1)} \cdot a^m = a^{m(n-1)+m} = a^{m[(n-1)+1]} = a^{mn}.$$

c) Nechť $ab = ba$. Pro $n = 1$ platí $(ab)^1 = ab = a^1 \cdot b^1$. Nechť $n > 1$ a nechť již platí $(ab)^{n-1} = a^{n-1} \cdot b^{n-1}$. Pak

$$a^n \cdot b^n = (a \cdot a^{n-1}) \cdot (b^{n-1} \cdot b) = a \cdot (a^{n-1} \cdot b^{n-1}) \cdot b = a \cdot (ab)^{n-1} \cdot b = a \cdot (ba)^{n-1} \cdot b = (ab)^n.$$

□

Definice. Pologrupa, v níž existuje jednotkový prvek, se nazývá **monoid**.

Poznámka 2.1.7 Nechť \mathcal{G} je monoid s jednotkovým prvkem e . Pak pro každý prvek $a \in G$ můžeme definovat i jeho nultou mocninu vztahem $a^0 = e$. Je zřejmé, že v \mathcal{G} platí rovnosti a), b), c) z věty 2.1.6 i pro případ, kdy některé z čísel n, m je rovno 0.

Při studiu vektorových prostorů a jejich vzájemných vztahů jsme viděli zvláštní význam homomorfismů a izomorfismů vektorových prostorů, tedy zobrazení, která „zachovávají“ operace ve vektorových prostorech. Analogické typy zobrazení zavedeme i pro libovolné algebraické struktury.

Definice. a) Jsou-li $\mathcal{G} = (G; \cdot)$ a $\mathcal{H} = (H; *)$ grupoidy, pak zobrazení $f : G \rightarrow H$ se nazývá **homomorfismus** grupoidu \mathcal{G} do grupoidu \mathcal{H} , platí-li

$$\forall a, b \in G; f(ab) = f(a) * f(b).$$

b) Jestliže f je navíc bijektivní, pak se nazývá **izomorfismus** grupoidu \mathcal{G} na grupoid \mathcal{H} .

c) Řekneme, že grupoid \mathcal{H} je **homomorfním obrazem** grupoidu \mathcal{G} , existuje-li surjektivní homomorfismus \mathcal{G} na \mathcal{H} .

d) Řekneme, že grupoid \mathcal{H} je **izomorfní s grupoidem** \mathcal{G} , existuje-li izomorfismus \mathcal{G} na \mathcal{H} .

Poznámka 2.1.8 a) Jestliže f je homomorfismus grupoidu \mathcal{G} do grupoidu \mathcal{H} a g je homomorfismus grupoidu \mathcal{H} do grupoidu \mathcal{K} , pak je zřejmé, že jejich složení $f \circ g$ je homomorfismus \mathcal{G} do \mathcal{K} . Podobně složení dvou izomorfismů grupoidů je opět izomorfismem. Navíc id_G je izomorfismem \mathcal{G} na \mathcal{G} a je také zřejmé, že inverzní zobrazení f^{-1} k izomorfismu f \mathcal{G} na \mathcal{H} je izomorfismem \mathcal{H} na \mathcal{G} .

Relace „být izomorfni s“ je tedy ekvivalencí na třídě všech grupoidů, a proto indukuje rozklad třídy všech grupoidů na třídy navzájem izomorfních grupoidů. Grupoidy, které patří do téže třídy rozkladu, mají stejné algebraické vlastnosti.

b) Protože relace „být izomorfni s“ je symetrická, můžeme v případě, kdy grupoid \mathcal{H} je izomorfní s grupoidem \mathcal{G} , říkat také, že grupoidy \mathcal{G} a \mathcal{H} jsou (navzájem) izomorfní. Označení: $\mathcal{G} \cong \mathcal{H}$.

Příklad 2.1.9 Uvažujme grupoidy $\mathcal{N} = (\mathbb{N}; +)$ a $2\mathcal{N} = (2\mathbb{N}; +)$. Pak zobrazení $f : \mathbb{N} \rightarrow \mathbb{N}$ takové, že $\forall a \in \mathbb{N}; f(a) = 2a$, je homomorfismus \mathcal{N} do \mathcal{N} , který není surjektivní.

Označme $\bar{f} : \mathbb{N} \rightarrow 2\mathbb{N}$ zobrazení, v němž opět platí, že $\forall a \in \mathbb{N}; \bar{f}(a) = 2a$. Pak platí, že \bar{f} je izomorfismus \mathcal{N} na $2\mathcal{N}$, tedy \mathcal{N} a $2\mathcal{N}$ jsou izomorfní.

Příklad 2.1.10 Ukažme, že grupoid $\mathcal{A} = (\{-1, 1\}; \cdot)$ je homomorfním obrazem grupoidu $\mathcal{Z} = (\mathbb{Z}; +)$.

Uvažujme zobrazení $f : \mathbb{Z} \rightarrow \{-1, 1\}$ takové, že

$$\forall a \in 2\mathbb{Z}; f(a) = 1, \quad \forall a \in 2\mathbb{Z} + 1; f(a) = -1.$$

Můžeme snadno ověřit, že f je homomorfismus \mathcal{Z} na \mathcal{A} . Přitom je zřejmé, že \mathcal{Z} a \mathcal{A} nejsou izomorfní.

Příklad 2.1.11 Uvažujme grupoidy $\mathcal{R} = (\mathbb{R}; +)$ a $\mathcal{R}_1 = (\mathbb{R}; \oplus)$, kde $\forall a, b \in \mathbb{R}; a \oplus b = a + b + 1$. Grupoidy \mathcal{R} a \mathcal{R}_1 jsou izomorfní, protože např. zobrazení $f : \mathbb{R} \rightarrow \mathbb{R}$ takové, že $\forall a \in \mathbb{R}; f(a) = a - 1$, je izomorfismem \mathcal{R} na \mathcal{R}_1 . Přesvědčte se.

Příklad 2.1.12 Na rozdíl od grupoidů z příkladu 2.1.9 platí, že grupoidy $\mathcal{N}_1 = (\mathbb{N}; \cdot)$ a $2\mathcal{N}_1 = (2\mathbb{N}; \cdot)$ nejsou izomorfní. Můžeme to ověřit sporem. Nechť f je izomorfismus \mathcal{N}_1 na $2\mathcal{N}_1$ a nechť $f(1) = 2x$. Pak

$$2x = f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = 2x \cdot 2x = 4x^2,$$

což ale nemůže platit pro žádné $x \in \mathbb{N}$, to je spor. Proto izomorfismus f neexistuje.

Připomeňme si, že má-li grupoid $\mathcal{G} = (G; \cdot)$ jednotkový prvek e a je-li $a \in G$, pak prvek $b \in G$ se nazývá inverzní k prvku a , platí-li $ab = e = ba$. Přitom platí, že v monoidu má každý prvek a nejvýše jeden inverzní prvek, který označujeme a^{-1} .

Věta 2.1.13 a) Homomorfní obraz komutativního grupoidu je komutativním grupoidem.

b) Homomorfní obraz pologrupy je pologrupou.

c) Homomorfní obraz grupoidu s jednotkovým prvkem je grupoidem s jednotkovým prvkem.

d) Homomorfní obraz monoidu je monoidem.

e) Jestliže f je homomorfismus grupoidu \mathcal{G} s jednotkovým prvkem na grupoid \mathcal{H} a má-li prvek $a \in G$ inverzní prvek $v \in \mathcal{G}$, pak jeho obraz $f(a)$ má inverzní prvek $v \in \mathcal{H}$.

Důkaz. Nechť f je homomorfismus grupoidu $\mathcal{G} = (G; \cdot)$ na grupoid $\mathcal{H} = (H; \circ)$.

- a) Nechť \mathcal{G} je komutativní. Uvažujme libovolné prvky $b_1, b_2 \in H$. Protože f je surjektivní, existují prvky $a_1, a_2 \in G$ takové, že $f(a_1) = b_1, f(a_2) = b_2$. Pak

$$b_1 \circ b_2 = f(a_1) \circ f(a_2) = f(a_1 \cdot a_2) = f(a_2 \cdot a_1) = f(a_2) \circ f(a_1) = b_2 \circ b_1.$$

- b) Předpokládejme, že \mathcal{G} je pologrupa a že $b_1, b_2, b_3 \in H$. Uvažujme $a_1, a_2, a_3 \in G$, pro něž $f(a_i) = b_i, i = 1, 2, 3$. Pak

$$\begin{aligned} b_1 \circ (b_2 \circ b_3) &= f(a_1) \circ (f(a_2) \circ f(a_3)) = f(a_1) \circ f(a_2 \cdot a_3) = f(a_1 \cdot (a_2 \cdot a_3)) = \\ &= f((a_1 \cdot a_2) \cdot a_3) = f(a_1 \cdot a_2) \circ f(a_3) = (f(a_1) \circ f(a_2)) \circ f(a_3) = \\ &= (b_1 \circ b_2) \circ b_3. \end{aligned}$$

- c) Předpokládejme, že grupoid \mathcal{G} má jednotkový prvek e . Jestliže $b \in H$, existuje $a \in G$ takový, že $f(a) = b$. Platí $b \circ f(e) = f(a) \circ f(e) = f(a \cdot e) = f(a) = b$. Podobně se ukáže, že $f(e) \circ b = b$, a protože b je libovolný prvek z H , platí, že \mathcal{H} má jednotkový prvek $e' = f(e)$.

- d) Plyne z b) a c).

- e) Nechť \mathcal{G} má jednotkový prvek e a nechť k prvku $a \in G$ existuje prvek $a' \in G$ takový, že $aa' = e = a'a$. Platí

$$f(a) \circ f(a') = f(a \cdot a') = f(e) = e', \quad f(a') \circ f(a) = e',$$

tedy $f(a')$ je inverzní prvek k prvku $f(a)$.

□

Poznámka 2.1.14 a) Podle důkazu části c) je vidět, že v homomorfismu f grupoidu \mathcal{G} na grupoid \mathcal{H} se jednotkový prvek e zobrazí na jednotkový prvek $f(e)$, a podle důkazu části e) v případě monoidů platí $f(a^{-1}) = (f(a))^{-1}$.

b) Žádné z tvrzení předchozí věty nelze obrátit. Např. označme $\mathcal{G} = (\mathbb{C}; \circ)$, kde $\forall a, b \in \mathbb{C}; a \circ b = a\bar{b}$, $\mathcal{H} = (\mathbb{R}_0^+; \cdot)$. Nechť $f : \mathbb{C} \rightarrow \mathbb{R}_0^+$ je zobrazení takové, že $\forall a \in \mathbb{C}; f(a) = |a|$. Pak

$$f(a \circ b) = f(a\bar{b}) = |a\bar{b}| = |a| \cdot |\bar{b}| = |a| \cdot |b| = f(a) \cdot f(b),$$

tedy f je homomorfismus \mathcal{G} do \mathcal{H} , který je navíc zřejmě surjektivní. Přitom \mathcal{H} je komutativní monoid, v němž každý prvek má inverzní prvek, ale \mathcal{G} nemá žádnou z uvedených vlastností.

2.2 Základní vlastnosti grup

Definice. Grupou nazýváme každý monoid, v němž má každý jeho prvek inverzní prvek.

Poznámka 2.2.1 a) Podle uvedené definice tedy platí, že $\mathcal{G} = (G; \cdot)$ je grupou právě tehdy, když

1. $\forall a, b, c \in G; a(bc) = (ab)c;$
2. $\exists e \in G \forall a \in G; ae = ea = a;$
3. $\forall a \in G \exists a^{-1} \in G; aa^{-1} = a^{-1}a = e.$

b) Komutativní grupu \mathcal{G} , tedy takovou, v níž platí $\forall a, b \in G; ab = ba$, budeme také nazývat **abelovská grupa**.

c) Z podmínky 3 je zřejmé, že

$$\forall a \in G; (a^{-1})^{-1} = a.$$

Jsou-li $a, b \in G$, pak

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e,$$

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = e,$$

proto v \mathcal{G} platí

$$\forall a, b \in G; (ab)^{-1} = b^{-1}a^{-1}.$$

Definice. a) Jestliže $\mathcal{G} = (G; \cdot)$ je taková grupa, že G má n prvků ($n \in \mathbb{N}$), pak řekneme, že grupa \mathcal{G} má **konečný řád n** .

b) Je-li G nekonečná, pak grupa \mathcal{G} je **nekonečného řádu**.

Věta 2.2.2 Pologrupa \mathcal{G} je grupou právě tehdy, když pro každé $a, b \in G$ jsou v \mathcal{G} řešitelné rovnice

$$ax = b, \quad ya = b.$$

Důkaz. „ \Rightarrow “: Jestliže \mathcal{G} je grupa, pak $x = a^{-1}b$ a $y = ba^{-1}$ jsou řešeními příslušných rovnic.

„ \Leftarrow “: Nechť jsou v pologrupě \mathcal{G} vždy řešitelné uvažované rovnice. Nechť $a \in G$. Pak existuje řešení rovnice $ax = a$, které označíme e . Nechť b je libovolný prvek z G a nechť $y \in G$ je takový, že $ya = b$. Platí

$$be = (ya)e = y(ae) = ya = b.$$

Analogicky se dokáže, že je-li $e' \in G$ řešením rovnice $ya = b$, pak pro každý $b \in G$ platí $e'b = b$. Přitom platí, že $e'e = e'$, $e'e = e$, tedy $e' = e$, což znamená, že e je jednotkový prvek v \mathcal{G} .

Nechť $a \in G$ a nechť a' , a'' jsou postupně řešeními rovnic $ax = e$, $ya = e$, tj. $aa' = e$, $a''a = e$. Pak

$$a' = ea' = (a''a)a' = a''(aa') = a''e = a'',$$

a tedy $a' = a'' = a^{-1}$. □

Poznámka 2.2.3 Věta 2.2.2 nám dává užitečné kritérium pro určování, zdali je konečný grupoid grupou. Je-li totiž dána Cayleyova tabulka grupy konečného řádu, pak v každém řádku a v každém sloupci se musí vyskytovat všechny její prvky. (Uvědomme si však, že tato podmínka je nutná, ale není postačující, protože nezaručuje asociativnost operace.)

Definice. Řekneme, že v grupoidu \mathcal{G} platí pravidlo o krácení, jestliže pro každé prvky $a, b, c, d \in G$ platí

$$ca = cb \implies a = b, \quad ad = bd \implies a = b.$$

Věta 2.2.4 V každé grupě platí pravidlo o krácení.

Důkaz. Nechť \mathcal{G} je grupa, $a, b, c \in G$ a nechť $ca = cb$. Víme, že k c existuje inverzní prvek c^{-1} . Platí: $ca = cb \implies c^{-1}(ca) = c^{-1}(cb) \implies a = b$.

Analogicky pro krácení zprava. □

Důsledek 2.2.5 Rovnice $ax = b$ a $ya = b$ jsou v každé grupě řešitelné jednoznačně.

Důkaz. Nechť pro $x', x'' \in G$ platí, že $ax' = b$, $ax'' = b$. Pak z $ax' = ax''$ dostaneme podle věty 2.2.4, že $x' = x''$. □

Poznámka 2.2.6 Vzhledem k tomu, že grupa \mathcal{G} má právě jeden jednotkový prvek e a že ke každému jejímu prvku a v ní existuje právě jeden inverzní prvek a^{-1} , můžeme na G zavést nulární operaci „ e “ a unární operaci „ -1 “ tak, že $e : G^0 \rightarrow G$, $e : \emptyset \mapsto e$, $-1 : G \rightarrow G$, $-1 : a \mapsto a^{-1}$ pro každý $a \in G$. Grupu \mathcal{G} pak můžeme uvažovat jako algebraickou strukturu $\mathcal{G} = (G; \cdot, e, -1)$ s jednou binární, jednou nulární a jednou unární operací, pro které platí:

1. $\forall a, b, c \in G; a(bc) = (ab)c;$
2. $\forall a \in G; ae = ea = a;$
3. $\forall a \in G; aa^{-1} = a^{-1}a = e.$

2.3 Podgrupy a normální podgrupy grup

Definice. Nechť $\mathcal{G} = (G; \cdot)$ je grupa, $\emptyset \neq A \subseteq G$. Řekneme, že podmnožina A je uzavřená vzhledem k operaci „ \cdot “, platí-li $\forall a, b \in A; ab \in A$.

Poznámka 2.3.1 Nebude-li nebezpečí nedorozumění, budeme stručněji říkat, že A je uzavřená podmnožina v \mathcal{G} . Jestliže $A \neq \emptyset$ je uzavřená podmnožina v \mathcal{G} , pak restrikce operace $\cdot : G^2 \rightarrow G$ na A^2 je binární operaci na množině A . Budeme ji nazývat *indukovanou operací* na množině A a k jejímu označení budeme používat také symbol „ \cdot “. (Je-li $f : X \rightarrow Y$ zobrazení a je-li $Z \subseteq X$, pak restrikcí f na Z rozumíme zobrazení $\bar{f} : Z \rightarrow Y$ takové, že $\forall z \in Z; \bar{f}(z) = f(z)$.)

Příklad 2.3.2 a) Množina \mathbb{N} je uzavřenou podmnožinou grupy $\mathcal{Z} = (\mathbb{Z}; +)$.

b) Množina $\{-1, 1\}$ je uzavřenou podmnožinou grupy $\mathcal{Q}_0 = (\mathbb{Q}_0; \cdot)$.

c) Množina $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ pro $1 < n \in \mathbb{N}$ není uzavřenou podmnožinou v grupě $\mathcal{Z} = (\mathbb{Z}; +)$.

Definice. Neprázdná podmnožina A grupy \mathcal{G} se nazývá *podgrupou* grupy \mathcal{G} , je-li uzavřenou podmnožinou v \mathcal{G} a je-li grupou vzhledem k indukované operaci. Skutečnost, že A je podgrupou grupy \mathcal{G} , budeme označovat $A \leq \mathcal{G}$.

Příklad 2.3.3 a) Uzavřená podmnožina \mathbb{N} grupy \mathcal{Z} není podgrupou v \mathcal{Z} .

b) $\{-1, 1\} \leq \mathcal{Q}_0$.

c) Přestože \mathbb{Z}_6 je grupou vzhledem ke sčítání modulo 6, neplatí $\mathbb{Z}_6 \leq \mathcal{Z}$.

Věta 2.3.4 Podmnožina A grupy \mathcal{G} je podgrupou v \mathcal{G} právě tehdy, když platí:

1. $\forall a, b \in A; ab \in A$;
2. $e \in A$;
3. $\forall a \in A; a^{-1} \in A$.

Důkaz. Platí, že pro $A \leq \mathcal{G}$ je jednotkový prvek podgrupy A roven jednotkovému prvku e grupy \mathcal{G} a že pro každý prvek $a \in A$ je jeho inverzní prvek v podgrupě A roven inverznímu prvku a^{-1} v grupě \mathcal{G} . Asociativnost násobení v A je dědičnou vlastností. \square

Poznámka 2.3.5 a) Označme $E = \{e\}$. Je zřejmé, že $E \leq \mathcal{G}$, $G \leq \mathcal{G}$. Podgrupu E budeme nazývat *jednotkovou*. Jednotková podgrupa a celá grupa \mathcal{G} se nazývají společně *triviální podgrupy* grupy \mathcal{G} .

b) Předpokládáme-li ve větě 2.3.4, že $A \neq \emptyset$, pak podmínu 2 můžeme vynechat, protože ji lze v tomto případě odvodit z podmínek 1 a 3.

c) Víme, že grupu \mathcal{G} můžeme také uvažovat jako algebraickou strukturu $\mathcal{G} = (G; \cdot, e, -1)$. V takovém případě pak podle věty 2.3.4 platí, že podmnožina A grupy \mathcal{G} je podgrupou v \mathcal{G} , právě když A je uzavřená vzhledem ke všem operacím „ \cdot “, „ e “, „ -1 “.

Ukažme, že podmínky z věty 2.3.4 můžeme v případě neprázdné podmnožiny nahradit jedinou podmínkou.

Věta 2.3.6 Jestliže \mathcal{G} je grupa, $\emptyset \neq A \subseteq G$, pak $A \leq \mathcal{G}$ právě tehdy, když platí

$$\forall a, b \in A; ab^{-1} \in A.$$

Důkaz. „ \Rightarrow “: Nechť $A \leq \mathcal{G}$, $a, b \in A$. Pak $b^{-1} \in A$, a tedy $ab^{-1} \in A$.

„ \Leftarrow “: Nechť $a \in A$. ($A \neq \emptyset$, proto takový prvek existuje.) Pak $e = aa^{-1} \in A$, tedy také $a^{-1} = ea^{-1} \in A$. Jestliže $a, b \in A$, pak $a, b^{-1} \in A$, a proto $ab = a(b^{-1})^{-1} \in A$. \square

Věta 2.3.7 Průnik libovolného systému podgrup grupy \mathcal{G} je také podgrupou v \mathcal{G} .

Důkaz. a) Nechť $\{A_\alpha; \alpha \in I\}$ je neprázdný systém podgrup $A_\alpha \leq \mathcal{G}$ a nechť $A = \bigcap_{\alpha \in I} A_\alpha$.

Je zřejmé, že $A \neq \emptyset$, protože A obsahuje alespoň jednotkový prvek e . Nechť $a, b \in A$. Pak pro každé $\alpha \in I$ platí, že $a, b \in A_\alpha$, tedy také $ab^{-1} \in A_\alpha$, a proto $ab^{-1} \in A$.

b) Pro prázdný systém podmnožin množiny G je průnik tohoto systému podle obvyklé definice roven G . \square

Právě dokázaná věta ukazuje na korektnost následující definice.

Definice. a) Nechť M je podmnožina grupy \mathcal{G} . Pak podgrupu v \mathcal{G} , která je průnikem všech podgrup v \mathcal{G} obsahujících M , nazveme *podgrupou v \mathcal{G} generovanou množinou M* a označíme ji $\langle M \rangle$. Pro $M = \{a_1, a_2, \dots, a_n\}$ píšeme také $\langle M \rangle = \langle a_1, a_2, \dots, a_n \rangle$.

b) Jestliže $\langle M \rangle = G$, pak M se nazývá *množina generátorů* grupy \mathcal{G} (nebo říkáme, že M *generuje* grupu \mathcal{G}).

c) Jestliže $a \in G$, pak $\langle a \rangle$ se nazývá *cyklická podgrupa* v \mathcal{G} generovaná prvkem a .

d) Grupa \mathcal{G} se nazývá *cyklická*, existuje-li v ní prvek a takový, že $\langle a \rangle = G$.

Vidíme, že podgrupa generovaná podmnožinou grupy se definuje analogicky jako lineární obal podmnožiny vektorového prostoru. Přitom je známo, že lineární obal neprázdné podmnožiny se skládá právě ze všech lineárních kombinací vektorů z této podmnožiny. Ukážeme si, že podobně přehledným způsobem lze charakterizovat i prvky podgrupy generované podmnožinou grupy. Nejprve rozšíříme pojem mocniny prvku. Připomeňme, že

v části 2.1 jsme definovali přirozené mocniny prvků pologrupy a celé nezáporné mocniny prvků monoidu. Pro prvky grupy můžeme zavést i celé záporné mocniny.

Definice. Nechť \mathcal{G} je grupa a nechť $a \in G$. Jestliže $n \in \mathbb{N}$, pak $(-n)$ -tou mocninou prvku a rozumíme prvek $a^{-n} \in G$ takový, že $a^{-n} = (a^n)^{-1}$.

Poznámka 2.3.8 Ukažme, že pro každé $n \in \mathbb{N}$ platí $a^{-n} = (a^n)^{-1}$. Skutečně

$$a^n \cdot (a^{-1})^n = a^{n-1} \cdot a \cdot a^{-1} \cdot (a^{-1})^{n-1} = a^{n-1} \cdot (a^{-1})^{n-1} = \dots = e.$$

Věta 2.3.9 Jestliže a, b jsou prvky grupy \mathcal{G} , $m, n \in \mathbb{Z}$, pak platí:

1. $a^m \cdot a^n = a^{m+n}$;
2. $(a^m)^n = a^{mn}$;
3. Jestliže $ab = ba$, pak $(ab)^n = a^n b^n$.

Důkaz. Podle věty 2.1.6 a za ní následující poznámky víme, že uvedené vztahy platí pro $m, n \geq 0$. Zbývá tedy ověřit jejich platnost i pro zbyvající případy.

1. a) Nechť $m > 0$, $n < 0$. Pak $n' = -n > 0$. Jestliže $m \geq n'$, pak $m - n' \geq 0$ a $m = (m - n') + n'$. Dostáváme

$$a^m \cdot a^n = a^m \cdot a^{-n'} = a^{(m-n')+n'} \cdot a^{-n'} = a^{m-n'} \cdot a^{n'} \cdot a^{-n'} = a^{m-n'} \cdot e = a^{m-n'} = a^{m+n}.$$

Nechť $m < n'$. Pak $n' - m > 0$, $n' = m + (n' - m)$ a platí

$$\begin{aligned} a^m \cdot a^n &= a^m \cdot a^{-n'} = a^m \cdot (a^{-1})^{n'} = a^m \cdot (a^{-1})^{m+(n'-m)} = a^m \cdot (a^{-1})^m \cdot (a^{-1})^{n'-m} = \\ &= (a^{-1})^{n'-m} = a^{m-n'} = a^{m+n}. \end{aligned}$$

b) Nechť $m < 0$, $n < 0$. Pak $m' = -m > 0$, $n' = -n > 0$. Platí

$$\begin{aligned} a^{m+n} &= a^{(-m') + (-n')} = a^{-(m'+n')} = (a^{-1})^{m'+n'} = (a^{-1})^{m'} \cdot (a^{-1})^{n'} = \\ &= a^{-m'} \cdot a^{-n'} = a^m \cdot a^n. \end{aligned}$$

2. a) Nechť $m > 0$, $n < 0$, $n' = -n > 0$. Pak

$$a^{mn} = a^{m(-n')} = a^{-mn'} = (a^{-1})^{mn'} = ((a^{-1})^m)^{n'} = ((a^m)^{-1})^{n'} = (a^m)^{-n'} = (a^m)^n.$$

b) Nechť $m < 0$, $n < 0$, $m' = -m > 0$, $n' = -n > 0$. Pak

$$a^{mn} = a^{(-m)(-n)} = a^{m'n'} = (a^{m'})^{n'} = (a^{-m})^{n'} = ((a^m)^{-1})^{n'} = (a^m)^{-n'} = (a^m)^n.$$

3. Nechť $ab = ba$, $n < 0$, $n' = -n > 0$. Pak

$$\begin{aligned} (ab)^n &= (ab)^{-n'} = (ba)^{-n'} = ((ba)^{n'})^{-1} = (b^{n'} a^{n'})^{-1} = (a^{n'})^{-1} (b^{n'})^{-1} = \\ &= a^{-n'} b^{-n'} = a^n b^n. \end{aligned}$$

□

Poznámka 2.3.10 Na základě věty 2.3.9(1) je zřejmé, že množina $\{a^n; n \in \mathbb{Z}\}$ je podgrupou grupy \mathcal{G} a že a je prvkem této podgrupy. Přitom každá podgrupa v \mathcal{G} , která obsahuje a , musí obsahovat také všechny celé mocniny prvku a . Platí tedy, že

$$\langle a \rangle = \{a^n; n \in \mathbb{Z}\}.$$

Navíc (opět podle věty 2.3.9(1)) vidíme, že $\langle a \rangle$ je abelovská.

Definice. Jsou-li všechny celé mocniny prvku $a \in G$ navzájem různé, pak řekneme, že a má nekonečný rád. V opačném případě říkáme, že prvek a je konečného rádu.

Poznámka 2.3.11 Nechť prvek $a \in G$ je konečného rádu. Pak existují $k, l \in \mathbb{Z}$, $k > l$, takové, že $a^k = a^l$. Platí tedy $a^{k-l} = e$, kde $k - l > 0$. Pro a proto existují mocniny s přirozenými exponenty, které jsou rovny e .

Definice. Je-li prvek $a \in G$ konečného rádu, pak jeho rádem rozumíme nejmenší číslo $n \in \mathbb{N}$ takové, že $a^n = e$.

Věta 2.3.12 Rád prvku a je roven rádu cyklické podgrupy $\langle a \rangle$.

Důkaz. Pro prvky nekonečného rádu je tvrzení zřejmé.

Nechť tedy prvek a má konečný rád n . Pak mocniny $e = a^0, a = a^1, a^2, \dots, a^{n-1}$ jsou navzájem různé. Nechť $k \in \mathbb{Z}$. Pak existují $q, r \in \mathbb{Z}$ taková, že $k = nq + r$, kde $0 \leq r < n$. Protože $a^n = e$, dostáváme

$$a^k = a^{nq+r} = (a^n)^q \cdot a^r = a^r,$$

což znamená, že každý prvek z $\langle a \rangle$ je obsažen v množině $\{e, a, a^2, \dots, a^{n-1}\}$. Tedy rád podgrupy $\langle a \rangle$ je roven n . \square

Nyní už můžeme řešit otázku charakterizace prvků podgrupy $\langle M \rangle$ grupy \mathcal{G} generované libovolnou podmnožinou $M \subseteq G$.

Věta 2.3.13 Nechť M je podmnožina grupy \mathcal{G} .

a) Jestliže $M = \emptyset$, pak $\langle M \rangle = E$.

b) Jestliže $M \neq \emptyset$, pak $\langle M \rangle = \{a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}; n \in \mathbb{N}, a_i \in M, \varepsilon_i = \pm 1, i = 1, \dots, n\}$.

Důkaz. a) Pro $M = \emptyset$ tvrzení plyne z faktu, že jednotkový prvek e patří do každé podgrupy grupy \mathcal{G} .

b) Nechť $M \neq \emptyset$ a $A = \{a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}; n \in \mathbb{N}, a_i \in M, \varepsilon_i = \pm 1, i = 1, \dots, n\}$. Zřejmě $M \subseteq A$. Ukažme, že $A \leq \mathcal{G}$. Nechť $a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}, b_1^{\eta_1} \dots b_m^{\eta_m} \in A$. Pak

$$(a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n})(b_1^{\eta_1} \dots b_m^{\eta_m})^{-1} = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} \cdot b_m^{-\eta_m} \dots b_1^{-\eta_1} \in A,$$

tedy podle věty 2.3.6 platí, že A je podgrupou v \mathcal{G} .

Zbývá ukázat, že A je nejmenší podgrupa v \mathcal{G} obsahující M . Nechť $B \subseteq \mathcal{G}$, $M \subseteq B$. Pak pro libovolný prvek $a = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} \in A$ platí, že $a_1^{\varepsilon_1}, \dots, a_n^{\varepsilon_n} \in B$, a tedy také $a \in B$. Proto $A = \langle M \rangle$. \square

Důsledek 2.3.14 Jestliže $M \neq \emptyset$ je množinou generátorů grupy \mathcal{G} , pak každý prvek z G lze vyjádřit ve tvaru součinu konečného počtu prvků z M a prvků inverzních k prvkům z M .

Příklad 2.3.15 Každá z množin $\{2, 3\}$, $\{1\}$, $\{-1\}$ je množinou generátorů grupy $\mathcal{Z} = (\mathbb{Z}; +)$. (Tedy mj. \mathcal{Z} je cyklická grupa.) Množina $\{2\}$ není množinou generátorů této grupy.

Operaci násobení prvků v libovolném grupoidu \mathcal{G} nyní rozšíříme na násobení podmnožin.

Definice. Jestliže \mathcal{G} je grupoid a $A, B \subseteq G$, pak jejich *součinem* AB rozumíme podmnožinu v G takovou, že

$$AB = \{ab; a \in A, b \in B\}.$$

Jestliže $a \in G$, $B \subseteq G$, pak místo $\{a\}B$ píšeme stručně aB a místo $B\{a\}$ píšeme Ba .

Příklad 2.3.16 Uvažujme grupu $\mathcal{Z}_6 = (\mathbb{Z}_6; +)$ a její podmnožiny $A = \{1, 3, 4\}$, $B = \{2, 5\}$. Pak $A + B = \{3, 0, 5, 2\}$.

Definice. Jestliže H je podgrupa grupy \mathcal{G} , $a \in G$, pak *levou třídou* (resp. *pravou třídou*) prvku a podle H nazýváme množinu aH (resp. Ha).

Věta 2.3.17 Systém všech levých tříd prvků grupy \mathcal{G} podle podgrupy H je rozkladem množiny G .

(Tento rozklad $(aH; a \in G)$ nazýváme *levý rozklad grupy \mathcal{G} podle podgrupy H* a značíme jej $G/_l H$. Protože $eH = H$, platí, že $H \in G/_l H$.)

Důkaz. Jestliže $a \in G$, pak platí (protože $e \in H$) $a = ea \in aH$. Tedy každý prvek z G leží ve své třídě, a proto $aH \neq \emptyset$ a $\bigcup_{a \in G} aH = G$.

Zbývá ověřit, že libovolné dvě levé třídy jsou buď disjunktní nebo splývají. Nechť $a, b \in G$, $aH \cap bH \neq \emptyset$, a nechť $c \in aH \cap bH$. Pak existují prvky $h_1, h_2 \in H$ takové, že $c = ah_1 = bh_2$. Pak platí mj. $a = bh_2h_1^{-1}$. Nechť $x = ah$ je libovolný prvek z aH . Pak

$$x = ah = (bh_2h_1^{-1})h = b(h_2h_1^{-1}h),$$

a protože $h_2 h_1^{-1} h \in H$, dostáváme $x \in bH$, tedy $aH \subseteq bH$.

Analogicky se dokáže, že $bH \subseteq aH$, tedy platí $aH = bH$. \square

Poznámka 2.3.18 Podobně bychom mohli ověřit, že také systém všech pravých tříd prvků grupy \mathcal{G} podle podgrupy H je rozkladem na G . Rozklad $(Ha; a \in G)$ nazýváme *pravý rozklad grupy \mathcal{G} podle podgrupy H* a značíme jej G/pH . Opět platí, že $H \in G/pH$.

