1-INF-155 Algebra 2

Martin Sleziak

12. mája 2010

Obsah

Kapitola 1

Úvod

Verzia: 12. mája 2010

1.1 Predhovor

V rámci tohoto textu sa budeme občas odkazovať aj na veci z minulého semestra. Takéto odkazy budú označené napríklad ako veta I-3.2.6. Časti označené hviezdičkou sú nepovinné – doplnil som ich preto, že by Vás niektoré z nich mohli zaujímať. V cvičeniach hviezdička označuje náročnejšie cvičenia a + označuje nepovinné cvičenia (napríklad tie, ktoré sa týkajú nepovinných častí).

Za opravy preklepov a chýb, by som chcel poďakovať viacerým študentom: Filip Hanes, Lukáš Jusko, Michal Klempa, Tomáš Kovačovský, Ivan Labáth, Marek Manduch, Michal Sabo.

1.2 Sylaby a literatúra

Sylaby predmetu: Základy teórie grúp - podgrupy, cyklické grupy, grupy permutácií, rozklad grupy podľa podgrupy, faktorizácia, základné vety o izomorfizmoch a homomorfizmoch.

Okruhy, ideály, maximálne ideály a prvoideály, vzťah k poliam a oborom integrity pri faktorizácii. Euklidovské okruhy, okruhy hlavných ideálov, gausovské okruhy. Teória deliteľnosti a veta o rozklade na ireducibilné prvky. Okruhy polynómov, rozklad polynómov na ireducibilné polynómy, (viacnásobné) korene polynómov, derivácia a Taylorov rozvoj polynómov.

Rozšírenia polí. Riešenie antických problémov (duplicita kocky, trisekcia uhla, kvadratúra kruhu). Konečné polia, klasifikácia konečných polí, šifrovanie RSA.

Literatúra: Základnou literatúrou pre tento kurz je [KGGS].

Kapitola 2

Grupy a podgrupy

2.1 Základné vlastnosti grúp

Definíciu a základné vlastnosti grúp sme sa naučili už v minulom semestri, pre zopakovanie však uveďme aspoň stručný prehľad.

Definícia 2.1.1. Dvojicu $(G, *)$, kde G je množina a $*$ je binárna operácia na G nazývame *grupa,* ak

(i) operácia $*$ je asociatívna

$$(\forall g, h, k \in G) g * (h * k) = (g * h) * k,$$

(ii) operácia $*$ má neutrálny prvok

$$(\exists e \in G)(\forall g \in G) e * g = g * e = g,$$

(iii) pre každý prvok $g \in G$ existuje inverzný prvok vzhľadom na operáciu $*$

$$(\forall g \in G)(\exists g^{-1} \in G) g * g^{-1} = g^{-1} * g = e.$$

Ak je binárna operácia $*$ komutatívna

$$(\forall g, h \in G) g * h = h * g,$$

hovoríme o *komutatívnej grupe.*

Ak platí len prvá z podmienok definície grupy, t.j. ak $*$ je asociatívna binárna operácia na množine G, tak dvojicu $(G, *)$ nazývame *pologrupa.* Ak navyše existuje neutrálny prvok pre operáciu $*$, tak $(G, *)$ voláme *pologrupa s jednotkou* alebo tiež *monoid.*

Často označenie pre grupovú operáciu vynechávame a píšeme ab namiesto $a * b$.

Asociatívnosť vlastne znamená, že môžeme vynechávať zátvorky – pri ľubovoľnom uzátvorkovaní dostaneme ten istý prvok. (V tvrdení I-3.1.14 sme dokázali zovšeobecnený asociatívny zákon, ktorý hovorí, že zátvorky môžeme vynechávať aj pri väčšom počte prvkov.)

V grupe platia zákony o krátení

$$\begin{aligned} g * h_1 = g * h_2 \qquad &\Rightarrow h_1 = h_2 \\ h_1 * g = h_2 * g \qquad &\Rightarrow h_1 = h_2 \end{aligned}$$

Zo zákonov o krátení sa dá odvodiť jednoznačnosť neutrálneho prvku aj inverzného prvku- Pre inverzný prvok v grupe platí

$$(g^{-1})^{-1} = g$$
$$(g * h)^{-1} = h^{-1} * g^{-1}$$

Veľa príkladov grúp poznáme z minulého semestra.

Príklad 2.1.2. Príklady grúp:
$(V, +)$ kde V je ľubovoľný vektorový priestor,
$(F, +)$ a $(F \setminus \{0\}, \cdot)$ pre ľubovoľné pole $(F, +, \cdot)$,
$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$,
$(\mathbb{Z}_n, \oplus)$ pre $n \in \mathbb{N}$, $n \geq 2$,
$(\mathbb{Z}_p \setminus \{0\}, \odot)$ kde p je prvočíslo.
Príkladom nekomutatívnej grupy je grupa S_n všetkých permutácií n-prvkovej množiny s operáciou skladania zobrazení pre $n \geq 3$ (úloha I-3.2.2, permutáciam sa budeme venovať aj tento semester v časti 2.5).

Príklad 2.1.3. Množina $\mathbb{C}_n = \{x \in \mathbb{C}; x^n = 1\}$ s operáciou násobenia komplexných čísel tvorí grupu. Asociatívnosť je zrejmá (zdedí sa z komplexných čísel), $1 \in \mathbb{C}_n$ je neutrálny prvok. Takisto ak $x^n = 1$ tak aj $\left(\frac{1}{x}\right)^n = \frac{1}{x^n} = \frac{1}{1} = 1$, čiže $\frac{1}{x}$ patrí do $\mathbb{C}_n$. Číslo $\frac{1}{x}$ je inverzný prvok k prvku x.

Príklad 2.1.4. Ak $(G, *_G)$ a $(H, *_H)$ sú grupy, tak aj $G \times H$ s operáciou $(a, b) * (a', b') = (a *_G a', b *_H b')$ je grupa (úloha 2.1.2).

Definícia 2.1.5. Grupu $G \times H$ z predchádzajúceho príkladu nazývame *priamy súčin grúp* G *a* H (alebo tiež *direktný súčin* grúp.)

Cvičenia

Úloha 2.1.1. Nech $(G, *)$ je grupa. Dokážte:
a) $x * y = y * x \Leftrightarrow x * y * x^{-1} * y^{-1} = e$.
b) Ak $x * x = e$ pre všetky $x \in G$, tak G je komutatívna.

Úloha 2.1.2. Overte, že $G \times H$ spolu s operáciou $*$ definovanou v príklade 2.1.4 tvorí grupu pre ľubovoľné grupy $(G, *_G)$ a $(H, *_H)$.

Úloha 2.1.3*. Nech $*$ je asociatívna binárna operácia na množine $G \neq \emptyset$. Nech pre každé $a, b \in G$ majú rovnice $a * x = b$, $y * a = b$ riešenia v G. (Inými slovami, pre každé $a, b \in G$ existujú $x \in G$ a $y \in G$ také, že $a * x = b$, $y * a = b$.) Dokážte, že $(G, *)$ je grupa. (Hint: Skúste začať dôkazom existencie ľavého a pravého neutrálneho prvku.)

Úloha 2.1.4. Nech $(G, \cdot)$ je grupa a $P(G)$ je systém všetkých podmnožín G. Dokážte, že operácia $\cdot$ na množine $P(G)$ daná predpisom

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

je asociatívna. Tvorí $P(G) \setminus \{\emptyset\}$ s touto operáciou grupu?

Úloha 2.1.5*. Každá konečná grupa s párnym počtom prvkov obsahuje prvok x taký, že $x = x^{-1}$.

2.2 Podgrupy

Pojem podgrupy, ktorý teraz zadefinujeme, predstavuje podmnožinu nejakej grupy, ktorá s tou istou operáciou opäť tvorí grupu. Je to do istej miery analógia pojmu podpriestoru vektorového priestoru, s ktorým sme sa zoznámili v minulom semestri.

Definícia 2.2.1. Nech $(G, *)$ je grupa a $H \subseteq G$ je ľubovoľná podmnožina G. Hovoríme, že H je *podgrupa* grupy G, ak H s binárnou operáciou $*$ zúženou na podmnožinu H tvorí grupu.

Budeme používať označenie $H \leq G$, prípadne $(H, *) \leq (G, *)$.

Pod zúžením operácie na podmnožinu rozumieme operáciu danú predpisom

$$h_1 *_H h_2 = h_1 *_G h_2$$

pre ľubovoľné $h_1, h_2 \in H$. (Kvôli zrozumiteľnosti sme tu použili rozličné označenie pre operáciu na grupe G a jej podgrupe H, ďalej však budeme používať rovnaké označenie pre obe operácie.)

Poznámka 2.2.2. Dôležité je všimnúť si, že definícia podgrupy zahŕňa aj požiadavku, aby zúženie operácie $*$ na podmnožinu H bola binárna operácia na H. To znamená, že množina H je uzavretá vzhľadom na operáciu $*$, čiže

$$h_1, h_2 \in H \Rightarrow h_1 * h_2 \in H.$$

Pretože každá grupa musí obsahovať neutrálny prvok, priamo z definície vyplýva, že $H \neq \emptyset$.

Z toho, že podgrupa má rovnako definovanú grupovú operáciu vyplýva, že aj inverzné prvky a neutrálny prvok sú v podgrupe rovnaké ako v celej grupe.

Lema 2.2.3. *Nech $(G, *)$ je grupa a H je jej podgrupa.*

(i) *Ak e_H je neutrálny prvok grupy H a e_G je neutrálny prvok grupy G, tak $e_H = e_G$. (Z toho špeciálne vyplýva $e_G \in H$, teda každá podgrupa musí obsahovať neutrálny prvok.)*

(ii) *Ak $a \in H$, b je inverzný prvok k a v G a c je inverzný prvok k a v H, tak $b = c$.*

Dôkaz. (i) Z toho, že e_G je neutrálny prvok grupy G dostaneme

$$e_G * e_H = e_H.$$

Súčasne platí

$$e_H * e_H = e_H$$

lebo e_H je neutrálny prvok grupy H. Dostávame teda rovnosť

$$e_G * e_H = e_H * e_H$$

a zo zákona o krátení (v grupe G) potom vyplýva $e_G = e_H$.

(ii) Opäť využijeme zákon o krátení. Z prvej časti vieme, že $e_G = e_H$, označme teda neutrálny prvok oboch grúp ako $e := e_G = e_H$. Ak b je inverzný prvok k a v grupe G, tak $a * b = e$. Podobne, z toho, že c je inverzný prvok k a v H máme $a * c = e$. Z rovnosti

$$a * b = a * c$$

vyplýva $b = c$. □

Príklad 2.2.4. $(\mathbb{Q}, +)$ je podgrupa grupy $(\mathbb{R}, +)$, lebo operácia $+$ na $\mathbb{Q}$ funguje rovnako ako sčitovanie reálnych čísel. Podobne $(\mathbb{Z}, +)$ je podgrupa $(\mathbb{Q}, +)$ a $(\mathbb{R}, +)$ je podgrupa grupy $(\mathbb{C}, +)$.

Podobne ako pri vektorových priestoroch, aj pri podgrupách máme pomerne jednoduché kritérium na zistenie, či nejaká podmnožina tvorí podgrupu danej grupy.

Veta 2.2.5 (Kritérium podgrupy). *Nech $(G, *)$ je grupa a $H \subseteq G$, $H \neq \emptyset$. Nasledujúce podmienky sú ekvivalentné*

(i) *H je podgrupa grupy G;*

(ii) *množina H je uzavretá vzhľadom na operáciu $*$ a na tvorenie inverzných prvkov v G, čiže platí (pre ľubovoľné $a, b \in H$)*

$$a, b \in H \ \Rightarrow a * b \in H$$
$$a \in H \Rightarrow a^{-1} \in H$$

(iii) *pre ľubovoľné $a, b \in H$ platí aj $a^{-1} * b \in H$*

Dôkaz. (i) $\Rightarrow$ (ii): Uzavretosť množiny H vzhľadom na operáciu $*$ vyplýva z toho, že zúženie operácie $*$ na H je binárna operácia na podmnožine H (poznámka 2.2.2). Ďalej z lemy 2.2.3 vieme, že inverzné prvky v H sú rovnaké ako v G. Preto inverzný prvok k ľubovoľnému $a \in H$ (v grupe G) musí patriť do H (je to inverzný prvok k a v grupe H).

(ii) $\Rightarrow$ (iii): Ak $a, b \in H$ tak aj $a^{-1} \in H$ (na základe prvej z dvoch podmienok uvedených v (ii)), na základe druhej podmienky (použitej pre a^{-1} a b) potom dostaneme $a^{-1} * b \in H$.

(iii) $\Rightarrow$ (ii): Pretože H je neprázdna množina, existuje aspoň jeden prvok $x \in H$. Použitím (iii) pre $b = a = x$ dostaneme $x^{-1} * x = e \in H$. Majme teraz ľubovoľné $a, b \in H$. Z (iii) pre prvky a a e dostaneme $a^{-1} * e = a^{-1} \in H$. Ak teraz použijeme tú istú podmienku pre a^{-1} a b, dostaneme $(a^{-1})^{-1} * b = a * b \in H$. Obe implikácie z (ii) sú teda splnené.

(ii) $\Rightarrow$ (i): Máme dokázať, že H so zúženou operáciou $*$ spĺňa podmienky z definície grupy. Uzavretosť na operáciu $*$ znamená, že zúženie operácie $*$ je binárna operácia na H (poznámka 2.2.2). Asociatívnosť sa automaticky zdedí z grupy G (pozri poznámku I-4.2.6). Ďalej by sme mali ukázať, že $e \in H$. Použijeme podobný postup, ako v predchádzajúcej časti dôkazu. Keďže $H \neq \emptyset$, existuje nejaký prvok $a \in H$ a z (ii) máme $a^{-1} * a = e \in H$. Zostáva nám dokázať, že každý prvok má v H inverzný prvok. Z predchádzajúcej lemy však vieme, že inverzné prvky v G a v H sú rovnaké a druhá časť podmienky (ii) hovorí, že podmnožina H je uzavretá vzhľadom na inverzné prvky. □

Predchádzajúce kritérium nám dáva inú možnosť ako dokázať, že nejaká množina G s operáciou $*$ tvorí grupu – v prípade, že ide o zúženie nejakej binárnej operácie na väčšej množine, o ktorej sme už ukázali, že tvorí grupu. Namiesto toho, aby sme overovali pre G podmienky z definície grupy, stačí nám overiť, že G spĺňa kritérium podgrupy.

Pri použití kritéria podgrupy potrebujeme overiť aj to, že podmnožina H je neprázdna. Pretože každá podgrupa musí obsahovať neutrálny prvok, je často najjednoduchšie začať overením, či ho daná podmnožina H naozaj obsahuje. (Ak zistíme, že $e \in H$, tak $H \neq \emptyset$ a môžeme použiť kritérium podgrupy. V opačnom prípade H nemôže byť podgrupa, takže ďalšie podmienky už nemusíme overovať.)

Poznámka 2.2.6. V skutočnosti ak je množina H konečná, je možné uvedené kritérium ešte o čosi zjednodušiť – stačí overovať podmienku $a, b \in H \Rightarrow a * b \in H$. Tento fakt dokážeme o niečo neskôr v dôsledku 2.4.5.

Príklad 2.2.7. Ak $(G, *)$ je grupa, tak G je podgrupa grupy G. Ak e je neutrálny prvok grupy G, tak $\{e\}$ je podgrupa grupy G. Čiže každá grupa obsahuje dve podgrupy – celú grupu G a jednoprvkovú podgrupu $\{e\}$ obsahujúcu len neutrálny prvok.

Uvedieme teraz dva príklady podgrúp grupy $(\mathbb{C} \setminus \{0\}, \cdot)$.

Príklad 2.2.8. Označme $S = \{x \in \mathbb{C}; |x| = 1\}$. Množina S tvorí podgrupu grupy $(\mathbb{C} \setminus \{0\}, \cdot)$. Skutočne:
Platí $1 \in S$, teda S je neprázdna.
Ak $x, y \in S$, znamená to $|x| = |y| = 1$. Potom $|xy| = |x||y| = 1$, teda aj $xy \in S$.
Ak $x \in S$, čiže $|x| = 1$, tak $\left|\frac{1}{x}\right| = \frac{1}{|x|} = 1$, čiže $\frac{1}{x} \in S$.

Príklad 2.2.9. Podmnožiny $\mathbb{R} \setminus \{0\}$, $\mathbb{Q} \setminus \{0\}$ sú podgrupy grupy $(\mathbb{C} \setminus \{0\}, \cdot)$. Stačí si uvedomiť, že podiel dvoch nenulových reálnych (racionálnych) čísel je opäť reálne (racionálne) číslo.

Príklad 2.2.10. Podmnožina $\mathbb{R}^+$ je podgrupa grupy $(\mathbb{R} \setminus \{0\}, \cdot)$. Vyplýva to z toho, že podiel dvoch kladných čísel je opäť kladné číslo.

Kritérium podgrupy môžeme využiť na dôkaz nasledujúcej jednoduchej lemy ako aj dôležitého tvrdenia 2.2.12 o prieniku podgrúp.

Lema 2.2.11. *Nech $(G, *)$ je grupa. Potom*

(i) *Ak $K \subset H \subset G$ a K, H sú podgrupy G, tak K je podgrupa H.*

(ii) *Ak H je podgrupa G a K je podgrupa H, tak K je aj podgrupa G.*

Dôkaz. Cvičenie. □

Tvrdenie 2.2.12. *Nech $(G, *)$ je grupa a H_i je podgrupa grupy G pre každé $i \in I$. Potom prienik týchto podgrúp*

$$H := \bigcap_{i \in I} H_i$$

je opäť podgrupa grupy G.

Dôkaz. Potrebujeme ukázať, že $H \neq \emptyset$ a H spĺňa podmienku (iii) z vety 2.2.5.

Pretože $e \in H_i$ pre všetky podgrupy H_i, neutrálny prvok e leží aj v ich prieniku, a teda $H \neq \emptyset$.

Nech teraz $a, b \in H$. To znamená, že $a, b \in H_i$ pre každé $i \in I$. Z kritéria podgrupy potom dostaneme $a^{-1} * b \in H_i$. Pretože tento prvok patrí do každej z množín H_i pre $i \in I$, patrí aj do ich prieniku, čiže $a^{-1} * b \in H = \bigcap_{i \in I} H_i$. □

Príklad 2.2.13. Už sme videli, že $S = \{x \in \mathbb{C}; |x| = 1\}$, $\mathbb{R} \setminus \{0\}$ aj $\mathbb{R}^+$ sú podgrupy grupy $(\mathbb{C} \setminus \{0\}, \cdot)$. Môžeme si všimnúť, že $S \cap (\mathbb{R} \setminus \{0\}) = \{\pm 1\}$ aj $S \cap \mathbb{R}^+ = \{1\}$ sú podgrupy $(\mathbb{C} \setminus \{0\}, \cdot)$.

Priamo z tvrdenia 2.2.12 dostaneme nasledujúci dôležitý dôsledok.

Dôsledok 2.2.14. *Ak $(G, *)$ je grupa a $A \subset G$ je ľubovoľná podmnožina G, tak prienik všetkých podgrúp obsahujúcich množinu A je tiež podgrupa G. Túto podgrupu nazývame* podgrupa generovaná podmnožinou *A a označujeme $[A]$. Ak $[A] = G$, hovoríme, že grupa G je generovaná podmnožinou A (alebo tiež, že A generuje G). V prípade, že $A = \{a\}$ je jednoprvková množina, tak namiesto $[\{a\}]$ budeme používať označenie $[a]$ a hovoríme o* podgrupe generovanej prvkom *a.*

Definíciu podgrupy generovanej množinou A môžeme stručne zapísať ako

$$[A] = \bigcap \{H \subseteq G; H \supseteq A \ \wedge \ H \text{ je podgrupa } G\}. \tag{2.1}$$

Poznámka 2.2.15. Podgrupa generovaná množinou A je najmenšia (vzhľadom na inklúziu) podgrupa grupy G, ktorá obsahuje A. Pod pojmom „najmenšia vzhľadom na inklúziu" rozumieme to, že pre ľubovoľnú podgrupu H, ktorá obsahuje A platí $[A] \supseteq H$. Inak povedané, je to najmenší prvok množiny tých podgrúp, ktoré obsahujú A, vzhľadom na čiastočné usporiadanie $\subseteq$ na tejto množine.[1]

Z toho, čo sme doteraz uviedli o podgrupe generovanej nejakou množinou je zrejmá analógia s pojmom vektorového podpriestoru generovaného nejakou množinou vektorov.

S týmto pojmom sa ešte stretneme, podrobnejšie sa budeme venovať najmä podgrupám generovaným jediným prvkom. Zatiaľ uveďme aspoň jeden jednoduchý príklad.

Príklad 2.2.16. Uvažujme grupu $(\mathbb{R}, +)$. Potom podgrupa generovaná prvkom 1 je $\mathbb{Z}$, čiže $\mathbb{Z} = [1]$.

Aby sme videli, že $\mathbb{Z} \subseteq [1]$, stačí si všimnúť, že keď nejaká podgrupa $(\mathbb{R}, +)$ obsahuje 1, musí obsahovať aj $2 = 1 + 1$, $3 = 2 + 1$ atď. Indukciou môžeme dokázať, že obsahuje všetky prirodzené čísla. Samozrejme, ako každá podgrupa, obsahuje aj neutrálny prvok 0 a z uzavretosti na inverzné prvky vyplýva, že musí obsahovať aj všetky záporné celé čísla. Takže podgrupa [1] určite obsahuje všetky prvky množiny $\mathbb{Z}$.

Na druhej strane, $\mathbb{Z}$ je podgrupa $(\mathbb{R}, +)$, ktorá obsahuje číslo 1. Takže je jednou z podgrúp vystupujúcich v prieniku (2.1), z čoho vyplýva $[1] \subseteq \mathbb{Z}$.

Takmer rovnakým spôsobom by sa dalo ukázať, že aj $[-1] = \mathbb{Z}$.

Príklad 2.2.17. Pozrime sa teraz na 6-prvkovú grupu $\mathbb{Z}_2 \times \mathbb{Z}_3$. (Usporiadané dvojice, kde na prvej súradnici sčitujeme modulo 2 a na druhej súradnici súradnici modulo 3 - pozri definíciu 2.1.5).

V tomto prípade (ako čitateľ ľahko overí) platí napríklad:
$[(1,0)] = \mathbb{Z}_2 \times \{0\}$;
$[(0,1)] = \{0\} \times \mathbb{Z}_3$;
$[(1,1)] = \mathbb{Z}_2 \times \mathbb{Z}_3$, keďže pomocou prvku $(1,1)$ postupne dostaneme prvky $(0,2)$, $(1,0)$, $(0,1)$, $(1,2)$ a $(0,0)$, čiže všetky prvky grupy.

Cvičenia

Úloha 2.2.1. Dokážte lemu 2.2.11.

Úloha 2.2.2. Nájdite všetky podgrupy $(\mathbb{Z}_6, \oplus)$.

Úloha 2.2.3. Dokážte, že matice typu $n \times n$, ktorých determinant je rovný 1, s operáciou násobenia matíc tvoria grupu.

Úloha 2.2.4. Dokážte: Ak H je podgrupa grupy $(G, \cdot)$ tak $H^2 = H \cdot H = H$.

Úloha 2.2.5. Ak A, B, C sú podgrupy G a $C \subseteq A \cup B$, tak $C \subseteq A$ alebo $C \subseteq B$.

Úloha 2.2.6. Tvoria pri sčitovaní/násobení matíc grupu štvorcové matice $n \times n$, ktoré sú: symetrické, antisymetrické, diagonálne, regulárne, horné trojuholníkové...

[1] S pojmom čiastočné usporiadanie a najmenší prvok ste sa pravedpodobne už stretli alebo ešte stretnete na iných prednáškach, pozri [OŠ].

Úloha 2.2.7. Nájdite príklad nekonečnej grupy, ktorá obsahuje netriviálnu konečnú podgrupu. (Pod netriviálnou podgrupou rozumieme podgrupu, ktorá má viac ako jeden prvok.)

Úloha 2.2.8. Matice typu $n \times n$, ktoré v každom riadku a každom stĺpci majú práve jednu jednotku a ostatné prvky sú nulové, s operáciou násobenia matíc tvoria grupu. (Hint: Súvisia tieto matice nejako s permutáciami? Akým lineárnym zobrazeniam zodpovedajú?)

Úloha 2.2.9. Ukážte, že $H = \{\frac{m}{n}; m, n \text{ sú nepárne}\}$ je podgrupa grupy $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Úloha 2.2.10. Nájdite všetky podgrupy grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$ a všetky podgrupy grupy $\mathbb{Z}_4$ (v oboch prípadoch operácia $\oplus$). Majú tieto grupy rovnaký počet dvojprvkových podgrúp? (Z toho, čo sa naučíme v ďalšej podkapitole sa na základe tejto úvahy bude dať zdôvodniť, že tieto dve grupy nie sú izomorfné.)

Úloha 2.2.11. Dokážte, alebo vyvráťte: Ak H_1 je podgrupa G_1 a H_2 je podgrupa G_2, tak $H_1 \times H_2$ je podgrupa $G_1 \times G_2$.

Úloha 2.2.12. Nech V je vektorový priestor nad poľom $\mathbb{R}$. Je aj každá podgrupa grupy $(V, +)$ podpriestorom priestoru V? Ako je to s vektorovými priestormi nad poľom $\mathbb{Z}_p$?

Úloha 2.2.13. Nech H je vlastná podgrupa grupy G (t.j. $H \neq G$). Dokážte, že $[G - H] = G$.

2.3 Homomorfizmy grúp

Pri vektorových priestoroch boli dôležité lineárne zobrazenia – zobrazenia zachovávajúce operácie určujúce vektorový priestor. Podobne aj pri štúdiu grúp sú užitočné zobrazenia medzi grupami, ktoré zachovávajú grupové operácie. Takéto zobrazenia voláme homomorfizmy. [2]

Definícia 2.3.1. Nech $(G, \circ)$, $(H, *)$ sú grupy. Potom zobrazenie $f\colon G \to H$ je *homomorfizmus,* ak

$$f(g_1 \circ g_2) = f(g_1) * f(g_2)$$

platí pre ľubovoľné $g_1, g_2 \in G$.

Na označenie homomorfizmu budeme niekedy používať stručnejší zápis $f\colon (G, \circ) \to (H, *)$ (t.j. týmto zápisom súčasne popíšeme ako označujeme homomorfizmus a aj ako označujeme grupové operácie.)