Věta 2.3.19 Nechť $H \leq \mathcal{G}$, $a, b \in G$. Pak

$$a) \quad aH = bH \iff b^{-1}a \in H;$$

$$b) \quad Ha = Hb \iff ab^{-1} \in H.$$

Důkaz. a) Nechť $aH = bH$. Pak $a \in bH$, tzn., že existuje prvek $h \in H$ takový, že $a = bh$, a tedy $b^{-1}a = h \in H$.

Obráceně, nechť $b^{-1}a = h \in H$. Pak $a = bh$, a tedy $a \in aH \cap bH$. To ovšem podle věty 2.3.17 znamená, že $aH = bH$.

b) Důkaz je analogický. \square

Připomeňme si, že dvě množiny A a B se nazývají *ekvivalentní*, existuje-li alespoň jedno bijektivní zobrazení jedné z nich na druhou. Je zřejmé, že vztah „být ekvivalentní s“ je relací ekvivalence. Pro dvě konečné množiny platí, že jsou ekvivalentní, právě když mají stejný počet prvků.

Věta 2.3.20 Pro libovolnou podgrupu H grupy \mathcal{G} platí, že rozklady G/lH a G/pH jsou ekvivalentní.

Důkaz. Nechť $a, b \in G$. Podle věty 2.3.19 platí, že $aH = bH \iff b^{-1}a \in H$ a $Ha^{-1} = Hb^{-1} \iff a^{-1}(b^{-1})^{-1} \in H$. Přitom ale $a^{-1}(b^{-1})^{-1} = a^{-1}b = (b^{-1}a)^{-1}$, a protože $H \leq \mathcal{G}$, platí $(b^{-1}a)^{-1} \in H \iff b^{-1}a \in H$. To znamená, že $aH = bH$ právě tehdy, když $Ha^{-1} = Hb^{-1}$. Proto zobrazení $f : G/lH \rightarrow G/pH$ takové, že pro každé $a \in G$ platí $f(aH) = Ha^{-1}$, je bijektivní. \square

Definice. a) Mají-li rozklady G/lH a G/pH nekonečný počet tříd, pak řekneme, že podgrupa H je *nekonečného indexu*.

b) Jestliže rozklady G/lH a G/pH mají konečný počet tříd, pak řekneme, že H má *konečný index*. Počet tříd každého z uvedených rozkladů se nazývá *index podgrupy H* .

Věta 2.3.21 Nechť $H \leq \mathcal{G}$, $a, b \in G$. Pak levá třída aH je ekvivalentní s pravou třídou Hb . (Tedy v případě konečné podgrupy H má každá levá třída a každá pravá třída podle H stejný počet prvků jako H).

Důkaz. Definujme zobrazení $f : H \rightarrow aH$ tak, že $f(h) = ah$ pro každý prvek $h \in H$. Je zřejmé, že f je surjekce. Nechť $h, h' \in H$ a nechť $f(h) = f(h')$, tj. $ah = ah'$. Po zkrácení prvkem a dostáváme $h = h'$. Tedy f je injekce.

Analogicky můžeme sestrojit bijekci $g : H \rightarrow Hb$. Pak ale platí, že $f^{-1} \circ g$ je bijekcí aH na Hb . \square

Věta 2.3.22 (Lagrangeova věta) Nechť \mathcal{G} je konečná grupa řádu n , H její podgrupa řádu k a nechť index H je roven i . Pak platí $n = k \cdot i$.

Důkaz. Podle věty 2.3.17 platí, že levé třídy podle podgrupy H tvoří rozklad množiny G . Podle věty 2.3.21 má každá levá třída rozkladu stejný počet prvků jako podgrupa H , tedy k . Podle předpokladu je počet navzájem různých levých tříd roven i . Tedy vskutku platí $n = k \cdot i$. \square

Poznámka 2.3.23 Lagrangeova věta má mj. velký praktický význam při hledání podgrup konečné grupy. Podle této věty totiž řád podgrupy dělí řád grupy, a tedy můžeme předem eliminovat všechny podmnožiny s počty prvků, které nedělí řád grupy.

Důsledek 2.3.24 Jestliže \mathcal{G} je konečná grupa a $a \in G$, pak řád prvku a dělí řád grupy \mathcal{G} .

Důkaz. Plyne z vět 2.3.12 a 2.3.22. \square

Příklad 2.3.25 Grupa $\mathcal{Z}_p = (\mathbb{Z}_p; +)$, kde p je prvočíslo, nemá netriviální podgrupy. Proto řád každého prvku $a \neq 0$ je roven číslu p .

Ke každé podgrupě H grupy \mathcal{G} jsme sestrojili dva rozklady, G/lH a G/pH . Je zřejmé, že v abelovské grupě vždy platí $G/lH = G/pH$. Zde dokonce pro každý prvek $a \in G$ platí $aH = Ha$. V nekomutativní grupě však pro podgrupu H může platit, že G/lH a G/pH jsou různé rozklady.

Příklad 2.3.26 Nechť S_3 je množina všech permutací na množině $\{1, 2, 3\}$. Pak $\mathcal{S}_3 = (S_3; \circ)$, kde „ \circ “ je operace skládání permutací, je nekomutativní grupa. Pro množinu $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$ platí $H \leq S_3$. Můžeme se snadno přesvědčit, že $S_3/lH \neq S_3/pH$.

Definice. Řekneme, že podgrupa H grupy \mathcal{G} je *normální v \mathcal{G}* , jestliže $G/lH = G/pH$.

Poznámka 2.3.27 a) Místo názvu „normální podgrupa“ se někdy používá také označení „normální dělitel“ nebo „invariantní podgrupa“.

b) V případě normální podgrupy H budeme společný levý a pravý rozklad označovat také stručněji G/H .

Věta 2.3.28 Jestliže H je podgrupa grupy \mathcal{G} , pak následující podmínky jsou ekvivalentní:

1. H je normální v \mathcal{G} .
2. $\forall a \in G; aH = Ha$.
3. $\forall a \in G, h \in H; aha^{-1} \in H$.

Důkaz. $1 \implies 2$: Podmínka 1 je formálně slabší než podmínka 2, protože podle ní pro každý prvek $a \in G$ existují prvky $b, c \in G$ takové, že $aH = Hb$, $Ha = cH$. Ukážeme však, že obě podmínky jsou rovnocenné. Nechť tedy H je normální podgrupa v \mathcal{G} a $a \in G$. Vzhledem k tomu, že $a \in aH \cap Ha$ a že podle předpokladu $Ha \in G/_l H$, musí podle věty 2.3.17 platit, že $aH = Ha$.

$2 \implies 3$: Nechť pro každý $a \in G$ platí $aH = Ha$. Pak pro libovolný prvek $h \in H$ existuje $h' \in H$ takový, že $ah = h'a$, tzn. $aha^{-1} = h' \in H$.

$3 \implies 2$: Nechť pro každé prvky $a \in G$ a $h \in H$ platí $aha^{-1} \in H$. Nechť $ah \in aH$. Protože $aha^{-1} = h_1 \in H$, platí $ah = h_1 a \in Ha$, a tedy $aH \subseteq Ha$.

Jestliže $ha \in Ha$, pak $a^{-1}ha = a^{-1}h(a^{-1})^{-1} \in H$, tedy $a^{-1}ha = h_2 \in H$, což znamená, že $ha = ah_2$. Proto $Ha \subseteq aH$, a tedy celkově $aH = Ha$.

$2 \implies 1$: Triviální. □

Poznámka 2.3.29 a) Jsou-li c, d prvky grupy \mathcal{G} , pak prvek d se nazývá *konjugovaný* s prvkem c , existuje-li prvek $x \in G$ takový, že $d = xc x^{-1}$. Podle věty 2.3.28 tedy platí, že podgrupa H je normální v \mathcal{G} právě tehdy, obsahuje-li s každým svým prvkem také všechny prvky s ním konjugované.

b) Skutečnost, že H je normální podgrupa v \mathcal{G} , budeme označovat $H \trianglelefteq \mathcal{G}$.

c) Pro každou grupu \mathcal{G} platí, že $E \trianglelefteq \mathcal{G}$, $G \trianglelefteq \mathcal{G}$.

Věta 2.3.30 Jestliže podgrupa H grupy \mathcal{G} má index 2, pak platí $H \trianglelefteq \mathcal{G}$.

Důkaz. Podle předpokladu existují právě dvě levé a dvě pravé třídy \mathcal{G} podle H . V obou případech jsou to třídy H a $G \setminus H$, tedy levý a pravý rozklad se sobě rovnají. □

Definice. Nechť \mathcal{G} je grupa a $H \leq \mathcal{G}$, $K \leq \mathcal{G}$. Pak spojením $H \vee K$ těchto podgrup rozumíme nejmenší podgrupu v \mathcal{G} obsahující obě podgrupy H a K . (Pomocí dříve zavedené symboliky tedy $H \vee K = \langle H \cup K \rangle$.)

Podle věty 2.3.13 umíme obecně vyjádřit prvky, které patří do podgrupy $\langle M \rangle$ generované neprázdnou podmnožinou $M \subseteq G$. Pro případ spojení dvou podgrup můžeme toto vyjádření zjednodušit.

Věta 2.3.31 Jestliže $H \leq \mathcal{G}$, $K \leq \mathcal{G}$, pak

$$H \vee K = \{a_1 b_1 a_2 b_2 \dots a_m b_m; m \in \mathbb{N}, a_i \in H, b_i \in K, i = 1, 2, \dots, m\}.$$

Důkaz. Podle věty 2.3.13 platí, že prvek $c \in G$ patří do $\langle H \cup K \rangle$ právě tehdy, když $c = c_1^{\varepsilon_1} c_2^{\varepsilon_2} \dots c_n^{\varepsilon_n}$, kde $n \in \mathbb{N}$, $c_i \in H \cup K$, $\varepsilon_i = \pm 1$, $i = 1, 2, \dots, n$. Pokud $c_i \in H$, pak také $c_i^{\varepsilon_i} \in H$. Podobně pro K . Vynásobením vedle sebe zapsaných prvků z H a vedle sebe zapsaných prvků z K dostaneme prvek c zapsaný ve tvaru součinu z formulace věty. \square

Ukažme si nyní, že v případě normálních podgrup můžeme tento výsledek ještě zjednodušit.

Věta 2.3.32 Jestliže $H \trianglelefteq \mathcal{G}$, $K \trianglelefteq \mathcal{G}$, pak $H \vee K = HK = KH$.

Důkaz. Nechť $H \trianglelefteq \mathcal{G}$, $K \trianglelefteq \mathcal{G}$, $c \in H \vee K$. Podle předchozí věty platí $c = a_1 b_1 \dots a_m b_m$, kde $a_i \in H$, $b_i \in K$, $i = 1, \dots, m$. Důkaz provedeme matematickou indukcí podle m .

Pro $m = 1$ je tvrzení triviální, protože $a_1 b_1 \in HK$.

Nechť tedy $m > 1$ a nechť tvrzení platí pro $m - 1$. Pak podle indukčního předpokladu $a_1 b_1 \dots a_{m-1} b_{m-1} = a' b'$, kde $a' \in H$, $b' \in K$. Protože $b' H = H b'$, existuje $a'_m \in H$ takový, že $b' a_m = a'_m b'$. Tedy

$$c = a_1 b_1 \dots a_m b_m = a' b' a_m b_m = a' a'_m b' b_m,$$

a položíme-li $a = a' a'_m$, $b = b' b_m$, platí $c = ab \in HK$, tzn. $H \vee K \subseteq HK$. Protože $HK \subseteq H \vee K$ pro libovolné podgrupy H a K , dostáváme $H \vee K = HK$.

Přitom $H \vee K = K \vee H$, tedy platí také $H \vee K = KH$. \square

Poznámka 2.3.33 Pozorný čtenář si jistě povšimnul, že v důkazu jsme použili normálnost jen jedné z podgrup H a K .

Definice. Jestliže $H_\alpha \leq \mathcal{G}$ ($\alpha \in I$), pak spojením podgrup H_α rozumíme podgrupu $\left\langle \bigcup_{\alpha \in I} H_\alpha \right\rangle$ v \mathcal{G} , kterou označíme $\bigvee_{\alpha \in I} H_\alpha$. V případě konečného počtu podgrup H_1, \dots, H_n používáme označení (podobně jako pro dvě podgrupy) $H_1 \vee \dots \vee H_n$.

Věta 2.3.34 a) Průnik libovolného systému normálních podgrup grupy \mathcal{G} je normální podgrupou v \mathcal{G} .

b) Spojení konečného počtu normálních podgrup grupy \mathcal{G} je normální podgrupou v \mathcal{G} .

Důkaz. a) Nechť $H_\alpha \trianglelefteq \mathcal{G}$, $\alpha \in I$, $H = \bigcap_{\alpha \in I} H_\alpha$. Podle věty 2.3.7 platí, že $H \trianglelefteq \mathcal{G}$. Nechť $a \in G$, $h \in H$. Pak pro každý $\alpha \in I$ je $h \in H_\alpha$, tedy také pro každý $\alpha \in I$ je $aha^{-1} \in H_\alpha$, a to znamená, že $aha^{-1} \in H$. Proto podle věty 2.3.28 platí, že podgrupa H je normální v \mathcal{G} .

b) Nechť jsou nejdříve dány dvě normální podgrupy H_1 a H_2 v \mathcal{G} . Podle věty 2.3.32 platí, že $H_1 \vee H_2 = H_1 H_2$. Uvažujme $a \in G$, $h_1 \in H_1$, $h_2 \in H_2$. Pak

$$ah_1 h_2 a^{-1} = ah_1 a^{-1} ah_2 a^{-1} \in H_1 H_2,$$

a tedy $H_1 \vee H_2 \trianglelefteq \mathcal{G}$.

Uvažujme nyní normální podgrupy H_1, H_2, \dots, H_n ($n \geq 2$) v \mathcal{G} . Důkaz toho, že $H_1 \vee H_2 \vee \dots \vee H_n \trianglelefteq \mathcal{G}$ provedeme indukcí.

Pro $n = 2$ jsme tvrzení právě dokázali. Nechť $n > 2$ a nechť tvrzení platí pro $n - 1$. Pak $H = H_1 \vee H_2 \vee \dots \vee H_{n-1} \trianglelefteq \mathcal{G}$, a tedy také $H_1 \vee H_2 \vee \dots \vee H_{n-1} \vee H_n = H \vee H_n \trianglelefteq \mathcal{G}$. \square

Připomeňme si nyní, že je-li N normální podgrupa v grupě \mathcal{G} , pak společný levý a pravý rozklad \mathcal{G} podle N značíme G/N .

Věta 2.3.35 Nechť \mathcal{G} je grupa a $N \trianglelefteq \mathcal{G}$. Pro libovolné prvky $a, b \in G$ položme $aN \cdot bN = abN$. Pak platí, že „ \cdot “ je binární operace na faktorové množině G/N a $G/N = (G/N; \cdot)$ je grupa.

Důkaz. Ukažme nejdříve, že v definici operace násobení pro třídy rozkladu podle N nezáleží na tom, které prvky z násobených tříd jsme si k zápisu těchto tříd vybrali (neboli že definice součinu těchto tříd nezávisí na výběru reprezentantů těchto tříd).

Nechť $a, a_1, b, b_1 \in G$ jsou takové, že $aN = a_1 N$, $bN = b_1 N$. Pak podle věty 2.3.19 platí $a^{-1} a_1 \in N$, $b^{-1} b_1 \in N$. Přitom

$$(ab)^{-1} (a_1 b_1) = b^{-1} a^{-1} a_1 b_1 = b^{-1} a^{-1} a_1 b b^{-1} b_1.$$

Tedy z $a^{-1} a_1 \in N$ a z normálnosti N vyplývá $b^{-1} (a^{-1} a_1) b \in N$. Navíc $b^{-1} b_1 \in N$, a proto dostáváme, že

$$[b^{-1} (a^{-1} a_1) b] (b^{-1} b_1) \in N.$$

Podle věty 2.3.19 tedy platí $abN = a_1 b_1 N$, což znamená, že definice násobení tříd grupy \mathcal{G} podle N je korektní.

Jestliže $a, b, c \in G$, pak

$$aN \cdot (bN \cdot cN) = aN \cdot bcN = a(bc)N = (ab)cN = abN \cdot cN = (aN \cdot bN) \cdot cN,$$

a tedy grupoid $(G/N; \cdot)$ je pologrupou. Jednotkovým prvkem v této pologrupě je normální podgrupa N . ($N \in G/N$, protože např. $N = eN$.) Pro libovolný $a \in G$ totiž platí

$$N \cdot aN = eN \cdot aN = eaN = aN, \quad aN \cdot N = aN.$$

Pro $aN \in G/N$ navíc platí

$$aN \cdot a^{-1} N = aa^{-1} N = eN = N, \quad a^{-1} N \cdot aN = N,$$

tedy ke každé třídě $aN \in G/N$ existuje inverzní třída $(aN)^{-1} \in G/N$ a platí $(aN)^{-1} = a^{-1}N$. \square

Definice. Grupa \mathcal{G}/N z věty 2.3.35 se nazývá *faktorová* (nebo *podílová*) *grupa* grupy \mathcal{G} podle normální podgrupy N .

Příklad 2.3.36 Uvažujme podgrupu $4\mathbb{Z} = \{4a; a \in \mathbb{Z}\}$ grupy $\mathcal{Z} = (\mathbb{Z}; +)$. Protože \mathcal{Z} je abelovská grupa, je $4\mathbb{Z}$ samozřejmě normální podgrupou v \mathcal{Z} . Pro faktorovou grupu $\mathcal{Z}/4\mathbb{Z} = (\mathbb{Z}/4\mathbb{Z}; \oplus)$ platí, že $\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$ a že sčítání je dán tabulkou:

\oplus	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

Poznámka 2.3.37 Požadavek normálnosti podgrupy N ve větě 2.3.35 je nutný, protože v opačném případě bychom nedefinovali operaci násobení tříd (např. levých) korektně a výsledek by závisel na výběru reprezentantů z těchto tříd.

Skutečně, nechť $H \leq \mathcal{G}$, ale nechť přitom neplatí $H \trianglelefteq \mathcal{G}$. Pak existují prvky $g \in G$ a $h \in H$ takové, že $g^{-1}hg \notin H$, tedy $gH \neq hgH$. Pokud bychom definovali násobení levých tříd \mathcal{G} podle H stejně jako ve větě 2.3.35, pak by platilo $eH = hH$ (tzn. e a h patří do téže třídy) a současně $eH \cdot gH = egH = gH$, $hH \cdot gH = hgH$, tedy $eH \cdot gH \neq hH \cdot gH$ a násobení by tak nebylo jednoznačné.

2.4 Věty o izomorfismu grup

Definice. a) Nechť $\mathcal{G} = (G; \cdot)$ a $\mathcal{G}' = (G'; \cdot)$ jsou grupy a $f : G \longrightarrow G'$ zobrazení. Pak f se nazývá *homomorfismus grupy* \mathcal{G} do grupy \mathcal{G}' , jestliže pro každé $a, b \in G$ platí $f(ab) = f(a)f(b)$.

b) Jestliže homomorfismus f je bijektivní, pak se nazývá *izomorfismus* \mathcal{G} na \mathcal{G}' .

Poznámka 2.4.1 Vidíme tedy, že homomorfismus grupy \mathcal{G} do grupy \mathcal{G}' se definuje stejně jako homomorfismus grupoidu \mathcal{G} do grupoidu \mathcal{G}' , tzn. že se pro něj vyžaduje jen přenášení binární operace násobení. Grupu však můžeme chápout, jak už víme, také jako algebraickou strukturu s jednou binární, jednou nulární a jednou unární operací. Je tedy otázka, zda je použitá definice homomorfismu dostatečná. Pozitivní odpověď je obsažena v následující větě.

Věta 2.4.2 Nechť f je homomorfismus grupy \mathcal{G} do grupy \mathcal{G}' a nechť e je jednotkový prvek grupy \mathcal{G} a e' je jednotkový prvek grupy \mathcal{G}' . Pak platí:

- a) $f(e) = e'$;
- b) $\forall a \in G; f(a^{-1}) = (f(a))^{-1}$.

Důkaz. a) Platí $f(e) = f(e \cdot e) = f(e) \cdot f(e)$, a tedy

$$e' = f(e)(f(e))^{-1} = f(e)f(e)(f(e))^{-1} = f(e).$$

b) Pro libovolný prvek $a \in G$ platí:

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e', \quad f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e',$$

tzn. $f(a^{-1}) = (f(a))^{-1}$. □

Poznámka 2.4.3 Pokud by f byl surjektivní homomorfismus (tzn. \mathcal{G}' by byla homomorfním obrazem \mathcal{G}), pak by tvrzení věty 2.4.2 bylo důsledkem vět, které se vztahují k vlastnostem homomorfismů grupoidů. Věta 2.4.2 však platí pro všechny homomorfismy grup.

Definice. Nechť f je homomorfismus grupy \mathcal{G} do grupy \mathcal{G}' a nechť e' je jednotkový prvek v \mathcal{G}' . Pak množinu $\text{Ker } f = \{a \in G; f(a) = e'\}$ nazýváme jádro homomorfismu f .

Věta 2.4.4 Homomorfismus f grupy \mathcal{G} do grupy \mathcal{G}' je injektivní právě tehdy, když $\text{Ker } f = \{e\}$.

Důkaz. Podle věty 2.4.2 vždy platí, že $e \in \text{Ker } f$.

- a) Jestliže f je injektivní, pak $\text{Ker } f$ obsahuje právě jeden prvek, tedy $\text{Ker } f = \{e\}$.
- b) Nechť $\text{Ker } f = \{e\}$, $a, b \in G$ a nechť platí $f(a) = f(b)$. Pak

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = f(a)(f(a))^{-1} = e',$$

a tedy $ab^{-1} \in \text{Ker } f = \{e\}$. Proto $ab^{-1} = e$, tzn. $a = b$. Ověřili jsme tak, že homomorfismus f je injektivní. □

Podle definice je $\text{Ker } f$ podmnožinou v G . Ukažme, že jádra homomorfismů mají v grupě \mathcal{G} důležité postavení.

Věta 2.4.5 Nechť f je homomorfismus grupy \mathcal{G} do grupy \mathcal{G}' . Pak $\text{Ker } f$ je normální podgrupou v \mathcal{G} .

Důkaz. Víme, že $e \in \text{Ker } f$, proto $\text{Ker } f \neq \emptyset$.

Nechť $a, b \in \text{Ker } f$. Pak

$$f(ab^{-1}) = f(a) \cdot (f(b))^{-1} = e'(e')^{-1} = e',$$

tedy $ab^{-1} \in \text{Ker } f$. Proto $\text{Ker } f \leq \mathcal{G}$.

Uvažujme prvky $a \in \text{Ker } f$, $b \in G$. Pak:

$$f(bab^{-1}) = f(b) \cdot f(a) \cdot (f(b))^{-1} = f(b) \cdot e' \cdot (f(b))^{-1} = e',$$

tedy $bab^{-1} \in \text{Ker } f$. Platí proto $\text{Ker } f \trianglelefteq \mathcal{G}$. \square

Ukážeme nyní, že také obráceně, každá normální podgrupa grupy \mathcal{G} je jádrem homomorfismu grupy \mathcal{G} do některé grupy.

Věta 2.4.6 Jestliže N je normální podgrupa grupy \mathcal{G} , pak zobrazení $\nu : G \longrightarrow G/N$ takové, že $\nu(a) = aN$ pro každý prvek $a \in G$, je homomorfismem grupy \mathcal{G} na faktorovou grupu \mathcal{G}/N . Přitom platí, že $\text{Ker } \nu = N$.

Důkaz. Je zřejmé, že ν je surjektivní zobrazení G na G/N . Ukážeme, že je homomorfismem. Nechť $a, b \in G$. Pak $\nu(ab) = abN = aN \cdot bN = \nu(a) \cdot \nu(b)$.

Zbývá ukázat, že $\text{Ker } \nu = N$. To ale platí, protože jednotkovým prvkem v \mathcal{G}/N je $eN = N$ a pro libovolný prvek $a \in G$ je $\nu(a) = aN = N$ ekvivalentní s $a \in N$. \square

Definice. Homomorfismus ν z věty 2.4.6 se nazývá *přirozený homomorfismus* grupy \mathcal{G} na faktorovou grupu \mathcal{G}/N .

Poznámka 2.4.7 Připomeňme si, že groupoidy \mathcal{G} a \mathcal{G}' se nazývají izomorfní (označení $\mathcal{G} \cong \mathcal{G}'$), existuje-li alespoň jeden izomorfismus jednoho z nich na druhý. Přitom relace „být izomorfní“ je relací ekvivalence na třídě všech groupoidů.

Groupoidy, které patří do téže třídy odpovídajícího rozkladu, mají stejné algebraické vlastnosti. Pro grupy jsme definovali pojem izomorfismu stejně jako pro groupoidy, proto také každá grupa jednoznačně patří do některé třídy uvedeného rozkladu a platí, že všechny groupoidy, které jsou izomorfní s danou grupou, jsou také grupami.

Příklad 2.4.8 Uvažujme grupy $(\mathbb{R}^+; \cdot)$ a $(\mathbb{R}; +)$ a zobrazení $\log : \mathbb{R}^+ \longrightarrow \mathbb{R}$ takové, že $\log : x \mapsto \log x$. Je zřejmé, že \log je bijektivní zobrazení \mathbb{R}^+ na \mathbb{R} , a je známo, že pro každé $x, y \in \mathbb{R}^+$ platí $\log(xy) = \log x + \log y$. Tedy $(\mathbb{R}^+; \cdot) \cong (\mathbb{R}; +)$.

Věta 2.4.9 (Věta o homomorfismu grup) Nechť f je surjektivní homomorfismus grupy \mathcal{G} na grupu \mathcal{G}' . Pak grupa \mathcal{G}' je izomorfní s faktorovou grupou $\mathcal{G}/\text{Ker } f$. Přitom platí, že existuje právě jeden izomorfismus g grupy \mathcal{G}' na faktorovou grupu $\mathcal{G}/\text{Ker } f$ takový, že $f \circ g$ je přirozeným homomorfismem \mathcal{G} na $\mathcal{G}/\text{Ker } f$.

Větu můžeme vyjádřit následujícím diagramem:

$$\begin{array}{ccc}
 \mathcal{G} & \xrightarrow{\nu} & \mathcal{G}/\text{Ker } f \\
 f \downarrow & & \nearrow g \\
 \mathcal{G}' & &
 \end{array}$$

Důkaz. Nechť f je surjektivní homomorfismus \mathcal{G} na \mathcal{G}' . Označme $N = \text{Ker } f$. Podle věty 2.4.5 platí, že N je normální podgrupa v \mathcal{G} , a tedy podle věty 2.3.35 existuje faktorová grupa \mathcal{G}/N . Prvky z \mathcal{G}/N (tj. (levé) třídy prvků z \mathcal{G} podle N) tvoří rozklad na \mathcal{G} , a protože rozklady množin a ekvivalence na množinách jsou ve vzájemně jednoznačném vztahu, platí podle věty 1.2.15, že \mathcal{G}/N a \mathcal{G}' jsou ekvivalentní a že existuje právě jedna bijekce g množiny \mathcal{G}' na faktorovou množinu \mathcal{G}/N taková, že $f \circ g = \nu$, kde ν je přirozené zobrazení \mathcal{G} na \mathcal{G}/N . (Pro připomenutí, jestliže $b \in \mathcal{G}'$ a $b = f(a)$, kde $a \in \mathcal{G}$, pak $g(b) = aN$.) Ukažme, že g je homomorfismus \mathcal{G}' na \mathcal{G}/N .

Nechť $b_1, b_2 \in \mathcal{G}'$, $a_1, a_2 \in \mathcal{G}$, $f(a_1) = b_1$, $f(a_2) = b_2$. Pak platí:

$$g(b_1 b_2) = g(f(a_1) f(a_2)) = g(f(a_1 a_2)) = a_1 a_2 N = a_1 N \cdot a_2 N = g(b_1) g(b_2).$$

□

Poznámka 2.4.10 Nechť \mathcal{A} je některá třída grup. Jestliže platí, že danou vlastnost mají právě všechny grupy z třídy \mathcal{A} a všechny grupy, které jsou izomorfní s některou grupou z \mathcal{A} , pak říkáme, že tuto vlastnost „mají, až na izomorfismus“, právě grupy z třídy \mathcal{A} . Právě dokázaná věta říká, že homomorfními obrazy grupy \mathcal{G} jsou, až na izomorfismus, právě všechny faktorové grupy podle normálních podgrup grupy \mathcal{G} .

Příklad 2.4.11 Určete všechny homomorfí obrazy grupy $\mathcal{Z} = (\mathbb{Z}; +)$.

Protože \mathcal{Z} je abelovská grupa, je každá její podgrupa normální. Přitom platí, že podgrupami grupy \mathcal{Z} jsou právě všechny množiny $n\mathbb{Z} = \{na; a \in \mathbb{Z}\}$. (Speciálně $0\mathbb{Z} = \{0\}$, $1\mathbb{Z} = \mathbb{Z}$.) Faktorová grupa $\mathcal{Z}/n\mathbb{Z}$ je izomorfní s grupou $\mathcal{Z}_n = (\mathbb{Z}_n; \oplus)$ čísel $\{0, 1, \dots, n-1\}$ se sčítáním modulo n . Podle věty 2.4.9 tedy platí, že homomorfí obrazy grupy \mathcal{Z} jsou, až na izomorfismus, právě všechny grupy \mathcal{Z}_n ($n \geq 0$).

Věta 2.4.12 Jestliže f je homomorfismus grupy \mathcal{G} do grupy \mathcal{G}' , pak $\text{Im } f = \{f(x); x \in \mathcal{G}\}$ je podgrupou grupy \mathcal{G}' .

Důkaz. Samozřejmě platí, že $\text{Im } f \neq \emptyset$. Nechť $b_1, b_2 \in \text{Im } f$. Pak existují prvky $a_1, a_2 \in \mathcal{G}$ takové, že $f(a_1) = b_1$, $f(a_2) = b_2$. Platí:

$$b_1 b_2^{-1} = f(a_1) (f(a_2))^{-1} = f(a_1) f(a_2^{-1}) = f(a_1 a_2^{-1}),$$

tzn. $b_1 b_2^{-1} \in \text{Im } f$, a tedy $\text{Im } f \leq \mathcal{G}'$. \square

Důsledek 2.4.13 Jestliže f je homomorfismus grupy \mathcal{G} do grupy \mathcal{G}' , pak $\text{Im } f$ je izomorfní s faktorovou grupou $\mathcal{G}/\text{Ker } f$.

Důkaz. Uvažujme zobrazení $h : G \rightarrow \text{Im } f$ takové, že pro každý $a \in G$ platí $h(a) = f(a)$. Je zřejmé, že h je surjektivní homomorfismus grupy \mathcal{G} na grupu $\text{Im } f$. Proto tvrzení dostaneme bezprostředně z věty o homomorfismu grup. \square

Věta 2.4.9, tj. věta o homomorfismu grup, popř. její modifikace s využitím právě dokázaného důsledku, se také nazývá **1. věta o izomorfismu grup**. Spolu s dalšími dvěma větami, které nyní dokážeme, tvoří celek zvaný věty o izomorfismu grup. V jejich formulacích a důkazech nebudeme pro jednoduchost rozlišovat mezi grupami a jejich nosiči.

Věta 2.4.14 (2. věta o izomorfismu) Nechť G je grupa, $H \trianglelefteq G$, $N \trianglelefteq G$ a $N \leq H$. Pak platí, že $(G/N)/(H/N) \cong G/H$.

Důkaz. Ukažme nejdříve, že faktorová grupa H/N je podgrupou grupy G/N . Jestliže $b_1, b_2 \in H$, pak $(b_1 N)^{-1} \cdot (b_2 N) = b_1^{-1} b_2 N$, a protože $b_1^{-1} b_2 \in H$, dostáváme, že $(b_1 N)^{-1} \cdot (b_2 N) \in H/N$. Proto $H/N \leq G/N$. Uvažujme nyní zobrazení $f : G/N \rightarrow G/H$ takové, že $f(xN) = xH$ pro každé $x \in G$. Zobrazení f je definováno korektně, protože z $xN = yN$ plyne $x^{-1}y \in N \subseteq H$, tedy $xH = yH$. Přitom je zřejmé, že f je surjektivní zobrazení G/N na G/H . Ukážeme, že f je homomorfismus.

Nechť $x, y \in G$. Pak

$$f(xN \cdot yN) = f(xyN) = xyH = xH \cdot yH.$$

Tedy f je surjektivní homomorfismus grupy G/N na grupu G/H a pro jeho jádro platí, že $\text{Ker } f = H/N$. Proto podgrupa H/N grupy G/N je normální a podle věty o homomorfismu platí $(G/N)/(H/N) \cong G/H$. \square

Věta 2.4.15 (3. věta o izomorfismu) Nechť G je grupa, $H \leq G$ a $N \trianglelefteq G$. Pak $N \cap H \trianglelefteq H$ a $NH/N \cong H/(N \cap H)$.

Důkaz. Nechť $\nu_H : H \rightarrow G/N$ je restrikce přirozeného homomorfismu $\nu : G \rightarrow G/N$ na podgrupu H . Pak $\text{Ker } \nu_H = N \cap H$ a podle 1. věty o izomorfismu platí $\text{Im } \nu_H \cong H/(N \cap H)$. Zbývá ukázat, že $\text{Im } \nu_H = NH/N$. Nechť $x \in G$. Pak $xN = hN$ pro některý $h \in H$, právě když $h^{-1}x \in N$, tj. $h^{-1}x = n \in N$, tedy právě když $x = hn$ pro některý $n \in N$, neboli $x \in NH$. \square

2.5 Kongruence grup

Úloha vytvořit homomorfní obrazy dané algebraické struktury se vyskytuje v algebře (ale i v dalších matematických disciplínách a jejich aplikacích) velmi často. Přitom nejjednodušším řešením je vždy konstrukce odpovídajících faktorových algebraických struktur.