Skôr než si tento pojem ilustrujeme na príkladoch, dokážeme si dve jednoduché vlastnosti, ktoré musí každý homomorfizmus spĺňať.

Veta 2.3.2. *Nech $(G, \circ)$, $(H, *)$ sú grupy a $f\colon G \to H$ je homomorfizmus. Označme ďalej e_G neutrálny prvok grupy G a e_H neutrálny prvok grupy H. (Inverzné prvky budeme v oboch prípadoch označovať pomocou horného indexu -1 ako obvykle.) Potom platí:*

(i) $f(e_G) = e_H$ *(teda homomorfizmus musí zobraziť neutrálny prvok na neutrálny prvok);*

(ii) $f(a^{-1}) = (f(a))^{-1}$ *(teda homomorfizmy zachovávajú aj inverzné prvky).*

Dôkaz. (i) Pretože

$$f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G),$$

dostávame rovnosť $f(e_G) * e_H = f(e_G) = f(e_G) * f(e_G)$. Zo zákona o krátení (použitého pre grupu H) potom dostaneme $f(e_G) = e_H$.

[2] Keďže pojem homomorfizmu sa definuje aj pre iné štruktúry než sú grupy, niekedy sa používa aj termín *grupový homomorfizmus.*

(ii) Z definície homomorfizmu tentokrát máme

$$f(a^{-1}) * f(a) = f(a^{-1} \circ a) = f(e_G) \overset{\text{(i)}}{=} e_H,$$

teda $f(a^{-1}) * f(a) = (f(a))^{-1} * f(a)$ a opäť stačí použiť zákon o krátení, aby sme dostali $f(a^{-1}) = (f(a))^{-1}$. □

Príklad 2.3.3. Ak $(G, *)$ a $(H, \circ)$ sú ľubovoľné grupy, tak $f\colon G \to H$ určené predpisom $f(g) = e_H$ pre všetky $g \in G$ je homomorfizmus.

Zobrazenie $id_G\colon G \to G$ je homomorfizmus pre každú grupu $(G, *)$.

Príklad 2.3.4. Uvažujme zobrazenie

$$f\colon (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot), \qquad f\colon x \mapsto e^x.$$

Priamo z vlastností exponenciálnej funkcie vyplýva, že f je homomorfizmus

$$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

Príklad 2.3.5. Definujme

$$g\colon (\mathbb{R}, +) \to (S, \cdot), \qquad g\colon \varphi \mapsto e^{i\varphi} = \cos\varphi + i\sin\varphi,$$

kde $S = \{z \in \mathbb{C}; |z| = 1\}$ je grupa z príkladu 2.2.8. (Zápis $e^{i\varphi}$ budeme chápať jednoducho ako skratku zápisu $\cos\varphi + i\sin\varphi$. Ide o tzv. goniometrický a exponenciálny tvar komplexného čísla, pozri podkapitolu I-B.4.)

Fakt, že ide o homomorfizmus vyplýva z Moivrovej vety I-B.2.3, ktorá hovorí, že pri násobení komplexných čísel sa uhly sčitujú (a absolútne hodnoty sa násobia).

$$g(\varphi_1+\varphi_2) = (\cos(\varphi_1+\varphi_2)+i\sin(\varphi_1+\varphi_2)) = (\cos\varphi_1+i\sin\varphi_1)\cdot(\cos\varphi_2+i\sin\varphi_2) = g(\varphi_1)\cdot g(\varphi_2)$$

Príklad 2.3.6. Homomorfizmus z predchádzajúceho príkladu teraz trochu zmodifikujeme.

Budeme pracovať s grupou $(\langle 0, 2\pi), +)$, v ktorej je sčitovanie definované modulo 2π. Formálne môžeme operáciu $+$ definovať ako

$$\alpha + \beta = 2\pi \left\lfloor \frac{\alpha + \beta}{2\pi} \right\rfloor.$$

(Význam znamienka $+$ na pravej strane predstavuje sčitovanie reálnych čísel, zatiaľčo na ľavej strane je operácia, ktorú definujeme. Na to ste si však už pravedpodobne zvykli, že niekedy označujeme rôzne veci rovnakým symbolom.)

Potom dostávame homomorfizmus

$$h\colon (\langle 0, 2\pi), +) \to (S, \cdot), \qquad h\colon \varphi \mapsto e^{i\varphi} = \cos\varphi + i\sin\varphi.$$

(Je to naozaj homomorfizmus, lebo zmena uhla φ o nejaký násobok 2π neovplyvní hodnotu čísla $\cos\varphi + i\sin\varphi$. Výsledok je teda rovnaký ako pri použití homomorfizmu z predchádzajúceho príkladu. Tento homomorfizmus je navyše bijektívny.)

Príklad 2.3.7. Nech $n \in \mathbb{N}$, $n \geq 2$. Zobrazenie $f\colon (\mathbb{Z}, +) \to (\mathbb{Z}_n, \oplus)$ dané predpisom

$$f(k) = k \bmod n$$

je homomorfizmus. (Rovnosť $f(k + l) = f(k) \oplus f(l)$ vyplýva z toho, že dostaneme rovnaký výsledok keď dve čísla sčítame a potom urobíme zvyšok po delení n a keď to urobíme v obrátenom poradí.)

Pripomeňme, čo rozumieme pod obrazom a vzorom množiny v danom zobrazení.

Definícia 2.3.8. Nech $f\colon X \to Y$, $A \subseteq X$, $B \subseteq Y$.
Potom *obraz množiny* A v zobrazení f je

$$f[A] = \{f(a); a \in A\}$$

a *vzor množiny* B v zobrazení f je

$$f^{-1}(B) = \{a \in A; f(a) \in B\}.$$

V prípade, že $B = \{b\}$, t.j. že množina B je jednoprvková, používame niekedy stručnejšie označenie $f^{-1}(b)$ namiesto $f^{-1}(\{b\})$. (Hoci niekedy by sa mohlo toto označenie pliesť s označením pre obraz prvku b v inverznej funkcii, z kontextu snáď vždy bude jasné, čo máme na mysli.)

Tvrdenie 2.3.9. *Nech $(G, \circ)$, $(H, *)$ sú grupy a $f\colon G \to H$ je homomorfizmus.*

(i) *Ak G' je podgrupa grupy G, tak aj jej obraz $f[G']$ je podgrupa grupy H.*

(ii) *Ak H' je podgrupa grupy H, tak aj jej vzor $f^{-1}(H')$ je podgrupa grupy G.*

Dôkaz. V oboch prípadoch použijeme kritérium podgrupy.
(i) Pretože $e_G \in G'$, z vety 2.3.2 máme $f(e_G) = e_H \in f[G']$, a teda $f[G'] \neq \emptyset$.
Nech $a, b \in f[G']$. To znamená, že existujú $a_1, b_1 \in G'$ také, že $f(a_1) = a$ a $f(b_1) = b$. Potom dostávame

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

Pretože G' je podgrupa, máme $a_1^{-1}b_1 \in G'$, a teda $a^{-1}b = f(a_1^{-1}b_1) \in f[G']$.
(ii) Opäť sa ľahko ukáže, že $e_G \in f^{-1}(H')$, teda táto podmnožina je neprázdna.
Ak $a, b \in f^{-1}(H')$, znamená to, že $f(a), f(b) \in H'$. Potom

$$f(a^{-1}b) = f(a^{-1})f(b) = f(a)^{-1}f(b) \in H',$$

lebo H' je podgrupa. Zistili sme, že $a^{-1}b \in f^{-1}(H')$, teda $f^{-1}(H')$ vyhovuje podmienke z kritéria podgrupy. □

Dôsledok 2.3.10. *Nech $(G, \circ)$, $(H, *)$ sú grupy a $f\colon G \to H$ je homomorfizmus. Potom* jadro

$$\operatorname{Ker} f = \{g \in G; f(g) = e_H\}$$

je podgrupa grupy G a

$$\operatorname{Im} f = \{f(g); g \in G\}$$

je podgrupa grupy H.

Dôkaz. Vyplýva z toho, že $\{e_H\}$ je podgrupa grupy H a G je podgrupa grupy G. □

Definícia 2.3.11. Nech $(G, \circ)$, $(H, *)$ sú grupy. Ak $f\colon G \to H$ je bijektívny homomorfizmus, hovoríme, že f je *izomorfizmus* alebo tiež, že grupy G a H sú izomorfné (označujeme $G \cong H$).

Opäť, podobne ako v prípade vektorových priestorov, existencia izomorfizmu znamená, že grupy G a H sú v podstate rovnaké, len ich prvky sú inak pomenované. Bijektívne zobrazenie f je „slovníkom“, ktorý prekladá medzi týmito dvoma pomenovaniami.

Lema 2.3.12. *Nech $(G,*)$, $(H,\circ)$, $(K,\odot)$ sú grupy.*

(i) *Ak $f\colon G\to H$ je izomorfizmus, tak aj $f^{-1}\colon H\to G$ je izomorfizmus.*

(ii) *Ak $f\colon G\to H$ a $g\colon H\to K$ sú homomorfizmy, tak aj $g\circ f\colon G\to K$ je homomorfizmus.*

(iii) *Ak $f\colon G\to H$ a $g\colon H\to K$ sú izomorfizmy, tak aj $g\circ f\colon G\to K$ je izomorfizmus.*

Dôkaz. (i): Nech $a,b\in H$. Pretože f je surjekcia, existujú $a_1,b_1\in G$ také, že $f(a_1)=a$, $f(b_1)=b$. Z definície homomorfizmu potom máme

$$a\circ b=f(a_1)\circ f(b_1)=f(a_1*b_1).$$

Potom priamo z definície inverzného zobrazenia vyplýva

$$f^{-1}(a\circ b)=a_1*b_1=f^{-1}(a)*f^{-1}(b).$$

(ii): Ak $a,b\in G$, dvojnásobným použitím definície homomorfizmu dostaneme

$$g(f(a*b))=g(f(a)\circ f(b))=g(f(a))\odot g(f(b))$$

(iii): Podľa (ii) je zloženie homomorfizmov opäť homomorfizmus. Súčasne vieme (tvrdenie I-2.2.13), že zloženie bijekcií je bijekcia. □

Z predchádzajúcej lemy vidíme, že:
a) ak grupa G je izomorfná s grupou H, tak aj H je izomorfná s G,
b) ak G je izomorfná s H a H je izomorfná s K, tak aj grupy G a K sú izomorfné.
Ak si navyše uvedomíme, že každá grupa je izomorfná sama so sebou (identické zobrazenie $id_G\colon G\to G$ je izomorfizmus), tak vidíme, že vzťah „byť izomorfný“ je relácia ekvivalencie.

Príklad 2.3.13. Zobrazenie $f\colon(\mathbb{R},+)\to(\mathbb{R}^+,\cdot)$, $f(x)=e^x$, z príkladu 2.3.4 je izomorfizmus. Aby sme videli, že f je bijekcia, stačí si všimnúť, že zobrazenie $f^{-1}\colon\mathbb{R}^+\to\mathbb{R}$ dané predpisom $f^{-1}(x)=\ln x$ je inverzné k zobrazeniu f. (Podľa predchádzajúcej lemy je teda aj toto zobrazenie homomorfizmom.)

Príklad 2.3.14. Homomorfizmus $h(\varphi)=e^{i\varphi}=\cos\varphi+i\sin\varphi$, $h\colon(\langle 0,2\pi),+)\to(S,\cdot)$, z príkladu 2.3.6 je tiež izomorfizmom.

Aby sme videli, že h je bijekcia, stačí si uvedomiť, že prvky grupy S predstavujú body jednotkovej kružnice a každý bod na jednotkovej kružnici je jednoznačne určený uhlom z intervalu $\langle 0,2\pi)$, ktorý sa naň zobrazí zobrazením g.

Aj surjektívne a injektívne homomorfizmy majú niektoré zaujímavé vlastnosti, preto sa nám v budúcnosti bude hodiť nasledovná terminológia.

Definícia 2.3.15. Nech $f\colon(H,\circ)\to(G,*)$ je homomorfizmus. Ak f je injektívne zobrazenie, tak hovoríme, že f je *monomorfizmus.* Ak f je surjektívne zobrazenie, tak hovoríme, že f je *epimorfizmus.*

Hovoríme, že grupa $(H,\circ)$ je *homomorfný obraz* grupy $(G,*)$, ak existuje epimorfizmus $f\colon(G,*)\to(H,\circ)$.

Videli sme napríklad, že pre každé $n\in\mathbb{N}$ je $(\mathbb{Z}_n,\oplus)$ homomorfný obraz grupy $(\mathbb{Z},+)$ (príklad 2.3.7), grupa $(S,\cdot)$ je homomorfný obraz grupy $(\mathbb{R},+)$ (príklad 2.3.4).

Cvičenia

Úloha 2.3.1. Zistite, či sú grupy G a H izomorfné a grupa H je homomorfným obrazom grupy G. Svoju odpoveď zdôvodnite!
a) $G = (\mathbb{R}, +) \times (\mathbb{R}, +)$, $H = (\mathbb{C}, +)$
b) $G = (\mathbb{Q}, +)$, $H = (\mathbb{R}, +)$
c) $G = (\mathbb{Q}, +)$, $H = (\mathbb{Q}^+, \cdot)$
d) $G = (\mathbb{C} \setminus \{0\}, \cdot)$, $H = (\mathbb{R} \setminus \{0\}, \cdot)$
e) $G = (\mathbb{Q}, +)$, $H = (\mathbb{Q} \setminus \{0\}, \cdot)$

Úloha 2.3.2. Zistite, či sú grupy G a H izomorfné a či je niektorá z nich homomorfným obrazom druhej. Svoju odpoveď zdôvodnite!
a) $G = (\mathbb{R}, +)$, $H = (\mathbb{R}^+, \cdot)$
b) $G = (\mathbb{R} \setminus \{0\}, \cdot)$, $H = (\mathbb{R}^+, \cdot)$
c) $G = (\mathbb{Z}_4, \oplus)$, $H = (\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$

Úloha 2.3.3. Nech $(G, \circ)$ je grupa. Je zobrazenie $g \mapsto g^{-1}$ izomorfizmus z G na G? Ak nie, vedeli by ste definovať binárnu operáciu $*$ na G, tak, aby toto zobrazenie bol izomorfizmus grúp $(G, \circ)$ a $(G, *)$? Je uvedené zobrazenie izomorfizmom, ak G je komutatívna?

Úloha 2.3.4. Nech G je ľubovoľná grupa. Dokážte, že zobrazenie $g \mapsto g \circ g$ je homomorfizmus z G do G práve vtedy, keď G je komutatívna.

Úloha 2.3.5. a) Dokážte, že $\mathbb{R} \times \mathbb{R} \setminus \{(0,0)\}$ s operáciou $*$ definovanou ako $(a, b) * (c, d) = (ac - bd, ad + bc)$ tvorí grupu.
b) Dokážte, že všetky nenulové matice tvaru $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ tvoria s násobením matíc grupu. (Hint k obom častiam úlohy: Možno vám pomôže nájsť jednoduchšie riešenie to, že táto úloha je v časti o homomorfizmoch.)

Úloha 2.3.6. Nech $f\colon G \to H$ je homomorfizmus grúp. Dokážte:
a) Zobrazenie f je surjektívne práve vtedy, keď $\operatorname{Im} f = H$.
b) Zobrazenie g je injektívne práve vtedy, keď $\operatorname{Ker} f = \{e\}$.

Úloha 2.3.7. Nech $g\colon G \to G'$ a $h\colon H \to H'$ sú homomorfizmy grúp. Potom aj zobrazenie $f\colon G \times H \to G' \times H'$ dané predpisom $f(x, y) = (g(x), h(y))$ je homomorfizmus. Ak g a h sú izomorfizmy (surjektívne homomorfizmy/injektívne homomorfizmy), tak f je izomorfizmus (surjektívny homomorfizmus/injektívny homomorfizmus).

Úloha 2.3.8. Nech $f, g\colon G \to H$ sú homomorfizmy grúp. Je množina $\{a; f(a) = g(a)\}$ podgrupa grupy G?

Úloha 2.3.9. Nech $f, g\colon (G, \circ) \to (H, *)$ sú homomorfizmy grúp. Definujme zobrazeníe $h\colon G \to H$ ako $h(x) = f(x) * g(x)$. Bude aj h homomorfizmus? Bude to platiť v prípade, že H je komutatívna?

Úloha 2.3.10. Nech $(H, \circ)$, $(G, *)$ sú grupy a $H \subseteq G$. Potom H je podgrupa G práve vtedy, keď zobrazenie $i\colon H \to G$ dané predpisom $i(h) = h$ je homomorfizmus.

Úloha 2.3.11. Nech $f\colon (G, *) \to (H, \circ)$ je homomorfizmus, ktorý je surjektívny ale nie injektívny.
a) Dokážte, že existuje aspoň jedno pravé inverzné zobrazenie k f, ktoré nie je homomorfizmom.
b) Ukážte na príklade, že môže nastať taká situácia, že žiadne pravé inverzné zobrazenie nie

je homomorfizmom.
c) Ukážte na príklade, že môže nastať aj taká situácia, že aspoň jedno pravé inverzné zobrazenie je homomorfizmom.

Rozhodnite podobné otázky pre injektívny ale nesurjektívny homomorfizmus a ľavé inverzné zobrazenie.

Úloha 2.3.12. Dokážte, že ak grupa H je homomorfným obrazom komutatívnej grupy G, tak aj H je komutatívna.

2.4 Cyklické grupy

V tejto kapitole budeme často využívať označenie pre opakované použitie binárnej operácie, t.j.

$$x^n = \underbrace{x \circ \ldots \circ x}_{n\text{-krát}}.$$

Formálne toto označenie zavedieme pomocou definície matematickou indukciou.

Definícia 2.4.1. Nech $(G, \circ)$ je grupa a $x \in G$. Potom pre $n \in \mathbb{N}$ definujeme indukciou $x^1 = x$ a

$$x^{n+1} = x^n \circ x.$$

Ďalej definujeme $x^0 = e$, kde e je neutrálny prvok grupy G a $x^{-n} = (x^{-1})^n$ pre ľubovoľné $n \in \mathbb{N}$. (Tým je výraz x^k definovaný pre ľubovoľné $k \in \mathbb{Z}$.)

Ukážeme, že práve zadefinovaná mocnina v grupe sa správa podobne, ako celočíselné mocniny. (Tvrdenia v nasledujúcej leme sú na prvý pohľad jasné a ich formálny dôkaz je len cvičením na matematickú indukciu.)

Lema 2.4.2. *Nech $(G, \circ)$ je grupa, $x, y \in G$, $m, n \in \mathbb{Z}$. Potom platí:*

(i) *Ak $x \circ y = y \circ x$, tak $x \circ y^n = y^n \circ x$.*

(ii) *Ak $x \circ y = y \circ x$, tak platí aj $(x \circ y)^n = x^n \circ y^n$.*

(iii) $x^{-n} = (x^n)^{-1}$

(iv) $x^{m+n} = x^m \circ x^n = x^n \circ x^m$

(v) $(x^m)^n = x^{mn}$

Dôkaz. (i): Uvedené tvrdenie dokážeme najprv pre $n \in \mathbb{N}$. Budeme postupovať matematickou indukciou vzhľadom na n.

1° Pre $n = 0$ máme $x \circ e = e \circ x$, pre $n = 1$ máme $x \circ y = y \circ x$, čo je náš predpoklad.

2° Ak platí $x \circ y^n = y^n \circ x$ (indukčný predpoklad), tak dostaneme

$$x \circ y^{n+1} = x \circ (y^n \circ y) = (x \circ y^n) \circ y \overset{IP}{=} (y^n \circ x) \circ y = y^n \circ (x \circ y) = y^n \circ (y \circ x) = (y^n \circ y) \circ x = y^{n+1} \circ x.$$

Ak $n < 0$, označme $k = -n$. Potom z už dokázanej časti tvrdenia máme

$$x \circ y^n = x \circ y^{-k} = x \circ (y^{-1})^k = (y^{-1})^k \circ = y^{-k} \circ x = y^n \circ x$$

(ii): Aj túto časť najprv overíme pre $n \in \mathbb{N}$.

Opäť pre $n = 0$ je platnosť tvrdenia zrejmá a pre $n = 1$ sa zhoduje priamo s predpokladom.

Predpokladajme, že (ii) platí pre n. Pre $n+1$ dostávame postupne

$$(x \circ y)^{n+1} = (x \circ y)^n \circ (x \circ y) \overset{IP}{=} (x^n \circ y^n) \circ (x \circ y) = x^n \circ (y^n \circ x) \circ y \overset{\text{(i)}}{=} x^n \circ (x \circ y^n) \circ y = (x^n \circ x) \circ (y^n \circ y) = x^{n+1} \circ y^{n+1}.$$

Rovnosť (ii) rozšírime na záporné čísla priamo použitím definície. Pre $n \in \mathbb{N}$ máme

$$(x \circ y)^{-n} = ((x \circ y)^{-1})^n = ((y \circ x)^{-1})^n = (x^{-1} \circ y^{-1})^n = (x^{-1})^n \circ (y^{-1})^n = x^{-n} \circ y^{-n}.$$

(iii): Najprv nech $n \in \mathbb{N}$. Z (ii) dostávame

$$x^{-n} \circ x^n = (x^{-1})^n \circ x^n = (x^{-1} \circ x)^n = e^n = e$$

(posledná rovnosť sa ľahko overí indukciou na n).

Rovnosť, ktorú sme odvodili, znamená, že $x^{-n} = (x^n)^{-1}$.

Ak $n < 0$, tak $n = -k$ pre nejaké $k \in \mathbb{N}$. Pre k už máme tvrdenie dokázané, čo znamená, že $x^{-k} = (x^k)^{-1}$ a

$$(x^n)^{-1} = ((x^k)^{-1})^{-1} = x^k = x^{-n}.$$

(iv) Overíme tvrdenie najprv pre $n \in \mathbb{N}$ a $m \geq -n$. Budeme postupovať indukciou vzhľadom na n. (T.j. indukciou na n dokazujeme výrok $(\forall m \geq -n) x^{m+n} = x^m \circ x^n = x^n \circ x^m$.)

1° Pre $n = 0$ máme $x^{m+0} = x^m \circ e = e \circ x^m$, čo evidentne platí.

2° Nech uvedená rovnosť platí pre n (a pre ľubovoľné $m \in \mathbb{N}$). Potom

$$x^{m+(n+1)} = x^{(m+n)+1} = x^{m+n} \circ x = (x^m \circ x^n) \circ x = x^m \circ (x^n \circ x) \overset{\text{IP}}{=} x^m \circ x^{n+1}$$

(Nerovnosť $m \geq -n$ sme potrebovali na to, aby $m + n \geq 0$, lebo iba v tomto prípade je $x^{(m+n)+1}$ definované uvedeným spôsobom. Takisto sme využili rovnosť $x^{n+1} = x^n \circ x$, ktorú zatiaľ máme len pre $n \geq 0$.)

Podobne dostaneme

$$x^{m+(n+1)} = x^{(m+n)+1} = x^{m+n} \circ x = (x^n \circ x^m) \circ x = x^n \circ (x^m \circ x) \overset{\text{(i)}}{=} x^n \circ (x \circ x^m) = (x^n \circ x) \circ x^m = x^{n+1} \circ x^m.$$

Tým sme dokázali (iv) pre ľubovoľné $n \in \mathbb{N}$ a $m + n \geq 0$. Zo symetrie vyplýva, že platí aj pre $m \in \mathbb{N}$ a $m + n \geq 0$, čiže vlastne už máme túto rovnosť dokázanú pre ľubovoľné celé čísla m, n také, že $m + n \geq 0$.

Teraz, ak $m, n \in \mathbb{Z}$ sú také, že $m + n < 0$, tak

$$x^{m+n} = (x^{-1})^{(-m)+(-n)} = (x^{-1})^{-m} \circ (x^{-1})^{-n} = x^m \circ x^n,$$

podobne možno odvodiť druhú časť rovnosti (kde sú iba vymenené m a n.)

(v): Najprv túto rovnosť dokážeme pre $n \in \mathbb{N}$, $m \in \mathbb{Z}$ pomocou (iv) indukciou vzhľadom na n. (T.j. výrok $V(n)$, ktorý dokazujeme indukciou, je $(\forall m \in \mathbb{Z})(x^m)^n = x^{mn}$.)

1° Pre $n = 0$ máme rovnosť $e = e$, pre $n = 1$ máme $x^m = x^m$; v oboch prípadoch rovnosť platí.

2° Nech (v) platí pre n. Pre $n + 1$ potom dostaneme

$$(x^m)^{n+1} = (x^m)^n \circ x^m \overset{IP}{=} x^{mn} \circ x^n \overset{\text{(iv)}}{=} x^{mn+n} = x^{m(n+1)}.$$

Na záporné čísla túto rovnosť rozšírime nasledovne

$$(x^m)^{-n} = ((x^m)^{-1})^n \overset{\text{(iii)}}{=} ((x)^{-m})^n = (x)^{-mn} \overset{\text{(iii)}}{=} x^{mn}.$$

□

Ako sme už spomínali pre definícii I-3.3.12, niekedy namiesto a^n používame zápis $n \times a$ (hlavne ak je grupová operácia označená ako $+$ alebo $\oplus$) – hovoríme o multiplikatívnom a aditívnom zápise grupovej operácie.

Definícia 2.4.3. Nech $(G, \circ)$ je grupa a $x \in G$. *Rád prvku* x v grupe G je najmenšie číslo $n \in \mathbb{N}$ také, že $n > 0$ a

$$x^n = e.$$

Ak také číslo neexistuje, rád prvku x sa definuje ako ∞.

Indukciou sa dá ľahko dokázať (úloha 2.4.1), že pre ľubovoľný homomorfizmus $f\colon (G, *) \to (H, \circ)$ platí

$$f(a^n) = f(a)^n. \tag{2.2}$$

Z toho môžeme odvodiť, že ak f je izomorfizmus, tak f zachováva rády prvkov. (T.j. rád prvku a v grupe G je rovnaký ako rád $f(a)$ v H. Pozri úlohu 2.4.1.)

Tento fakt môžeme využiť, ak chceme dokázať, že medzi niektorými dvoma grupami neexistuje izomorfizmus.

Príklad 2.4.4. Ukážeme, že grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$ a $\mathbb{Z}_4$ nie sú izomorfné.