V případě grup k tomu postačuje nalezení všech normálních podgrup. V obecném případě ale analogické podstruktury (až na výjimky – např. pro okruhy) neexistují. Proto je nutné ke konstrukci faktorových struktur v obecnosti užít univerzálnější metodu založenou na pojmu kongruence. Ukážeme si tento přístup na grpoidech. Pro grupy, které jsou speciálním případem grupoidů, jsou však obě konstrukce faktorových grup (tj. pomocí normálních podgrup a pomocí kongruencí) ekvivalentní.

Definice. Nechť $\mathcal{G} = (G; \cdot)$ je grupoid. Pak *kongruencí* grupoidu \mathcal{G} rozumíme každou relaci ekvivalence ϱ na G , pro kterou je splněna podmínka

$$\forall a, b, c, d \in G; ((a, b) \in \varrho \wedge (c, d) \in \varrho) \implies (ac, bd) \in \varrho.$$

Příklad 2.5.1 Jestliže $n \in \mathbb{N}$, pak relace kongruence podle modulu n je grupoidovou kongruencí na grupoidu $\mathcal{Z}' = (\mathbb{Z}; \cdot)$.

Vskutku, nechť $a, b, c, d \in \mathbb{Z}$, $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$. Pak existují $x, y \in \mathbb{Z}$ taková, že $a - b = nx$, $c - d = ny$. Tedy

$$ac - bd = ac - ad + ad - bd = a(c - d) + (a - b)d = any + nxd = n(ay + xd),$$

a proto $ac \equiv bd \pmod{n}$.

Věta 2.5.2 Jestliže ϱ je kongruence grupoidu $\mathcal{G} = (G; \cdot)$ a jestliže pro libovolné $a, b \in G$ položíme $[a]_\varrho \cdot [b]_\varrho = [a \cdot b]_\varrho$, pak $(G/\varrho; \cdot)$ je grupoid.

Důkaz. Stačí ukázat, že definice operace „.“ na G/ϱ je korektní. Nechť $a, a_1, b, b_1 \in G$, $[a] = [a_1]$, $[b] = [b_1]$. Pak $(a, a_1) \in \varrho$, $(b, b_1) \in \varrho$, a proto $(ab, a_1b_1) \in \varrho$. To však znamená, že $[ab] = [a_1b_1]$, a tedy výsledek zavedené operace nezávisí na výběru reprezentantů z tříd odpovídajících ekvivalenci ϱ . \square

Definice. Grupoid $\mathcal{G}/\varrho = (G/\varrho; \cdot)$ z věty 2.5.2 se nazývá *faktorový grupoid* grupoidu \mathcal{G} podle kongruence ϱ .

Příklad 2.5.3 Jestliže stejně jako v příkladě 2.5.1 uvažujeme grupoid $\mathcal{Z}' = (\mathbb{Z}; \cdot)$ a kongruenci podle modulu n ($n \in \mathbb{N}$), pak faktorovým grupoidem \mathcal{Z}' podle této kongruence je množina všech zbytkových tříd podle modulu n . Přitom např. pro $n = 4$ je Cayleyova tabulka pro násobení ve faktorovém grupoidu následující (víme, že $0 + 4\mathbb{Z} = 4\mathbb{Z}$):

	$4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$
$4\mathbb{Z}$	$4\mathbb{Z}$	$4\mathbb{Z}$	$4\mathbb{Z}$	$4\mathbb{Z}$
$1 + 4\mathbb{Z}$	$4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$
$2 + 4\mathbb{Z}$	$4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$4\mathbb{Z}$	$2 + 4\mathbb{Z}$
$3 + 4\mathbb{Z}$	$4\mathbb{Z}$	$3 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$

Definice. Jestliže $\mathcal{G} = (G; \cdot)$ je grupa, pak *grupovou kongruencí grupy \mathcal{G}* rozumíme právě každou kongruenci grupoidu $(G; \cdot)$.

(Proto přívlastek „grupová“ můžeme vynechávat.)

Věta 2.5.4 Nechť ϱ je kongruence grupy \mathcal{G} a nechť $a, b \in G$. Pak platí:

$$(a, b) \in \varrho \implies (a^{-1}, b^{-1}) \in \varrho.$$

Důkaz. Nechť $(a, b) \in \varrho$. Pak, protože $(a^{-1}, a^{-1}) \in \varrho$, platí také $(aa^{-1}, ba^{-1}) \in \varrho$, tzn. $(e, ba^{-1}) \in \varrho$. Odtud analogicky dostaneme $(b^{-1}e, b^{-1}ba^{-1}) \in \varrho$, neboli $(b^{-1}, a^{-1}) \in \varrho$, a tedy $(a^{-1}, b^{-1}) \in \varrho$. \square

Věta 2.5.5 Nechť H je podgrupa grupy \mathcal{G} . Pak ekvivalence ϱ_H na G odpovídající levému rozkladu G/H grupy \mathcal{G} podle H je kongruencí grupy \mathcal{G} právě tehdy, když H je normální podgrupou.

Důkaz. Předpokládejme, že $H \leq \mathcal{G}$ a že ekvivalence $\varrho = \varrho_H$ je kongruencí grupy \mathcal{G} . Uvažujme $a \in G, h \in H$. Pak $e^{-1}h = eh = h \in H$, proto podle věty 2.3.19 a) platí $(e, h) \in \varrho$. Odtud dostaneme $(a^{-1}, ha^{-1}) \in \varrho$, a tedy také $(e, aha^{-1}) \in \varrho$. Proto $e^{-1} \cdot aha^{-1} \in H$, neboli $aha^{-1} \in H$. Podle věty 2.3.28 platí, že H je normální v \mathcal{G} .

Obráceně, nechť podgrupa H grupy \mathcal{G} je normální, $a, b, c, d \in G$ a nechť $(a, b) \in \varrho, (c, d) \in \varrho$. Máme dokázat, že $(ac, bd) \in \varrho$, tj. $(bd)^{-1}(ac) \in H$. Protože $(a, b) \in \varrho, (c, d) \in \varrho$, platí $b^{-1}a \in H, d^{-1}c \in H$, tedy existují prvky $h_1, h_2 \in H$ takové, že $b^{-1}a = h_1, d^{-1}c = h_2$. Odtud

$$(bd)^{-1}(ac) = d^{-1}b^{-1}ac = d^{-1}b^{-1}add^{-1}c = d^{-1}h_1dh_2,$$

a protože $d^{-1}h_1d \in H$, platí $(bd)^{-1}(ac) \in H$. Tedy ϱ je kongruence na \mathcal{G} . \square

Věta 2.5.6 Binární relace ϱ na G je kongruencí grupy $\mathcal{G} = (G; \cdot)$ právě tehdy, když existuje normální podgrupa N grupy \mathcal{G} taková, že

$$\forall a, b \in G; (a, b) \in \varrho \iff b^{-1}a \in N.$$

V takovém případě relace ϱ je ekvivalencí indukovanou rozkladem G/N .

Důkaz. a) Nechť ϱ je kongruence na \mathcal{G} . Označme $N = \{x \in G; (x, e) \in \varrho\}$. Ukážeme, že N je normální podgrupou grupy \mathcal{G} .

Zřejmě $e \in N$, proto $N \neq \emptyset$. Nechť $n_1, n_2 \in N$. Pak $(n_1, e) \in \varrho, (n_2, e) \in \varrho$, tedy podle věty 2.5.4 také $(n_1, e) \in \varrho, (n_2^{-1}, e) \in \varrho$, a proto $(n_1n_2^{-1}, e) \in \varrho$, neboli $n_1n_2^{-1} \in N$. To znamená, že $N \leq \mathcal{G}$. Předpokládejme dále, že $a \in G, n \in N$. Pak $(a, a) \in \varrho, (n, e) \in \varrho, (a^{-1}, a^{-1}) \in \varrho$, proto $(ana^{-1}, e) \in \varrho$, a tedy $ana^{-1} \in N$. Podle věty 2.3.28 to znamená, že N je normální podgrupou v \mathcal{G} .

Nechť $a, b \in \mathcal{G}$. Jestliže $(a, b) \in \varrho$, pak $(b^{-1}a, e) \in \varrho$, tedy $b^{-1}a \in N$.

Obráceně, jestliže $b^{-1}a \in N$, pak $(b^{-1}a, e) \in \varrho$, proto také $(bb^{-1}a, be) = (a, b) \in \varrho$.

Dokázali jsme tak, že pro kongruenci ϱ existuje normální podgrupa N taková, že pro libovolné $a, b \in G$ platí $(a, b) \in \varrho$ právě tehdy, když $b^{-1}a \in N$.

b) Nechť k binární relaci ϱ na G existuje $N \trianglelefteq \mathcal{G}$ taková, že

$$\forall a, b \in G; (a, b) \in \varrho \iff b^{-1}a \in N.$$

Pak podle věty 2.5.5 platí, že podmínka $b^{-1}a \in N$ je ekvivalentní s tím, že $(a, b) \in \varrho_N$, kde ϱ_N je ekvivalence indukovaná rozkladem G/N , a tedy $\varrho = \varrho_N$. Podle věty 2.5.5 je tedy ϱ kongruencí grupy \mathcal{G} . \square

Poznámka 2.5.7 Podle předchozího vidíme, že existuje vzájemně jednoznačná korespondence mezi normálními podgrupami grupy \mathcal{G} a kongruencemi této grupy, která je dána vztahy z věty 2.5.6. Odpovídající si kongruence ϱ a normální podgrupa N přitom určují stejnou faktorovou strukturu, kterou proto můžeme označovat \mathcal{G}/ϱ nebo \mathcal{G}/N . (Mj. odtud dostáváme, že faktorový grupoid grupy je vždy grupou.)

2.6 Cyklické a permutační grupy

V dalším textu si ukážeme vlastnosti cyklických grup a dokážeme, že libovolnou grupu lze interpretovat jako některou grupu permutací. Připomeňme si, že grupa \mathcal{G} se nazývá cyklická právě tehdy, existuje-li prvek $a \in G$ takový, že $\mathcal{G} = \langle a \rangle = \{a^n; n \in \mathbb{Z}\}$. Příklady cyklických grup jsou $\mathcal{Z} = (\mathbb{Z}; +)$, kde $\mathcal{Z} = \langle 1 \rangle = \langle -1 \rangle$, popř. $\mathcal{Z}_n = (\mathbb{Z}_n; \oplus)$ ($n \in \mathbb{N}$), kde vždy mj. $\mathcal{Z}_n = \langle 1 \rangle$. Existují tedy cyklické grupy nekonečného řádu i libovolného konečného řádu.

Věta 2.6.1 Každá nekonečná cyklická grupa je izomorfní s grupou $\mathcal{Z} = (\mathbb{Z}; +)$. Každá konečná cyklická grupa řádu n je izomorfní s grupou $\mathcal{Z}_n = (\mathbb{Z}_n; \oplus)$.

Důkaz. Nechť $\mathcal{G} = (G; \cdot) = \langle a \rangle$ je cyklická grupa kteréhokoli řádu a nechť $f : \mathbb{Z} \rightarrow G$ je zobrazení takové, že $f(n) = a^n$ pro každé $n \in \mathbb{N}$. Je zřejmé, že f je surjektivní zobrazení. Přitom platí pro libovolné $m, n \in \mathbb{Z}$

$$f(m+n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n),$$

tedy f je homomorfismus \mathcal{Z} na \mathcal{G} .

a) Pokud jsou všechny mocniny prvku a navzájem různé, pak f je injektivní, a proto f je izomorfismus \mathcal{Z} na \mathcal{G} .

b) Nechť $\mathcal{G} = \langle a \rangle$ má řád n . Nechť $m \in \mathbb{Z}$ a $n|m$, tj. $m = nx$, kde $x \in \mathbb{Z}$. Pak

$$a^m = a^{nx} = (a^n)^x = e^x = e.$$

Nechť naopak $a^m = e$, $m = nx + r$, $0 \leq r < n$. Pak

$$e = a^m = (a^n)^x \cdot a^r = e \cdot a^r = a^r,$$

tedy (protože řád prvku a je n) platí $r = 0$. To ovšem znamená, že $f(m) = e$ právě tehdy, když $n|m$, tzn. $\text{Ker } f = n\mathbb{Z}$. Tedy \mathcal{G} je izomorfní s faktorovou grupou $\mathcal{Z}/n\mathbb{Z}$. Přitom je zřejmé, že $\mathcal{Z}/n\mathbb{Z}$ je izomorfní s \mathcal{Z}_n . \square

Poznámka 2.6.2 Vidíme tedy, že, až na izomorfismus, existuje jediná cyklická grupa nekonečného rádu, a to $\mathcal{Z} = (\mathbb{Z}; +)$. Podobně pro libovolné $n \in \mathbb{N}$ existuje cyklická grupa konečného rádu n , která je také, až na izomorfismus, určena jednoznačně.

Věta 2.6.3 a) *Každá podgrupa a každý homomorfní obraz cyklické grupy je cyklickou grupou.*

b) *Každá podgrupa nekonečné cyklické grupy různá od E je nekonečnou cyklickou grupou.*

Důkaz. a) Nechť $\mathcal{G} = \langle a \rangle$ je cyklická grupa, $f : G \longrightarrow G'$ surjektivní homomorfismus grupy \mathcal{G} na některou grupu G' a $b \in G'$. Pak existuje $k \in \mathbb{Z}$ takové, že $f(a^k) = b$. Tedy $b = f(a^k) = [f(a)]^k$, a proto $G' = \langle f(a) \rangle$, což znamená, že grupa G' je cyklická. Tím jsme dokázali, že homomorfní obraz cyklické grupy je cyklickou grupou.

Nyní ukážeme, že každá podgrupa cyklické grupy je cyklická. Podle předchozí věty stačí uvažovat jen cyklické grupy \mathcal{Z} a $\mathcal{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}$).

Nechť $H \leq \mathcal{Z}$ a nechť k je nejmenší přirozené číslo ležící v H . Je zřejmé, že $\langle k \rangle \subseteq H$. Nechť naopak $m \in H$. Pak existují $q, r \in \mathbb{Z}$ taková, že $m = kq + r$ a $0 \leq r < k$. Tedy $r = m - kq$, a proto $r \in H$. Ovšem z $0 \leq r < k$ pak dostaneme $r = 0$, tzn. $H \subseteq \langle k \rangle$, a tedy $H = \langle k \rangle$.

Nechť nyní $\overline{H} \leq \mathcal{Z}/n\mathbb{Z}$. Označme H množinu všech prvků $x \in \mathbb{Z}$ takových, že $\nu(x) \in \overline{H}$. (Zde ν označuje přirozený homomorfismus grupy \mathcal{Z} na grupu $\mathcal{Z}/n\mathbb{Z}$.) Pak H je podgrupa v \mathcal{Z} a platí $\overline{H} = H/n\mathbb{Z}$. Ovšem H , jako podgrupa v \mathcal{Z} , je cyklická, proto podle předchozí části také grupa $\overline{H} = H/n\mathbb{Z}$ je cyklická.

b) Dokázali jsme již, že každá podgrupa v \mathcal{Z} různá od E je ve tvaru $\langle k \rangle$, kde $k \in \mathbb{N}$. Odtud vyplývá tvrzení. \square

Věta 2.6.4 a) *Cyklická grupa \mathcal{Z} má právě dva generátory 1 a -1 .*

b) *Jestliže $\mathcal{G} = \langle a \rangle$ je konečná cyklická grupa rádu n a $k \in \mathbb{N}$, pak $\langle a^k \rangle = \mathcal{G}$ právě tehdy, když čísla k a n jsou nesoudělná.*

Důkaz. a) Zřejmě.

b) Nechť $D(k, n) = 1$. (Zde $D(k, n)$ značí největší společný dělitel čísel k a n .) Pak existují čísla $x, y \in \mathbb{Z}$ taková, že $kx + ny = 1$. Tedy

$$a = a^{kx+ny} = (a^k)^x \cdot (a^n)^y = (a^k)^x \cdot e = (a^k)^x \in \langle a^k \rangle,$$

tzn. $\langle a \rangle \subseteq \langle a^k \rangle$. Protože vždy platí $\langle a^k \rangle \subseteq \langle a \rangle$, dostáváme $\langle a^k \rangle = \langle a \rangle$.

Obráceně, nechť $\langle a^k \rangle = \langle a \rangle$. Pak existuje $x \in \mathbb{Z}$ takové, že $a = (a^k)^x = a^{kx}$, a tedy $a^{kx-1} = e$. Ovšem podle důkazu věty 2.6.1 platí pro libovolné $m \in \mathbb{Z}$, že $a^m = e$ právě

tehdy, když $n|m$. (Zde $n|m$ znamená, že číslo n je dělitelem čísla m .) To znamená, že $n|(kx - 1)$, proto $kx - 1 = ny$ pro některé $y \in \mathbb{Z}$, neboli $kx - ny = 1$. Jestliže $t \in \mathbb{N}$ je takové, že $t|n$, $t|k$, pak $t|(kx - ny)$, tedy $t|1$. Proto $D(k, n) = 1$. \square

Věta 2.6.5 *Každá grupa prvočíselného řádu je cyklická.*

Důkaz. Nechť \mathcal{G} je grupa řádu p , kde p je prvočíslo. Jestliže $e \neq a \in G$, pak, protože řád prvku a je roven řádu cyklické podgrupy $\langle a \rangle$, platí podle Lagrangeovy věty, že řád prvku a dělí p . Ovšem řád prvku a je větší než 1, proto je roven p , a to znamená, že $G = \langle a \rangle$. \square

Důsledek 2.6.6 *Pro každé prvočíslo p existuje, až na izomorfismus, právě jedna grupa řádu p .*

Víme, že pro libovolnou konečnou neprázdnou množinu M je množina všech permutací na M uvažovaná spolu s operací skládání permutací grupou. Označujeme ji $S(M)$ a nazýváme *symetrická grupa* množiny M . Všechny sudé permutace na M tvoří podgrupu $A(M) \leq S(M)$, kterou nazýváme *alternující grupa* množiny M .

Věta 2.6.7 *Jestliže M je konečná neprázdná množina, pak alternující grupa $A(M)$ je normální podgrupou symetrické grupy $S(M)$.*

Důkaz. Protože víme, že $A(M) \leq S(M)$, stačí ukázat normálnost $A(M)$ v $S(M)$. Je ovšem zřejmé, že index $A(M)$ je roven 2, a tedy vskutku platí $A(M) \trianglelefteq S(M)$. \square

Ukažme si nyní, že grupy permutací mají v teorii grup zcela obecný význam, protože v sobě obsahují, samozřejmě až na izomorfismus, jakoukoliv grupu. Abychom se o tom přesvědčili, rozšířme pojem permutace i na nekonečné množiny.

Definice. Jestliže M je libovolná neprázdná množina, pak *permutací* na M budeme rozumět libovolné bijektivní zobrazení množiny M na množinu M .

Poznámka 2.6.8 Je zřejmé, že označíme-li $S(M)$ množinu všech permutací na M , pak $S(M)$ tvoří spolu se skládáním permutací grupu, kterou budeme také označovat $S(M) = (S(M); \circ)$ a nazývat symetrickou grupou množiny M .

Věta 2.6.9 (Cayleyova věta) *Každá grupa je izomorfní s některou podgrupou symetrické grupy některé množiny.*

Důkaz. Nechť $\mathcal{G} = (G; \cdot)$ je grupa. Za množinu M budeme považovat přímo nosič G této grupy. Jestliže $a \in G$, označme f_a permutaci na G takovou, že $f_a(x) = xa$ pro každý prvek $x \in G$. Ukažme, že $f_a \in S(G)$, tedy že f_a je bijekcí G na G . Předpokládejme nejdříve, že pro prvky $x, y \in G$ platí $f_a(x) = f_a(y)$. Pak $xa = ya$, a protože v grupě můžeme krátit,

dostáváme $x = y$, tzn. f_a je injektivní. Nechť dále $z \in G$. Pak existuje prvek $x \in G$ takový, že $xa = z$. Pak ale $f_a(x) = z$, a tedy f_a je také surjektivní.

Uvažujme nyní zobrazení $\varphi : G \rightarrow S(G)$ takové, že $\varphi : a \mapsto f_a$ pro každý $a \in G$. Nechť $a, b \in G$ a nechť $a \neq b$. Pak platí

$$f_a(e) = ea = a, \quad f_b(e) = eb = b,$$

tedy $f_a(e) \neq f_b(e)$, a proto $f_a \neq f_b$. To ovšem znamená, že zobrazení φ je injektivní.

Nechť $a, b, x \in G$. Pak

$$\begin{aligned} [\varphi(a) \circ \varphi(b)](x) &= (f_a \circ f_b)(x) = f_b(f_a(x)) = f_b(xa) = (xa)b = x(ab) \\ &= f_{ab}(x) = \varphi(ab)(x), \end{aligned}$$

tedy φ je homomorfismus grupy \mathcal{G} do grupy $S(G)$.

Pak však platí, že $\text{Im } \varphi = \{\varphi(a); a \in G\}$ je podgrupou grupy $S(G)$, a protože φ je injektivní, dostáváme, že grupy \mathcal{G} a $\text{Im } \varphi$ jsou izomorfní. \square

2.7 Automorfismy grup

V této části se budeme věnovat automorfismům a vnitřním automorfismům grup a dalším pojmem, které s nimi souvisejí.

Definice. Jestliže $\mathcal{G} = (G; \cdot)$ je grupa, pak jejím *automorfismem* rozumíme každý izomorfismus grupy \mathcal{G} na grupu \mathcal{G} .

Všude dále v této části nebudeme opět rozlišovat mezi grupou \mathcal{G} a jejím nosičem G .

Věta 2.7.1 Nechť G je grupa a nechť $a \in G$. Pak zobrazení $\varphi^a : G \rightarrow G$ takové, že $\varphi^a : x \mapsto a^{-1}xa$ pro každý $x \in G$, je automorfismem grupy G .

Důkaz. Nechť $x, y \in G$. Pak

$$\varphi^a(xy) = a^{-1}(xy)a = (a^{-1}xa) \cdot (a^{-1}ya) = \varphi^a(x) \cdot \varphi^a(y),$$

tedy φ^a je homomorfismus G do G .

Jestliže $x \in G$, pak $\varphi^a(x) = e$, právě když $a^{-1}xa = e$, tedy právě když $x = e$. Proto $\text{Ker } \varphi^a = \{e\}$, a proto podle věty 2.4.4 platí, že φ^a je injektivní.

Nechť $x \in G$. Pak

$$\varphi^a(axa^{-1}) = a^{-1}(axa^{-1})a = x,$$

tedy φ^a je surjektivní.

Celkově tak dostáváme, že φ^a je automorfismus grupy G . \square

Definice. Automorfismus φ^a se nazývá *vnitřní automorfismus* grupy G určený prvkem a .

Označme $\text{Aut } G$ množinu všech automorfismů a $\text{Int } G$ množinu všech vnitřních automorfismů grupy G . Z vlastností izomorfismů je vidět, že $\text{Aut } G$ spolu s operací skládání zobrazení je grupou.

Věta 2.7.2 Pro libovolnou grupu G platí, že $\text{Int } G$ je normální podgrupou grupy $\text{Aut } G$.

Důkaz. Nechť $a, b \in G$. Pak pro libovolný prvek $x \in G$ platí

$$(\varphi^a \circ \varphi^b)(x) = \varphi^b(a^{-1}xa) = b^{-1}a^{-1}xab = (ab)^{-1}x(ab) = \varphi^{ab}(x),$$

proto $\varphi^a \circ \varphi^b = \varphi^{ab} \in \text{Int } G$, a to znamená, že $\text{Int } G$ je uzavřená vzhledem ke skládání zobrazení. Dále $\text{id}_G = \varphi^e$ a $\varphi^a \circ \varphi^{a^{-1}} = \varphi^{aa^{-1}} = \varphi^e = \text{id}_G$, tedy $\text{Int } G \leq \text{Aut } G$.

Nechť nyní $\psi \in \text{Aut } G$ a $\varphi^a \in \text{Int } G$. Jestliže $x \in G$, pak

$$(\psi^{-1} \circ \varphi^a \circ \psi)(x) = \psi(a^{-1} \cdot \psi^{-1}(x) \cdot a) =$$

$$\psi(a^{-1}) \cdot x \cdot \psi(a) = \psi(a)^{-1} \cdot x \cdot \psi(a) = \varphi^{\psi(a)}(x),$$

tedy $\psi \circ \varphi^a \circ \psi^{-1} = \varphi^{\psi(a)} \in \text{Int } G$.

Dostali jsme tak, že $\text{Int } G \trianglelefteq \text{Aut } G$. □

Poznámka 2.7.3 Nechť G je grupa, $H \leq G$ a $f : G \rightarrow G$ zobrazení. Pak říkáme, že H je invariantní vzhledem k f , jestliže pro každý $a \in H$ platí, že $f(a) \in H$. Vidíme, že podgrupa H grupy G je normální, právě když je invariantní vzhledem ke všem vnitřním automorfismům grupy G . Proto se normální podgrupy také někdy nazývají invariantními podgrupami grupy G .

Definice. Nechť G je grupa. Pak množina $C(G) = \{a \in G; ax = xa \text{ pro každý } x \in G\}$ se nazývá centrum grupy G .

Věta 2.7.4 Nechť G je grupa. Pak její centrum $C(G)$ je normální podgrupou v G . Navíc platí, že jestliže $H \leq G$ a $H \subseteq C(G)$, pak $H \trianglelefteq G$.

Důkaz. Zřejmě $e \in C(G)$. Nechť $a, b \in C(G)$, $x \in G$. Pak $(ab^{-1})x = (x^{-1}ba^{-1})^{-1} = (bx^{-1}a^{-1})^{-1} = axb^{-1} = x(ab^{-1})$, proto $ab^{-1} \in C(G)$, tzn. $C(G) \leq G$. Protože navíc pro libovolné $a \in C(G)$ a $x \in G$ platí $xax^{-1} = a$, dostáváme $C(G) \trianglelefteq G$, a analogicky dokážeme, že $H \trianglelefteq G$ pro každou $H \leq C(G)$. □

Věta 2.7.5 Pro libovolnou grupu G platí, že $G/C(G) \cong \text{Int } G$.

Důkaz. Nechť $\alpha : G \rightarrow \text{Int } G$ je zobrazení takové, že $\alpha(a) = \varphi^a$ pro každý prvek $a \in G$. Nechť $a, b, x \in G$. Pak

$$\begin{aligned} \alpha(ab)(x) &= \varphi^{ab}(x) = (ab)^{-1} \cdot x \cdot (ab) = b^{-1}(a^{-1}xa)b = b^{-1}\varphi^a(x)b = \\ &= (\varphi^a \circ \varphi^b)(x) = (\alpha(a) \circ \alpha(b))(x), \end{aligned}$$

tedy $\alpha(ab) = \alpha(a) \circ \alpha(b)$.

Proto α je homomorfismus, který je navíc surjektivní.

Nechť $a \in G$. Pak $a \in \text{Ker } \alpha$, právě když $\varphi^a = \text{id}_G$, neboli právě když $a^{-1}xa = x$ pro každý $x \in G$, tzn., právě když $a \in C(G)$. Tedy $\text{Ker } \alpha = C(G)$. Podle 1.věty o izomorfismu pak dostáváme, že $\text{Int } G \cong G/\text{Ker } \alpha = G/C(G)$. □

Poznámka 2.7.6 Podle definice centra grupy je vidět, že $C(G) = G$ právě tehdy, když grupa G je abelovská. V takovém případě pak $\text{Int } G = \{\text{id}_G\}$.

Definice. Nechť G je grupa a $x, y \in G$. Pak prvek $[x, y] = x^{-1}y^{-1}xy$ se nazývá *komutátor prvků* x a y (v tomto pořadí).

Podgrupa G' grupy G generovaná množinou všech komutátorů prvků z G se nazývá *komutant grupy* G .

Věta 2.7.7 Jestliže G je libovolná grupa, pak komutant G' je normální podgrupou grupy G .

Důkaz. Pro libovolné prvky $x, y \in G$ platí $[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y, x]$. Proto jestliže $b \in G'$, pak podle věty 2.3.13 platí, že $b = [x_1, y_1] \cdot [x_2, y_2] \cdots [x_n, y_n]$ pro některé prvky $x_1, y_1, x_2, y_2, \dots, x_n, y_n \in G$.

Nechť $a \in G$. Pak

$$\begin{aligned} a^{-1}ba &= a^{-1}([x_1, y_1] \cdot [x_2, y_2] \cdots [x_n, y_n])a = \varphi^a([x_1, y_1] \cdot [x_2, y_2] \cdots [x_n, y_n]) = \\ &= [\varphi^a(x_1), \varphi^a(y_1)] \cdot [\varphi^a(x_2), \varphi^a(y_2)] \cdots [\varphi^a(x_n), \varphi^a(y_n)] \in G'. \end{aligned}$$

Proto $G' \trianglelefteq G$. □

Poznámka 2.7.8 Grupa G je abelovská právě tehdy, když $G' = \{e\}$.

Věta 2.7.9 Nechť G je grupa a $H \leq G$. Pak $H \trianglelefteq G$ a faktorová grupa G/H je abelovská, právě když $G' \subseteq H$.

Důkaz. Nechť $H \trianglelefteq G$ a nechť $x, y \in G$. Pak $xH \cdot yH = yH \cdot xH$, právě když $xyH = yxH$, tedy právě když $(yx)^{-1}(xy) = x^{-1}y^{-1}xy \in H$. Označme K množinu všech komutátorů prvků z G . Pak G/H je abelovská grupa, právě když $K \subseteq H$, tedy právě když $M' = \langle K \rangle \subseteq H$.

Nechť nyní $H \trianglelefteq G$ je taková, že $G' \subseteq H$. Jestliže $a \in G$ a $b \in H$, pak $b^{-1}a^{-1}ba \in G' \subseteq H$, a proto také $a^{-1}ba = bb^{-1}a^{-1}ba \in H$. Tedy $H \trianglelefteq G$. □

2.8 Direktní součiny grup

V této části se budeme věnovat konstrukcím, které umožňují sestrojit z daných grup grupy nové a složitější, popř. obráceně, umožňují vyjádřit složité grupy pomocí jednodušších grup.

Jestliže $\mathcal{G} = (G; \cdot)$ je grupa, pak znova nebudeme rozlišovat, pokud to bude zřejmé z kontextu, mezi \mathcal{G} a G .

Připomeňme si, že jestliže G je grupa a $H_\alpha \leq G$ ($\alpha \in I$), pak spojením systému podgrup $(H_\alpha; \alpha \in I)$ rozumíme podgrupu $\bigvee_{\alpha \in I} H_\alpha = \left\langle \bigcup_{\alpha \in I} H_\alpha \right\rangle$ generovanou sjednocením $\bigcup_{\alpha \in I} H_\alpha$.

Definice. Nechť G je grupa a $(H_\alpha; \alpha \in I)$ je systém normálních podgrup grupy G . Pak říkáme, že grupa G je *vnitřním direktním součinem* podgrup H_α ($\alpha \in I$), a píšeme $G = \prod_{\alpha \in I}^*$, platí-li

$$\text{a)} \quad G = \bigvee_{\alpha \in I} H_\alpha;$$

$$\text{b)} \quad H_\alpha \cap \bigvee \{H_\beta; \beta \in I, \beta \neq \alpha\} = \{e\} \text{ pro každé } \alpha \in I.$$

Jestliže I je konečná množina indexů, např. $I = \{1, \dots, n\}$, pak píšeme také $G = H_1 \times \dots \times H_n$.

Věta 2.8.1 Jestliže $(H_\alpha; \alpha \in I)$ je systém podgrup grupy G , pak $G = \prod_{\alpha \in I}^* H_\alpha$, právě tehdy, když

$$1. \quad \forall \alpha, \beta \in I, \alpha \neq \beta, h_\alpha \in H_\alpha, h_\beta \in H_\beta; h_\alpha h_\beta = h_\beta h_\alpha,$$

2. každý prvek $e \neq g \in G$ je možno zapsat jednoznačně, až na pořadí činitelů, ve tvaru součinu

$$g = h_1 h_2 \cdots h_n, \quad (1)$$

kde $e \neq h_i \in H_{\alpha_i}$, a $\alpha_i \neq \alpha_j$ pro $i \neq j$.

Důkaz. a) Nechť $G = \prod_{\alpha \in I}^* H_\alpha$ a nechť $h_i \in H_{\alpha_i}$, $h_j \in H_{\alpha_j}$, $\alpha_i \neq \alpha_j$. Podle předpokladu $H_{\alpha_i} \trianglelefteq G$, $H_{\alpha_j} \trianglelefteq G$, proto podle věty 2.3.28

$$h_i^{-1}(h_j^{-1}h_i h_j) = (h_i^{-1}h_j^{-1}h_i)h_j \in H_{\alpha_i} \cap H_{\alpha_j} \subseteq H_{\alpha_i} \cap \bigvee \{H_\beta; \beta \in I, \beta \neq \alpha_i\} = \{e\},$$

tedy $h_i^{-1}h_j^{-1}h_i h_j = e$, tzn. $h_i h_j = h_j h_i$. Protože $G = \bigvee_{\alpha \in I} H_\alpha$, dostáváme podle věty 2.3.13,

že každý prvek $e \neq g \in G$ je možno vyjádřit aspoň jedním způsobem ve tvaru součinu (1), kde $e \neq h_i \in H_{\alpha_i}$ a $\alpha_i \neq \alpha_j$ pro $i \neq j$. Předpokládejme, že existují dvě taková vyjádření prvku g . Nechť tedy $g = h_1 h_2 \cdots h_n = k_1 k_2 \cdots k_m$, kde $e \neq h_i \in H_{\alpha_i}$, $e \neq k_j \in H_{\beta_j}$, $i = 1, \dots, n$, $j = 1, \dots, m$. Pak mohou nastat dvě možnosti.