Stačí si uvedomiť, že v grupe $\mathbb{Z}_4$ je rád prvku 1 rovný 4. Ak by bola táto grupa izomorfná s grupou $\mathbb{Z}_2 \times \mathbb{Z}_2$, tak by aj v nej musel existovať prvok rádu 4. Prvky $(1,0)$, $(1,1)$, $(0,1)$ však majú rád 2 a neutrálny prvok $(0,0)$ má rád 1. Teda v $\mathbb{Z}_2 \times \mathbb{Z}_2$ nie je žiadny prvok rádu 4.

Postup z predchádzajúceho príkladu je dosť často používaný v prípade, že chceme dokázať neexistenciu izomorfizmu medzi dvoma grupami. Nájdeme nejakú vlastnosť, ktorú izomorfizmy zachovávajú (invariant) a ukážeme, že jedna z grúp túto vlastnosť nemá. Z vlastností s ktorými sme sa doteraz stretli sa dajú použiť napríklad rád prvku, veľkosť grupy alebo jej podgrúp (v zmysle počtu prvkov alebo kardinality[3]), existencia prvku spĺňajúceho nejakú identitu (ako napríklad $x * x = x$, $x^3 = a^2$ alebo $x * y \neq y * x$ – existencia prvkov, ktoré nekomutujú), atď. Niektoré z týchto vlastností sa dajú použiť aj na dôkaz, že neexistuje (surjektívny) homomorfizmus z jednej grupy do druhej.

Ľahko sa dá ukázať, že v konečnej grupe má každý prvok konečný rád (úloha 2.4.4). Tento fakt možno overiť veľmi podobným spôsobom, aký použijeme v nasledujúcom dôkaze.

Tvrdenie 2.4.5. *Nech $(G, *)$ je grupa a $H \subseteq G$, $H \neq \emptyset$ je jej konečná podmnožina. Potom H je podgrupa G práve vtedy, keď platí*

$$a, b \in H \;\Rightarrow a * b \in H. \tag{2.3}$$

Dôkaz. Implikácia $\boxed{\Rightarrow}$ je zrejmá.

$\boxed{\Leftarrow}$ Podľa vety 2.2.5(ii) nám stačí overiť, že pre každý prvok $a \in H$ aj inverzný prvok a^{-1} patrí do H.

Na to nám stačí ukázať, že prvok $a \in H$ má konečný rád – ak totiž vieme, že existuje prirodzené číslo n také, že $a^n = e$, tak $a^{n-1} * a = a * a^{n-1} = e$, čo znamená, že a^{n-1} je inverzný prvok k a. Z (2.3) však indukciou ľahko dostaneme, že $a^{n-1} \in H$. (Môžeme predpokladať, že $a \neq e$, a teda $n > 1$. Pre neutrálny prvok e dokazovaná implikácia očividne platí.)

Nech teda $a \in H$. Vieme, že pre ľubovoľné n aj $a^n \in H$. Keďže množina H je konečná, existujú $m \neq k$ také, že $a^m = a^k$. Bez ujmy na všeobecnosti, nech $m > k$. Potom z rovnosti $a^m = a^k$ dostaneme $a^{m-k} = e$. Ukázali sme teda existenciu prirodzeného čísla $n := m - k$ takého, že $a^n = e$. □

[3] S pojmom kardinality (mohutnosti) množiny ste sa už pravdepodobne stretli na niektorej inej prednáške.

Definícia 2.4.6. *Cyklická grupa* je grupa G, ktorá je generovaná nejakým jej prvkom $a \in G$.
Prvok a, ktorý generuje grupu G, nazývame *generátor* grupy G.

Príklad 2.4.7. V príklade 2.2.16 sme videli, že $\mathbb{Z} = [1]$, teda $(\mathbb{Z}, +)$ je cyklická grupa. Súčasne platí $\mathbb{Z} = [-1]$, teda generátor cyklickej grupy nemusí byť jednoznačne určený.

Lema 2.4.8. *Ak $(G, *)$ je grupa a $a \in G$, tak $H = \{a^n; n \in \mathbb{Z}\}$ je podgrupa grupy G.*

Dôkaz. Pretože $e = a^0 \in H$, množina H je neprázdna. Overme, či pre H platí kritérium podgrupy.
Ak $a^n, a^m \in H$, tak aj $a^n * a^m = a^{n+m} \in H$.
Ak $a^n \in H$, tak aj $(a^n)^{-1} = a^{-n} \in H$. □

Veta 2.4.9. *Ak G je cyklická grupa a a je jej generátor, tak*

$$G = \{a^n; n \in \mathbb{Z}\},$$

t.j. G pozostáva práve z mocnín generátora a.

Dôkaz. Z predchádzajúcej lemy vieme, že $H = \{a^n; n \in \mathbb{Z}\}$ je podgrupa G obsahujúca prvok a. Preto $[a] \subseteq H$. Z predpokladu, že G je generovaná prvkom a potom máme $G \subseteq H$ a keďže H je podmnožina G, musí platiť $G = H$. □

V predchádzajúcom dôkaze sme vlastne súčasne ukázali, že

$$[a] = \{a^n; n \in \mathbb{Z}\}.$$

Lema 2.4.8 hovorí vlastne to, že pre každý prvok a obsahuje G cyklickú podgrupu generovanú prvkom a.

Pripomeňme, že pod označením $a \mid b$ (a delí b), kde $a, b \in \mathbb{Z}$ rozumieme to, že existuje nejaké celé číslo c také, že $b = c.a$.

$$a \mid b \qquad \Leftrightarrow \qquad (\exists c \in \mathbb{Z})(b = c.a)$$

Lema 2.4.10. *Ak $a \in G$, kde G je grupa, a rád prvku a je $n \in \mathbb{N}$, tak*

$$a^m = a^k \qquad \Leftrightarrow \qquad n \mid m - k.$$

Ak rád prvku a je ∞, tak

$$a^m = a^k \qquad \Leftrightarrow \qquad m = k.$$

Dôkaz. Uvažujme najprv prípad, že rád a je n.
$\boxed{\Rightarrow}$ Ak $a^m = a^k$, tak $a^{m-k} = e$. Nech $l = (m-k) \bmod n$ je zvyšok čísla $m-k$ po delení n. Potom $a^l = e$ a $0 \leq l < n$. Ak by platilo $l > 0$, dostali by sme spor s tým, že n je najmenšie číslo s touto vlastnosťou. Preto musí platiť $l = 0$. Keďže $m - k$ má nulový zvyšok po delení číslom n, je to násobok čísla n.
$\boxed{\Leftarrow}$ Ak $m - k = cn$, t.j. $m = k + cn$, tak $a^m = a^{k+cn} = a^k(a^n)^c = a^k e^c = a^k e = a^k$.
Dôkaz prípadu, keď rád a je ∞, je veľmi podobný, snáď len s tým rozdielom, že implikácia $\boxed{\Leftarrow}$ je v tomto prípade zrejmá. Dokážme teda netriviálny smer.
$\boxed{\Rightarrow}$ Bez ujmy na všeobecnosti môžeme predpokladať $m \geq k$. Ak $a^m = a^k$, tak $a^{m-k} = e$. Pretože rád a je ∞, neexistuje číslo $n > 0$ také, že $a^n = e$. To znamená, že $m - k = 0$ a $m = k$. □

Veta 2.4.11. *Nech G je cyklická grupa a a je jej generátor. Ak rád prvku a je $n \in \mathbb{N}$, tak $G \cong (\mathbb{Z}_n, \oplus)$. Ak rád prvku a je ∞, tak $G \cong (\mathbb{Z}, +)$. (Teda každá cyklická grupa je izomorfná so $\mathbb{Z}$ alebo so $\mathbb{Z}_n$).*

Dôkaz. Najprv nech rád generátora a je rovný n. Definujme zobrazenie $f\colon k \mapsto a^k$, $f\colon \mathbb{Z}_n \to G$. Ukážeme, že f je izomorfizmus. Z lemy 2.4.2 máme

$$a^{k+l} = a^k a^l.$$

Súčasne, z lemy 2.4.10, máme

$$a^{k+l} = a^{k \oplus l}$$

pretože čísla $k + l$ a $k \oplus l$ sa líšia o nejaký násobok čísla n.

Ďalej ukážeme, že zobrazenie f je bijektívne.

Surjektívnosť: Keďže a je generátor grupy G, každý prvok tejto grupy má tvar a^s pre nejaké s (veta 2.4.9). Ak s' je zvyšok čísla s po delení číslom n, tak $s' \in \mathbb{Z}_n$ a navyše $n \mid s - s'$, takže (podľa predchádzajúcej lemy) $a^s = a^{s'} = f(s')$.

Injektívnosť: Ak $f(s) = f(t)$, čiže $a^s = a^t$, máme $n \mid s - t$. Ak $s, t \in \{0, 1, \ldots, n-1\}$, tak $s - t \in \{0, \pm 1, \ldots, \pm(n-1)\}$. Jediné číslo z tejto množiny, ktoré je deliteľné n, je 0, a teda $s - t = 0$ a $s = t$.

Zostáva nám ešte ukázať druhý prípad, t.j. rád a je ∞. (Dôkaz v tomto prípade je veľmi podobný.) Definujeme $f\colon \mathbb{Z} \to G$ ako $f(n) = a^n$.

Homomorfizmus:

$$f(k + l) = a^{k+l} = a^k a^l = f(k)f(l)$$

podľa lemy 2.4.2.

Surjektívnosť: Každý prvok z G je tvaru $a^n = f(n)$ pre nejaké $n \in \mathbb{Z}$ podľa vety 2.4.9.

Injektívnosť: Druhá časť lemy 2.4.10. □

Špeciálne z predchádzajúcej vety vidíme, že každá netriviálna grupa musí obsahovať podgrupu homeomorfnú so $(\mathbb{Z}, +)$ alebo s niektorým $(\mathbb{Z}_n, \oplus)$. Takisto si môžeme všimnúť, že rád prvku je presne počet prvkov podgrupy generovanej týmto prvkom.

Ešte sa skúsme zaoberať otázkou, či z cyklickej grupy dostaneme opäť cyklickú grupu pomocou niektorých základných operácií – podgrupa, homomorfný obraz, priamy súčin grúp (definícia 2.1.5).

Veta 2.4.12. *Každá podgrupa cyklickej grupy je cyklická.*

Dôkaz. Nech G je cyklická grupa s generátorom a a H je nejaká jej podgrupa. Nech d je najmenšie prirodzené číslo také, že $d > 0$ a $a^d \in H$. (Ak $H \neq \{e\}$, tak existuje aspoň jedno také číslo.) Dokážeme, že a^d generuje H (a teda H je cyklická).

Najprv si uvedomme, aké prvky patria do podgrupy $[a^d]$ generovanej prvkom a^d. Podľa vety 2.4.9 sú to presne prvky tvaru $(a^d)^k = a^{kd}$ pre $k \in \mathbb{Z}$, čiže tie mocniny generátora a, pre ktoré je exponent násobkom d.

Postupujme sporom. Nech by existoval prvok $a^s \in H$ taký, že. $a^s \notin [a^d]$. Číslo s môžeme prepísať ako $s = k.d + s'$, kde $0 \leq s' < d$ (číslo s sme vydelili číslom d, zvyšok sme označili s'). Ak predpokladáme, že $a^s \notin [a^d]$, tak $s' \neq 0$. (V opačnom prípade by totiž platilo $a^s = a^{kd}$ a už sme ukázali, že prvky takéhoto tvaru patria do $[a^d]$.) Z rovnosti $a^s = a^{kd}a^{s'}$ dostaneme

$$a^{s'} = (a^{kd})^{-1}a^s,$$

a pretože $a^{kd}, a^s \in H$ a H je podgrupa, z tejto rovnosti vyplýva $a^{s'} \in H$. Pretože $0 < s' < d$, dostávame tak spor s predpokladom, že d je najmenší možný exponent taký, že $a^d \in H$. □

Veta 2.4.13. *Homomorfný obraz cyklickej grupy je cyklická grupa.*

Dôkaz. Ak $f\colon G \to H$ je epimorfizmus a a je generátor G, tak ľahko možno vidieť, že $f(a)$ je generátor grupy H.

Skutočne, každý prvok z H je tvaru $f(a^n)$ pre nejaké $n \in \mathbb{Z}$ (na základ surjektívnosti f) a podľa (2.2) platí $f(a^n) = f(a^n)$, čiže ho vieme dostať ako mocninu prvku $f(a)$. □

Na vyriešenie otázky, kedy je súčin cyklických grúp opäť cyklická grupa, budeme potrebovať pomocné tvrdenie týkajúce sa najväčšieho spoločného deliteľa. Nebudeme ho na tomto mieste dokazovať, keďže neskôr dokážeme všeobecnejšiu verziu tohoto výsledku – konkrétne v tvrdení 4.4.22. Ak by Vás zaujímal jeho dôkaz už teraz, môžete si ho pozrieť napríklad v [ŠHHK, Lema 3.1.3], [Č], [S] (a v podstate v takmer každom úvodnom texte zaoberajúcom sa deliteľnosťou). Najprv však pripomeňme definíciu najväčšieho spoločného deliteľa.

Definícia 2.4.14. Najväčší spoločný deliteľ čísel $a, b \in \mathbb{Z}$ je číslo $d \in \mathbb{N} \setminus \{0\}$ s vlastnosťami

(i) $d \mid a \wedge d \mid b$ (čiže d delí obe čísla);

(ii) ak $c \mid a$ a $c \mid b$, tak $c \leq d$ (čiže d je najväčšie číslo s uvedenou vlastnosťou).

Tvrdenie 2.4.15. *Ak $d = (m, n)$ je najväčší spoločný deliteľ dvoch čísel $m, n \in \mathbb{N}$ tak existujú také $u, v \in \mathbb{Z}$, že platí $um + vn = d$.*

Napríklad pre čísla 3 a 7 máme $(3, 7) = 1$ a skutočne platí $(-2).3 + 1.7 = 1$.

Veta 2.4.16. *Grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ je cyklická práve vtedy, keď m a n sú nesúdeliteľné, t.j. ich najväčší spoločný deliteľ $(m, n) = 1$. V taktomto prípade je prvok $(1, 1)$ jej generátorom.*

Dôkaz. $\boxed{\Rightarrow}$ Najprv ukážeme, že ak $\mathbb{Z}_m \times \mathbb{Z}_n$ je cyklická grupa, tak dvojica $(1, 1)$ je jej generátorom. Nech (g_1, g_2) je ľubovoľný generátor. Zrejme potom g_1 je generátor $\mathbb{Z}_m$ a g_2 je generátor $\mathbb{Z}_n$. Potom priradenie $g \mapsto 1$ jednoznačne určuje homomorfizmus $f_1\colon \mathbb{Z}_m \to \mathbb{Z}_m$ a priradenie $g_2 \mapsto 1$ nám dáva homomorfizmus $f_2\colon \mathbb{Z}_n \to \mathbb{Z}_n$. Potom $f\colon \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n$ je tiež homomorfizmus (úloha 2.3.7). Platí $f(g_1, g_2) = (1, 1)$, čiže $(1, 1)$ je generátor.

Ak $d = (m, n) > 1$, tak podgrupa $[(1, 1)]$ generovaná dvojicou $(1, 1)$ neobsahuje dvojicu $(1, 0)$. Skutočne, ak by platilo pre nejaké $k \in \mathbb{Z}$ v tejto grupe $k \times (1, 1) = (1, 0)$, znamenalo by to, že v celých číslach platia rovnosti

$$k = am + 1$$
$$k = bn$$

z čoho $bn - am = 1$. Pritom však d delí obe čísla m aj n, teda $d \mid bn - am = 1$, čo je spor. (Jediné celočíselné delitele čísla 1 sú ± 1, my sme predpokladali $d > 1$.)

$\boxed{\Leftarrow}$ Očividne $[(1, 0), (0, 1)] = \mathbb{Z}_m \times \mathbb{Z}_n$, stačí teda ukázať, že pomocou $(1, 1)$ vieme vygenerovať dvojice $(1, 0)$ a $(0, 1)$. Ak $am + bn = 1$, tak v grupe $\mathbb{Z}_m \times \mathbb{Z}_n$ platia rovnosti (zapísané aditívne)

$$am \times (1, 1) = (0, 1)$$
$$bn \times (1, 1) = (1, 0)$$

□

V príklade 2.2.17 sme videli, že grupa $\mathbb{Z}_2 \times \mathbb{Z}_3$ je skutočne generovaná prvkom $(1, 1)$.

Cvičenia

Úloha 2.4.1. Nech $f\colon (G,*) \to (H,\circ)$ je homomorfizmus. Dokážte, že potom platí:
a) $f(a^n) = f(a)^n$
b) $a^n = e_G \Rightarrow f(a)^n = e_H$
c) Ak f je navyše izomorfizmus, tak $a^n = e_G \Rightarrow f(a)^n = e_H$.
d) Izomorfizmus zachováva rád prvku, t.j. rád prvku a v grupe G je rovnaký ako rád prvku $f(a)$ v grupe H.

Úloha 2.4.2. Nech $(G,*)$ je cyklická grupa a a je jej generátor. Potom ľubovoľný homomorfizmus z G do nejakej grupy $(H,\circ)$ je jednoznačne určený obrazom prvku a.

Úloha 2.4.3. Nájdite všetky izomorfizmy medzi $(\mathbb{Z}_4,\oplus)$ a $(\mathbb{Z}_5 \setminus \{0\},\odot)$.

Úloha 2.4.4. Ukážte, že ak G je konečná grupa, tak každý jej prvok má konečný rád.

Úloha 2.4.5. Nájdite všetky homomorfizmy:
a) zo $\mathbb{Z}_4$ do $\mathbb{Z}_2 \times \mathbb{Z}_2$,
b) zo $\mathbb{Z}_2 \times \mathbb{Z}_2$ do $\mathbb{Z}_4$,

Úloha 2.4.6. Zistite, či sú grupy G a H izomorfné. Svoju odpoveď zdôvodnite!
a) $G = (\mathbb{Z}_7 \setminus \{0\},\odot)$, $H = (\mathbb{Z}_6,\oplus)$
b) $G = (\mathbb{Z},+)$, $H = (\mathbb{Q},+)$
c) $G = (\mathbb{Z}_6,\oplus)$, $(\mathbb{Z}_2,\oplus) \times (\mathbb{Z}_3,\oplus)$

Úloha 2.4.7. V každej grupe majú nasledujúce prvky rovnaký rád: x a yxy^{-1}; ab a ba; abc, bca a cab. Naopak, prvky abc a cba môžu mať rôzny rád. (Hint: Jedna z možností ako dokázať, že dva prvky $g,h \in G$ majú rovnaký rád je dokázať ekvivalenciu $x^n = e \Leftrightarrow y^n = e$. Iná možnosť je nájsť izomorfizmus $f\colon G \to G$ taký, že $f(g) = h$, a použiť úlohu 2.4.1a).)

Úloha 2.4.8. Nech $a,b \in G$, kde G je grupa, $a,b \neq e$ také, že $ab = ba$ a $b^3 = 1$. Dokážte, že $\{a^n, ba^n, b^2a^n; n \in \mathbb{Z}\}$ je podgrupa grupy G.

Úloha 2.4.9. Nech $n \in \mathbb{N} \setminus \{0\}$. Pre každé $k \mid n$ existuje k-prvková podgrupa grupy $(\mathbb{Z}_n,\oplus)$.

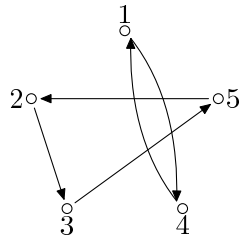
Úloha 2.4.10. Ak rád prvku a v grupe G je n a e je neutrálny prvok tejto grupy, tak pre prirodzené čísla $k \in \mathbb{N}$ platí $a^k = e$ práve vtedy, keď $n \mid k$. Ďalej pre každé $s \in \mathbb{N}$ existuje $m \in \mathbb{N}$ také, že $a^s = a^m$ a $0 \leq m \leq n-1$.

Úloha 2.4.11. Nech x je prvok rádu n. Potom:
a) Rád prvku x^m delí n.
b*) Rád prvku x^m je $\frac{n}{(m,n)}$, kde (m,n) označuje najväčší spoločný deliteľ čísel m a n. (Hint: Tvrdenie 2.4.15.)

Úloha 2.4.12. Ak $f\colon G \to H$ je homomorfizmus grúp a $g \in G$ je prvok konečného rádu, tak rád prvku $f(g)$ delí rád prvku G.

Úloha 2.4.13. Nech G je grupa regulárnych matíc typu 2×2 nad $\mathbb{R}$ s násobením a $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$. Dokážte, že A má rád 4, B má rád 3, ale AB má rád ∞.

Úloha 2.4.14. Nech x a y sú prvky konečného rádu grupy G a nech $xy = yx$. Dokážte, že ak $[x] \cap [y] = \{e\}$, čiže prienik podgrúp generovaných týmito prvkami je triviálna podgrupa, tak rád prvku xy je najmenší spoločný násobok rádov prvkov x a y. Platia tieto tvrdenia aj ak x a y nekomutujú?



Obr. 2.1: Príklad permutácie 5-prvkovej množiny. Vidíme, že z každého prvku vychádza aj do každého prvku vchádza práve jedna šípka.

Úloha 2.4.15*. Nech x a y sú prvky konečného rádu grupy G a nech $xy = yx$. Dokážte, že ak ich rády k a l sú nesúdeliteľné, tak rád prvku xy je kl. Dokážte, že existujú exponenty m a n, také, že rád prvku $x^m y^n$ je rovný $[k, l]$ (najmenší spoločný násobok rádov). Platia tieto tvrdenia aj ak x a y nekomutujú? (Hint: V tomto priklade môže byť užitočné tvrdenie 2.4.15.)

2.5 Permutácie

S permutáciami sme sa už stretli pri definícii determinantu (kapitola I-6).

Z minuléhoho semestra už vieme, že pod *permutáciou* konečnej[4] množiny M rozumieme bijekciu z M od M. Tiež sme sa dohodli na označení permutácií množiny $\{1, \ldots, n\}$ pomocou zápisu

$$\left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ \varphi(1) & \varphi(2) & \cdots & \varphi(n) \end{smallmatrix}\right),$$

Napríklad permutáciu znázornenú na obrázku 2.1 by sme zapísali ako

$$\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{smallmatrix}\right)$$

Tiež vieme, že zloženie permutácií je permutácia a inverzné zobrazenie k danej permutácii je permutácia. Pomocou týchto faktov vieme ukázať, že permutácie danej konečnej množiny tvoria grupu. Množinu všetkých permutácií n-prvkovej množiny $\{1, 2, \ldots, n\}$ budeme označovať S_n a nazývať *symetrická grupa.*

V tejto časti sa budeme zaoberať o niečo podrobnejšie grupou S_n všetkých permutácií n-prvkovej množiny a niektorými jej podgrupami. Začneme tým, že si povieme o rozklade permutácie na jednoduchšie permutácie (budeme ich volať cykly), ktorý nám (okrem iného) umožní vyrátať rád ľubovoľného prvku v grupe S_n.

2.5.1 Rozklad na súčin disjunktných cyklov

Ak sa pozrieme na permutáciu na obrázku 2.1 vidíme, že na tomto obrázku sa po jednotlivých šípkach z prvku 1 dostaneme do prvku 4 a potom naspäť znovu do prvku 1. Podobne z prvku 2 sa dostaneme do 3 a 5 a potom opäť do 2.

Toto musí platiť pre ľubovoľnú permutáciu. Ak začneme s ľubovoľným prvkom, opakovaným aplikovaním tej istej permutácie po konečnom počte krokov dostaneme znovu ten istý

[4]Názov permutácia sa niekedy vyskytuje aj ako pomenovanie bijekcie nekonečnej množiny na seba. My sa budeme držať terminológie, ktorú sme zaviedli už v minulom semestri – t.j. pri permutáciach automaticky predpokladáme, že ide o konečnú množinu.

prvok. Dôvodom je, že máme len konečný počet prvkov – teda po istom čase sa niektorý prvok zopakuje. Ak by to bol iný prvok, ako ten z ktorého sme začali, dané zobrazenie by nebola bijekcia. (Podrobnejšie tento argument vysvetlíme v dôkaze tvrdenia 2.5.7.) Vďaka tomu môžeme každú permutáciu rozdeliť na cykly.

Celá táto časť je venovaná spôsobu ako môžeme práve uvedený jednoduchý fakt formálne zapísať a dokázať. Tiež si povieme, prečo je tento poznatok užitočný.

Najprv potrebujeme zaviesť pojem cyklu.

Definícia 2.5.1. Permutáciu φ konečnej množiny M nazveme *cyklus,* alebo *cyklická permutácia* ak existujú prvky $a_1, a_2, \ldots, a_k$ také, že

$$\begin{cases} \varphi(a_i) = a_{i+1} \text{ pre } i = 1, 2, \ldots, k-1, \\ \varphi(a_k) = a_1, \\ \varphi(a) = a \text{ pre ostatné prvky } a \neq a_i. \end{cases}$$

Pre cyklus tohoto tvaru budeme používať zápis $(a_1 a_2 \ldots a_k)$.

V definícii cyklu pripúšťame aj nulový počet prvkov. *Prázdny cyklus,* ktorý označujeme $()$, sa rovná identickej permutácii.

Všimnime si, že zápis pomocou cyklov môžeme použiť pre ľubovoľnú množinu. Tento zápis však neidentifikuje množinu, ktorej permutáciu robíme – tá musí byť zadaná zvlášť.

Príklad 2.5.2. Uvažujme permutácie množiny $\{1, 2, 3, 4, 5\}$

Zápis $\varphi = (14)$ označuje permutáciu s vlastnosťou $\varphi(1) = 4$ a $\varphi(4) = 1$, ktorá prvky 2, 3 a 5 nemení (teda $\varphi(2) = 2$, $\varphi(3) = 3$, $\varphi(5) = 5$).

Zápis $\tau = (235)$ znamená permutáciu určenú predpisom $\tau(1) = 1$, $\tau(2) = 3$, $\tau(3) = 5$, $\tau(4) = 4$, $\tau(5) = 2$.

Všimnime si, že ten istý cyklus môže byť zapísaný viacerými spôsobmi: $\tau = (235) = (352) = (523)$.

Príklad 2.5.3. Vieme, že inverzné zobrazenie k permutácii je tiež permutácia. Ak máme cyklus $\varphi = (a_1 a_2 \ldots a_n)$, tak inverzná permutácia je tiež cyklus $\varphi^{-1} = (a_n a_{n-1} \ldots a_1)$. Zodpovedá to tomu, že poprechádzame po tých istých šípkach tvoriacich cyklus, ale v opačnom poradí.

Pre cykly z predchádzajúceho príkladu máme $\varphi^{-1} = (14)$ a $\tau^{-1} = (253)$.