Předpokládejme nejdříve, že existuje α_i takové, že $\alpha_i \neq \beta_j$ pro každé $j = 1, \dots, m$, např., že $\alpha_1 \neq \beta_j$ pro každé $j = 1, \dots, m$. Pak $e \neq h_1 = k_1 k_2 \cdots k_m h_n^{-1} \cdots h_2^{-1} \in H_{\alpha_1} \cap$

$(\bigvee\{H_\beta; \beta \in I, \beta \neq \alpha_1\}) = \{e\}$, což je spor. Analogicky dojdeme ke sporu, když budeme předpokládat, že existuje β_j takové, že $\beta_j \neq \alpha_i$ pro každé $i = 1, \dots, n$.

Nechť tedy každá α_i se rovná některému β_j a obráceně. Pak $m = n$ a při vhodném očíslování $\alpha_i = \beta_j$, $i = 1, \dots, n$. V takovém případě ale musí existovat i takové, že $h_i \neq k_i$, např. $h_1 \neq k_1$. Pak $e \neq k_1^{-1}h_1 = k_2 \cdots k_n h_n^{-1} \cdots h_2^{-1} \in H_{\alpha_1} \cap (\bigvee\{H_\beta; \beta \in I, \beta \neq \alpha_1\}) = \{e\}$, tedy opět docházíme ke sporu.

Proto vyjádření prvku g ve tvaru (1) je jednoznačné.

b) Nechť jsou splněny podmínky 1 a 2. Ukažme nejdříve, že podgrupy H_α ($\alpha \in I$) jsou normální. Uvažujme $h \in H_{\alpha_i}$ a $e \neq g \in G$. Pak $g = h_1 h_2 \cdots h_n$, kde $e \neq h_j \in H_{\beta_j}$, $j = 1, 2, \dots, n$. Jestliže $\alpha_i \neq \beta_j$ pro každé $j = 1, 2, \dots, n$, pak $gh = hg$ podle předpokladu 1. Nechť existuje $j \in \{1, 2, \dots, n\}$ takové, že $\alpha_i = \beta_j$. Pak $g^{-1}hg = h_j^{-1}hh_j \in H_{\alpha_i}$, proto $H_{\alpha_i} \trianglelefteq G$. Dostáváme tak, že $H_\alpha \trianglelefteq G$ pro každá $\alpha \in I$. Použitím věty 2.3.13 pak z předpokladu 2 vyplývá, že $\bigvee_{\alpha \in I} H_\alpha = G$.

Zbývá ukázat, že je splněna podmínka b) z definice vnitřního direktního součinu. Nechť pro některou podgrupu H_{α_i} existuje prvek $e \neq h \in H_{\alpha_i} \cap (\bigvee\{H_\beta; \beta \in I, \beta \neq \alpha_i\})$. Pak ale prvek h je ve tvaru $h = h_1 h_2 \cdots h_n$, kde $e \neq h_j \in H_{\alpha_i}$, $e \neq h_j \in H_{\beta_j}$ a $\alpha_i \neq \beta_j$ pro každé $j = 1, 2, \dots, n$, což je spor s předpokladem jednoznačnosti v podmínce 2. Proto musí platit, že $H_{\alpha_i} \cap (\bigvee\{H_\beta; \beta \in I, \beta \neq \alpha_i\}) = \{e\}$. \square

Jestliže grupa G je vnitřním direktním součinem dvou svých podgrup H_1 a H_2 , pak podle věty 2.8.1 pro každý prvek $e \neq g \in G$ existuje jediná dvojice prvků $h_1 \in H_1$ a $h_2 \in H_2$ takových, že $g = h_1 h_2 = h_2 h_1$. Navíc platí:

Věta 2.8.2 Nechť H_1 a H_2 jsou podgrupy grupy G takové, že $G = H_1 \times^\bullet H_2$. Pak $G/H_1 \cong H_2$ a $G/H_2 \cong H_1$.

Důkaz. Protože $G = H_1 \times^\bullet H_2$, podle definice vnitřního direktního součinu a podle věty 2.3.32 platí, že $G = H_1 \vee H_2 = H_1 H_2 = H_2 H_1$ a $H_1 \cap H_2 = \{e\}$. Podle 3. věty o izomorfismu proto dostaneme $G/H_1 = H_1 H_2 / H_1 \cong H_2 / (H_1 \cap H_2) = H_2 / \{e\} \cong H_2$ a analogicky $G/H_2 \cong H_1$. \square

Právě dokázaná věta naznačuje, že zavedení pojmu vnitřní direktní součin grup bylo umožněno vzájemně jednoznačným vztahem mezi normálními podgrupami a kongruencemi grup popsaným ve větách 2.5.5 a 2.5.6. Nyní ale zavedeme pojem vnějšího direktního součinu, který je použitelný mj. i pro libovolné grupoidy. Z našeho hlediska bude podstatné, že v případě grup jsou tyto součiny rovnocenné s vnitřním součinu.

Nejdříve zobecníme pojem kartézského součinu pro libovolné systémy množin.

Definice. Nechť $(G_\alpha; \alpha \in I)$ je neprázdný systém neprázdných množin. Pak množina $G = \prod_{\alpha \in I} G_\alpha$ všech zobrazení $g : I \longrightarrow \bigcup_{\alpha \in I} G_\alpha$ takových, že $g(\alpha) \in G_\alpha$ pro každý $\alpha \in I$, se nazývá *kartézský součin množin* daného systému.

Jestliže $g \in G$, pak jej můžeme také zapsat ve tvaru $g = (g(\alpha); \alpha \in I)$. Prvek $g(\alpha)$ se pak nazývá α -tá složka prvku g . Místo $g(\alpha)$ budeme často pro α -tou složku používat označení g_α , takže prvek g pak bude zapsán ve tvaru $g = (g_\alpha; \alpha \in I)$.

Jestliže množina indexů I je konečná, např. $I = \{1, \dots, n\}$, pak pro $G = \prod_{i \in I} G_i$ použijeme také označení $G = \prod_{i=1}^n G_i = G_1 \times \dots \times G_n$. Je zřejmé, že v tomto případě je definice G ekvivalentní s původní definicí kartézského součinu množin G_1, \dots, G_n , jako množiny všech uspořádaných n -tic prvků z $G_1 \dots G_n$.

Nechť nyní $(G_\alpha = (G_\alpha; \cdot_\alpha), \alpha \in I)$ je neprázdný systém grupoidů. Na kartézském součinu $G = \prod_{\alpha \in I} G_\alpha$ jejich nosičů můžeme definovat binární operaci „ \cdot “ takto:

Jestliže $g = (g_\alpha; \alpha \in I)$ a $h = (h_\alpha; \alpha \in I)$ jsou prvky z G , pak položíme

$$g \cdot h = (g_\alpha; \alpha \in I) \cdot (h_\alpha; \alpha \in I) := (g_\alpha \cdot_\alpha h_\alpha; \alpha \in I).$$

Definice. Nechť $(G_\alpha = (G_\alpha; \cdot_\alpha), \alpha \in I)$ je neprázdný systém grupoidů a $G = \prod_{\alpha \in I} G_\alpha$. Pak grupoid $G = (G; \cdot)$ se nazývá *kartézský součin* nebo také *úplný vnější direktní součin grupoidů G_α ($\alpha \in I$)*. Píšeme pak $G = \prod_{\alpha \in I} G_\alpha$ (nebo $G = \prod_{\alpha \in I} G_\alpha$, pokud nebude nebezpečí z nedorozumění).

Nechť $\beta \in I$. Označme p_β zobrazení kartézského součinu $G = \prod_{\alpha \in I} G_\alpha$ do G_β takové, že pro každý prvek $g = (g_\alpha; \alpha \in I) \in G$ je $p_\beta(g) = g_\beta$. Je zřejmé, že p_β je surjektivní zobrazení G na G_β . Budeme jej nazývat β -tá projekce. Navíc platí, že jsou-li $g, h \in G$, pak $p_\beta(gh) = g_\beta h_\beta = p_\beta(g)p_\beta(h)$, a tedy p_β je homomorfismus grupoidu G na grupoid G_β . To znamená, že projekce p_β je pro každé $\beta \in I$ surjektivním homomorfismem kartézského součinu G grupoidů G_α ($\alpha \in I$) na grupoid G_β .

Věta 2.8.3 Jestliže v systému $(G_\alpha; \alpha \in I)$ je každý grupoid G_α grupou, pak kartézský součin $G = \prod_{\alpha \in I} G_\alpha$ je také grupa.

Důkaz. Vzhledem k tomu, že součiny prvků v G jsou určeny pomocí součinů jejich složek v jednotlivých G_α , je násobení v G asociativní, tedy G je pologrupa.

Označíme-li e_α jednotkový prvek grupy G_α ($\alpha \in I$), pak prvek $e = (e_\alpha; \alpha \in I)$ je jednotkovým prvkem v G .

Inverzním prvkem k prvku $g = (g_\alpha; \alpha \in I)$ je pak zřejmě prvek $g^{-1} = (g_\alpha^{-1}; \alpha \in I)$. □

Definice. Jestliže $(G_\alpha; \alpha \in I)$ je neprázdný systém grup, pak *vnějším direktním součinem grup G_α ($\alpha \in I$)* budeme rozumět podgrupu $\tilde{\prod}_{\alpha \in I} G_\alpha$ kartézského součinu $\prod_{\alpha \in I} G_\alpha$ grup

G_α takovou, že $g = (g_\alpha; \alpha \in I)$ patří do $\prod_{\alpha \in I} G_\alpha$ právě tehdy, když $g_\beta \neq e_\beta$ jen pro konečný počet $\beta \in I$.

Pro libovolné $\alpha \in I$ označme $\overline{G}_\alpha = \{g \in \prod_{\beta \in I} G_\beta; g_\beta = e_\beta \text{ pro každé } \beta \neq \alpha\}$. Vidíme, že \overline{G}_α je podgrupa v $\prod_{\beta \in I} G_\beta$. Jestliže $g \in \overline{G}_\alpha$, pak jej budeme označovat také \bar{g}_α .

Věta 2.8.4 *Vnější direktní součin* $H = \prod_{\alpha \in I} G_\alpha$ grup G_α je *vnitřním direktním součinem* $\prod_{\alpha \in I} \overline{G}_\alpha$ podgrup \overline{G}_α grupy $G = \prod_{\alpha \in I} G_\alpha$.

Důkaz.

1. Nechť $\alpha, \beta \in I$, $\alpha \neq \beta$ a nechť $h \in \overline{G}_\alpha$, $k \in \overline{G}_\beta$. Pak je zřejmé, že $hk = kh$.
2. Uvažujme $e \neq g \in \prod_{\alpha \in I} G_\alpha$. Nechť $\alpha_1, \dots, \alpha_n$ jsou všechny navzájem různé indexy z I takové, že $g_{\alpha_1} \neq e_{\alpha_1}, \dots, g_{\alpha_n} \neq e_{\alpha_n}$. Pak $g = \bar{g}_{\alpha_1} \cdots \bar{g}_{\alpha_n}$, kde $\bar{g}_{\alpha_1} \in \overline{G}_{\alpha_1}, \dots, \bar{g}_{\alpha_n} \in \overline{G}_{\alpha_n}$, a takové vyjádření prvku g ve tvaru součinu nejednotkových prvků z grup \overline{G}_α s navzájem různými indexy je, až na pořadí činitelů, jediné.

Tedy podle věty 2.8.1 platí, že $H = \prod_{\alpha \in I} \overline{G}_\alpha$. □

Věta 2.8.5 Nechť grupa G je *vnitřním direktním součinem* svých podgrup H_α ($\alpha \in I$). Pak platí, že G je izomorfní s *vnějším direktním součinem* $\prod_{\alpha \in I} H_\alpha$ grup H_α .

Důkaz. Nechť $e \neq g \in G$. Pak existuje jednoznačně určený rozklad $g = h_1 \cdots h_n$, kde $e \neq h_i \in H_{\alpha_i}$ a $\alpha_j \neq \alpha_k$ pro $j \neq k$. Definujme zobrazení $\varphi : G \longrightarrow \prod_{\alpha \in I} H_\alpha$ takové, že $\varphi(e) = e = (e_\alpha; \alpha \in I)$ a $\varphi(g) = \bar{h}_{\alpha_1} \cdots \bar{h}_{\alpha_n}$ pro každý $e \neq g \in G$. Pak φ je izomorfismus grupy G na grupu $\prod_{\alpha \in I} H_\alpha$. □

Poznámka 2.8.6 Na základě vět 2.8.4 a 2.8.5 se ukazuje, že algebraické vlastnosti vnitřních a vnějších direktních součinů grup jsou stejné. Proto v konkrétních situacích můžeme použít tu definici, která je momentálně výhodnější, a pro oba typy součinů budeme používat společného názvu *direktní součin grup*.

Cvičení

1. Určete, které z vlastností komutativnost, asociativnost, existence neutrálního prvku a existence symetrických prvků mají následující grupoidy:

- a) $(\mathbb{N}; \square)$, kde $a \square b = a^b$;
- b) $(\mathbb{N}; +)$;
- c) $(\mathbb{Z}; +)$;
- d) $(\mathbb{Z}; \cdot)$;
- e) $(\mathbb{R}; \cdot)$;
- f) $(\mathbb{Q} \setminus \{0\}; \cdot)$;
- g) $(\mathbb{C}; \circ)$, kde $\alpha \circ \beta = \alpha \cdot \bar{\beta}$ ($\bar{\beta}$ je číslo komplexně sdružené s β);
- h) $(M_n(\mathcal{T}); +)$, kde \mathcal{T} je číselné těleso;
- i) $(M_n(\mathcal{T}); \cdot)$;
- j) $(\text{Reg}_n(\mathcal{T}); \cdot)$, kde $\text{Reg}_n(\mathcal{T})$ označuje množinu všech regulárních matic v $M_n(\mathcal{T})$;
- k) $(\text{Sing}_n(\mathcal{T}); \cdot)$, kde $\text{Sing}_n(\mathcal{T})$ označuje množinu všech singulárních matic v $M_n(\mathcal{T})$.

2. Dokažte, že množina všech uspořádaných dvojic reálných čísel (a, b) , kde $a \neq 0$, tvoří grupu vzhledem k operaci

$$(a, b) \circ (c, d) = (ac, ad + b).$$

3. Nechť $n \in \mathbb{N}$. Dokažte, že množina všech n -tých odmocnin z čísla 1 (tj. množina všech komplexních čísel α takových, že $\alpha^n = 1$) tvoří grupu řádu n vzhledem k násobení komplexních čísel.

4. Nechť $K = \{e, a, b, c\}$ a nechť na K je definováno násobení pomocí následující Cayleyovy tabulky.

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Ověřte, že $(K; \cdot)$ je abelovská grupa (tzv. *Kleinova grupa*).

5. Nechť M je množina všech zákrytových zobrazení rovnostranného trojúhelníka. (Skládá se ze 3 otočení a 3 osových souměrností.) Ověřte, že M je grupou vzhledem ke skládání zobrazení.

6. Dokažte, že množina všech zobrazení $f : \mathbb{R} \rightarrow \mathbb{R}$ tvoří spolu se sčítáním zobrazení abelovskou grupu. (Jsou-li $f : \mathbb{R} \rightarrow \mathbb{R}$, $g : \mathbb{R} \rightarrow \mathbb{R}$ zobrazení, pak $(f + g)(x) = f(x) + g(x)$ pro každé $x \in \mathbb{R}$.)

7. Dokažte, že množina všech funkcí f reálné proměnné x takových, že

$$f(x) = \frac{ax + b}{cx + d},$$

kde $a, b, c, d \in \mathbb{R}$, $ad - bc = 1$, tvoří grupu vzhledem ke skládání funkcí.

8. Nechť \mathcal{V} je vektorový prostor nad číselným tělesem \mathcal{T} . Dokažte, že množina všech izomorfismů \mathcal{V} na \mathcal{V} tvoří grupu vzhledem ke skládání zobrazení.

9. Jestliže $\mathcal{G} = (G; \cdot)$ je grupoid, $a \in G$, pak a se nazývá *idempotentní prvek*, platí-li $a^2 = a$. Dokažte, že je-li \mathcal{G} grupa, pak jediným idempotentním prvkem v \mathcal{G} je jednotkový prvek e .

10. Nechť M je množina a $\mathcal{P}(M) = \{X; X \subseteq M\}$ její potenční množina. Pro libovolné $X, Y \in \mathcal{P}(M)$ označme

$$X \div Y = (X \setminus Y) \cup (Y \setminus X).$$

($X \div Y$ se nazývá *symetrický rozdíl* množin X a Y .) Dokažte, že $(\mathcal{P}(M); \div)$ je abelovská grupa.

11. Nechť $A = \{1, 2, 3\}$ a nechť $\mathcal{S}_3 = (S_3; \circ) = (S(A); \circ)$ je grupa všech permutací (neboli symetrická grupa) množiny A . Najděte všechny podgrupy grupy \mathcal{S}_3 .

12. Najděte všechny podgrupy

- a) grupy $(\mathbb{Z}; +)$;
- b) grupy $(\mathbb{Z}_7; \oplus)$;
- c) grupy $(\mathbb{Z}_6; \oplus)$.

13. Zjistěte, je-li množina H podgrupou grupy \mathcal{G} .

- a) $H = \mathbb{Q}^+$, $\mathcal{G} = (\mathbb{Q} \setminus \{0\}; \cdot)$;
- b) $H = \mathbb{Z}_2$, $\mathcal{G} = (\mathbb{Z}_4; +)$;
- c) $H = \{1, -1\}$, $\mathcal{G} = (\mathbb{R}; +)$;
- d) $H = \{-1, 1\}$, $\mathcal{G} = (\mathbb{R} \setminus \{0\}; \cdot)$;
- e) $H = \{\alpha \in \mathbb{C}; \alpha^n = 1 \text{ pro některé } n \in \mathbb{N}\}$, $\mathcal{G} = (\mathbb{C} \setminus \{0\}; \cdot)$.

14. Určete průnik podgrup $H_1 = \langle 4 \rangle$ a $H_2 = \langle 6 \rangle$ grupy $\mathcal{Z} = (\mathbb{Z}; +)$.

15. Jestliže $\mathcal{G} = (G; \cdot)$ je grupa, $a \in G$, pak *normalizátorem* prvku a se nazývá množina $N_a = \{x \in G; xa = ax\}$. Dokažte, že normalizátor libovolného prvku z G je podgrupou v \mathcal{G} .

16. Podgrupa H grupy \mathcal{G} se nazývá *charakteristická*, je-li invariantní ke všem (nejen vnitřním) automorfismům grupy \mathcal{G} . Dokažte, že centrum $C(\mathcal{G})$ libovolné grupy \mathcal{G} je charakteristickou podgrupou grupy \mathcal{G} .

17. Libovolný homomorfismus grupy \mathcal{G} do \mathcal{G} se nazývá *endomorfismus* grupy \mathcal{G} . Podgrupa $H \leq \mathcal{G}$ se nazývá *úplně invariantní*, jestliže H je invariantní vzhledem ke všem endomorfismům grupy \mathcal{G} . Dokažte, že komutant G' libovolné grupy \mathcal{G} je úplně invariantní podgrupa v \mathcal{G} .
18. Dokažte, že pro libovolné prvky a, b grupy \mathcal{G} platí, že součiny ab a ba mají stejný řád.
19. Najděte všechny cyklické podgrupy generované prvky symetrické grupy S_3 .
20. Dokažte, že množina všech transpozic je množinou generátorů symetrické grupy S_n pro libovolné $n > 1$.
21. Sestrojte levé a pravé rozklady symetrické grupy S_3 podle všech jejích podgrup. Rozhodněte, které z těchto podgrup jsou normální.
22. Nechť

$$\begin{aligned}\mathcal{A} &= \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}; \quad a, b \in \mathbb{R}, \quad a \neq 0 \right\}, \\ \mathcal{B} &= \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}; \quad b \in \mathbb{R} \right\}, \\ \mathcal{C} &= \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}; \quad a \in \mathbb{R}, \quad a \neq 0 \right\}.\end{aligned}$$

Dokažte, že $(\mathcal{A}; \cdot)$ je grupa, \mathcal{B} je normální podgrupa grupy $(\mathcal{A}; \cdot)$ a \mathcal{C} je podgrupa grupy $(\mathcal{A}; \cdot)$, která není normální podgrupou.

23. Dokažte, že, až na izomorfismus, existují právě dvě navzájem neizomorfní grupy řádu 4. (Využijte cvičení 4.)
24. Dokažte, že symetrická grupa S_3 je izomorfní s grupou zákrytových zobrazení rovnostranného trojúhelníka.
25. Dokažte, že pro každé $n \in \mathbb{N}$ je multiplikativní grupa n -tých odmocnin z čísla 1 izomorfní s aditivní grupou \mathbb{Z}_n .
26. Dokažte, že grupa $(\mathcal{A}; \cdot)$ z cvičení 22 je izomorfní s grupou uspořádaných dvojic reálných čísel z cvičení 2.
27. a) Dokažte, že v každé abelovské grupě \mathcal{G} je zobrazení $\varphi : G \longrightarrow G$ takové, že

$$\forall a \in G; \quad \varphi : a \longmapsto a^{-1}, \tag{*}$$

automorfismem grupy \mathcal{G} .

- b) Dokažte, že je-li v dané grupě \mathcal{G} zobrazení $\varphi : G \rightarrow G$ s vlastností (*) automorfismem grupy \mathcal{G} , pak \mathcal{G} je abelovská.
- 28.** Dokažte, že cyklickou grupu řádu 8 lze homomorfně zobrazit na cyklickou grupu řádu 4.
- 29.** Nechť $\mathcal{R}^* = (\mathbb{R} \setminus \{0\}; \cdot)$ a nechť $\psi : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{0\}$ je takové zobrazení, že $\psi : a \mapsto |a|$ pro každé $a \in \mathbb{R} \setminus \{0\}$.
- Dokažte, že ψ je endomorfismus \mathcal{R}^* do \mathcal{R}^* .
 - Popište jádro $\text{Ker } \psi$.
- 30.** Nechť $\mathcal{C}^* = (\mathbb{C} \setminus \{0\}; \cdot)$ a $\chi : \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C} \setminus \{0\}$ je zobrazení takové, že $\chi : \alpha \mapsto |\alpha|$ pro každé $\alpha \in \mathbb{C} \setminus \{0\}$.
- Dokažte, že χ je homomorfismus grupy \mathcal{C}^* do grupy \mathcal{R}^* .
 - Popište jádro $\text{Ker } \chi$.
- 31.** Sestrojte faktorovou grupu symetrické grupy S_3 podle její normální podgrupy A_3 , jejíž prvky jsou právě všechny sudé permutace.
- 32.** Najděte všechny homomorfní obrazy grupy $\mathcal{Z}_6 = (\mathbb{Z}_6; \oplus)$.
- 33.** Nechť \mathcal{G} je grupa, $H \leq \mathcal{G}$, $N \trianglelefteq \mathcal{G}$, $H \cap N = \{e\}$, $H \cup N = G$. Dokažte, že pak platí $G/N \cong H$.
- 34.** Nechť f je homomorfismus grupy \mathcal{G} na grupu \mathcal{G}' . Nechť $H' \leq \mathcal{G}'$ (resp. $H' \trianglelefteq \mathcal{G}'$). Dokažte, že úplný vzor $H = f^{-1}[H'] = \{x \in G; f(x) \in H'\}$ podgrupy H' je podgrupou (resp. normální podgrupou) grupy \mathcal{G} .

Kapitola 3

Okruhy, obory integrity, tělesa

3.1 Základní vlastnosti okruhů

V této části se budeme věnovat algebraickým strukturám se dvěma binárními operacemi. Nejdříve si znovu připomeneme základní definice.

Definice. Algebraická struktura $\mathcal{M} = (M; +, \cdot)$ se nazývá *okruh*, platí-li, že $(M; +)$ je abelovská grupa, $(M; \cdot)$ je pologrupa a násobení je distributivní zleva i zprava vzhledem ke sčítání, tj.

$$\forall a, b, c \in M; \quad a(b+c) = ab+ac, \quad (b+c)a = ba+ca.$$

Poznámka 3.1.1 Jestliže $a, b \in M$, označme $a - b = a + (-b)$. Je zřejmé, že odčítání je také binární operací na M . Z dřívějska už víme, že násobení je distributivní také vzhledem k odčítání, tedy že

$$\forall a, b, c \in M; \quad a(b - c) = ab - ac, \quad (b - c)a = ba - ca.$$

Nulový prvek okruhu \mathcal{M} (tj. nulový prvek aditivní grupy $(M; +)$) budeme označovat o . Platí

$$\forall a \in M; \quad ao = o = oa,$$

což se někdy vyjadřuje formulací, že o je *agresivní prvek* pologrupy $(M; \cdot)$.

Konečně platí, jak už také víme, že

$$\forall a, b \in M; \quad a(-b) = (-a)b = -ab.$$

Definice. a) Jestliže pro okruh $\mathcal{M} = (M; +, \cdot)$ platí, že pologrupa $(M; \cdot)$ je komutativní, pak se i *okruh \mathcal{M}* nazývá *komutativní*.

b) Je-li $(M; \cdot)$ monoid s jednotkovým prvkem e , pak e se nazývá *jednotkový prvek okruhu \mathcal{M}* .

Příklad 3.1.2 a) $\mathcal{Z} = (\mathbb{Z}; +, \cdot)$ je komutativní okruh s jednotkovým prvkem 1.

b) $\mathcal{Z}_n = (\mathbb{Z}_n; \oplus, \otimes)$, kde operace „ \oplus “ a „ \otimes “ jsou sčítání a násobení modulo n , je komutativní okruh s jednotkovým prvkem 1.

c) $2\mathcal{Z} = (2\mathbb{Z}; +, \cdot)$ je komutativní okruh, který nemá jednotkový prvek.

d) Množina všech polynomů jedné proměnné nad \mathcal{R} , popř. nad libovolným číselným tělesem \mathcal{T} je vzhledem ke sčítání a násobení polynomů komutativním okruhem, v němž je jednotkovým prvkem konstantní polynom 1.

e) Množina $M_n(\mathcal{T})$ všech čtvercových matic stupně $n \geq 2$ nad číselným tělesem \mathcal{T} tvoří okruh vzhledem ke sčítání a násobení matic. Tento okruh není komutativní, ale má jednotkový prvek (kterým je jednotková matice stupně n).

Definice. Jestliže $\mathcal{M} = (M; +, \cdot)$ je okruh a $\emptyset \neq A \subseteq M$, pak A se nazývá *uzavřená podmnožina*, je-li uzavřená vzhledem k oběma binárním operacím okruhu, tj. platí-li

$$\forall a, b \in A; a + b \in A, ab \in A.$$

Poznámka 3.1.3 Na uzavřené podmnožině A můžeme uvažovat restrikce „ $+_A$ “ a „ \cdot_A “ operací „ $+$ “ a „ \cdot “ okruhu \mathcal{M} . Budeme je ovšem bez nebezpečí z nedorozumění označovat také symboly „ $+$ “ a „ \cdot “.

Definice. Neprázdná podmnožina A okruhu $\mathcal{M} = (M; +, \cdot)$ se nazývá *podokruh* okruhu \mathcal{M} (označení: $A \leq \mathcal{M}$), jestliže A je uzavřenou podmnožinou a je okruhem vzhledem k indukovaným operacím.

Poznámka 3.1.4 Je zřejmé, že vždy platí $\{o\} \leq \mathcal{M}$ a $M \leq \mathcal{M}$. Podokruh $\{o\}$ budeme nazývat *nulovým* a oba podokruhy $\{o\}$ a M nazveme *triviálními podokruhy* okruhu \mathcal{M} .

Věta 3.1.5 Jestliže $\mathcal{M} = (M; +, \cdot)$ je okruh a $A \subseteq M$, pak $A \leq \mathcal{M}$ právě tehdy, jsou-li splněny následující podmínky:

1. $\forall a, b \in A; a + b \in A,$
2. $o \in A,$
3. $\forall a \in A; -a \in A,$
4. $\forall a, b \in A; ab \in A.$

Důkaz. Z definice podokruhu je zřejmé, že pro uzavřenou podmnožinu $A \subseteq M$ platí, že je podokruhem okruhu \mathcal{M} právě tehdy, když $(A; +)$ je podgrupou grupy $(M; +)$ a současně $(A; \cdot)$ je podpologrupou pologrupy $(M; \cdot)$.

Ovšem z kapitoly 2 víme, že $(A; +)$ je podgrupou v $(M; +)$ právě tehdy, když jsou splněny podmínky 1, 2 a 3. Podmínka 4 je samozřejmě ekvivalentní s tím, že $(A; \cdot)$ je podpologrupou v $(M; \cdot)$. \square

Poznámka 3.1.6 a) Jestliže navíc předpokládáme, že $A \neq \emptyset$, pak platí $A \subseteq M$ právě tehdy, když A splňuje podmínky 1, 3 a 4. Je-li totiž $a \in A$, pak $o = a + (-a) \in A$.

b) Analogicky jako v případě grup, okruh můžeme uvažovat jako algebraickou strukturu $M = (M; +, o, -(.), \cdot)$ se dvěma binárními operacemi „+“ a „·“, s jednou nulární operací „o“ a s jednou unární operací „ $-(.)$ “, pro které platí

$$\forall a, b, c \in M; a + (b + c) = (a + b) + c,$$

$$\forall a \in M; a + o = o + a = a,$$

$$\forall a \in M; a + (-a) = (-a) + a = o,$$

$$\forall a, b, c \in M; a(bc) = (ab)c.$$

V takovém případě pak podle věty 3.1.5 vidíme, že $A \subseteq M$ je podokruhem okruhu $M = (M; +, o, -(.), \cdot)$ právě tehdy, když A je uzavřená vzhledem ke všem čtyřem jeho operacím.

Věta 3.1.7 Pro neprázdnou podmnožinu A okruhu M platí, že $A \subseteq M$ právě tehdy, když

1. $\forall a, b \in A; a - b \in A$,
2. $\forall a, b \in A; ab \in A$.

Důkaz. Tvrzení plyne ihned z věty 3.1.5 a věty 2.3.6. \square

Definice. a) Okruh $J = (J; +, \cdot)$ se nazývá *obor integrity*, jestliže je komutativní, má jednotkový prvek $e \neq o$ a nemá netriviální dělitele nuly, tj.

$$\forall a, b \in J; ab = o, a \neq o \implies b = o.$$

b) Každý alespoň dvouprvkový okruh $T = (T; +, \cdot)$ takový, že $(T \setminus \{o\}; \cdot)$ je grupa, se nazývá *těleso*.

Poznámka 3.1.8 a) Podle definice tělesa je zřejmé, že je-li $T = (T; +, \cdot)$ těleso, pak ke každému nenulovému prvku $a \in T$ existuje v T inverzní prvek a^{-1} , který je také nenulový. Proto v rovnostech můžeme multiplikativně krátit nenulovými prvky zleva i zprava. Tj., pro libovolné prvky $a, b, c \in T$ platí, že jestliže $ab = ac$, $a \neq o$, pak $b = c$, a také z $ba = ca$, $a \neq o$ plyne $b = c$. Odtud je také vidět, jak jsme již ostatně dokázali dříve, že každé komutativní těleso je oborem integrity.

b) Podokruh okruhu M , který je vzhledem k indukovaným operacím oborem integrity (popř. tělesem), budeme nazývat *podoborem integrity* (popř. *podtělesem*) okruhu M . Přitom okruh M nemusí být ani oborem integrity ani tělesem. (Viz příklad 3.1.10.)

Příklad 3.1.9 Uvažujme okruh $\mathcal{Z}_n = (\mathbb{Z}_n; \oplus, \otimes)$ kde $n > 1$ je přirozené číslo.

a) Nechť n je složené číslo a nechť $a, b \in \mathbb{N}$, $1 < a, b < n$, $ab = n$. Pak v \mathcal{Z}_n platí $a \otimes b = 0$, tzn., že obě čísla a, b jsou netriviálními děliteli nuly. V takovém případě tedy platí, že \mathcal{Z}_n je komutativní okruh s jednotkovým prvkem 1, který ale není oborem integrity.

b) Nechť n je prvočíslo, $k, a \in \mathbb{N}$, $0 < k, a < n$, $k \otimes a = 0$. Pak existuje $x \in \mathbb{N}$ tak, že $ka = nx$, tedy $n | ka$. Protože n je prvočíslo, platí $n | k$ nebo $n | a$, což je spor s volbou čísel k a a . Tedy $k \otimes a \neq 0$ pro každá $0 < k, a < n$, a proto „ \otimes “ je binární operace na $\mathbb{Z}_n \setminus \{0\}$.

Ukažme, že $(\mathbb{Z}_n \setminus \{0\}; \otimes)$ je grupa. Samozřejmě $1 \in \mathbb{Z}_n \setminus \{0\}$. Zbývá tedy dokázat, že ke každému prvku $a \in \mathbb{Z}_n \setminus \{0\}$ existuje v $\mathbb{Z}_n \setminus \{0\}$ inverzní prvek a^{-1} . Nechť $a, k, l \in \mathbb{N}$, $0 < a < n$, $0 < k, l < n$, $k \geq l$, $k \otimes a = l \otimes a$. To ovšem znamená, že $ka \equiv la \pmod{n}$, proto $ka - la = nx$, kde $x \in \mathbb{Z}$. Tedy $(k - l)a = nx$, a protože n je prvočíslo, musí platit $n | (k - l)$. Ovšem pak podle volby čísel k a l dostáváme, že $k - l = 0$, a tedy $k = l$. Proto jsou všechna čísla $1 \otimes a, 2 \otimes a, \dots, (n-1) \otimes a$ navzájem různá, a vzhledem k tomu, že všechna patří do $\mathbb{Z}_n \setminus \{0\}$, platí $\mathbb{Z}_n \setminus \{0\} = \{1 \otimes a, 2 \otimes a, \dots, (n-1) \otimes a\}$. Proto musí existovat $k \in \mathbb{Z}_n \setminus \{0\}$ takové, že $k \otimes a = 1$, tzn. $a^{-1} = k$. Platí tedy, že je-li $n \in \mathbb{N}$ prvočíslo, pak \mathcal{Z}_n je komutativním tělesem (a tedy i oborem integrity).