Definícia 2.5.4. Dve permutácie φ a τ tej istej množiny M nazveme *disjunktné,* ak pre každý prvok $a \in M$ platí $\varphi(a) = a$ alebo $\tau(a) = a$. (Teda každý prvok zostáva nezmenený pri aspoň jednej z týchto dvoch permutácií.)

Špeciálne, dva cykly $(a_1 a_2 \ldots a_k)$ a $(b_1 b_2 \ldots b_l)$ sú disjunktné, ak platí rovnosť $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_l\} = \emptyset$.

Nasledujúca lema hovorí, že poradie disjunktných permutácií môžeme pri skladaní vymeniť – disjunktné permutácie komutujú.

Lema 2.5.5. *Ak φ a τ sú disjunktné permutácie, tak*

$$\varphi \circ \tau = \tau \circ \varphi.$$

Dôkaz. Stačí priamym výpočtom overiť, že permutácia na ľavej aj pravej strane rovnosti nadobúda rovnaké hodnoty; čiže $\tau(\varphi(m)) = \varphi(\tau(m))$.

Dokážme túto rovnosť najprv pre prípad, že $\varphi(m) \neq m$. Potom z injektívnosti zobrazenia φ máme $\varphi(\varphi(m)) \neq \varphi(m)$. Pretože φ a τ sú disjunktné, permutácia τ nemení prvky m ani $\varphi(m)$, teda $\tau(m) = m$ a $\tau(\varphi(m)) = \varphi(m)$. Použitím týchto rovností dostaneme

$$\tau(\varphi(m)) = \varphi(m) = \varphi(\tau(m)).$$

Prípad $\tau(m) \neq m$ je symetrický.

Zostáva už len možnosť $\tau(m) = \varphi(m) = m$, vtedy však na oboch stranách rovnosti dostaneme m:

$$\tau(\varphi(m)) = \varphi(\tau(m)).$$

□

Príklad 2.5.6. Ľahko si môžeme všimnúť, že pre permutácie, ktoré nie sú disjunktné, predchádzajúce tvrdenie neplatí. Zoberme napríklad cykly $\varphi = (12)$ a $\tau = (135)$. Potom dostaneme

$$\varphi \circ \tau = (1352) \qquad \text{a} \qquad \tau \circ \varphi = (1235).$$

Tvrdenie 2.5.7. *Každú permutáciu možno zapísať ako zloženie disjunktných cyklov. Tento zápis je jednoznačný až na poradie cyklov (a vynechanie prázdneho cyklu). Nazývame ho* rozklad permutácie na súčin disjunktných cyklov.

Dôkaz. Uvažujme ľubovoľnú permutáciu φ množiny M.

Existenciu rozkladu permutácie φ na súčin disjunktných dokážeme indukciou vzhľadom na počet prvkov množiny M. Pre jednoprvkovú množinu máme jedinú možnú permutáciu id_M, ktorá sa rovná prázdnemu cyklu.

Predpokladajme teraz, že M má n prvkov a pre ľubovoľnú množinu s menej ako n prvkami tvrdenie platí. Zoberme teraz ľubovoľný prvok $a \in M$. Položme $a_1 = a$, $a_{i+1} = \varphi(a^i)$ pre všetky $i = 1, 2, \ldots$. Nech k je najmenšie číslo také, že $k \geq 1$ a $a_{k+1} = a$. Ukážeme najprv, že také číslo musí existovať.

Pretože množina M je konečná, musia sa niektoré prvky v postupnosti (a_k) opakovať, t.j. existujú nejaké čísla s vlastnosťou $a_s = a_t$ a $s \neq t$. Tvrdíme, že ak s je najmenšie množné takéto číslo, tak $s = 1$. Skutočne, v opačnom prípade máme $\varphi(a_{s-1}) = \varphi(a_{t-1})$ a z injektívnosti zobrazenia φ dostaneme $a_{s-1} = a_{t-1}$.

Zistili sme, že existuje aspoň jedno číslo s horeuvedenými vlastnosťami, preto môžeme definovať k ako najmenšie číslo, ktoré má tieto vlastnosti. Pomocou neho definujeme cyklus

$$\tau = (a_1 a_2 \ldots a_k).$$

Položme ďalej $\psi = \tau^{-1}\varphi$. Ukážeme, že permutácie ψ a τ sú disjunktné a že $\psi(a) = a$.

Skutočne, pre ľubovoľný z prvkov $a_1, a_2, \ldots, a_{k-1}$ platí $\varphi(a_i) = a_{i+1}$ a $\tau^{-1}(a_{i+1}) = a_i$, teda $\psi(a_i) = \tau^{-1}(\varphi(a_i)) = a_i$. Podobne môžeme overiť, že $\psi(a_k)\tau^{-1}(\varphi(a_k)) = \tau^{-1}(a_1) = a_k$. Vidíme, že permutácia ψ nemení žiadny z prvkov, ktoré mení cyklus τ teda tieto permutácie sú disjunktné. Špeciálne, ψ nemení prvok $a_1 = a$.

Teraz si stačí uvedomiť, že ψ (resp. zúženie tohoto zobrazenia) môžeme chápať ako permutáciu množiny $M \setminus \{a_1, \ldots, a_k\}$, ktorá má menej prvkov ako množina M. Podľa indukčného predpokladu teda existuje rozklad $\psi = \tau_1\tau_2 \ldots \tau_l$ tejto permutácie na disjunktné cykly. Potom

$$\varphi = \tau(\tau^{-1}\varphi) = \tau\psi = \tau\tau_1 \ldots \tau_l$$

je rozklad permutácie φ na disjunktné cykly.

Jednoznačnosť. Predpokladajme, že máme 2 rozklady

$$\varphi_1 \ldots \varphi_s = \psi_1 \ldots \psi_t$$

tej istej permutácie na disjunktné cykly, pričom v rozkladoch sa nevyskytuje prázdny cyklus. Postupujme indukciou vzhľadom na s.

Ak $s = 0$, teda na ľavej strane rovnosti je identita, musí byť aj počet disjunktných cyklov na pravej strane nulový. V opačnom prípade by sme mali na pravej strane aspoň jeden neprázdny cyklus, teda permutácia na pravej strane by menila aspoň jeden prvok, čiže permutácia na pravej strane by nebola identita.

Predpokladajme teraz, že $s > 0$, čiže daná permutácia nie je identita. Nech a je nejaký prvok, ktorý táto permutácia mení. Tento prvok sa musí vyskytovať v aspoň jednom z cyklov, súčasne z disjunktnosti vyplýva, že sa nemôže vyskytovať vo viacerých cyklov. Teda prvok a sa vyskytuje práve v jednom z cyklov vystupujúcich na ľavej strane rovnosti, podobne v práve jednom z cyklov na pravej strane. Bez ujmy na všeobecnosti (cykly môžeme poprehadzovať) predpokladajme, že sú to cykly φ_1 a τ_1. Potom dostaneme $\varphi_1(a) = \varphi(a) = \tau_1(a)$, podobne $\varphi_1^2(a) = \varphi^2(a) = \tau_1^2(a)$ atď. Čiže všetky prvky vyskytujúce sa v cykle φ_1 sa zobrazia rovnako aj cyklom τ_1 a obrátene. Platí teda $\varphi_1 = \tau_1$. Z toho dostaneme rovnosť $\varphi_2 \dots \varphi_s = \psi_2 \dots \psi_t$. Pre tieto cykly už môžeme použiť indukčný predpoklad. □

Príklad 2.5.8. Pre permutáciu $\varphi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{smallmatrix}\right)$ (obrázok 2.1) dostaneme rozklad $\varphi = (14)(235)$.
Z toho vieme hneď zistiť aj $\varphi^{-1} = (14)(253)$.

Rozklad na súčin disjunktných cyklov môže byť užitočný pri výpočte rádu permutácie (v zmysle rádu prvku grupy všetkých permutácií danej množiny).

Definícia 2.5.9. Ak φ je permutácia konečnej množiny M, tak *rád permutácie* φ je najmenšie prirozdené číslo $n \geq 1$ také, že

$$\varphi^n = id_M.$$

Napríklad v príklade I-2.3.2 sme zistili, že rád permutácie $\varphi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{smallmatrix}\right)$ je 3. (Všimnime si, že ide o cyklickú permutáciu.)

Lema 2.5.10. *Rád cyklu je rovný jeho dĺžke, t.j. ak $\varphi = (a_1 \dots a_n)$, tak rád φ je rovný n.*

Dôkaz. Pre $k = 1, 2, \dots, n-1$ je $\varphi^k(a_1) = a_k \neq a_1$. Až pre $k = n$ prvýkrát dostaneme $\varphi^k(a_1) = a_1$. Úplne rovnaké zdôvodnenie prejde aj pre ostatné prvky cyklu, čiže máme $\varphi^n = id$ a navyše n je najmenšie číslo z množiny $\{1, 2, 3, \dots\}$ s touto vlastnosťou. □

Z predchádzajúcej lemy vidíme, že ak n je rád cyklu φ, tak $\varphi^k = id_M$ platí práve vtedy, keď k je násobkom n, t.j. $n \mid k$.

Veta 2.5.11. *Rád permutácie je najmenší spoločný násobok dĺžok disjunktných cyklov, ktoré vystupujú v jej rozklade.*

Dôkaz. Nech $\varphi = \tau_1 \dots \tau_m$ je rozklad permutácie na φ na disjunktné cykly. Pretože disjunktné cykly komutujú, mocniny permutácie φ môžeme vyjadriť ako

$$\varphi^n = \tau_1^n \dots \tau_m^n.$$

Pritom permutácie $\tau_1^n, \dots, \tau_m^n$ sú opäť disjunktné. Z toho vyplýva, že aby sme dostali identické zobrazenie, musí pre každé $i = 1, 2, \dots, m$ platiť $\tau_i^n = id_M$. To nastane práve vtedy, keď n je násobkom rádu τ_i (pre všetky i). Teda najmenšie možné n s takouto vlastnosťou je najmenší spoločný násobok rádov jednotlivých disjunktných cyklov. Podľa lemy 2.5.10 sú to presne dĺžky jednotlivých cyklov. □

Príklad 2.5.12. Vypočítajme rád permutácie $\varphi = \left(\begin{smallmatrix}1&2&3&4&5\\4&3&5&1&2\end{smallmatrix}\right) = (14)(235)$. Podľa predchádzajúcej vety by to mal byť najmenší spoločný násobok čísel 2 a 3, čiže 6.

Keď sa to pokúsime overiť na základe definície, dospejeme k tomu istému výsledku:
$\varphi^2 = (253)$,
$\varphi^3 = (14)$,
$\varphi^4 = (235)$,
$\varphi^5 = (14)(253)$,
$\varphi^6 = id$.

2.5.2 Parita permutácie

S pojmom inverzie sme sa už stretli pri definícii determinantu. Teraz ho použijeme na zadefinovanie pojmu párnej a nepárnej permutácie.

Definícia 2.5.13. Dvojica $(\varphi(k), \varphi(s))$ sa volá *inverzia* permutácie φ, ak $k < s$ ale $\varphi(k) > \varphi(s)$.

Ak má permutácia φ párny počet inverzií, hovoríme, že je to *párna permutácia,* v opačnom prípade hovoríme o *nepárnej permutácii.*

Príklad 2.5.14. Permutácia $\varphi = \left(\begin{smallmatrix}1&2&3&4&5\\4&3&5&1&2\end{smallmatrix}\right)$ má 7 inverzií: (4,3), (4,1), (4,2), (3,1), (3,2), (5,1) a (5,2). Teda táto permutácia je nepárna.

Na dôkaz niektorých vlastností parity permutácií sa nám budú hodiť cykly dĺžky dva.

Definícia 2.5.15. Permutáciu tvaru (a_1a_2) (t.j. dvojprvkový cyklus) budeme nazývať *transpozícia.*

Príklad 2.5.16. Ukážeme, že transpozícia je nepárna permutácia. Bez ujmy na všeobecnosti, nech $a_1 < a_2$. Nech $\varphi = (a_1a_2)$, t.j. $\varphi(a_1) = a_2$, $\varphi(a_2) = a_1$ a $\varphi(a) = a$ pre $a \neq a_1, a_2$. Potom všetky inverzie permutácie φ sú $(a_2 = \varphi(a_1), i)$ a $(i, a_1 = \varphi(a_2))$ pre $a_1 < i < a_2$ (týchto je párny počet) a inverzia (a_2, a_1).

Tvrdenie 2.5.17. *Každú permutáciu možno zapísať ako zloženie transpozícií. Navyše, pri každom takomto zápise je parita počtu transpozícií rovná parite permutácie.* (*Teda permutácia je párna práve vtedy, keď ju je možné získať zložením párneho počtu transpozícií. Permutácia je nepárna práve vtedy, keď sa dá dostať zložením nepárneho počtu transpozícií.*)

Dôkaz. Na dôkaz prvej časti stačí ukázať, že každý cyklus sa dá rozložiť na transpozície (pretože podľa tvrdenia 2.5.7 sa dá každá permutácia rozložiť na cykly). Jedna z možností, ako rozložiť cyklus dĺžky $n \geq 2$ na transpozície je

$$(a_1a_2 \dots a_n) = (a_1a_n)(a_1a_{n-1}) \dots (a_1a_2).$$

Na dôkaz druhej časti si stačí uvedomiť dve skutočnosti. Prvou z nich je, že transpozícia je nepárna permutácia – pozri príklad 2.5.16 Keď ďalej dokážeme, že pri zložení ľubovoľnej permutácie s nejakou transpozíciou sa zmení parita, dôkaz je hotový.