Příklad 3.1.10 a) Označme A množinu všech zobrazení \mathbb{R} do \mathbb{R} a definujme pro libovolná $f, g \in A$ zobrazení $f + g$ a $f \cdot g$ takto:

$$\forall x \in \mathbb{R}; (f + g)(x) = f(x) + g(x), (f \cdot g)(x) = f(x) \cdot g(x).$$

Je zřejmé, že $f + g$ a $f \cdot g$ jsou opět zobrazení \mathbb{R} do \mathbb{R} a že vzhledem k operacím „+“ a „·“ je A okruhem. Tento okruh je navíc komutativní a má jednotkový prvek, kterým je konstantní zobrazení 1 takové, že $1 : x \mapsto 1$ pro každé $x \in \mathbb{R}$. Okruh $\mathcal{A} = (A; +, \cdot)$ ale není oborem integrity. Např. pro $f, g \in A$ takové, že

$$\forall x < 0; f(x) = -x, g(x) = 0, \quad \forall x \geq 0; f(x) = 0, g(x) = x,$$

platí $f \cdot g = 0$, ale $f \neq 0$ a $g \neq 0$. (Zde 0 označuje konstantní zobrazení, v němž obrazy všech reálných čísel jsou rovny číslu 0.) Přitom množina B všech konstantních zobrazení \mathbb{R} do \mathbb{R} je podokruhem okruhu \mathcal{A} , který je izomorfní s tělesem \mathbb{R} , a proto B je podtělesem okruhu \mathcal{A} .

b) Nechť \mathcal{T} je libovolné číselné těleso a $T[x]$ je množina všech polynomů jedné proměnné nad \mathcal{T} . Pak $T[x]$ je vzhledem ke sčítání a násobení polynomů oborem integrity $T[x]$, který není tělesem, a přitom množina všech konstantních polynomů (tj. polynomů stupně 0 spolu s nulovým polynomem) je podtělesem v $T[x]$.

3.2 Ideály a homomorfismy okruhů

V teorii grup jsme mezi všemi podgrupami dané grupy vyčlenili normální podgrupy, jejichž význam se ukázal např. při konstrukci faktorových grup a ve větě o homomorfismu (a v dalších větách o izomorfismu) grup. Analogickým pojmem k normální podgrupě je v teorii okruhů pojem (oboustranného) ideálu okruhu.

Definice. Neprázdná podmnožina I okruhu \mathcal{M} se nazývá *ideál* okruhu \mathcal{M} (označení: $I \trianglelefteq \mathcal{M}$), platí-li

1. $\forall a, b \in I; a - b \in I;$
2. $\forall a \in I, r \in M; ra \in I, ar \in I.$

Příklad 3.2.1 Ideálem oboru integrity \mathcal{Z} je např. množina všech sudých celých čísel $2\mathbb{Z}$.

Poznámka 3.2.2 a) Někdy se používají i pojmy jednostranných (tj. levých a pravých) ideálů. Neprázdná množina I se pak nazývá *levý* (popř. *pravý*) *ideál* v \mathcal{M} , platí-li podmínka 1 z definice ideálu a platí-li pro každé $a \in I$ a $r \in M$, že $ra \in I$ (popř., že $ar \in I$). V takovém případě se pak ideál podle původní definice nazývá *oboustranný ideál*.

b) Je zřejmé, že každý ideál je podokruhem okruhu \mathcal{M} . Přitom ale podokruh nemusí být ideálem v \mathcal{M} .

Příklad 3.2.3 Uvažujme znovu okruh \mathcal{A} všech zobrazení \mathbb{R} do \mathbb{R} (neboli okruh všech reálných funkcí jedné proměnné s definičním oborem \mathbb{R}) z příkladu 3.1.10. Snadno vidíme, že množina C všech omezených funkcí z A je podokruhem v \mathcal{A} , který ale není ideálem v \mathcal{A} .

Poznámka 3.2.4 Jestliže \mathcal{M} je okruh a $A, B \subseteq M$, pak *součtem podmnožin* A a B budeme rozumět množinu $A + B \subseteq M$ takovou, že

$$A + B = \{a + b; a \in A, b \in B\}.$$

Jestliže $A = \{a\}$, pak místo $\{a\} + B$ píšeme $a + B$. Podobně můžeme definovat *rozdíl* a *součin* podmnožin A a B okruhu \mathcal{M} :

$$A - B = \{a - b; a \in A, b \in B\},$$

$$AB = \{ab; a \in A, b \in B\}.$$

(Pozor: V případě podmnožin okruhu nezaměňujme jejich rozdíl $A - B$ ve smyslu teorie okruhů s množinovým rozdílem $A \setminus B$.)

Definice podokruhu a ideálu okruhu \mathcal{M} pak můžeme přeformulovat takto:

Neprázdná podmnožina A okruhu \mathcal{M} je podokruhem v \mathcal{M} (tj. $A \leq \mathcal{M}$) právě tehdy, když $A - A \subseteq A$, $AA \subseteq A$.

Neprázdná podmnožina I okruhu \mathcal{M} je ideálem v \mathcal{M} (tj. $I \trianglelefteq \mathcal{M}$) právě tehdy, když $I - I \subseteq I$, $MI \subseteq I$, $IM \subseteq I$.

Definice. Nechť $\mathcal{M} = (M; +, \cdot)$ je okruh, $A \leq \mathcal{M}$, $x \in M$. Pak třídou prvku x vzhledem k podokruhu A rozumíme množinu $x + A$, tj. (levou) třídu prvku x v aditivní grupě $(M; +)$ vzhledem k její podgrupě $(A; +)$.

Poznámka 3.2.5 Vzhledem k tomu, že $(M; +)$ je abelovská grupa, je každá její podgrupa normální (a tedy také levé a pravé třídy prvků splývají). Proto faktorová množina M/A je (abelovskou) grupou vzhledem k operaci „+“, kde

$$\forall x, y \in M : (x + A) + (y + A) = (x + y) + A.$$

Nulovým prvkem v $(M/A; +)$ je podokruh A , opačným prvkem ke třídě $x + A$ je třída $(-x) + A$.

Věta 3.2.6 Nechť I je ideál okruhu \mathcal{M} . Jestliže pro libovolné prvky $x, y \in M$ položíme $(x + I) \cdot (y + I) = xy + I$, pak „·“ je binární operace na M/I .

Důkaz. Nechť $I \trianglelefteq \mathcal{M}$ a nechť $x, x_1, y, y_1 \in M$ jsou takové, že $x_1 + I = x + I$ a $y_1 + I = y + I$. Pak $x_1 - x \in I$ a $y_1 - y \in I$, tedy platí

$$x_1 y_1 - xy = x_1 y_1 - x_1 y + x_1 y - xy = x_1(y_1 - y) + (x_1 - x)y \in MI + IM,$$

a protože I je ideál, dostáváme

$$x_1 y_1 - xy \in MI + IM \subseteq I.$$

To ovšem znamená, že $x_1 y_1 + I = xy + I$, a proto definice součinu tříd podle I je korektní (tj., nezávisí na výběru reprezentantů z jednotlivých tříd). \square

Věta 3.2.7 Jestliže I je ideál okruhu \mathcal{M} , pak $\mathcal{M}/I = (M/I; +, \cdot)$ je okruh.

Důkaz. Každý ideál okruhu je jeho podokruhem, proto podle poznámky 3.2.5 platí, že $(M/I; +)$ je abelovská grupa. Podle věty 3.2.6 je $(M/I; \cdot)$ grupoid a díky asociativnosti násobení v M je i $(M/I; \cdot)$ pologrupou. Stejně snadno lze ověřit, že násobení v M/I je zleva i zprava distributivní vzhledem ke sčítání. \square

Definice. Okruh \mathcal{M}/I se nazývá faktorový okruh okruhu \mathcal{M} podle ideálu I .

Definice. a) Nechť $\mathcal{M} = (M; +, \cdot)$ a $\mathcal{M}' = (M'; +, \cdot)$ jsou okruhy a nechť f je zobrazení množiny M do množiny M' . Pak f se nazývá homomorfismus okruhu \mathcal{M} do okruhu \mathcal{M}' , platí-li

$$\forall a, b \in M; f(a + b) = f(a) + f(b), f(ab) = f(a)f(b),$$

tedy jestliže f je současně homomorfismem grupy $(M; +)$ do grupy $(M'; +)$ a homomorfismem pologrupy $(M; \cdot)$ do pologrupy $(M'; \cdot)$.

b) Řekneme, že okruh \mathcal{M}' je *homomorfním obrazem* okruhu \mathcal{M} , existuje-li alespoň jeden surjektivní homomorfismus \mathcal{M} na \mathcal{M}' .

c) Bijektivní homomorfismus okruhu \mathcal{M} na okruh \mathcal{M}' se nazývá *izomorfismus*.

d) Okruhy \mathcal{M} a \mathcal{M}' se nazývají *izomorfní*, existuje-li alespoň jeden izomorfismus jednoho z těchto okruhů na druhý.

Poznámka 3.2.8 Podobně jako v případě grup platí, že identické zobrazení je izomorfismem okruhu \mathcal{M} na okruh \mathcal{M} , že složení dvou izomorfismů okruhů je opět izomorfismem okruhů, a že je-li f izomorfismus okruhu \mathcal{M} na okruh \mathcal{M}' , pak inverzní zobrazení f^{-1} je izomorfismem okruhu \mathcal{M}' na okruh \mathcal{M} . Proto relace „být izomorfní s“ je ekvivalencí na třídě všech okruhů, a tedy rozkládá tuto třídu na třídy navzájem izomorfních okruhů, které mají stejné algebraické vlastnosti. To znamená, že i zde můžeme používat formulaci, že „danou vlastnost mají, až na izomorfismus, právě jisté okruhy“.

Definice. Jestliže f je homomorfismus okruhu \mathcal{M} do okruhu \mathcal{M}' , pak *jádrem* f budeme rozumět množinu $\text{Ker } f \subseteq M$ takovou, že $\text{Ker } f = \{x \in M; f(x) = o'\}$, kde o' je nulový prvek okruhu \mathcal{M}' .

Věta 3.2.9 Jestliže f je homomorfismus okruhu \mathcal{M} do okruhu \mathcal{M}' , pak $\text{Ker } f \trianglelefteq M$.

Důkaz. Z teorie grup víme, že $\text{Ker } f$ je (normální) podgrupou aditivní grupy $(M; +)$. Nechť tedy $a \in \text{Ker } f$, $x \in M$. Pak

$$\begin{aligned} f(ax) &= f(a)f(x) = o' \cdot f(x) = o', \\ f(xa) &= f(x)f(a) = f(x) \cdot o' = o', \end{aligned}$$

tzn., že $ax \in \text{Ker } f$ a $xa \in \text{Ker } f$, a proto $\text{Ker } f$ je ideál okruhu \mathcal{M} . \square

Věta 3.2.10 Jestliže \mathcal{M} je okruh a $I \trianglelefteq M$, pak zobrazení $\nu : M \longrightarrow M/I$ takové, že $\nu : x \longmapsto x + I$ pro každý $x \in M$, je homomorfismem \mathcal{M} na faktorový okruh M/I . Přitom $\text{Ker } \nu = I$.

Důkaz. Na základě analogické věty z teorie grup platí, že ν je surjektivní homomorfismus aditivní grupy $(M; +)$ na faktorovou grupu $(M/I; +)$. Nechť $x, y \in M$. Pak

$$\nu(xy) = xy + I = (x + I) \cdot (y + I) = \nu(x) \cdot \nu(y),$$

a tedy ν je také homomorfismem multiplikativní pologrupy $(M; \cdot)$ na pologrupu $(M/I; \cdot)$, tzn. ν je surjektivním homomorfismem okruhů. Přitom pro každý $x \in M$

$$x \in \text{Ker } \nu \iff \nu(x) = I \iff x + I = I \iff x \in I.$$

\square

Definice. Zobrazení ν z předchozí věty se nazývá *přirozený homomorfismus* okruhu \mathcal{M} na faktorový okruh M/I .

Věta 3.2.11 (Věta o homomorfismu okruhů) Nechť f je surjektivní homomorfismus okruhu $\mathcal{M} = (M; +, \cdot)$ na okruh $\mathcal{M}' = (M'; +, \cdot)$. Pak okruh \mathcal{M}' je izomorfní s faktorovým okruhem $\mathcal{M}/\text{Ker } f$ a přitom existuje právě jeden izomorfismus g okruhu \mathcal{M}' na okruh $\mathcal{M}/\text{Ker } f$ takový, že $f \circ g = \nu$, kde ν je přirozený homomorfismus \mathcal{M} na $\mathcal{M}/\text{Ker } f$.

Obsah věty můžeme znázornit diagramem:

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{\nu} & \mathcal{M}/\text{Ker } f \\ f \downarrow & & \nearrow g \\ \mathcal{M}' & & \end{array}$$

Důkaz. Označme $I = \text{Ker } f$. Víme, že I je ideál okruhu \mathcal{M} , proto $(I; +)$ je podgrupou aditivní grupy $(M; +)$. Ovšem $(M; +)$ je komutativní, tedy I je její normální podgrupou. Navíc, pokud se omezíme jen na operaci sčítání, f je homomorfismus grupy $(M; +)$ na grupu $(M'; +)$. Proto podle věty o homomorfismu grup platí, že grupy $(M'; +)$ a $(M/I; +)$ jsou izomorfní a že existuje právě jeden izomorfismus g grupy $(M'; +)$ na grupu $(M/I; +)$ takový, že $f \circ g = \nu$. (Pro připomenutí, g je takové zobrazení, že pro každý prvek $b \in M'$ platí $g : b \mapsto a + I$, kde a je libovolný prvek z M , který se v homomorfismu f zobrazí na b .)

Zbývá proto jenom dokázat, že g je také homomorfismem okruhů. Nechť $b_1, b_2 \in M'$, $a_1, a_2 \in M$, $f(a_1) = b_1$, $f(a_2) = b_2$. Pak

$$g(b_1 b_2) = g(f(a_1) f(a_2)) = g(f(a_1 a_2)) = a_1 a_2 + I = (a_1 + I) \cdot (a_2 + I) = g(b_1) \cdot g(b_2).$$

□

Poznámka 3.2.12 a) Podle vět 3.2.9 a 3.2.10 platí, že jádry homomorfismů okruhu \mathcal{M} do dalších okruhů jsou právě všechny ideály okruhu \mathcal{M} . Přitom podle věty 3.2.10 je faktorový okruh okruhu \mathcal{M} podle jeho libovolného ideálu I homomorfním obrazem okruhu \mathcal{M} a jedním z homomorfismů \mathcal{M} na \mathcal{M}/I je odpovídající přirozený homomorfismus. Věta 3.2.11 pak říká, že, až na izomorfismus, neexistují jiné homomorfní obrazy okruhu \mathcal{M} než jeho faktorové okruhy a že každý homomorfismus okruhu \mathcal{M} na některý jeho homomorfní obraz pak může být nahrazen přirozeným homomorfismem.

Máme-li tedy za úkol určit všechny homomorfní obrazy daného okruhu \mathcal{M} , pak jej můžeme vyřešit tak, že najdeme všechny ideály okruhu \mathcal{M} a pak sestrojíme faktorové okruhy okruhu \mathcal{M} podle těchto ideálů. Tím je daný úkol, až na izomorfismus, zcela vyřešen. Tzn., že homomorfní obrazy okruhu \mathcal{M} jsou právě všechny jeho faktorové okruhy a okruhy s nimi izomorfní.

b) Připomeňme si, že pro algebraické struktury s jednou binární operací platí např., že homomorfní obraz pologrupy je opět pologrupou, homomorfní obraz grupy je také grupou,

atd. U algebraických struktur se dvěma binárními operacemi, kterým se věnujeme, je ale situace složitější. Např. homomorfní obraz oboru integrity nemusí být oborem integrity. K tomu stačí uvažovat okruhy \mathcal{Z} a \mathcal{Z}_4 a zobrazení $f : \mathbb{Z} \rightarrow \mathbb{Z}_4$ takové, že je-li $a \in \mathbb{Z}$, pak $f : a \mapsto r_a$, kde r_a je nejmenší nezáporný zbytek při dělení čísla a číslem 4. Platí, že f je homomorfismus \mathcal{Z} na \mathcal{Z}_4 a přitom \mathcal{Z} je obor integrity, zatímco \mathcal{Z}_4 má netriviální dělitele nuly.

Na druhé straně ale homomorfní obraz oboru integrity, který není tělesem, může být tělesem. Např. stačí uvažovat obor integrity \mathcal{Z} a těleso \mathcal{Z}_5 a použít pro ně analogický homomorfismus \mathcal{Z} na \mathcal{Z}_5 jako v předchozím případě.

c) Nechť $\mathcal{M} = (M; +, \cdot)$ je libovolný okruh a nechť I a J jsou jeho ideály. Pak $(I \cap J; +)$ a $(I + J; +)$ jsou podle vět o (normálních) podgrupách grup (věty 2.17 a 2.18) podgrupami aditivní grupy $(M; +)$. Dále pro libovolný prvek $a \in I \cap J$ a libovolný prvek $x \in M$ platí, že $ax \in I \cap J$ a $xa \in I \cap J$. Konečně pro libovolný $b \in I + J$, kde $b = b_1 + b_2$, $b_1 \in I$, $b_2 \in J$, a libovolný $y \in M$ platí $by = (b_1 + b_2)y = b_1y + b_2y \in I + J$ a také analogicky $yb \in I + J$. Tedy $I \cap J$ a $I + J$ jsou ideály okruhu \mathcal{M} .

Na základě této skutečnosti bychom mohli zformulovat, stejně jako pro grupy, tři věty o izomorfismu okruhů (věta o homomorfismu okruhů je speciálním případem jedné z nich) a ověřit jejich pravdivost analogicky jako u vět o izomorfismu grup.

Příklad 3.2.13 Uvažujme okruh \mathcal{Z} . Snadno se můžeme přesvědčit, že ideály tohoto okruhu jsou právě všechny množiny $n\mathbb{Z}$, kde $0 \leq n \in \mathbb{Z}$. Proto libovolný okruh, který je homomorfním obrazem okruhu \mathcal{Z} , je izomorfní s některým faktorovým okruhem $\mathcal{Z}/n\mathbb{Z}$ okruhu \mathcal{Z} podle některého ideálu $n\mathbb{Z}$.

Můžeme sestrojit např. faktorový okruh $\mathcal{Z}/3\mathbb{Z}$, který má tyto tabulky operací:

\oplus	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	\otimes	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$3\mathbb{Z}$	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$3\mathbb{Z}$	$3\mathbb{Z}$	$3\mathbb{Z}$	$3\mathbb{Z}$
$1 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$2 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$

Pak např. okruh \mathcal{Z}_3 je izomorfní s $\mathcal{Z}/3\mathbb{Z}$.

Podle věty o homomorfismu okruhů je každý homomorfní obraz daného okruhu izomorfní s faktorovým okruhem toho okruhu podle některého z jeho ideálů. Ukažme si proto některé vztahy mezi vlastnostmi ideálů a odpovídajících faktorových okruhů, a to pro případ komutativních okruhů s jednotkovými prvky.

Definice. Nechť \mathcal{M} je okruh a nechť $I \trianglelefteq \mathcal{M}$, $I \neq M$. Pak I se nazývá

- a) *maximální ideál* v \mathcal{M} , jestliže pro každý $J \trianglelefteq \mathcal{M}$ takový, že $I \subseteq J \subseteq M$, platí $J = I$ nebo $J = M$;
- b) *prvoideál* v \mathcal{M} , jestliže

$$\forall a, b \in M; ab \in I \implies a \in I \text{ nebo } b \in I.$$

Věta 3.2.14 Nechť \mathcal{M} je netriviální komutativní okruh s jednotkovým prvkem e a nechť $I \trianglelefteq \mathcal{M}$, $I \neq M$. Pak

- a) \mathcal{M}/I je obor integrity právě tehdy, když I je prvoideál;
- b) \mathcal{M}/I je (komutativní) těleso právě tehdy, když I je maximální ideál.

Důkaz. Zřejmě \mathcal{M}/I je komutativní okruh s jednotkovým prvkem. Proto platí:

a) \mathcal{M}/I je obor integrity právě tehdy, když neobsahuje netriviální dělitele nuly, neboli právě tehdy, když pro každé $a, b \in M$ z $ab + I = (a + I) \cdot (b + I) = I$ vyplývá $a + I = I$ nebo $b + I = I$. To je pak ovšem ekvivalentní s tím, že jsou-li $a, b \in M$ takové, že $ab \in I$, pak $a \in I$ nebo $b \in I$, neboli že I je prvoideál.

b) Nechť ideál I je maximální a $b \in M \setminus I$. Označme $B = \{c + bx; c \in I, x \in M\}$. Pak $B \trianglelefteq \mathcal{M}$ a $I \cup \{b\} \subseteq B$, proto $B = M$. Tedy speciálně $e \in B$, tzn., že existuje prvek $a \in M$ takový, že $e = c + ba$. Odtud dostáváme, že $e + I = (c + I) + (b + I) \cdot (c + I) = (b + I) \cdot (a + I)$, a tedy pro každou třídu $b + I$ existuje inverzní třída $(b + I)^{-1} = a + I$. Proto \mathcal{M}/I je těleso.

Z postupu je vidět, že platí i obrácená implikace. \square

Důsledek 3.2.15 Jestliže \mathcal{M} je komutativní okruh s jednotkovým prvkem, pak každý maximální ideál v \mathcal{M} je prvoideálem v \mathcal{M} .

Poznámka 3.2.16 Obrácená implikace obecně neplatí.

3.3 Charakteristiky okruhů a prvookruhy okruhů

V další části se budeme věnovat pojmu charakteristika okruhu, k jejímuž zavedení budeme pracovat s řády prvků okruhu vzhledem k jeho aditivní grupě. Znamená to tedy, že je-li $\mathcal{M} = (M; +, \cdot)$ okruh, pak budou pro nás podstatné řády prvků z M v grupě $(M; +)$. Protože se jedná o aditivní symboliku, budeme používat celé násobky prvků. Připomeňme si, že jestliže $a \in M$, $n \in \mathbb{N}$, pak

$$\begin{aligned} 1 \times a &= a, \quad (n+1) \times a = (n \times a) + a, \\ 0 \times a &= 0, \quad (-n) \times a = -(n \times a) = n \times (-a). \end{aligned}$$

Pak řád prvku $a \in M$ je definován takto:

- a) Jestliže pro každé $n \in \mathbb{N}$ platí $n \times a \neq 0$, pak a má nekonečný řád.
- b) Jestliže existují přirozená čísla n taková, že $n \times a = 0$, pak řádem prvku a je nejmenší z těch čísel.

Věta 3.3.1 Jestliže okruh \mathcal{M} nemá netriviální dělitele nuly, pak všechny nenulové prvky z M mají stejný řád.

Důkaz. Ukažme nejdříve, že v každém okruhu pro každé dva jeho prvky a a b a pro každé $k \in \mathbb{N}$ platí, že $(k \times a)b = k \times ab = a(k \times b)$. Zřejmě $(1 \times a)b = ab = 1 \times ab = a(1 \times b)$.

Předpokládejme nyní, že pro $n \in \mathbb{N}$ už platí $(n \times a)b = n \times ab = a(n \times b)$. Pak

$$((n+1) \times a)b = ((n \times a) + a)b = ((n \times a)b) + ab = (n \times ab) + ab = (n+1) \times ab,$$

proto dokazované rovnosti platí pro všechna přirozená čísla.

Dále vidíme, že

$$(0 \times a)b = ob = o = 0 \times ab = a(0 \times b)$$

a pro každé $n \in \mathbb{N}$

$$((-n) \times a)b = (n \times (-a))b = n \times (-a)b = n \times (-ab) = (-n) \times ab,$$

a tedy rovnosti platí pro všechna celá čísla.

Nechť tedy \mathcal{M} nemá netriviální dělitele nuly, $a, b \in M$, $a \neq o \neq b$. Jestliže $k \times a = o$, pak $(k \times a)b = o$, proto také $a(k \times b) = o$, a tedy $k \times b = o$. Podobně z $k \times b = o$ dostaneme $k \times a = o$. Tedy $k \times a = o$ právě tehdy, když $k \times b = o$, a odtud již dostáváme tvrzení. \square

Poznámka 3.3.2 Jestliže však \mathcal{M} má netriviální dělitele nuly, pak jeho různé nenulové prvky mohou mít různé řády.

Příklad 3.3.3 Uvažujme okruh \mathbb{Z}_6 . Pak čísla 1 a 5 mají řád 6, čísla 2 a 4 mají řád 3 a číslo 3 má řád 2.

Definice. a) Řekneme, že okruh \mathcal{M} má charakteristiku k ($k \in \mathbb{N}$), jestliže k je nejmenší přirozené číslo takové, že $k \times a = o$ pro všechny prvky $a \in M$.

b) Jestliže takové přirozené číslo k neexistuje, pak říkáme, že \mathcal{M} je nekonečné charakteristiky (nebo že má charakteristiku 0).

Věta 3.3.4 Má-li okruh \mathcal{M} jednotkový prvek e , pak charakteristika okruhu \mathcal{M} je rovna řádu prvku e .

Důkaz. Jestliže prvek e má řád k , pak pro každý $a \in M$ platí $k \times a = k \times ea = (k \times e)a = oa = o$. Přitom žádné číslo $l \in \mathbb{N}$, $l < k$ nemá tuto vlastnost, protože $l \times e \neq o$.

Jestliže e má nekonečný řád, pak samozřejmě i charakteristika okruhu \mathcal{M} je nekonečná. \square

Poznámka 3.3.5 a) Právě dokázaná věta velice podstatně zjednoduší určování charakteristiky okruhu \mathcal{M} , pokud \mathcal{M} má jednotkový prvek. Podle původní definice totiž musíme hledat (pokud existuje) nejmenší přirozené číslo k splňující $k \times a = o$ pro každý prvek $a \in M$, tzn., že nalezení konečného řádu některého z nenulových prvků ještě nedává téměř žádnou informaci o charakteristice okruhu. Pro okruh \mathcal{M} s jednotkovým prvkem e však stačí k určení charakteristiky okruhu \mathcal{M} nalézt řád *jediného* prvku, a to prvku e .

Podobně pro charakteristiku okruhu bez netriviálních děliteů nuly stačí podle věty 3.3.1 určit řád kteréhokoliv z nenulových prvků toho okruhu.

b) Podle věty 3.3.4 můžeme také snadno ověřit, že každé přirozené číslo n je charakteristikou některého okruhu. Stačí k tomu uvažovat okruh \mathbb{Z}_n . Protože \mathbb{Z}_n má jednotkový prvek 1, je jeho charakteristika rovna řádu čísla 1, tj. je rovna n .

c) Pro charakteristiky oborů integrity a těles však platí podstatná omezení, jak je ukázáno v následující větě.

Věta 3.3.6 Nechť \mathcal{M} je nenulový okruh bez netriviálních dělitelů nuly. Pak \mathcal{M} je buď nekonečné charakteristiky nebo jeho charakteristikou je prvočíslo.

Důkaz. Nechť \mathcal{M} má konečnou charakteristiku k a nechť $k = m \cdot n$, kde $1 < m < k$, $1 < n < k$. Pak pro libovolný prvek $o \neq a \in M$ platí

$$\begin{aligned} (m \times a)(n \times a) &= m \times (a(n \times a)) = m \times (n \times a^2) = mn \times a^2 = k \times a^2 = \\ &= (k \times a)a = o \times a = o, \end{aligned}$$

tzn., že $m \times a = o$ nebo $n \times a = o$. Protože podle věty 3.3.1 je číslo k také řádem prvku a , nemůže platit ani $m \times a = o$ ani $n \times a = o$, tedy dostáváme spor. \square

Důsledek 3.3.7 Každý obor integrity a každé těleso má buď nekonečnou nebo prvočíselnou charakteristiku.

Věta 3.3.8 Nechť \mathcal{M} je okruh a A_α ($\alpha \in I$) jsou podokruhy okruhu \mathcal{M} . Pak $A = \bigcap_{\alpha \in I} A_\alpha$ je také podokruhem okruhu \mathcal{M} .

Důkaz. Na základě analogické věty z teorie grup víme, že A je podgrupou aditivní grupy $(M; +)$. Stačí proto ukázat, že A je uzavřená vzhledem k násobení. Nechť $a, b \in A$. Pak $a, b \in A_\alpha$ pro každé $\alpha \in I$, proto také do každého A_α patří ab , a tedy $ab \in A$. \square

Pro každou podmnožinu okruhu \mathcal{M} existují podokruhy v \mathcal{M} , které tuto podmnožinu obsahují. (Např. okruh \mathcal{M} .) Proto můžeme zformulovat následující definici.

Definice. Jestliže \mathcal{M} je okruh a $B \subseteq M$, pak průnik všech podokruhů okruhu \mathcal{M} , které obsahují B , se nazývá *podokruh v \mathcal{M} generovaný množinou B* . Označíme jej $\langle B \rangle$.

Poznámka 3.3.9 a) $\langle B \rangle$ je tedy nejmenší podokruh okruhu \mathcal{M} obsahující B , tzn., že je obsažen v každém podokruhu okruhu \mathcal{M} , který obsahuje B .

b) Jestliže $B = \{b\}$, pak místo $\langle \{b\} \rangle$ budeme stručněji psát $\langle b \rangle$.

Věta 3.3.10 Nechť \mathcal{M} je okruh bez dělitelů nuly, který má jednotkový prvek e .

a) Jestliže \mathcal{M} má nekonečnou charakteristiku, pak obsahuje podokruh izomorfní s obořem integrity \mathcal{Z} .

b) Jestliže \mathcal{M} má konečnou (tzn. prvočíselnou) charakteristiku p , pak obsahuje podokruh izomorfní s tělesem \mathcal{Z}_p .

Důkaz. Dokažme nejdříve, že vždy platí $\langle e \rangle = \{n \times e; n \in \mathbb{Z}\}$. Je zřejmé, že $\{n \times e; n \in \mathbb{Z}\} \subseteq \langle e \rangle$. Obráceně, nechť $m, n \in \mathbb{Z}$. Pak platí

$$(m \times e) - (n \times e) = (m - n) \times e, \quad (m \times e)(n \times e) = mn \times e^2 = mn \times e,$$

tedy množina $\langle e \rangle$ je podokruhem v \mathcal{M} , který obsahuje e , a proto $\langle e \rangle = \{n \times e; n \in \mathbb{Z}\}$.

a) Nechť \mathcal{M} má nekonečnou charakteristiku. Uvažujeme zobrazení $f : \mathbb{Z} \longrightarrow \langle e \rangle$ takové, že $f(n) = n \times e$ pro každé $n \in \mathbb{Z}$. Je zřejmé, že f je surjektivní. Navíc pro libovolná $m, n \in \mathbb{Z}$ platí, že

$$f(m+n) = (m+n) \times e = (m \times e) + (n \times e) = f(m) + f(n),$$

$$f(mn) = mn \times e = (m \times e)(n \times e) = f(m)f(n).$$

Proto f je homomorfismus okruhu \mathcal{Z} na $\langle e \rangle$.

Předpokládejme, že existují $m, n \in \mathbb{Z}$, $m > n$ taková, že $m \times e = n \times e$. Pak

$$(m \times e) - (n \times e) = (m - n) \times e = o,$$

a protože $m - n > 0$, dostáváme spor s tím, že \mathcal{M} je nekonečné charakteristiky. Proto taková m a n nemohou existovat, a tedy f je injektivní.

Dokázali jsme tak, že f je izomorfismus \mathcal{Z} na $\langle e \rangle$, tedy $\mathcal{Z} \cong \langle e \rangle$.

b) Předpokládejme nyní, že \mathcal{M} má konečnou charakteristiku p . Samozřejmě platí, že p je prvočíslo. Protože p řádem prvku e v grupě $(M; +)$, platí pro každé číslo $k \in \mathbb{Z}$, že $k \times e = o$ právě tehdy, když $p \mid k$. Tedy $m \times e = n \times e$ právě tehdy, když $p \mid (m - n)$, tj. právě když $m \equiv n \pmod{p}$. Označíme-li tedy \bar{m} a \bar{n} zbytkové třídy modulo p určené čísla m a n , pak $\bar{m} = \bar{n}$ právě tehdy, když $m \times e = n \times e$.

Označme $g : \mathbb{Z}_p \longrightarrow \langle e \rangle$ zobrazení takové, že $g(\bar{n}) = n \times e$ pro každé $n \in \mathbb{Z}$. Podle předchozích úvah platí, že g je injektivní. Přitom surjektivnost je zřejmá. Skutečnost, že g je izomorfismus okruhů se dokáže analogicky jako pro zobrazení f v části a). Tedy g je izomorfismus okruhu \mathcal{Z}_p na $\langle e \rangle$, tzn., že $\mathcal{Z}_p \cong \langle e \rangle$. \square

Definice. Jestliže okruh \mathcal{M} má jednotkový prvek e , pak podokruh $\langle e \rangle$ se nazývá *prvookruh* okruhu \mathcal{M} .

Poznámka 3.3.11 Podle věty 3.3.10 platí, že je-li \mathcal{M} obor integrity, pak jeho prvoocíslu je izomorfní buď s oborem integrity \mathcal{Z} (pokud \mathcal{M} je nekonečné charakteristiky) nebo s tělesem \mathcal{Z}_p , kde p je prvoocíslu (pokud \mathcal{M} má konečnou charakteristiku p).

Věta 3.3.12 Jestliže T je těleso, a jestliže A_α ($\alpha \in I$) jsou podtělesa tělesa T , pak $A = \bigcap_{\alpha \in I} A_\alpha$ je také podtěleso tělesa T .

Důkaz. Podle věty 3.3.8 platí, že A je podokruh v T . Navíc je zřejmé, že jednotkový prvek e tělesa T patří do A . Přitom jestliže $o \neq a \in A$, pak $a \in A_\alpha$ pro každé $\alpha \in I$, tedy i $a^{-1} \in A_\alpha$ pro každé $\alpha \in I$, a to znamená, že $a^{-1} \in A$. \square

Protože každá podmnožina tělesa T je obsažena alespoň v jednom podtělese tělesa T , můžeme pro tělesa zavést pojem analogický s pojmem prvoocíslu okruhu.

Definice. Jestliže T je těleso a $B \subseteq T$, pak průnik všech podtěles tělesa T obsahujících podmnožinu B se nazývá podtěleso tělesa T generované B . Značíme jej $\overline{\langle B \rangle}$. Jestliže $b \in T$, pak místo $\overline{\langle \{b\} \rangle}$ píšeme $\overline{\langle b \rangle}$.

Věta 3.3.13 Nechť T je komutativní těleso.

- a) Jestliže T má konečnou charakteristiku p , pak T obsahuje podtěleso izomorfní s tělesem \mathcal{Z}_p .
- b) Jestliže T má nekonečnou charakteristiku, pak T obsahuje podtěleso izomorfní s tělesem \mathbb{Q} .

Důkaz. Nechť e je jednotkový prvek tělesa T .

a) Podle věty 3.3.10 platí, že má-li T charakteristiku p , pak pro podokruh $\langle e \rangle$ generovaný prvkem e platí $\langle e \rangle \cong \mathcal{Z}_p$, a protože pro prvoocíslu p platí, že \mathcal{Z}_p je těleso, je tělesem i podokruh $\langle e \rangle$. Tedy $\overline{\langle e \rangle} = \langle e \rangle = \mathcal{Z}_p$.

b) Nechť T má nekonečnou charakteristiku. Pak do podtělesa $\overline{\langle e \rangle}$ patří nejenom násobky $n \times e$, kde $n \in \mathbb{Z}$, ale také všechny podíly $(m \times e)(n \times e)^{-1}$, kde $m, n \in \mathbb{Z}$, $n \neq 0$. (Takový podíl existuje pro všechna taková m, n , protože z $n \neq 0$ vyplývá díky nekonečné charakteristice, že $n \times e \neq o$.) Množina všech takových prvků už tvoří podtěleso tělesa T a přitom tyto prvky patří do každého podtělesa v T , které obsahuje e . Proto

$$\overline{\langle e \rangle} = \{(m \times e)(n \times e)^{-1}; m, n \in \mathbb{Z}, n \neq 0\}.$$

Označme $f : \mathbb{Q} \longrightarrow \overline{\langle e \rangle}$ takové zobrazení, že $f(\frac{m}{n}) = (m \times e)(n \times e)^{-1}$ pro každá $m, n \in \mathbb{Z}$, $n \neq 0$. Podle předchozích úvah vidíme, že f je surjekce. Dokážeme také injektivnost zobrazení f . Nechť $m, n, k, l \in \mathbb{Z}$, $n \neq 0$, $l \neq 0$, a nechť $f(\frac{m}{n}) = f(\frac{k}{l})$. Pak

$$(m \times e)(n \times e)^{-1} = (k \times e)(l \times e)^{-1},$$

tedy

$$(m \times e)(l \times e) = (k \times e)(n \times e),$$

neboli

$$ml \times e = kn \times e,$$

tzn.

$$ml = kn,$$

což je ekvivalentní s

$$\frac{m}{n} = \frac{k}{l}.$$

(Víme, že každé racionální číslo se dá vyjádřit nekonečně mnoha způsoby ve tvaru podílu dvou celých čísel. V právě provedeném důkazu injektivnosti jsme současně dokázali, že zobrazení f bylo definováno korektně, tedy že obraz racionálního čísla a v tomto zobrazení nezávisí na tom, které vyjádření čísla a ve tvaru zlomku celých čísel jsme si vybrali.)

Zbývá dokázat, že f je homomorfismus. Nechť opět $m, n, k, l \in \mathbb{Z}$, $n \neq 0$, $l \neq 0$. Pak

$$\begin{aligned} f\left(\frac{m}{n} + \frac{k}{l}\right) &= f\left(\frac{ml + kn}{nl}\right) = ((ml + kn) \times e)(nl \times e)^{-1} = \\ &= ((ml \times e) + (kn \times e))(nl \times e)^{-1} = \\ &= ((m \times e)(l \times e) + (k \times e)(n \times e))(n \times e)^{-1}(l \times e)^{-1} = \\ &= (m \times e)(n \times e)^{-1} + (k \times e)(l \times e)^{-1} = f\left(\frac{m}{n}\right) + f\left(\frac{k}{l}\right), \end{aligned}$$

$$\begin{aligned} f\left(\frac{m}{n} \cdot \frac{k}{l}\right) &= f\left(\frac{mk}{nl}\right) = (mk \times e)(nl \times e)^{-1} = (m \times e)(k \times e)(n \times e)^{-1}(l \times e)^{-1} = \\ &= (m \times e)(n \times e)^{-1}(k \times e)(l \times e)^{-1} = f\left(\frac{m}{n}\right) \cdot f\left(\frac{k}{l}\right). \end{aligned}$$

□

Definice. Podtěleso $\overline{\langle e \rangle}$ tělesa \mathcal{T} se nazývá *prvotěleso tělesa \mathcal{T}* .

Poznámka 3.3.14 Na základě věty 3.3.13 tedy platí, že je-li \mathcal{T} komutativní těleso, pak prvotěleso tělesa \mathcal{T} je izomorfní buď s tělesem racionálních čísel \mathbb{Q} (pokud \mathcal{T} má nekonečnou charakteristiku) nebo s tělesem \mathbb{Z}_p , kde p je prvočíslo (pokud \mathcal{T} má konečnou charakteristiku p).

Zatím jsme vždy pracovali s komutativními tělesy nekonečné charakteristiky (např. s číselnými tělesy) nebo v případě těles konečné charakteristiky s tělesy \mathbb{Z}_p , kde p je prvočíslo. Ukažme si proto alespoň dvě základní obecné vlastnosti libovolných konečných těles.

Věta 3.3.15 Má-li konečné komutativní těleso T charakteristiku p , pak počet prvků v T je roven mocnině čísla p .

Důkaz. Jestliže T má charakteristiku p , pak jeho prvotěleso je izomorfní s tělesem \mathbb{Z}_p , a protože nerozlišujeme mezi navzájem izomorfními tělesy, můžeme pak \mathbb{Z}_p považovat za podtěleso tělesa T . Potom T můžeme uvažovat jako vektorový prostor nad tělesem \mathbb{Z}_p . (Tzn., že vektory jsou prvky z T a skaláry jsou prvky ze \mathbb{Z}_p . Všechny axiomy vektorového prostoru jsou díky vlastnostem komutativních těles triviálně splněny.) Protože těleso T je konečné, má jako vektorový prostor nad \mathbb{Z}_p konečnou dimenzi. Předpokládejme, že $\dim T = n$ a že množina $\{u_1, \dots, u_n\}$ je bází prostoru T . Každý prvek $a \in T$ je pak možno vyjádřit právě jedním způsobem ve tvaru lineární kombinace $a = a_1u_1 + \dots + a_nu_n$, kde $a_1, \dots, a_n \in \mathbb{Z}_p$. Ovšem existuje právě p^n navzájem různých n -tic prvků ze \mathbb{Z}_p , tedy i prvků v T je právě p^n . \square

Poznámka 3.3.16 Z teorie grup víme, že pro každé přirozené číslo n existuje alespoň jedna grupa řádu n (např. aditivní grupa \mathbb{Z}_n). Podobně každé $n \in \mathbb{N}$ je počtem prvků některého okruhu (opět např. komutativního okruhu \mathbb{Z}_n). Ovšem podle právě dokázané věty 3.3.15 obdobná situace nenastane pro komutativní tělesa, protože počet prvků libovolného konečného komutativního tělesa je roven mocnině některého prvočísla, takže např. neexistuje žádné komutativní těleso, které by mělo právě šest prvků. (Ve skutečnosti nemůže existovat vůbec žádné těleso, jehož počet prvků by nebyl mocninou některého prvočísla, protože platí, že každé konečné těleso je komutativní. Tento fakt zde ale nebudeme dokazovat, protože bychom se dostali mimo rámec našeho učebního textu.)

Věta 3.3.17 Má-li konečné komutativní těleso T q prvků, pak pro každý prvek $a \in T$ platí $a^q = a$.

Důkaz. Zřejmě $a^q = a$. Nechť tedy $a \neq o \in T$. Víme, že nenulové prvky z T tvoří multiplikativní grupu řádu $q - 1$. Podle Lagrangeovy věty z teorie grup platí, že řád prvku a dělí $q - 1$. Tedy $a^{q-1} = e$, a to znamená, že $a^q = a$. \square

3.4 Podílová tělesa oborů integrity

V této části se budeme věnovat vztahům mezi obory integrity a tělesy. V oboru integrity, na rozdíl od tělesa, nemusí ke každému nenulovému prvku existovat jeho inverzní prvek, tedy zde obecně neexistují operace dělení. Na druhé straně ale mají obory integrity a tělesa hodně společných vlastností: např. neexistují v nich netriviální dělitelé nuly (a je tedy možno v nich krátit při násobení nenulovými prvky), jejich charakteristika je buď nekonečná nebo prvočíselná, atd. Ukážeme, že každý obor integrity \mathcal{J} můžeme přirozeným způsobem rozšířit na komutativní těleso $\overline{\mathcal{J}}$, které má pro \mathcal{J} analogický význam, jako má těleso \mathcal{Q} pro obor integrity \mathcal{Z} .

Definice. Nechť $\mathcal{J} = (J; +, \cdot)$ je obor integrity. Zlomkem nad \mathcal{J} rozumíme každou uspořádanou dvojici (a, b) , kde $a, b \in J, b \neq o$.

Na množině $J^* = J \times (J \setminus \{o\})$ všech zlomků nad \mathcal{J} zavedeme binární relaci „ \equiv “ takto:

$$\forall a, a_1, b, b_1 \in J, b \neq o \neq b_1; (a, b) \equiv (a_1, b_1) \iff ab_1 = a_1b.$$

Věta 3.4.1 Relace „ \equiv “ je relací ekvivalence na množině J^* .

Důkaz. Reflexivnost a symetričnost relace „ \equiv “ jsou zřejmé. Ukažme, že tato relace je také tranzitivní.

Nechť $(a, b), (a_1, b_1), (a_2, b_2) \in J^*$, $(a, b) \equiv (a_1, b_1)$, $(a_1, b_1) \equiv (a_2, b_2)$. Pak $ab_1 = a_1b$, $a_1b_2 = a_2b_1$, tedy také $ab_1b_2 = a_1bb_2$, $a_1b_2b = a_2b_1b$. Protože rovnost na J je tranzitivní, dostáváme odtud $ab_1b_2 = a_2b_1b$, neboli $ab_2b_1 = a_2bb_1$. Podle předpokladu $b_1 \neq o$, proto jím můžeme v poslední rovnosti krátit, tedy $ab_2 = a_2b$. Ovšem to znamená, že $(a, b) \equiv (a_2, b_2)$. \square

Nechť $(a, b), (c, d) \in J^*$. Definujme $(a, b) + (c, d) = (ad + bc, bd)$, $(a, b) \cdot (c, d) = (ac, bd)$. Protože \mathcal{J} je obor integrity a protože $b \neq o \neq d$, platí $bd \neq o$ a tedy „ $+$ “ a „ \cdot “ jsou binární operace na J^* .

Označme $\bar{J} = J^*/\equiv$. Jestliže $(a, b) \in J^*$, pak označíme $[(a, b)]$ třídu rozkladu (tzn. prvek faktorové množiny \bar{J}), indukovaného ekvivalencí „ \equiv “, v níž leží prvek (a, b) . Na \bar{J} nyní zavedeme dvě binární operace, které budeme také značit „ $+$ “ a „ \cdot “. Jestliže $[(a, b)], [(c, d)] \in \bar{J}$, pak položíme

$$[(a, b)] + [(c, d)] = [(a, b) + (c, d)], [(a, b)] \cdot [(c, d)] = [(a, b) \cdot (c, d)].$$

Věta 3.4.2 Jestliže $\mathcal{J} = (J; +, \cdot)$ je obor integrity, pak operace „ $+$ “ a „ \cdot “ jsou na \bar{J} definovány korektně a platí, že $\bar{\mathcal{J}} = (\bar{J}; +, \cdot)$ je komutativní těleso, které obsahuje podobor integrity izomorfní s oborem integrity \mathcal{J} .

Důkaz. Ukážeme nejdříve korektnost zavedení obou operací, tzn., ukážeme, že výsledky operací nezávisejí na výběru konkrétních reprezentantů z tříd navzájem ekvivalentních prvků.

Nechť $[(a, b)], [(a_1, b_1)], [(c, d)], [(c_1, d_1)] \in J^*$ a nechť platí, že $[(a, b)] = [(a_1, b_1)]$ a $[(c, d)] = [(c_1, d_1)]$. Pak $(a, b) \equiv (a_1, b_1)$ a $(c, d) \equiv (c_1, d_1)$, tedy $ab_1 = a_1b$ a $cd_1 = c_1d$. Odtud dostaneme $ab_1dd_1 = a_1bdd_1$, $cd_1bb_1 = c_1dbb_1$, a proto také $ab_1dd_1 + cd_1bb_1 = a_1bdd_1 + c_1dbb_1$, neboli $(ad + bc)b_1d_1 = (a_1d_1 + b_1c_1)bd$. Podle definice ekvivalence „ \equiv “ tedy platí $(ad + bc, bd) \equiv (a_1d_1 + b_1c_1, b_1d_1)$, neboli $(a, b) + (c, d) \equiv (a_1, b_1) + (c_1, d_1)$, tzn. $[(a, b) + (c, d)] = [(a_1, b_1) + (c_1, d_1)]$.

Pro násobení z $ab_1 = a_1b$ a $cd_1 = c_1d$ dostaneme $ab_1c_1 = a_1bc_1d$, neboli $acb_1d_1 = a_1c_1bd$. Odtud dostaneme $(ac, bd) \equiv (a_1c_1, b_1d_1)$, a to znamená, že $[(a, b) \cdot (c, d)] = [(a_1, b_1) \cdot (c_1, d_1)]$.

Ověřili jsme tak, že relace ekvivalence „ \equiv “ je kongruencí na algebraické struktuře $\mathcal{J}^* = (J^*; +, \cdot)$. Nyní budeme zjišťovat, zdali odpovídající faktorová struktura $\overline{\mathcal{J}} = \mathcal{J}^*/\equiv$ má všechny vlastnosti komutativního tělesa.

Komutativnost a asociativnost obou binárních operací v \mathcal{J}^* lze snadno ověřit využitím vlastností odpovídajících operací v oboru integrity \mathcal{J} . Proto i operace „ $+$ “ a „ \cdot “ na $\overline{\mathcal{J}}$ jsou komutativní a asociativní.

Ověřme, že násobení je v $\overline{\mathcal{J}}$ distributivní vzhledem ke sčítání. Platí:

$$(a, b) \cdot ((c, d) + (f, g)) = (a, b) \cdot (cg + df, dg) = (acg + adf, bdg),$$

$$(a, b) \cdot (c, d) + (a, b) \cdot (f, g) = (ac, bd) + (af, bg) = (acbg + bda, bdbg).$$

Přitom

$$(acg + adf, bdg) \equiv (acbg + bda, bdbg),$$

tedy

$$[(a, b)] \cdot [(c, d) + (f, g)] = [(a, b)] \cdot [(c, d)] + [(a, b)] \cdot [(f, g)].$$

Navíc platí, že nulovým prvkem v $\overline{\mathcal{J}}$ je $[(o, e)]$, jednotkovým prvkem je $[(e, e)]$ a že opačným prvkem ke třídě $[(a, b)]$ je třída $[(−a, b)]$.

Nechť $[(a, b)] \neq [(o, e)]$. Pak $(a, b) \not\equiv (o, e)$, tedy $a \cdot e \neq b \cdot o$, neboli $a \neq o$. Proto $(b, a) \in J^*$ a platí, že třída $[(b, a)]$ je inverzním prvkem ke třídě $[(a, b)]$.

Dokázali jsme tak, že $\overline{\mathcal{J}} = (\overline{J}; +, \cdot)$ je komutativní těleso.

Zbývá dokázat, že $\overline{\mathcal{J}}$ obsahuje podobor integrity izomorfní s \mathcal{J} . Označme k tomu $\varphi : J \longrightarrow \overline{J}$ takové zobrazení, že $\varphi : a \longmapsto [(a, e)]$ pro každý prvek $a \in J$.

Protože pro libovolné prvky $a, b \in J$ platí

$$(a, e) + (b, e) = (a + b, e), \quad (a, e) \cdot (b, e) = (ab, e),$$

a protože pro libovolné prvky $a, b \in J$ navíc platí

$$(a, e) \equiv (b, e) \iff a = b,$$

dostáváme, že φ je injektivní homomorfismus oboru integrity \mathcal{J} do tělesa $\overline{\mathcal{J}}$. Přitom $\text{Im } \varphi = \{[(a, e)] ; a \in J\}$, a proto $\mathcal{J}_0 = \text{Im } \varphi$ je podobor integrity v tělese $\overline{\mathcal{J}}$ izomorfní s \mathcal{J} . \square

Definice. Těleso $\overline{\mathcal{J}}$ se nazývá *podílové těleso* oboru integrity \mathcal{J} .

Definice. Nechť \mathcal{M} a \mathcal{M}' jsou okruhy. Řekneme, že \mathcal{M} lze izomorfně vnořit do \mathcal{M}' , existuje-li injektivní homomorfismus okruhu \mathcal{M} do okruhu \mathcal{M}' . Takový homomorfismus se pak nazývá *vnoření* \mathcal{M} do \mathcal{M}' .

Důsledek 3.4.3 *Každý obor integrity lze vnořit do jeho podílového tělesa.*

Poznámka 3.4.4 Protože nerozlišujeme mezi navzájem izomorfními algebraickými strukturami, budeme zpravidla ztotožňovat obor integrity \mathcal{J} s jeho izomorfním obrazem \mathcal{J}_0 v tělese $\overline{\mathcal{J}}$, tzn., že každý prvek $a \in J$ ztotožníme s prvkem $[(a, e)] \in J_0$. V tomto pojetí je pak obor integrity \mathcal{J} chápán přímo jako podobor integrity tělesa $\overline{\mathcal{J}}$.

Ukážeme nyní možnost jednoduchého vyjádření prvků z podílového tělesa pomocí prvků z \mathcal{J} (které také odůvodňuje volbu názvu pro toto těleso).

Věta 3.4.5 Nechť \mathcal{J} je obor integrity. Pak platí:

- a) Každý prvek podílového tělesa $\overline{\mathcal{J}}$ lze vyjádřit jako podíl dvou prvků z J .
- b) Jestliže ψ je vnoření oboru integrity \mathcal{J} do libovolného komutativního tělesa T , pak ψ lze rozšířit na vnoření $\overline{\psi}$ tělesa $\overline{\mathcal{J}}$ do tělesa T .

Důkaz. a) Nechť $[(a, b)] \in \overline{\mathcal{J}}$. Pak $[(a, b)] = [(a, e)] \cdot [(e, b)] = [(a, e)] \cdot [(b, e)]^{-1} = ab^{-1}$.

b) Označme $\overline{\psi} : \overline{\mathcal{J}} \longrightarrow T$ takové zobrazení, že

$$\overline{\psi}(ab^{-1}) = \psi(a) \cdot \psi(b)^{-1}$$

pro každý prvek $ab^{-1} \in \overline{\mathcal{J}}$. Nechť $ab^{-1} = cd^{-1}$. Pak $ad = bc$, tedy $\psi(ad) = \psi(bc)$, a to znamená, že $\psi(a) \cdot \psi(d) = \psi(b) \cdot \psi(c)$. Proto $\psi(a) \cdot \psi(b)^{-1} = \psi(c) \cdot \psi(d)^{-1}$, a tedy $\overline{\psi}(ab^{-1}) = \overline{\psi}(cd^{-1})$.

Tím jsme ověřili, že zobrazení $\overline{\psi}$ je definováno korektně, tedy že nezáleží na výběru reprezentantů z tříd navzájem ekvivalentních zlomků.

Navíc platí, že $\overline{\psi}$ je injektivní, protože všechny implikace, které jsme při ověřování korektnosti definice $\overline{\psi}$ používali, jsou ve skutečnosti ekvivalence.

Ukážeme, že $\overline{\psi}$ je rozšířením zobrazení ψ , tj., že pro každý prvek $a \in J$ platí $\overline{\psi}(a) = \psi(a)$. Platí totiž:

$$\overline{\psi}(a) = \overline{\psi}(a \cdot e^{-1}) = \psi(a) \cdot \psi(e)^{-1} = \psi(a) \cdot e' = \psi(a).$$

Zbývá dokázat, že $\overline{\psi}$ je homomorfismus tělesa $\overline{\mathcal{J}}$ do tělesa T . Nechť $ab^{-1}, cd^{-1} \in \overline{\mathcal{J}}$. Pak

$$\begin{aligned} \overline{\psi}(ab^{-1} + cd^{-1}) &= \overline{\psi}(ad + bc)(bd)^{-1} = \psi(ad + bc) \cdot \psi(bd)^{-1} = \\ &= (\psi(a) \cdot \psi(d) + \psi(b) \cdot \psi(c)) \cdot \psi(b)^{-1} \cdot \psi(d)^{-1} = \\ &= \psi(a) \cdot \psi(b)^{-1} + \psi(c) \cdot \psi(d)^{-1} = \overline{\psi}(ab^{-1}) + \overline{\psi}(cd^{-1}), \end{aligned}$$

$$\begin{aligned} \overline{\psi}(ab^{-1} \cdot cd^{-1}) &= \overline{\psi}(ac \cdot (bd)^{-1}) = \psi(ac) \cdot \psi(bd)^{-1} = \psi(a) \cdot \psi(c) \cdot \psi(b)^{-1} \cdot \psi(d)^{-1} = \\ &= \psi(a) \cdot \psi(b)^{-1} \cdot \psi(c) \cdot \psi(d)^{-1} = \overline{\psi}(ab^{-1}) \cdot \overline{\psi}(cd^{-1}). \end{aligned}$$

□

Poznámka 3.4.6 Podle části b) právě dokázané věty tedy platí, že podílové těleso je nejmenší ze všech komutativních těles, která obsahují podobory integrity izomorfní s \mathcal{J} , neboli do nichž lze \mathcal{J} izomorfně vnořit.

Cvičení

1. Zjistěte, které z následujících algebraických struktur se dvěma binárními operacemi jsou okruhy. V kladném případě určete, má-li tento okruh jednotkový prvek, je-li komutativní, má-li netriviální dělitele nuly a je-li oborem integrity, popř. tělesem.
 - a) $\mathcal{Z} = (\mathbb{Z}; +, \cdot)$;
 - b) $\mathcal{N} = (\mathbb{N}; +, \cdot)$;
 - c) $\mathcal{Q} = (\mathbb{Q}; +, \cdot)$;
 - d) $\mathcal{C} = (\mathbb{C}; +, \cdot)$;
 - e) $2\mathcal{Z} = (2\mathbb{Z}; +, \cdot)$;
 - f) $\mathcal{M}_n(\mathcal{T}) = (M_n((\mathcal{T}); +, \cdot))$, kde \mathcal{T} je libovolné číselné těleso;
 - g) $\mathcal{Z}_8 = (\mathbb{Z}_8; \oplus, \otimes)$;
 - h) $\mathcal{Z}_7 = (\mathbb{Z}_7; \oplus, \otimes)$;
 - i) $\mathcal{Z}' = (\mathbb{Z}; \triangle, \triangledown)$, kde pro každé $a, b \in \mathbb{Z}$, $a \triangle b = a + b + 1$, $a \triangledown b = a + b + ab$;
 - j) $\mathcal{R}' = (\mathbb{R}; \triangle, \triangledown)$, kde operace jsou zavedeny analogicky jako v předchozím případě.
2. Označme A množinu všech spojitých funkcí jedné reálné proměnné definovaných na intervalu $\langle -1, 1 \rangle$. Dokažte, že A vzhledem ke sčítání a násobení funkcí tvoří komutativní okruh s jednotkovým prvkem, který ale není oborem integrity.
3. Definujme na \mathbb{Z}^2 následující operace:

$$\forall a, b, c, d \in \mathbb{Z}; (a, b) \oplus (c, d) = (a + c, b + d), (a, b) \odot (c, d) = (ac, bd).$$

Dokažte, že $\mathcal{Z}^2 = (\mathbb{Z}^2; \oplus, \odot)$ je komutativní okruh s jednotkovým prvkem, v němž existují netriviální dělitelé nuly.

4. Na množině A zaveděte operace sčítání a násobení tak, aby algebraická struktura $\mathcal{A} = (A; +, \cdot)$ byla tělesem.
 - a) $A = \{a, b\}$;
 - b) $A = \{a, b, c\}$.
5. Nechť \mathcal{J} a \mathcal{K} jsou obory integrity, nechť \mathcal{J} je podoborem integrity v \mathcal{K} a nechť $c \in K \setminus J$. Potom podobor integrity v \mathcal{K} generovaný $J \cup \{c\}$ označíme $\mathcal{J}[c]$. (Budeme říkat, že obor integrity $\mathcal{J}[c]$ vznikl adjunkcí prvku c k podoboru integrity \mathcal{J}). Ověřte, že uvažujeme-li \mathcal{Z} jako podobor integrity tělesa \mathcal{C} , pak
 - a) $\mathcal{Z}[\sqrt{2}] = \{a + b\sqrt{2} ; a, b \in \mathbb{Z}\}$;
 - b) $\mathcal{Z}[i] = \{a + bi ; a, b \in \mathbb{Z}\}$.

($\mathcal{Z}[i]$ se nazývá obor integrity *Gaussových celých čísel*).

6. Jestliže \mathcal{T} je vlastní podtěleso tělesa \mathcal{S} a $d \in S \setminus T$, pak podtěleso v \mathcal{S} generované $T \cup \{d\}$ označíme $\mathcal{T}(d)$ a řekneme, že těleso $\mathcal{T}(d)$ vzniklo z \mathcal{T} adjunkcí prvku d .

Těleso \mathcal{Q} můžeme uvažovat např. jako podtěleso tělesa \mathcal{R} .

- Ověřte, že $\mathcal{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$.
- Dokažte, že $\mathcal{Q}(\sqrt{2}) = \mathcal{Q}(\sqrt{8})$.
- Dokažte, že $\mathcal{Q}(1 + \sqrt{3}) = \mathcal{Q}(1 - \sqrt{3})$.
- Označme $\mathcal{Q}(\sqrt{2}, \sqrt{3}) = (\mathcal{Q}(\sqrt{2}))(\sqrt{3})$. Ověřte, že

$$\mathcal{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}; a, b, c, d \in \mathbb{Q}\}.$$

- Dokažte, že $\mathcal{Q}(\sqrt{2}, \sqrt{3}) = \mathcal{Q}(\sqrt{2} + \sqrt{3})$.
- Ověřte, že $\mathcal{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}; a, b, c \in \mathbb{Q}\}$.

7. Dokažte, že množina všech čtvercových matic tvaru

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$$

kde $a, b \in \mathbb{Q}$, tvorí okruh vzhledem ke sčítání a násobení matic. Zjistěte vlastnosti tohoto okruhu.

8. Nechť M je množina a $\mathcal{P}(M) = \{X; X \subseteq M\}$. Pro libovolné $X, Y \in \mathcal{P}(M)$ označme

$$X \div Y = (X \setminus Y) \cup (Y \setminus X), \quad X \cdot Y = X \cap Y.$$

Ověřte, že $(\mathcal{P}(M); \div, \cdot)$ je okruh s jednotkovým prvkem.

- Dokažte, že množina všech diagonálních matic stupně n ($n \in \mathbb{N}$) nad číselným tělesem \mathcal{T} je podokruhem okruhu $\mathcal{M}_n(\mathcal{T}) = (M_n(\mathcal{T}); +, \cdot)$.
- Nechť \mathcal{A} je okruh spojitých funkcí jedné reálné proměnné definovaných na intervalu $(-1, 1)$ (viz příklad 2). Označme $B = \{f \in A; f(0) = 0\}$. Ověřte, že B je ideálem okruhu \mathcal{A} .
- Dokažte, že každé těleso \mathcal{T} má jen triviální ideály $\{0\}$ a \mathcal{T} .
- Je dán okruh \mathcal{M} a prvky $a_1, a_2, \dots, a_n \in M$. Označme

$$P = \{x_1a_1 + x_2a_2 + \cdots + x_na_n; x_1, x_2, \dots, x_n \in M\}.$$

Dokažte, že P je levým ideálem okruhu \mathcal{M} .

- Dokažte, že množina všech skalárních matic stupně n ($n \in \mathbb{N}$) nad číselným tělesem \mathcal{T} tvoří vzhledem ke sčítání a násobení matic těleso izomorfní s tělesem \mathcal{T} .

14. Dokažte, že množina všech matic tvaru

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

kde $a, b \in \mathbb{R}$, tvoří vzhledem ke sčítání a násobení matic těleso izomorfní s tělesem komplexních čísel \mathcal{C} .

- 15.** Nechť $\mathcal{R}' = (\mathbb{R}; \Delta, \nabla)$, kde pro každé $a, b \in \mathbb{R}$, $a \Delta b = a + b + 1$, $a \nabla b = a + b + ab$. Dokažte, že algebraická struktura \mathcal{R}' je izomorfní s tělesem \mathcal{R} , a že je tedy také komutativním tělesem. (Srovnejte s příkladem 1j.)
- 16.** Dokažte, že okruh matic z příkladu 7 je tělesem, které je izomorfní s tělesem $\mathcal{Q}(\sqrt{2})$.
- 17.** Automorfismem libovolného okruhu \mathcal{M} rozumíme každý izomorfismus okruhu \mathcal{M} na okruh \mathcal{M} . Najděte všechny automorfismy f tělesa komplexních čísel \mathcal{C} takové, že $f(a) = a$ pro každý prvek $a \in \mathbb{R}$.
- 18.** Najděte všechny automorfismy tělesa racionálních čísel \mathcal{Q} .
- 19.** Určete všechny homomorfní obrazy okruhu $\mathcal{Z}_6 = (\mathbb{Z}_6; \oplus, \otimes)$.
- 20.** Najděte všechny homomorfní obrazy okruhu $\mathcal{Z}_{12} = (\mathbb{Z}_{12}; \oplus, \otimes)$.
- 21.** Nechť \mathcal{M} je okruh, I a I' ideály v \mathcal{M} a nechť $I' \subseteq I$. Ukažte, že existuje (právě jeden) homomorfismus $f : \mathcal{M}/I' \longrightarrow \mathcal{M}/I$ takový, že pro každý $x \in M$ platí $f : x + I' \longmapsto x + I$.
- 22.** Nechť $m, n \in \mathbb{N}$ a nechť n dělí m . S využitím předchozího cvičení najděte homomorfismus okruhu $\mathcal{Z}/m\mathbb{Z}$ na okruh $\mathcal{Z}/n\mathbb{Z}$.
- 23.** Dokažte, že jsou-li obory integrity \mathcal{J} a \mathcal{J}' izomorfní, pak jsou izomorfní i jejich podílová tělesa $\overline{\mathcal{J}}$ a $\overline{\mathcal{J}'}$.
- 24.** Platí, že \mathcal{Q} je podílovým tělesem oboru integrity \mathcal{Z} . Zjistěte, je-li $\mathcal{Q}(i)$ podílovým tělesem oboru integrity $\mathcal{Z}(i)$.
- 25.** Dokažte, že má-li komutativní těleso \mathcal{T} konečnou charakteristiku p , pak

$$\forall a, b \in T; (a + b)^p = a^p + b^p, (a - b)^p = a^p - b^p.$$

Kapitola 4

Dělitelnost v oborech integrity

4.1 Základní vlastnosti dělitelů prvků

V této kapitole se budeme zabývat otázkami souvisejícími s relací dělitelnosti v libovolném oboru integrity, zejména otázkami existence či neexistence největších společných dělitelů daných prvků a možnostmi určování těchto největších společných dělitelů standardními metodami (např. algoritmy).

Definice. Nechť $\mathcal{J} = (J; +, \cdot)$ je obor integrity a $a, b \in J$. Řekneme, že prvek a dělí prvek b (značíme $a | b$), existuje-li prvek $c \in J$ takový, že $b = ac$. V opačném případě budeme říkat, že a nedělí b (označení $a \nmid b$).

Definice. Jestliže pro prvky $a, b \in J$ platí současně $a | b$ a $b | a$, pak říkáme, že prvky a a b jsou *asociované*. (Značíme $a \parallel b$.) V opačném případě použijeme označení $a \nparallel b$.

Všude v dalším bude \mathcal{J} označovat obor integrity. Jeho jednotkový prvek budeme označovat e .

Definice. a) Prvek $a \in J$ se nazývá *jednotka* oboru integrity \mathcal{J} , platí-li $a \parallel e$.

b) Prvek $a \in J$, který není jednotkou v \mathcal{J} , se nazývá *vlastním dělitelem* prvku b , když $a | b$ a $a \nparallel b$.

Nevlastními dělitieli prvku b rozumíme všechny jednotky v \mathcal{J} a všechny prvky asociované s b .

Věta 4.1.1 Nechť $a, b, c, x, y \in J$. Pak platí:

- a) $a | a$, $e | a$;
- b) $a | b$, $b | c \implies a | c$;
- c) $a | b$, $a | c \implies a | (bx + cy)$;

- d) $a | b \implies ac | bc;$
- e) $a | o;$
- f) $o | a \iff a = o;$
- g) a je jednotka v \mathcal{J} právě tehdy, když k prvku a existuje inverzní prvek $v (J; \cdot)$;
- h) $a \parallel b$ právě tehdy, když existuje jednotka $j \in J$ v \mathcal{J} taková, že $b = aj$;
- i) a je vlastním dělitelem prvku $b \neq o$ právě tehdy, když existuje prvek $d \in J$ takový, že $b = ad$ a $d \nparallel e$, $d \nparallel b$.

Důkaz. a) Platí $a = a \cdot e = e \cdot a$, tedy $a | a$ a $e | a$.

b) Jestliže $a | b$ a $b | c$, pak existují $u, v \in J$ takové, že $b = au$ a $c = bv$. Tedy $c = (au)v = a(uv)$, tzn. $a | c$.

c) Nechť $a | b$ a $a | c$. Pak existují $u, v \in J$ takové, že $b = au$ a $c = av$. Jestliže $x, y \in J$, pak $bx + cy = aux + avy = a(ux + vy)$, a tedy $a | (bx + cy)$.

d) Jestliže $a | b$, pak existuje $d \in J$ takový, že $b = ad$, tedy také $bc = acd$. Odtud vyplývá, že $ac | bc$.

e) $o = ao$, tedy $a | o$.

f) Podle e) platí $o | o$. Obráceně, nechť $o | a$. Pak existuje $u \in J$ takový, že $a = a \cdot o = o$, tedy $a = o$.

g) Nechť a je jednotka v \mathcal{J} . Pak $a | e$, tzn., že existuje $c \in J$ takový, že $e = ac$, tedy $c = a^{-1}$. Obráceně, jestliže existuje inverzní prvek a^{-1} prvku a , pak $e = aa^{-1}$, tedy $a | e$, a proto podle a) platí $a \parallel e$.

h) Nechť $a \parallel b$, tj. $a | b$ a $b | a$. Pak existují $j_1, j_2 \in J$, pro které $b = aj_1$ a $a = bj_2$. Odtud $b = aj_1 = bj_2j_1$.

Jestliže $b \neq o$, pak $j_2j_1 = e$, a tedy j_1 a j_2 jsou jednotky v \mathcal{J} . Jestliže $b = o$, pak také $a = o$, a proto $b = a \cdot e$, $a = b \cdot e$.

Obráceně, nechť $b = aj_1$, kde j_1 je jednotka v \mathcal{J} . Pak existuje $j_2 \in J$ takový, že $j_1j_2 = e$. Z $b = aj_1$ dostáváme $a | b$ a z $bj_2 = aj_1j_2 = ae = a$ plyne $b | a$, tzn. $a \parallel b$.

i) Nechť prvek a je vlastní dělitel prvku b . Pak $b = au$ pro některý $u \in J$. Jestliže $u \parallel e$, pak podle h) platí $a \parallel b$, spor. Jestliže $u \parallel b$, pak podle h) existuje jednotka j v \mathcal{J} taková, že $u = bj$. Pak $b = au = abj = baj$, a protože $b \neq o$, platí $aj = e$. Proto a je jednotka v \mathcal{J} , spor. Platí tedy $u \nparallel e$ a $u \nparallel b$.

Obráceně, nechť existuje prvek $u \in J$ takový, že $u \nparallel e$, $u \nparallel b$ a že $b = au$. Jestliže $a \parallel e$, pak podle h) platí $u \parallel b$, spor. Jestliže $a \parallel b$, pak podle h) existuje jednotka j taková, že $a = bj$. Potom platí $b = au = bju$, a protože $b \neq o$, dostáváme $uj = e$, tzn. $u \parallel e$, spor. \square

Poznámka 4.1.2 Je zřejmé, že binární relace „„být asociovaný s““ je relací ekvivalence na J . (Symetričnost je obsažena přímo v definici asociovaných prvků a reflexivnost s transitivností vyplývají z částí a) a b) věty 4.1.1.) Proto tato relace indukuje rozklad množiny J na třídy navzájem asociovaných prvků.

Příklad 4.1.3 a) V oboru integrity \mathcal{Z} jsou jednotkami právě čísla 1 a -1 . Jestliže $a \in \mathbb{Z}$, pak s ním asociované prvky jsou právě a a $-a$.

b) Nechť \mathcal{T} je komutativní těleso. Víme, že jestliže $a \in T$, pak v \mathcal{T} existuje inverzní prvek a^{-1} k prvku a právě tehdy, když $a \neq 0$. Proto jednotkami v \mathcal{T} jsou právě všechny jeho nenulové prvky.

Nechť $a, b \in T$, $a \neq 0 \neq b$. Pak $a = (ab^{-1})b$, a tedy $b \mid a$. Podobně dokážeme, že $a \mid b$, a proto $a \parallel b$.

To ovšem znamená, že otázky dělitelnosti v komutativních tělesech jsou triviální a že má proto smysl se dělitelností zabývat jen v takových oborech integrity, které nejsou tělesy.

c) Nechť \mathcal{T} je číselné těleso a $\mathcal{T}[x]$ je obor integrity polynomů jedné proměnné nad \mathcal{T} . Pak jednotkami v $\mathcal{T}[x]$ jsou právě všechny polynomy stupně 0, tj. všechny nenulové konstantní polynomy. Je-li proto $f(x) \in \mathcal{T}[x]$, pak $g(x) \in \mathcal{T}[x]$ je asociovaný s $f(x)$ právě tehdy, když $g(x) = a \cdot f(x)$, kde $0 \neq a \in \mathcal{T}$.

Příklad 4.1.4 Nechť $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$. Pak $\mathcal{Z}[i] = (\mathbb{Z}[i]; +, \cdot)$ je číselný obor integrity, který se nazývá *obor integrity Gaussových celých čísel*. Určíme jednotky v $\mathcal{Z}[i]$.

Jestliže $\alpha = a + bi \in \mathbb{Z}[i]$, pak označíme $\|\alpha\| = \alpha\bar{\alpha} = a^2 + b^2$. ($\|\alpha\|$ se také nazývá *norma čísla α* .) Pokud $\|\alpha\| = 1$, pak $\alpha\bar{\alpha} = 1$, tzn., že α je jednotka v $\mathcal{Z}[i]$. Obráceně, nechť α je jednotka v $\mathcal{Z}[i]$. Pak existuje $\beta \in \mathbb{Z}[i]$ takové, že $\alpha\beta = 1$. Odtud $\alpha\bar{\beta} = \bar{1} = 1$, tedy $1 = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = \|\alpha\| \cdot \|\beta\|$, tzn. $\|\alpha\| = 1$.

Proto α je jednotka v $\mathcal{Z}[i]$ právě tehdy, když $\|\alpha\| = a^2 + b^2 = 1$, tj. právě když $a = \pm 1$, $b = 0$ nebo $a = 0$, $b = \pm 1$. Tedy jednotkami v $\mathcal{Z}[i]$ jsou právě čísla $1, -1, i, -i$.

Definice. a) Nechť $a_1, a_2, \dots, a_n \in J$. Prvek $c \in J$ se nazývá *společný dělitel* prvků a_1, a_2, \dots, a_n , platí-li $c \mid a_i$ pro každé $i = 1, 2, \dots, n$.

b) Prvek $d \in J$ se nazývá *největší společný dělitel* prvků a_1, a_2, \dots, a_n , jestliže je jejich společným dělitelem a jestliže pro každý společný dělitel c těchto prvků platí $c \mid d$. (Největší společný dělitel prvků a_1, a_2, \dots, a_n budeme označovat $D(a_1, a_2, \dots, a_n)$.)

c) Prvky a_1, a_2, \dots, a_n nazýváme *nesoudělné*, platí-li $D(a_1, a_2, \dots, a_n) = e$.

Poznámka 4.1.5 Nechť prvky a_1, a_2, \dots, a_n mají aspoň jeden největší společný dělitel a nechť každý z prvků d a d_1 je největším společným dělitelem těchto prvků. Pak $d \mid d_1$ a $d_1 \mid d$, tedy $d \parallel d_1$.

Obráceně, nechť $D(a_1, a_2, \dots, a_n) = d$ a nechť $d_1 \parallel d$. Protože $d_1 \mid d$ a $d \mid a_i$ pro každé $i = 1, 2, \dots, n$, je d_1 společným dělitelem prvků a_1, a_2, \dots, a_n . Nechť c je libovolný společný dělitel prvků a_1, a_2, \dots, a_n . Pak $c \mid d$, a protože $d \mid d_1$, dostáváme $c \mid d_1$. Tedy d_1 je také největším společným dělitelem prvků a_1, a_2, \dots, a_n .

Znamená to tedy, že pokud největší společný dělitel d daných prvků existuje, pak dalšími největšími děliteli těch prvků jsou právě všechny prvky asociované s d . Můžeme proto také

říci, že největší společný dělitel daných prvků (pokud existuje) je určen jednoznačně až na asociovanost.

Věta 4.1.6 *Jestliže v oboru integrity \mathcal{J} existuje ke každým dvěma prvkům jejich největší společný dělitel, pak také k libovolnému konečnému počtu prvků z J existuje jejich největší společný dělitel v \mathcal{J} .*

Důkaz. Nechť $a_1, a_2, \dots, a_n \in J$. Důkaz provedeme indukcí podle počtu prvků n .

Pro $n = 1$ je tvrzení triviální, protože $D(a_1) = a_1$, pro $n = 2$ platí podle předpokladu.

Nechť $n > 2$ a nechť pro $n - 1$ je už pravdivost tvrzení ověřena. Pak tedy existují $u = D(a_1, a_2, \dots, a_{n-1})$ a $d = D(u, a_n)$. Ukážeme, že $d = D(a_1, a_2, \dots, a_n)$. Platí $u \mid a_i$ ($i = 1, 2, \dots, n - 1$), $d \mid u$, $d \mid a_n$, proto s využitím tranzitivnosti relace dělitelnosti (věta 4.1.1 b)) dostáváme $d \mid a_i$ pro každé $i = 1, 2, \dots, n$, tzn. že d je společným dělitelem prvků a_1, a_2, \dots, a_n . Nechť $d_1 \mid a_i$ ($i = 1, 2, \dots, n$). Pak $d_1 \mid u$ a $d_1 \mid a_n$, proto $d_1 \mid d$, tedy vskutku d je největším společným dělitelem prvků a_1, a_2, \dots, a_n . \square

Poznámka 4.1.7 Uvedený důkaz dává také návod, jak určit $D(a_1, a_2, \dots, a_n)$, pokud v \mathcal{J} existuje největší společný dělitel pro libovolnou dvojici prvků z J . Můžeme jej totiž najít např. takto:

$$D(a_1, a_2, \dots, a_n) = D(D(a_1, a_2, \dots, a_{n-1}), a_n).$$

Speciálně pro $n = 3$ dostáváme

$$D(a_1, a_2, a_3) = D(D(a_1, a_2), a_3),$$

ale také např.

$$D(a_1, a_2, a_3) = D(a_1, D(a_2, a_3)).$$

Věta 4.1.8 *Nechť $a, b, c \in J$ a nechť v \mathcal{J} existují $D(a, b)$ a $D(ca, cb)$. Pak*

$$D(ca, cb) = c \cdot D(a, b).$$

Důkaz. Označme $d = D(a, b)$, $u = D(ca, cb)$. Pro $c = o$ nebo $d = o$ je tvrzení zřejmé.

Budeme proto předpokládat, že $c \neq o$ a $d \neq o$. Protože $d \mid a$ a $d \mid b$, platí podle věty 4.1.1 d) také $cd \mid ca$ a $cd \mid cb$, a proto $cd \mid u$. Tedy existují prvky $v, x, y \in J$ takové, že $u = cdv$, $ca = ux$, $cb = uy$, tzn. $ca = cdvx$ a $cb = cdvy$. Protože $c \neq o$, platí $a = dvx$ a $b = dvy$, tedy dv je společný dělitel prvků a a b , a proto $dv \mid d$. To znamená, že $d = dvs$ pro některý $s \in J$. Podle předpokladu $d \neq o$, tedy $vs = e$, proto v je jednotka v \mathcal{J} . Ovšem $u = cdv$, tedy $u \parallel cd$, a proto cd je největší společný dělitel prvků ca a cb . \square

Věta 4.1.9 *Nechť $a_1, a_2 \in J$, nechť existuje $d = D(a_1, a_2)$ a nechť $a_1 = db_1$, $a_2 = db_2$. Pak prvky b_1 a b_2 jsou nesoudělné.*

Důkaz. Podle věty 4.1.8 platí

$$d = D(a_1, a_2) = D(db_1, db_2) = d \cdot D(b_1, b_2),$$

tedy $D(b_1, b_2) = e$. □

Věta 4.1.10 Nechť $a, b, c \in J$ jsou takové prvky, že $D(a, b) = e = D(a, c)$. Existují-li $D(ac, bc)$ a $D(a, bc)$, pak $D(a, bc) = e$.

Důkaz. Platí $a \mid ac$, proto $D(a, ac) = a$. Dále podle věty 4.1.8 platí $D(ac, bc) = D(a, b) \cdot c = c$. Proto dostáváme

$$D(a, bc) = D(D(a, ac), bc) = D(a, ac, bc) = D(a, D(ac, bc)) = D(a, c) = e.$$

□

Věta 4.1.11 Nechť $a, b, c \in J$ jsou takové, že $a \mid bc$. Existuje-li $D(ac, bc)$ a platí-li $D(a, b) = e$, pak $a \mid c$.

Důkaz. Podle předpokladu $a \mid bc$, proto $D(a, bc) = a$. Navíc z $D(a, b) = e$ vyplývá (podle věty 4.1.8) $D(ac, bc) = c$. Proto dostáváme

$$a = D(a, bc) = D(D(a, ac), bc) = D(a, ac, bc) = D(a, D(ac, bc)) = D(a, c),$$

tedy $a \mid c$. □

Zavedeme nyní „duální“ pojmy k pojmu společný dělitel a největší společný dělitel daných prvků.

Definice. a) Nechť $a_1, a_2, \dots, a_n \in J$. Prvek $v \in J$ se nazývá *společný násobek* prvků a_1, a_2, \dots, a_n , platí-li $a_i \mid v$ pro každé $i = 1, 2, \dots, n$.

b) Prvek $u \in J$ se nazývá *nejmenší společný násobek* prvků a_1, a_2, \dots, a_n , je-li jejich společným násobkem a platí-li pro každý společný násobek v těchto prvků, že $u \mid v$. (Nejmenší společný násobek prvků a_1, a_2, \dots, a_n budeme označovat $n(a_1, a_2, \dots, a_n)$.)

Poznámka 4.1.12 Podobně jako pro největší společné dělitele bychom mohli ověřit, že pokud $n(a_1, a_2, \dots, a_n)$ existuje, pak je určen jednoznačně až na asociovanost. Platí také analogie věty 4.1.6, tj., existuje-li nejmenší společný násobek ke každým dvěma prvkům z J , pak existuje nejmenší společný násobek také ke každé konečné podmnožině oboru integrity \mathcal{J} .

Věta 4.1.13 Nechť $a, b, c \in J$ a nechť existuje $d = D(a, b)$. Pak platí, že jestliže c je společný násobek prvků a a b , pak $ab \mid cd$.

Speciálně, jestliže $D(a, b) = e$, pak pro libovolný společný násobek c prvků a a b platí $ab \mid c$.

Důkaz. Nechť $d = D(a, b)$, $a \mid c$, $b \mid c$. Pak $D(a, c) = a$, $D(b, c) = b$. Platí tedy

$$\begin{aligned} D(ab, cd) &= D(ab, c \cdot D(a, b)) = D(ab, D(ca, cb)) = D(D(ab, ac), bc) = \\ &= D(a \cdot D(b, c), bc) = D(ab, bc) = b \cdot D(a, c) = ab, \end{aligned}$$

proto $ab \mid cd$. □

Ukážeme nyní, jaké jsou vztahy mezi existencí největších společných dělitelů a nejménších společných násobků prvků z oboru integrity \mathcal{J} .

Věta 4.1.14 *Nechť v oboru integrity \mathcal{J} k libovolným dvěma prvkům existuje jejich největší společný dělitel. Pak k libovolným dvěma prvkům z \mathcal{J} existuje také jejich nejménší společný násobek.*

Důkaz. Předpokládejme, že ke každým dvěma prvkům z \mathcal{J} existuje jejich největší společný dělitel.

Nechť $a, b \in J$. Jestliže $a = o$ nebo $b = o$, pak $n(a, b)$ existuje, protože $n(a, b) = o$. Nechť tedy $a \neq o \neq b$. Označme $d = D(a, b)$. Je zřejmé, že $d \neq o$. Označme u, v prvky z J takové, že $a = du$, $b = dv$. Podle věty 4.1.10 platí $D(u, v) = e$. Nechť $w = duv$. Platí $w = av$, $w = bu$, tedy w je společný násobek prvků a a b . Předpokládejme, že $w_1 \in J$ a že $a \mid w_1$, $b \mid w_1$. Pak samozřejmě $d \mid w_1$, proto existuje $z \in J$ takový, že $w_1 = dz$. Můžeme tedy vztahy $a \mid w_1$ a $b \mid w_1$ zapsat ve tvaru $du \mid dz$ a $dv \mid dz$, a protože $d \neq o$, platí $u \mid z$ a $v \mid z$. Protože $D(u, v) = e$, platí podle věty 4.1.13 $uv \mid z$. Odtud dostáváme $duv \mid dz$, tedy $w \mid w_1$. To však znamená, že $w = n(a, b)$. □

Poznámka 4.1.15 V dalším textu budeme hledat podmínky pro existenci největších společných dělitelů. Podle věty 4.1.14 ovšem v takových případech se nebudeme muset zvlášť věnovat analogickému hledání podmínek pro existenci nejménších společných násobků.

Následující věta navíc dává metodu výpočtu nejménšího společného násobku pomocí největšího společného dělitele.

Věta 4.1.16 *Nechť k libovolným dvěma prvkům z J existuje v \mathcal{J} jejich největší společný dělitel. Pak pro každé prvky $a, b \in J$ platí*

$$D(a, b) \cdot n(a, b) = ab.$$

Speciálně, jestliže $D(a, b) = e$, pak $n(a, b) = ab$.

Důkaz. Tato věta vyplývá z důkazu věty 4.1.14. Skutečně, nechť $a, b \in J$. Označme $d = D(a, b)$, $w = n(a, b)$, $a = du$, $b = dv$. Podle důkazu věty 4.1.14 platí $w = duv$. Proto

$$d \cdot w = d \cdot duv = dav = adv = ab.$$



4.2 Existence největších společných dělitelů

V dalším textu budeme studovat některé typy oborů integrity, v nichž bude zaručena existence největších společných dělitelů, popř. navíc i existence algoritmů pro výpočet největších společných dělitelů (a tedy i nejmenších společných násobků).

Věta 4.2.1 *Jestliže \mathcal{M} je okruh a $I_\alpha \trianglelefteq \mathcal{M}$ ($\alpha \in \Gamma$), pak $I = \bigcap_{\alpha \in \Gamma} I_\alpha$ je také ideálem okruhu \mathcal{M} .*

Důkaz. Víme, že průnik libovolného systému podokruhů okruhu \mathcal{M} je také podokruhem v \mathcal{M} . Protože každý ideál okruhu je podokruhem toho okruhu, platí $I \trianglelefteq \mathcal{M}$. Nechť $a \in I$, $r \in M$. Pak pro každé $\alpha \in \Gamma$ platí $a \in I_\alpha$, proto $ra \in I_\alpha$ pro každé $\alpha \in \Gamma$, a tedy $ra \in I$. Podobně se ukáže, že také $ar \in I$, tzn., že $I \trianglelefteq \mathcal{M}$. \square

Definice. Nechť B je podmnožina okruhu \mathcal{M} . Pak průnik všech ideálů okruhu \mathcal{M} , které obsahují B , nazveme *ideál generovaný množinou B* a budeme jej označovat $[B]$. Jestliže $B = \{a_1, \dots, a_n\}$, budeme psát stručněji $B = [a_1, \dots, a_n]$ místo $B = [\{a_1, \dots, a_n\}]$.

Poznámka 4.2.2 Podle věty 4.2.1 je $[B]$ ideál v \mathcal{M} . Můžeme jej charakterizovat jako nejmenší ideál v \mathcal{M} obsahující B . Speciálně pro $B = \emptyset$ platí $[B] = \{o\}$. Často ovšem budeme muset rozhodovat o prvku z M , zdali patří nebo nepatří do ideálu $[B]$ pro některou danou neprázdnou podmnožinu $B \subseteq M$. V následující větě ukážeme, jak lze o odpovědi na tuto otázkou rozhodnout v okruzích s jednotkovým prvkem.

Věta 4.2.3 *Nechť okruh \mathcal{M} má jednotkový prvek e . Pak pro libovolnou podmnožinu $\emptyset \neq B \subseteq M$ platí, že*

$$[B] = \left\{ \sum_{i=1}^k x_i a_i y_i; a_i \in B, x_i, y_i \in M, k \in \mathbb{N} \right\}.$$

Důkaz. Uvažujme neprázdnou podmnožinu B okruhu \mathcal{M} a označme

$$C = \left\{ \sum_{i=1}^k x_i a_i y_i; a_i \in B, x_i, y_i \in M, k \in \mathbb{N} \right\}.$$

Nechť $a \in B$. Pak $a = e \cdot a \cdot e$, tzn. $a \in C$, a tedy platí $B \subseteq C$.

Předpokládejme, že $c = \sum_{i=1}^k x_i a_i y_i \in C$, $d = \sum_{j=1}^l u_j b_j v_j \in C$, $z \in M$, $l \in \mathbb{N}$. Platí

$$c - d = \sum_{i=1}^k x_i a_i y_i + \sum_{j=1}^l (-u_j) b_j v_j,$$

a tedy $c - d \in C$. Dále

$$\begin{aligned} zc &= z \cdot \sum_{i=1}^k x_i a_i y_i = \sum_{i=1}^k (zx_i) a_i y_i, \\ cz &= \left(\sum_{i=1}^k x_i a_i y_i \right) \cdot z = \sum_{i=1}^k x_i a_i (y_i z), \end{aligned}$$

tzn. $zc \in C$ a $cz \in C$.

Proto C je ideál v \mathcal{M} obsahující B .

Nechť I je ideál v \mathcal{M} takový, že $B \subseteq I$. Pak $x_i a_i \in I$, proto také $(x_i a_i) y_i \in I$ pro každé $i = 1, \dots, k$. Přitom I je uzavřený vzhledem k součtům, a proto $c = \sum_{i=1}^k x_i a_i y_i \in I$. Vzhledem k tomu, že podobné úvahy platí pro kterýkoliv prvek z C , platí $C \subseteq I$.

Dokázali jsme tím, že C je nejmenší ideál v \mathcal{M} obsahující B , a to znamená, že $C = [B]$. \square

Definice. Jestliže \mathcal{M} je okruh a $a \in M$, pak $[a]$ se nazývá *hlavní ideál v \mathcal{M} generovaný prvkem a* .

Poznámka 4.2.4 a) Nechť okruh \mathcal{M} má jednotkový prvek, $a \in M$ a $b \in [a]$. Pak b lze vyjádřit ve tvaru $b = \sum_{i=1}^k x_i a y_i = \left(\sum_{i=1}^k x_i \right) \cdot a \cdot \left(\sum_{i=1}^k y_i \right)$. Přitom jsou-li $x, y \in M$, pak $xay \in [a]$. Platí tedy (podle věty 4.2.3), že $[a] = \{xay; x, y \in M\}$.

b) Můžeme snadno ověřit, že v oboru integrity celých čísel \mathbb{Z} platí pro libovolné $n \in \mathbb{Z}$, že $n\mathbb{Z}$ je ideálem v \mathbb{Z} a že platí $n\mathbb{Z} = [n]$.

Definice. Obor integrity \mathcal{J} se nazývá *oborem integrity hlavních ideálů*, je-li každý ideál v \mathcal{J} hlavní.

Příklad 4.2.5 Ukážeme, že \mathcal{Z} je obor integrity hlavních ideálů.

Pro ideál $\{0\}$ platí $\{0\} = [0]$.

Nechť tedy $I \trianglelefteq \mathcal{Z}$ a $I \neq \{0\}$. Jestliže $0 \neq a \in I$, pak čísla a i $-a$ patří do I , a tedy I obsahuje i některá přirozená čísla. Nechť n je nejmenší přirozené číslo, které patří do I . Pak $[n] = n\mathbb{Z} \subseteq I$. Předpokládejme, že $a \in I$. Pak existují čísla $q, r \in \mathbb{Z}$ taková, že $a = nq + r$, $0 \leq r < n$. To znamená, že $r = a - nq$, proto $r \in I$. Ovšem n je nejmenší přirozené číslo z I , proto musí platit $r = 0$. Tedy $a = nq$, proto $a \in n\mathbb{Z}$, tzn. $I \subseteq n\mathbb{Z}$. Protože jsme odvodili i platnost obrácené inkluze, platí $I = n\mathbb{Z}$.

Věta 4.2.6 Nechť \mathcal{J} je obor integrity hlavních ideálů a nechť $a_1, a_2, \dots, a_n \in J$. Pak existují prvky $x_1, x_2, \dots, x_n \in J$ takové, že $\sum_{i=1}^n a_i x_i$ je největším společným dělitelem prvků a_1, a_2, \dots, a_n .

Důkaz. Nechť $a_1, a_2, \dots, a_n \in J$. Protože \mathcal{J} je obor integrity hlavních ideálů, musí existovat prvek $d \in J$ takový, že $[a_1, a_2, \dots, a_n] = [d]$. Proto podle věty 4.2.3 uvažované pro komutativní případ platí, že existují prvky $u_1, u_2, \dots, u_n \in J$ takové, že $a_1 = du_1, a_2 = du_2, \dots, a_n = du_n$. Podobně existují prvky $x_1, x_2, \dots, x_n \in J$ takové, že $d = \sum_{i=1}^n a_i x_i$.

Ukažme, že d je největší společný dělitel prvků a_1, a_2, \dots, a_n . Podle předchozích úvah bezprostředně vidíme, že d je společným dělitelem těchto prvků. Nechť d' je další společný dělitel prvků a_1, a_2, \dots, a_n . Pak podle věty 4.1.1 c) platí $d' \mid \sum_{i=1}^n a_i x_i$, tedy $d' \mid d$. Proto opravdu $d = D(a_1, a_2, \dots, a_n)$. \square

Důsledek 4.2.7 Jestliže \mathcal{J} je obor integrity hlavních ideálů, pak k libovolnému konečnému počtu prvků z J existuje v \mathcal{J} jejich největší společný dělitel.

Poznámka 4.2.8 Existují ovšem také obory integrity, v nichž některé konečné množiny prvků nemají největší společný dělitel. Podle věty 4.2.6 pak ale musí platit, že v těchto oborech integrity existují i ideály, které nejsou hlavní.

Příklad 4.2.9 Uvažujme množinu $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5}; a, b \in \mathbb{Z}\}$. Platí, že $\mathbb{Z}[i\sqrt{5}]$ je číselný obor integrity, v němž jsou jednotkami právě čísla 1 a -1 . Uvažujme čísla 9 a $6 + 3i\sqrt{5}$, která patří do $\mathbb{Z}[i\sqrt{5}]$. Můžeme se přesvědčit, že jejich společnými dělителяmi jsou právě čísla $\pm 1, \pm 3, \pm(2 + i\sqrt{5})$. Přitom ale žádné z těchto čísel není největším dělitelem čísel 9 a $6 + 3i\sqrt{5}$. Ukažme např., že $3 \nmid (2 + i\sqrt{5})$ a $(2 + i\sqrt{5}) \nmid 3$. Kdyby totiž platilo, že $3 \mid (2 + i\sqrt{5})$, pak by existovalo číslo $x + i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ takové, že $3(x + yi\sqrt{5}) = 2 + i\sqrt{5}$, a tedy by muselo platit $3x = 2$ a $3y = 1$, ovšem taková $x, y \in \mathbb{Z}$ neexistují. Podobně, kdyby platilo, že $(2 + i\sqrt{5}) \mid 3$, pak by existovalo číslo $u + vi\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ takové, že $(2 + i\sqrt{5})(u + vi\sqrt{5}) = 3$. Tedy by platilo, že $2u - 5v = 3$, $2v + u = 0$, ovšem tato soustava rovnic nemá řešení se složkami v \mathbb{Z} .

Ověřením zbývajících možností zjistíme, že největší společný dělitel čísel 9 a $6 + 3i\sqrt{5}$ v $\mathbb{Z}[i\sqrt{5}]$ neexistuje. Proto mj. v tomto oboru integrity existují i ideály, které nejsou hlavními.

4.3 Eukleidovské obory integrity

Definice. Obor integrity \mathcal{J} se nazývá *eukleidovský obor integrity*, jestliže existuje zobrazení ν množiny $J \setminus \{0\}$ do množiny všech celých nezáporných čísel takové, že platí

$$(1) \quad \forall a, b \in J; a \mid b, b \neq 0 \implies \nu(a) \leq \nu(b),$$

(2) $\forall a, b \in J, a \neq o \neq b \exists q, r \in J; a = bq + r$ a $r = o$ nebo $\nu(r) < \nu(b)$.

(Obraz $\nu(a)$ prvku $a \in J$ budeme také nazývat *norma prvku a.*)

Věta 4.3.1 Jestliže \mathcal{J} je eukleidovský obor integrity, $a, b \in J, a \neq o \neq b$, pak platí:

- (a) $a \parallel b \implies \nu(a) = \nu(b)$;
- (b) $a | b, \nu(a) = \nu(b) \implies a \parallel b$;
- (c) jestliže $a | b$, pak a je vlastním dělitelem prvku b právě tehdy, když prvek a není jednotka v \mathcal{J} a $\nu(a) < \nu(b)$;
- (d) jestliže k je nejmenší číslo v množině $\{\nu(a); o \neq a \in J\}$, pak $b \in J$ je jednotka v \mathcal{J} právě tehdy, když $\nu(b) = k$.

Důkaz. a) Nechť $a \parallel b$. Pak $a | b$ a $b | a$, tedy $\nu(a) \leq \nu(b) \leq \nu(a)$, a to znamená, že $\nu(a) = \nu(b)$.

b) Nechť $a | b$ a $\nu(a) = \nu(b)$. Pak existují prvky $c, q, r \in J$ takové, že $b = ac$ a $a = bq + r$, kde $r = o$ nebo $\nu(r) < \nu(b)$. Tedy $a = bq + r = acq + r$, proto $r = a - acq = a(e - cq)$, tzn. $a | r$. Nechť $r \neq o$. Pak ze skutečnosti, že $a | r$, vyplývá $\nu(a) \leq \nu(r) < \nu(b) = \nu(a)$, což je ale spor. Proto musí platit $r = o$, a tedy $a = bq$, a tak $b | a$. Ovšem podle předpokladu platí také $a | b$, a proto $a \parallel b$.

c) Nechť a je vlastním dělitelem prvku b . Pak $a \nmid e, a \nmid b$, proto podle (b) platí $\nu(a) < \nu(b)$. Obráceně, nechť $a | b, a \nmid e$ a $\nu(a) < \nu(b)$. Pak (opět podle (b)) $a \nmid b$, a tedy a je vlastním dělitelem b .

d) Nechť k splňuje předpoklady v (d). Nechť b je jednotka v \mathcal{J} . Pak pro každý prvek $a \in J$ platí $b | a$, tedy pokud $a \neq o$, pak $\nu(b) \leq \nu(a)$. Proto $\nu(b) = k$.

Obráceně, nechť $\nu(b) = k$. Potom platí, protože e je jednotka v \mathcal{J} , že $\nu(b) = \nu(e) = k$, a protože $e | b$, dostáváme podle (b), že $e \parallel b$, tj. b je jednotka v \mathcal{J} . \square

V souvislosti s dělitelností jsme zatím zavedli dva typy oborů integrity. V další větě ukážeme, jaký je vztah mezi třídami těchto oborů integrity.

Věta 4.3.2 Každý eukleidovský obor integrity je oborem integrity hlavních ideálů.

Důkaz. Nechť \mathcal{J} je eukleidovský obor integrity a nechť I je ideál v \mathcal{J} . Jestliže $I = \{o\}$, pak $I = [o]$. Předpokládejme proto, že $I \neq \{o\}$ a uvažujme takový prvek $o \neq a \in I$, že $\nu(a)$ je nejmenší číslo v množině $\{\nu(x); o \neq x \in I\}$. Zřejmě $[a] \subseteq I$. Nechť $o \neq b \in I$. Pak existují prvky $q, r \in J$ takové, že $b = aq + r$, kde $r = o$ nebo $\nu(r) < \nu(a)$. Nechť $r \neq o$. Protože $r = b - aq \in I$ a protože $\nu(r) < \nu(a)$, dostáváme spor. Proto $r = o$, neboli $b = aq \in [a]$. Tedy $I \subseteq [a]$, což spolu s obrácenou inkluzí znamená, že $I = [a]$. \square

Poznámka 4.3.3 Podle právě dokázané věty 4.3.2 a podle věty 4.2.6 tedy platí, že každá konečná podmnožina eukleidovského oboru integrity \mathcal{J} má v \mathcal{J} největší společný dělitel. Věta 4.2.6 však jen dokazuje jeho existenci, nedává však explicitní metodu pro jeho nalezení. V následující větě ukážeme, že pro eukleidovské obory integrity existuje jednotný algoritmus pro nalezení největšího společného dělitele dvou, a tedy také následně libovolného konečného počtu prvků.

Věta 4.3.4 (Eukleidův algoritmus)

Nechť \mathcal{J} je eukleidovský obor integrity, $a, b \in J$, $a \neq o \neq b$. Pak v J existují prvky $q_0, q_1, \dots, q_n, r_1, r_2, \dots, r_n$ takové, že $r_n = D(a, b)$ a

$$\begin{aligned} a &= bq_0 + r_1, & \nu(r_1) &< \nu(b), \\ b &= r_1q_1 + r_2, & \nu(r_2) &< \nu(r_1), \\ &\dots & & \\ r_{i-1} &= r_iq_i + r_{i+1}, & \nu(r_{i+1}) &< \nu(r_i), \\ &\dots & & \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & \nu(r_n) &< \nu(r_{n-1}), \\ r_{n-1} &= r_nq_n. & & \end{aligned}$$

Důkaz. Je zřejmé, že prvky q_i a r_i splňující uvedené podmínky existují, protože \mathcal{J} je eukleidovský obor integrity. Přitom $\nu(b)$ je celé nezáporné číslo a platí $\nu(b) > \nu(r_1) > \nu(r_2) > \dots \geq 0$, proto po konečném počtu kroků dostaneme $r_{n+1} = 0$.

Důkaz věty tedy bude kompletní, dokážeme-li, že $r_n = D(a, b)$.

Z $r_{n-1} = r_nq_n$ dostaneme $r_n \mid r_{n-1}$. Odtud podle věty 4.1.1 c) platí že $r_n \mid (r_{n-1}q_{n-1} + r_n)$, tedy $r_n \mid r_{n-2}$. Pokud takto postupujeme dále, dojdeme až k rovnosti $b = r_1q_1 + r_2$ a díky předchozím výsledkům tak dostaneme, že $r_n \mid b$. Z rovnosti $a = bq_0 + r_1$ pak odvodíme, že $r_n \mid a$. Prvek r_n je tedy společný dělitel prvků a a b .

Nechť d je nyní libovolný společný dělitel prvků a a b . Pak z $a = bq_0 + r_1$ plyne podle věty 4.1.1 c), že $d \mid r_1$, z $b = r_1q_1 + r_2$ pak plyne, že $d \mid r_2$, atd., až z $r_{n-2} = r_{n-1}q_{n-1} + r_n$ vyplývá, že $d \mid r_n$. Proto opravdu platí, že $r_n = D(a, b)$. \square

Příklad 4.3.5 Platí, že \mathbb{Z} je eukleidovský obor integrity. K tomu, abychom to ověřili, stačí pro každé nenulové číslo $a \in \mathbb{Z}$ položit $\nu(a) = |a|$. Obě podmínky z definice normy eukleidovského oboru integrity jsou zde samozřejmě splněny, přičemž druhá z nich využívá známé možnosti dělení celých čísel se zbytkem.

Příklad 4.3.6 V příkladě 4.1.4 jsme se věnovali oboru integrity Gaussových celých čísel $\mathcal{Z}[i]$, který se skládá právě z komplexních čísel tvaru $a + bi$, kde $a, b \in \mathbb{Z}$. Ukážeme, že $\mathcal{Z}[i]$ je eukleidovský obor integrity.

Jestliže $0 \neq \alpha \in \mathbb{Z}[i]$, $\alpha = a + bi$ ($a, b \in \mathbb{Z}$), pak položíme $\nu(\alpha) = \|\alpha\| = a^2 + b^2$. Ověříme, že $\nu : (\mathbb{Z}[i] \setminus \{0\}) \longrightarrow \mathbb{Z}_0^+$ má vlastnosti normy eukleidovského oboru integrity.

a) Nechť $a + bi, c + di \in \mathbb{Z}[i]$, $a + bi \neq 0 \neq c + di$ a $(a + bi) \mid (c + di)$. Pak existuje číslo $0 \neq u + vi \in \mathbb{Z}[i]$ takové, že $(a + bi)(u + vi) = c + di$. Platí

$$\begin{aligned}\nu((a + bi)(u + vi)) &= \nu((au - bv) + (av + bu)i) = \\ &= a^2u^2 - 2abuv + b^2v^2 + a^2v^2 + 2abuv + b^2u^2 = \\ &= a^2(u^2 + v^2) + b^2(u^2 + v^2) = (a^2 + b^2)(u^2 + v^2),\end{aligned}$$

a zároveň $\nu(a + bi) = a^2 + b^2$, proto $\nu(a + bi) \leq \nu(c + di)$.

b) Nechť opět $a + bi, c + di \in \mathbb{Z}[i]$, $a + bi \neq 0 \neq c + di$, a nechť

$$\frac{a + bi}{c + di} = x + yi.$$

Zřejmě platí, že $x, y \in \mathbb{Q}$. Máme určit $q_1 + q_2i, r_1 + r_2i \in \mathbb{Z}[i]$ takové, že

$$a + bi = (c + di)(q_1 + q_2i) + (r_1 + r_2i),$$

kde $r_1 + r_2i = 0$ nebo $\nu(r_1 + r_2i) < \nu(c + di)$. Jestliže $x, y \in \mathbb{Z}$, pak $q_1 + q_2i = x + yi$ a $r_1 + r_2i = 0$.

Jestliže $x \notin \mathbb{Z}$ nebo $y \notin \mathbb{Z}$, pak zvolíme $q_1, q_2 \in \mathbb{Z}$ taková, že $|x - q_1| \leq \frac{1}{2}$, $|y - q_2| \leq \frac{1}{2}$. Pro $r_1 + r_2i$ musí platit:

$$r_1 + r_2i = (c + di)(x + yi) - (c + di)(q_1 + q_2i) = (c + di)((x - q_1) + (y - q_2)i).$$

Položme $x - q_1 = p_1$, $y - q_2 = p_2$. Pak

$$r_1 + r_2i = (c + di)(p_1 + p_2i).$$

Ukážeme, že $\nu(r_1 + r_2i) < \nu(c + di)$. Platí

$$\nu(r_1 + r_2i) = \nu((c + di)(p_1 + p_2i)) = (c^2 + d^2)(p_1^2 + p_2^2),$$

$$\nu(c + di) = c^2 + d^2,$$

$$p_1^2 + p_2^2 = (x - q_1)^2 + (y - q_2)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2},$$

proto $\nu(r_1 + r_2i) < \nu(c + di)$.

Příklad 4.3.7 Nechť T je číselné těleso. Pak polynomy jedné neurčité (nebo jedné proměnné) x nad T tvoří obor integrity $T[x]$. Pro libovolný nenulový polynom $f(x) \in T[x]$ položíme $\nu(f(x))$ rovno stupni polynomu $f(x)$. Pak ν je zobrazení, které má vlastnosti normy, a proto $T[x]$ je eukleidovský obor integrity.

4.4 Gaussovy obory integrity

V této části budeme z pohledu dělitelnosti studovat další typy oborů integrity. K tomu bude užitečné všimnout si prvků majících vlastnosti analogické těm, které mají v oboru integrity \mathcal{Z} právě všechna prvočísla (a čísla k nim opačná).

Definice. Nechť \mathcal{J} je libovolný obor integrity, $p \in J$, $p \neq o$, $p \nmid e$. Pak prvek p se nazývá

- a) *ireducibilní*, jestliže má pouze nevlastní dělitele (tj. jen jednotky a prvky asociované s p);
- b) *prvočinitel*, platí-li pro libovolné prvky $a, b \in J$, že pokud $p \mid ab$, pak $p \mid a$ nebo $p \mid b$.

Poznámka 4.4.1 Je zřejmé, že každou z vlastností „být ireducibilní“ a „být prvočinitelem“ vždy má nebo nemá každý prvek z třídy vzájemně asociovaných prvků.

Věta 4.4.2 Jestliže \mathcal{J} je obor integrity, pak každý prvočinitel v \mathcal{J} je také ireducibilní v \mathcal{J} .

Důkaz. Nechť p je prvočinitel v \mathcal{J} a nechť $c \in J$, $c \nmid e$, $c \mid p$. Pak existuje prvek $d \in J$ takový, že $p = cd$. To ovšem znamená, že $p \mid cd$, a tedy $p \mid c$ nebo $p \mid d$.

Jestliže $p \mid c$, pak $p \parallel c$.

Nechť $p \mid d$. Tedy existuje prvek $q \in J$ takový, že $d = pq$. Pak $p = cd = pcq$, proto $cq = e$, což znamená, že $c \parallel e$. Ovšem to je spor.

Proto musí platit $p \parallel c$, a tedy p je ireducibilní v \mathcal{J} . \square

Poznámka 4.4.3 Obrácená implikace ale obecně neplatí, tzn. existují takové obory integrity, v nichž pojmy prvočinitele a ireducibilního prvku nesplývají.

Příklad 4.4.4 Uvažujme obor integrity $\mathcal{Z}[i\sqrt{5}]$. Platí, že číslo 3 je ireducibilním prvkem v $\mathcal{Z}[i\sqrt{5}]$, že $3 \mid 9$ a že $9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$. Avšak v příkladě 4.2.9 jsme ověřili, že $3 \nmid (2 + i\sqrt{5})$. Podobně bychom mohli ověřit, že $3 \nmid (2 - i\sqrt{5})$. Tedy v $\mathcal{Z}[i\sqrt{5}]$ ireducibilní prvek 3 není prvočinitelem.

Víme, však, že v oboru integrity celých čísel \mathcal{Z} jsou ireducibilními prvky i prvočinitely právě všechna prvočísla a čísla k nim opačná. V následující větě ukážeme, že analogickou vlastnost (tj., že ireducibilní prvky a prvočinitelé jsou tytéž) zaručuje pro širokou třídu oborů integrity jednoduchá postačující podmínka.

Věta 4.4.5 Jestliže v oboru integrity \mathcal{J} ke každým dvěma prvkům existuje jejich největší společný dělitel, pak každý irreducibilní prvek z \mathcal{J} je také prvočinitelem v \mathcal{J} .

Důkaz. Nechť p je irreducibilní prvek v \mathcal{J} a nechť $a, b \in J$, $p \mid ab$. Jestliže $p \nmid a$, pak $D(p, a) = e$, protože p nemá vlastní dělitele. Proto podle věty 4.1.11 platí $p \mid b$, a tedy p je prvočinitelem v \mathcal{J} . \square

Jako bezprostřední důsledek tak speciálně dostaváme:

Věta 4.4.6 Jestliže \mathcal{J} je eukleidovský obor integrity a $a \in J$, pak a je v \mathcal{J} irreducibilní právě tehdy, když a je prvočinitelem v \mathcal{J} .

Nyní se budeme věnovat možnostem rozložitelnosti prvků daného oboru integrity na součiny irreducibilních prvků. Víme, že např. v oboru integrity \mathcal{Z} jsou takové rozklady velmi praktické při určování největších společných děliteleů a nejmenších společných násobků dvou i více celých čísel.

Definice. Řekneme, že obor integrity \mathcal{J} splňuje podmínu konečnosti řetězců vlastních dělitelů (KD), jestliže pro každou posloupnost a_1, a_2, \dots prvků z \mathcal{J} takovou, že $a_{i+1} \mid a_i$ pro každé $i = 1, 2, \dots$, existuje index $n \in \mathbb{N}$ takový, že

$$a_n \parallel a_{n+1}, a_n \parallel a_{n+2}, \dots (*)$$

Věta 4.4.7 Každý eukleidovský obor integrity splňuje podmínu (KD).

Důkaz. Nechť \mathcal{J} je eukleidovský obor integrity a a_1, a_2, \dots posloupnost prvků v \mathcal{J} , pro kterou platí $a_{i+1} \mid a_i$, $i = 1, 2, \dots$. Jestliže $a_i = o$ pro každé $i = 1, 2, \dots$, pak jsou všechny prvky z této posloupnosti vzájemně asociovány.

Jestliže existuje $a_k \neq o$, pak $a_{k+1} \neq o$, $a_{k+2} \neq o, \dots$. Protože původní posloupnost splňuje podmínu (*) právě tehdy, když tuto podmínu splňuje posloupnost $a_k, a_{k+1}, a_{k+2}, \dots$, můžeme v takovém případě bez újmy na obecnosti předpokládat, že všechny prvky a_1, a_2, \dots jsou nenulové. Pro jejich normy pak platí

$$\nu(a_1) \geq \nu(a_2) \geq \dots \geq 0.$$

V této číselné posloupnosti norem však může být ostrá nerovnost jen na konečném počtu míst, a proto existuje $n \in \mathbb{N}$ takové, že $\nu(a_{n+i}) = \nu(a_n)$ pro každé $i = 1, 2, \dots$. Protože $a_{n+i} \mid a_n$, platí podle věty 4.3.1 b), že $a_{n+i} \parallel a_n$ pro každé $i = 1, 2, \dots$, tedy daná posloupnost splňuje podmínu (*). \square

Věta 4.4.8 Jestliže obor integrity \mathcal{J} splňuje podmínu (KD), pak každý jeho nenulový prvek a , který není jednotkou, je možno rozložit na součin konečného počtu irreducibilních prvků v \mathcal{J} .

Důkaz. Nejdříve ukážeme, že jestliže $o \neq a \in J$ a $a \nmid e$, pak a je dělitelný alespoň jedním ireducibilním prvkem. Důkaz provedeme sporem.

Nechť a nemá žádného ireducibilního dělitele. Protože pak a také není ireducibilní v \mathcal{J} , existuje vlastní dělitel $a_1 \in J$ prvku a . Tedy $a = a_1 b_1$, kde $b_1 \in J$. Prvek a_1 není ireducibilní, proto existuje jeho vlastní dělitel $a_2 \in J$, a proto $a_1 = a_2 b_2$, kde $b_2 \in J$. Předpokládejme, že jsme takto již sestojili prvky $a_1, a_2, \dots, a_n \in J$. Je zřejmé, že $a_n \mid a$, a tedy a_n nemůže být ireducibilní. To ovšem znamená, že a_n má vlastního dělitele a_{n+1} . Matematickou indukcí takto sestojíme nekonečnou posloupnost a_1, a_2, \dots prvků z J takovou, že a_{i+1} je vlastním dělitelem a_i pro každé $i = 1, 2, \dots$, což je ve sporu s předpokladem platnosti podmínky (KD) v \mathcal{J} .

Proto a musí mít alespoň jednoho ireducibilního dělitele v \mathcal{J} .

Předpokládejme nyní, že existuje nenulový prvek $a \in J$, který není jednotkou a který nelze v \mathcal{J} rozložit na součin ireducibilních prvků. Prvek a není ireducibilní a podle předchozí části důkazu má vlastního ireducibilního dělitele p_1 . Platí $a = p_1 a_1$, kde $a_1 \in J$ je vlastní dělitel prvku a . Předpokládejme, že jsme takto postupně už našli ireducibilní prvky $p_1, p_2, \dots, p_n \in J$ takové, že pro každé $i = 1, 2, \dots, n$ platí $a = a_0 = p_1 p_2 \cdots p_i a_i$. (Prvek a_i je pak vlastní dělitel prvku a_{i-1} .) Prvek a_n není ireducibilní (jinak by prvek a byl součinem ireducibilních prvků), proto má ireducibilního dělitele p_{n+1} , pro kterého platí $a_n = p_{n+1} a_{n+1}$, kde a_{n+1} je vlastní dělitel prvku a_n . Matematickou indukcí tak sestojíme posloupnost $a = a_0, a_1, a_2, \dots$ prvků z J , v níž a_{i+1} je vlastním dělitelem a_i , $i = 0, 1, 2, \dots$. To je ale spor s podmínkou (KD).

Proto každý nenulový prvek $a \in J$, který není jednotkou v \mathcal{J} , je v \mathcal{J} rozložitelný na konečný součin ireducibilních prvků. \square

Následující věta je bezprostředním důsledkem předchozích dvou vět.

Věta 4.4.9 Jestliže \mathcal{J} je eukleidovský obor integrity a jestliže a je nenulový prvek z J , který není jednotkou v \mathcal{J} , pak a je rozložitelný v \mathcal{J} na součin konečného počtu ireducibilních prvků.

Při otázkách rozložitelnosti prvků daného oboru integrity na součiny ireducibilních prvků se jedná nejenom o existenci takových rozkladů, ale také o jejich jednoznačnost.

Příklad 4.4.10 a) V oboru integrity \mathcal{Z} platí např.

$$60 = 2 \cdot 2 \cdot 3 \cdot 5 = (-3) \cdot 2 \cdot (-5) \cdot 2.$$

b) V oboru integrity $\mathcal{Z}[i\sqrt{5}]$ např. platí

$$9 = 3 \cdot 3 = (2 + i\sqrt{5}) \cdot (2 - i\sqrt{5}).$$

Definice. Nechť \mathcal{J} je obor integrity, nechť $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_m$ jsou ireducibilní prvky v \mathcal{J} a nechť

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m.$$

Pak řekneme, že tyto dva rozklady prvku $a \in J$ jsou spolu asociovány, jestliže $n = m$ a po vhodném očíslování prvků q_1, q_2, \dots, q_n platí $p_i \parallel q_i$ pro každé $i = 1, 2, \dots, n$.

Příklad 4.4.11 V příkladě 4.4.10 jsou v části a) rozklady čísla 60 spolu asociovány, zatímco v části b) uvedené dva rozklady čísla 9, na základě příkladů 4.2.9 a 4.4.4, spolu asociovány nejsou.

Definice. Obor integrity \mathcal{J} se nazývá *Gaussův obor integrity* (nebo také *obor integrity s jednoznačným rozkladem*), jestliže pro každý prvek $o \neq a \in J$, $a \nparallel e$, existuje jeho rozklad na součin ireducibilních prvků a jestliže každé dva takové rozklady prvku a jsou spolu asociovány.

Příklad 4.4.12 Obor integrity $\mathbb{Z}[i\sqrt{5}]$ není Gaussův.

Věta 4.4.13 Jestliže obor integrity \mathcal{J} splňuje podmínu (KD) a jestliže ke každým jeho dvěma prvkům existuje v \mathcal{J} jejich největší společný dělitel, pak \mathcal{J} je Gaussův obor integrity.

Důkaz. Nechť \mathcal{J} splňuje předpoklady a nechť $o \neq a \in J$, $a \nparallel e$. Podle věty 4.4.8 existuje aspoň jeden rozklad prvku a na součin ireducibilních prvků. Předpokládejme, že $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ jsou dva takové rozklady a že $n \leq m$. Indukcí podle n dokážeme, že uvedené rozklady jsou spolu asociovány.

Nechť $n = 1$, tj. $a = p_1 = q_1 q_2 \cdots q_m$. Podle věty 4.4.5 platí, že $a = p_1$ je prvočinitel v \mathcal{J} , proto musí existovat index $k \in \{1, \dots, m\}$ takový, že $a \mid q_k$. Avšak q_k je ireducibilní v \mathcal{J} a $a \nparallel e$, proto $p_1 \parallel q_k$.

Dále ukážeme, že $m = 1$. Nechť $m > 1$. Protože $p_1 = q_k(q_1 \cdots q_{k-1} q_{k+1} \cdots q_m)$, musí platit, že součin $q_1 \cdots q_{k-1} q_{k+1} \cdots q_m$ je jednotkou v \mathcal{J} , a proto i každý z jeho činitelů je jednotkou v \mathcal{J} . Podle předpokladu ale každý z prvků $q_1 q_2 \cdots q_m$ je ireducibilní v \mathcal{J} , což je spor. Proto $m = 1$.

Předpokládejme, že $n > 1$ a že tvrzení už platí pro všechny rozklady takové, že kratší rozklad má nejvíše $n - 1$ prvků. Nechť $a = p_1 p_2 \cdots p_n$. Platí $p_n(p_1 p_2 \cdots p_{n-1}) = q_1 q_2 \cdots q_m$, tedy $p_n \mid q_1 q_2 \cdots q_m$. Přitom p_n je prvočinitel, proto existuje q_j ($j \in \{1, 2, \dots, m\}$) takový, že $p_n \mid q_j$. Můžeme předpokládat, že $p_n \mid q_m$. Pak ale z ireducibilnosti prvku q_m a z předpokladu, že $p_n \nparallel e$, dostáváme $p_n \parallel q_m$. Proto existuje jednotka j v \mathcal{J} taková, že $q_m = jp_n$. Pak $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_{m-1} j p_n$, tedy $p_1 p_2 \cdots p_{n-1} = q_1 q_2 \cdots q_{m-1} j$. Protože levý rozklad má $n - 1$ prvků, podle indukčního předpokladu platí $n - 1 = m - 1$, tedy $n = m$, a po

vhodném očíslování platí $p_1 \parallel q_1, p_2 \parallel q_2, \dots, p_{n-1} \parallel q_{n-1}$. A protože také $p_n \parallel q_n$, jsou původní rozklady $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ asociovány. \square

Následující věta je nyní bezprostředním důsledkem vět 4.3.4, 4.4.7 a 4.4.13.

Věta 4.4.14 *Každý eukleidovský obor integrity je Gaussovým oborem integrity.*

Poznámka 4.4.15 Obrácená věta neplatí. Můžeme se o tom přesvědčit na příkladě oboru integrity $\mathcal{Z}[x]$ polynomů jedné proměnné nad oborem integrity \mathcal{Z} .

Nechť \mathcal{J} je Gaussův obor integrity, $o \neq a \in J$, $a \nmid e$, a nechť $a = q_1 q_2 \cdots q_m$ je rozklad prvku a na součin irreducibilních prvků. Upravíme tento rozklad tak, že sdružíme vždy všechny navzájem asociované činitele. Pak můžeme zapsat prvek a ve tvaru $a = j p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$, kde j je jednotka v \mathcal{J} , p_1, p_2, \dots, p_n jsou vzájemně neasociované irreducibilní prvky z původního rozkladu prvku a , $k_1, k_2, \dots, k_n \in \mathbb{N}$ a $k_1 + k_2 + \cdots + k_n = m$. Rozklad $a = j p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ se nazývá *kanonický rozklad prvku a*.

Nechť nyní $a, b \in J$, $a \neq o \neq b$, $a \nmid e$, $b \nmid e$, a nechť p_1, p_2, \dots, p_n jsou právě všechny vzájemně neasociované irreducibilní prvky z \mathcal{J} , které dělí aspoň jeden z prvků a, b . Pak kanonické rozklady prvků a a b můžeme rozšířit na tvar $a = j p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$, $b = j' p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}$, kde j a j' jsou jednotky v \mathcal{J} , $k_i \geq 0$, $l_i \geq 0$ ($i = 1, 2, \dots, n$). Uvedené rozklady pak nazýváme *zobecněné kanonické rozklady prvků a a b*.

Právě zavedených pojmu využijeme k důkazu skutečnosti, že v Gaussově oboru integrity mají libovolné dva jeho prvky největší společný dělitel.

Věta 4.4.16 *Nechť \mathcal{J} je Gaussův obor integrity, $a, b \in J$, $a \neq o \neq b$, $a \nmid e$, $b \nmid e$, a nechť $a = j p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ a $b = j' p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}$ jsou jejich zobecněné kanonické rozklady. Pak platí:*

- Prvek b je dělitelem prvku a právě tehdy, když $l_i \leq k_i$ pro každé $i = 1, 2, \dots, n$.*
- Označíme-li $r_i = \min(k_i, l_i)$ a $s_i = \max(k_i, l_i)$, $i = 1, 2, \dots, n$, pak*

$$D(a, b) = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}, \quad n(a, b) = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}.$$

Důkaz. a) Nechť $l_i \leq k_i$, $i = 1, 2, \dots, n$. Položíme $v_i = k_i - l_i$ ($i = 1, 2, \dots, n$) a $c = j(j')^{-1} p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n}$. Pak

$$bc = j' p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n} \cdot j(j')^{-1} p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n} = j p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} = a,$$

tedy $b \mid a$.

Obráceně, nechť $b \mid a$, tj. existuje prvek $c \in J$ takový, že $a = bc$. Jestliže p je irreducibilní prvek v \mathcal{J} takový, že $p \mid c$, pak $p \mid a$, a tedy $p \in \{p_1, \dots, p_n\}$. Proto prvek c můžeme vyjádřit ve tvaru $c = j'' p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}$, kde j'' je jednotka v \mathcal{J} a $t_i \geq 0$, $i = 1, 2, \dots, n$. Platí tedy

$$bc = j' p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n} \cdot j'' p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n} = j' j'' p_1^{l_1+t_1} p_2^{l_2+t_2} \cdots p_n^{l_n+t_n},$$

a protože $a = bc$, dostáváme

$$j p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} = j' j'' p_1^{l_1+t_1} p_2^{l_2+t_2} \cdots p_n^{l_n+t_n}.$$

Protože libovolné dva rozklady téhož prvku jsou v \mathcal{J} spolu asociovány, platí $j = j' j''$ a $k_i = l_i + t_i$, $i = 1, 2, \dots, n$. Protože $t_i \geq 0$, platí $l_i \leq k_i$ pro každé $i = 1, 2, \dots, n$.

b) Označme $d = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$. Protože $r_i \leq k_i$ a $r_i \leq l_i$ pro každé $i = 1, 2, \dots, n$, prvek d je podle a) společným dělitelem prvků a a b . Nechť $d' = j_1 p_1^{w_1} p_2^{w_2} \cdots p_n^{w_n}$ je libovolný společný dělitel prvků a a b . Pak podle a) platí $w_i \leq k_i$, $w_i \leq l_i$, $i = 1, 2, \dots, n$. To však znamená, že $w_i \leq \min(k_i, l_i) = r_i$, $i = 1, 2, \dots, n$, tedy $d' \mid d$, a proto platí, že $d = D(a, b)$.

Tvrzení pro $n(a, b)$ se odvodí analogicky. \square

Právě dokázaná věta umožňuje určit přímo největší společné dělitely nejenom pro dvojice prvků Gaussových oborů integrity, ale i pro libovolný konečný počet prvků těchto oborů integrity. K tomu postačí sestavit zobecněné kanonické rozklady současně pro všechny uvažované prvky.

Příklad 4.4.17 V oboru integrity \mathcal{Z} určíme největší společný dělitel trojice čísel 4 500, 1 176 a 5 292. Nejdříve sestavíme zobecněné kanonické rozklady:

$$4\ 500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7^0, \quad 1\ 176 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^2, \quad 5\ 292 = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^2,$$

Podle věty 4.4.16 pak platí

$$D(4\ 500, 1\ 176, 5\ 292) = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 12,$$

$$n(4\ 500, 1\ 176, 5\ 292) = 2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 = 1\ 323\ 000.$$

Ukažme nyní, že implikace ve větě 4.4.13 je ve skutečnosti ekvivalencí.

Věta 4.4.18 *Obor integrity \mathcal{J} je Gaussovým oborem integrity právě tehdy, když \mathcal{J} splňuje podmínu (KD) a ke každým dvěma prvkům z J existuje v \mathcal{J} jejich největší společný dělitel.*

Důkaz. a) Nechť \mathcal{J} je Gaussův obor integrity. Pak podle věty 4.4.16 k libovolným dvěma prvkům existuje jejich největší společný dělitel.

Ověříme tedy, že \mathcal{J} splňuje podmínu (KD). Nechť a_1, a_2, \dots je libovolná posloupnost prvků z J taková, že $a_{i+1} \mid a_i$, $i = 1, 2, \dots$. Předpokládejme, že $a_i \neq o$ pro každé $i = 1, 2, \dots$. Pak pro a_1 můžeme uvažovat některý jeho kanonický rozklad $a_1 = jp_1^{k_1}p_2^{k_2}\dots p_n^{k_n}$. Podle věty 4.4.16 pak ke každému prvku a_2, a_3, \dots existuje jeho zobecněný kanonický rozklad používající tytéž irreducibilní prvky p_1, p_2, \dots, p_n , přičemž pro každý prvek p_l ($l = 1, 2, \dots, n$) příslušné exponenty tvoří nerostoucí posloupnost celých nezáporných čísel. Pokud $a_{i+1} \nmid a_i$, pak v rozkladu prvku a_{i+1} musí být exponent alespoň u jednoho p_l ostře menší než odpovídající exponent v rozkladu prvku a_i . Proto v dané posloupnosti a_1, a_2, \dots prvků z J může být nejvýše $k_1 + k_2 + \dots + k_n$ prvků, které nejsou spolu asociované. Proto existuje $m \in \mathbb{N}$ takové, že pro každé $i \in \mathbb{N}$ platí $a_m \parallel a_{m+i}$. Tedy \mathcal{J} splňuje podmínu (KD):

b) Obrácená implikace byla dokázána ve větě 4.4.13. \square

Cvičení

1. Nechť $\mathcal{J} = (J; +, \cdot)$ je obor integrity. Dokažte, že relace asociovanosti v \mathcal{J} je relací ekvivalence na J .
2. a) Nechť \mathcal{J} je obor integrity, $a, b, u, v \in J$ a nechť u a v jsou jednotky v \mathcal{J} . Dokažte, že platí-li $a \mid b$, pak platí $ua \mid vb$.
b) Nechť $a, b, c \in J$, $c \neq o$, a nechť $ac \mid bc$. Dokažte, že pak $a \mid b$.
3. Nechť \mathcal{J} je obor integrity, $a, a', b, b' \in J$ a nechť $a \parallel a'$ a $b \parallel b'$. Dokažte, že
 - a) $ab \parallel a'b'$;
 - b) obecně neplatí $(a+b) \parallel (a'+b')$.
4. Dokažte, že v libovolném oboru integrity \mathcal{J} platí

$$\forall a, b, c, d \in J; (a \neq o, a \parallel b, ac \parallel bd) \implies c \parallel d.$$
5. Dokažte, že v oboru integrity $\mathcal{Z}[\sqrt{5}] = \{a + b\sqrt{5}; a, b \in \mathbb{Z}\}$
 - a) všechny celočíselné mocniny čísla $2 + \sqrt{5}$ a všechna čísla k nim opačná jsou jednotkami;
 - b) $(1 - \sqrt{5}) \parallel (11 + 5\sqrt{5})$.
 - c) Zjistěte, zdali $3\sqrt{5} \parallel (114 + 255\sqrt{5})$.
6. Dokažte, že v oboru integrity $\mathcal{Z}[i\sqrt{5}]$ jsou jednotkami právě čísla 1 a -1 .
7. Dokažte, že čísla 3 , $2 + i\sqrt{5}$ a $2 - i\sqrt{5}$ jsou irreducibilními prvky v oboru integrity $\mathcal{Z}[i\sqrt{5}]$.

8. Nechť \mathcal{J} je obor integrity a $a, b \in J$. Dokažte, že
- $a | b \iff [b] \subseteq [a]$;
 - $a \parallel b \iff [a] = [b]$.
9. Dokažte, že obor integrity $\mathbb{Z}[\sqrt{2}]$ je eukleidovský. (Návod: Položte $\nu(a + b\sqrt{2}) = |a^2 - 2b^2|$.)
10. Ověřte, že jestliže \mathcal{J} je eukleidovský obor integrity a $a, b \in J$, pak existují prvky $c, d \in J$ takové, že $D(a, b) = ac + bd$.
11. V oboru integrity \mathcal{Z} určete čísla c, d taková, že $504c + 60d = D(504, 60)$. Určete pak $n(a, b)$.
12. a) V oboru integrity $\mathcal{Z}[i]$ určete $D(60, 8 + 6i)$ a $n(60, 8 + 6i)$.
 b) Najděte čísla $a + bi, c + di \in \mathcal{Z}[i]$ taková, že
- $$60 \cdot (a + bi) + (8 + 6i) \cdot (c + di) = D(60, 8 + 6i).$$
13. Nechť $f_1(x) = x^4 - x^3 - 4x^2 + 4x + 1$ a $f_2(x) = x^2 - x - 1$ jsou polynomy z $\mathcal{R}[x]$. Určete polynomy $g_1(x)$ a $g_2(x)$ z $\mathcal{R}[x]$ takové, že
- $$f_1(x) \cdot g_1(x) + f_2(x) \cdot g_2(x) = D(f_1(x), f_2(x)).$$

Rejstřík

A

- adjunkce prvku, 80, 81
- algebra, 21
- automorfismus, 49
 - vnitřní, 49

C

- centrum grupy, 50

D

- direktní součin
 - grup, 55
 - vnitřní, 52
 - vnější, 54
 - úplný vnější, 54
- dělitel
 - nevlastní, 83
 - společný, 85
 - největší, 85
 - vlastní, 83

E

- ekvivalence, 13
 - indukovaná rozkladem, 17
 - indukovaná zobrazením, 18
 - spojení ekvivalencí, 15
- endomorfismus, 58

F

- faktorová množina, 17

G

- grupa, 27
 - abelovská, 27
 - alternující, 48
 - cyklická, 30
 - faktorová, 39

symetrická, 48

- grupoid, 21
 - faktorový, 44
 - komutativní, 21

H

- homomorfismus, 24, 39, 66
 - jádro homomorfismu, 40, 67
 - přirozený, 41, 67

CH

- charakteristika okruhu, 71

I

- ideál okruhu, 65
 - generovaný množinou, 89
 - hlavní, 90
 - levý, 65
 - maximální, 69
 - oboustranný, 65
 - pravý, 65
- index podgrupy, 34
- invariantní vzhledem k, 50
- izomorfismus, 24, 39, 67

J

- jednotka, 83

K

- kartézský
 - mocnina, 7
 - součin, 7, 53
- komutant, 51
- komutátor, 51
- kongruence, 44
 - grupová, 45

M

monoid, 24

N

norma, 85, 92

normalizátor, 57

násobek

společný, 87

nejmenší, 87

O

obor integrity, 63

eukleidovský, 91

Gaussových celých čísel, 80, 85

Gaussův, 98

hlavních ideálů, 90

s jednoznačným rozkladem, 98

okruh, 61

faktorový, 66

komutativní, 61

operace

n -ární, 21

indukovaná, 29

P

permutace, 48

podgrupa, 29

charakteristická, 57

cyklická, 30

generovaná množinou, 30

invariantní, 50

jednotková, 30

normální, 35

triviální, 30

úplně invariantní, 58

podmnožina

uzavřená, 29, 62

podmínka konečnosti řetězců, 96

podobor integrity, 63

podokruh, 62

generovaný množinou, 72

nulový, 62

triviální, 62

podtěleso, 63

pologrupa, 21

pravidlo o krácení, 28

projekce, 54

prvek

agresívni, 61

idempotentní, 57

inverzní, 25

ireducibilní, 95

jednotkový, 21, 61

konjugovaný, 36

prvky

asociované, 83

nesoudělné, 85

prvoideál, 69

prvookruh, 73

prvotěleso, 75

prvočinitel, 95

přirozené zobrazení, 17

R

relace

n -ární, 7

binární, 7

antisymetrická, 10

inverzní, 8

reflexivní, 10

složení relací, 8

symetrická, 10

tranzitivní, 10

zaměnitelné, 15

kvaternární, 7

ternární, 7

unární, 7

restrikce, 10

rozdíl

podmnožin, 65

symetrický, 57

rozklad

grupy

levý, 33

pravý, 34

množiny, 16

prvku

kanonický, 99
zobecněný kanonický, 99

Ř

řád

grupy, 27
prvku, 32, 70

S

součet podmnožin, 65
součin podmnožin, 65

T

tranzitivní uzávěr, 12

těleso, 63

podílové, 78

třída

množiny, 17
prvku, 33, 66

V

vnoření, 78

Z

zlomek, 77