Majme teda ľubovoľnú permutáciu φ a uvažujme transpozíciu $\tau = (ij)$, pričom $i < j$. Potom

$$\psi = \varphi \circ \tau = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ \varphi(1) & \dots & \varphi(i) & \dots & \varphi(j) & \dots & \varphi(n) \end{pmatrix} (ij) = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ \varphi(1) & \dots & \varphi(j) & \dots & \varphi(i) & \dots & \varphi(n) \end{pmatrix}.$$

(Predchádzajúcim zápisom sa myslí to, že jediné miesta, na ktorých sa ψ a φ líšia, sú i-te a j-te miesto, t.j. líšia sa len obrazy prvkov i a j. Preto sme vyznačili iba tieto prvky a okrem nich prvý a posledný prvok a ich obrazy.)

Pokúsme sa zistiť, ako sa líši počet inverzií permutácií φ a ψ. Zrejme jediné inverzie, ktoré sme mohli ovplyvniť, sú tie, ktoré obsahovali prvky i a j.

Je zrejmé, že ak $(\varphi(i), \varphi(j))$ je inverzia, t.j. ak $i < j$, tak dvojica $(\psi(i), \psi(j))$ už inverziu netvorí. Takisto obrátene, ak tieto dva prvky netvoria inverziu permutácie φ, dostaneme z nich inverziu v ψ.

Skúsme nájsť ešte aj ostatné inverzie, ktoré mohli „vzniknúť“ alebo „zaniknúť“.

Inverzie, ktoré sa ešte mohli zmeniť môžu byť jedine také, že jeden prvok z dvojice, ktorá je „zanikajúcou“ alebo „vznikajúcou“ inverziou je buď $\varphi(i)$ alebo $\varphi(j)$ a druhý prvok je $\varphi(k)$ pre niektoré $i < k < j$.

Navyše, charakter každej takejto dvojice sa zmení na opačný. T.j. ak $(\varphi(i), \varphi(k))$ je inverzia φ, tak $(\varphi(k), \varphi(i)) = (\psi(k), \psi(j))$ už nie je inverzia. A takisto obrátene, ak táto dvojica pôvodne netvorila inverziu, v permutácii ψ ju už určite tvorí. Takých dvojíc je práve $j - i - 1$.

Podobná úvaha však samozrejme platí aj keď zoberieme j namiesto i.

Celkove sme teda zistili, že pri zložení s transpozíciou (ij) sa zmení počet inverzií o ± 1 pre $2(j - i - 1) + 1$ dvojíc, čo je nepárne číslo. Teda parita permutácie sa musí zmeniť. □

Všimnime si, že v dôkaze predchádzajúceho tvrdenia sme okrem iného ukázali aj to, že cyklus párnej dĺžky je nepárna permutácia a obrátene cyklus nepárnej dĺžky je párna permutácia. (Pretože cyklus dĺžky n sme rozložili na $n + 1$ transpozícií.)

Dôsledok 2.5.18. *Zložením dvoch permutácií rovnakej parity dostaneme párnu permutáciu. Zložením párnej a nepárnej permutácie dostaneme nepárnu permutáciu.*

Príklad 2.5.19. Uvažujeme permutáciu z predchádzajúceho príkladu a pozrime sa na jej rozklad na disjunktné cykly.

$$\varphi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{smallmatrix}\right) = (14)(235).$$

Je zložená z 2 cyklov, jeden z nich je párnej dĺžky, teda je to nepárna permutácia. Druhý z nich má nepárnu dĺžku, čiže ide o párnu permutáciu. Permutácia φ je teda zložením párnej a nepárnej permutácie, preto φ je nepárna permutácia.

Dôsledok 2.5.20. *Párne permutácie tvoria podgrupu grupy S_n. Grupu tvorenú párnymi permutáciami množiny $\{1, 2, \ldots, n\}$ budeme označovať A_n a nazývať* alternujúca grupa.

Dôkaz. Zrejme $id \in A_n$, preto $A_n \neq \emptyset$. Podľa predchádzajúceho dôsledku je táto množina uzavretá na skladanie. Zostáva dokázať uzavretosť na inverzné prvky.

Ak permutácia φ patrí do A_n, tak sa dá rozložiť na párny počet transpozícií $\varphi = \tau_1 \tau_2 \ldots \tau_{2k}$. Pretože pre ľubovoľnú transpozíciu τ platí $\tau^{-1} = \tau$, máme

$$\varphi^{-1} = \tau_{2k} \tau_{2k-1} \ldots \tau_1,$$

čiže aj φ^{-1} je párna permutácia. □

V oblasti zábavnej matematiky sa tiež môžeme stretnúť s podgrupami S_n. Ako grupy permutácií možno chápať povolené transformácie Rubikovej kocky (pozri [KGGS, Kapitola 3.2]) alebo tiež „hra 15“ (pozri [KGGS, Cvičenia 3.6.9*, 3.6.10*]).

Cvičenia

Úloha 2.5.1. V tomto cvičení budeme pracovať s permutáciami množiny $\{1, 2, 3, 4, 5, 6, 7, 8\}$ (čiže prvkami grupy S_8) a budeme zadané permutácie aj výsledky vždy zapisovať ako súčiny disjunktných cyklov: Označme

$\varphi = (14)(235)(78)$
$\psi = (234)(67)$
$\tau = (135)(24)(68)$
a) Vypočítajte $(\varphi \circ \psi) \circ \tau$ a $\varphi \circ (\psi \circ \tau)$
b) Ku každej z uvedených permutácií vypočítajte inverznú permutáciu.
c) Zistite rád a paritu permutácií φ, ψ, τ a aj permutácií, ktoré sme dostali ako výsledky v predchádzajúcich častiach tejto úlohy.

Úloha 2.5.2. Pre dané permutácie určte rád, paritu, a rozklad na disjunktné cykly:
$\varphi = \left(\begin{smallmatrix}1&2&3&4&5\\2&3&4&5&1\end{smallmatrix}\right)$, $\tau = \left(\begin{smallmatrix}1&2&3&4&5\\2&1&4&5&3\end{smallmatrix}\right)$, $\psi = \left(\begin{smallmatrix}1&2&3&4&5\\3&2&1&5&4\end{smallmatrix}\right)$.
Ďalej vypočítajte permutácie $\varphi\tau\psi$, φ^{-1}, τ^{-1}, ψ^{-1}.

Úloha 2.5.3. Vypočítajte $\varphi \circ \psi$ a $\psi \circ \varphi$ pre:
a) $\varphi = (14)(5678)$, $\psi = (23)(5678)$
b) $\varphi = (124)(5678)$, $\psi = (23)(5678)$.
Je niektorý z týchto prípadov príkladom nedisjunktných permutácií, ktoré komutujú?

Úloha 2.5.4. V grupe $(S_7, \circ)$ nájdite rád a paritu permutácie $\varphi = (12)(14)(35)(26)(21)(67)$. Vypočítajte φ^{127}. Nájdite cyklickú podgrupu S_7 generovanú touto permutáciou. S ktorou grupou $(\mathbb{Z}_n, \oplus)$ je táto podgrupa izomorfná?

Úloha 2.5.5. Zostavte tabuľku grupovej operácie pre grupu S_3.

Úloha 2.5.6. Nájdite všetky podgrupy grupy S_3.

Úloha 2.5.7. Ak počet inverzií permutácie $\left(\begin{smallmatrix}1&2&\cdots&n\\a_1&a_2&\cdots&a_n\end{smallmatrix}\right)$ je k, zistite počet inverzií permutácie $\left(\begin{smallmatrix}1&2&\cdots&n\\a_n&a_{n-1}&\cdots&a_1\end{smallmatrix}\right)$.

Úloha 2.5.8. Dokážte, že grupa S_n je generovaná:
a) Množinou všetkých transpozícií.
b) Množinou transpozícií $\{(12), (13), \ldots, (1n)\}$.
c) Množinou transpozícií $\{(12), (23), \ldots, (n-1, n)\}$.
d) Transpozíciou (12) a cyklom $(12\ldots n)$. (Hint: Skúste vyrátať $(12\ldots n)^{-k}(12)(12\ldots n)^k$.)
Dokážte, že S_4 nie je generovaná pomocou (13) a (1234). (Teda S_4 síce je generovaná cyklom dĺžky 4 a transpozíciou, túto transpozíciu však nemôžem vybrať ľubovoľne.)

Úloha 2.5.9. Dokážte, že alternujúca grupa A_n je generovaná:
a) Množinou všetkých cyklov (ijk) dĺžky 3.
b) Množinou cyklov dĺžky 3 tvaru $(123), (124), \ldots, (12n)$.

Úloha 2.5.10. Popíšte permutácie z grupy S_n, ktoré majú rád 2. Aký je ich počet? (Stačí nájsť rekurzívny predpis pre počet takých prvkov.)

Úloha 2.5.11. Čomu sa rovná najväčší možný rád prvku grupy S_{12}.

2.6 Cayleyho veta

Ľahko vieme overiť že pre danú množinu M všetky bijekcie z M do M tvoria s operáciou skladania zobrazení grupu. (Dôkaz je presne rovnaký ako pre permutácie v prípade, že M bola konečná.) Túto grupu budeme označovať $(S(M), \circ)$ alebo stručnejšie $S(M)$.

Definícia 2.6.1. Pod *grupou transformácií množiny* M budeme rozumieť ľubovoľnú podgrupu grupy $(S(M), \circ)$.

Ekvivalentne by sme mohli grupu transformácií definovať tak, že je to množina bijekcií z M do M uzavretá na skladanie a inverzné zobrazenie. (V [KGGS] sa grupa transformácií definuje takto, pretože tento pojem je tu zavedený skôr než pojem grupy. Aj historické poradie, v akom matematici definovali tieto pojmy, je rovnaké.)

V tejto časti ukážeme Cayleyho vetu, ktorá hovorí, že každá grupa je izomorfná s nejakou grupou transformácií. To znamená, že keby sme sa zaoberali len grupami, v ktorých je binárnou operáciou skladanie zobrazení, v podstate by sme nič nestratili.

Definícia 2.6.2. Nech $(G, *)$ a $a \in G$.
Zobrazenie $f_a \colon G \to G$ dané predpisom $f_a(x) = a * x$ voláme *ľavá translácia.*
Zobrazenie $g_a \colon G \to G$ dané predpisom $g_a(x) = x * a$ voláme *pravá translácia.*

Lema 2.6.3. *Každá ľavá (pravá) translácia je bijekcia.*

Dôkaz. Surjektívnosť f_a: Pre každé $x \in G$ máme $f(a^{-1} * x) = a * a^{-1} * x = x$.
Injektívnosť f_a: Ak $f_a(x) = f_a(y)$, znamená to, že $a * x = a * y$. Zo zákona o krátení potom vyplýva $x = y$.
Ukázali sme, že ľavé translácie sú bijekcie; dôkaz pre pravé translácie je úplne analogický. □

Dôsledok 2.6.4. *Pre všetky $a \in G$ platí $f_a, g_a \in S(G)$.*

Lema 2.6.5. *Pre ľavé translácie platí*

$$f_b \circ f_a = f_{b*a}$$

Dôkaz. Pre $x \in G$ máme

$$(f_b \circ f_a)(x) = f_b(f_a(x)) = b * (a * x) = (b * a) * x = f_{b*a}(x).$$

□

Dôsledok 2.6.6. *Zobrazenie $a \mapsto f_a$ je homomorfizmus z G do $S(G)$.*

Dôsledok 2.6.7. *Ľavé translácie tvoria podgrupu grupy $S(G)$.*

Dôkaz. Ľavé translácie sú presne obrazom G v zobrazení $a \mapsto f_a$ z G do $S(G)$. Pretože toto zobrazenie je homomorfizmus, podľa tvrdenia 2.3.9 tvoria ľavé translácie podgrupu. □

Aby sme dokázali Cayleyho vetu, stačí už len ukázať, že práve uvedený homomorfizmus je v skutočnosti izomorfizmus na svoj obraz, t.j. že je injektívny.

Veta 2.6.8 (Cayley). *Každá grupa $(G, *)$ je izomorfná s nejakou grupou transformácií. Presnejšie, $(G, *)$ je izomorfná s podgrupou grupy $S(G)$ tvorenou všetkými ľavými transláciami.*

Dôkaz. Z toho, čo sme dokázali doteraz už vieme, že ľavé translácie sú skutočne podgrupou $S(G)$ a zobrazenie $a \mapsto f_a$ je surjektívny homomorfizmus z G na túto podgrupu. (Surjektívnosť vyplýva z toho, že táto podgrupa je priamo obrazom grupy G v uvedenom zobrazení.)
Zostáva teda dokázať len injektívnosť. Ak platí $f_a = f_b$ (v zmysle rovnosti zobrazení), tak potom aj $a = a * e = f_a(e) = f_b(e) = b * e = b$. □

Dôsledok 2.6.9. *Ľubovoľná konečná grupa rádu n (t.j. taká, ktorá má n prvkov) je izomorfná s podgrupou grupy permutácií S_n.*

Príklad 2.6.10. Ilustrujme si Cayleyho vetu na príklade grupy $(\mathbb{Z}, +)$. (Keďže ide o komutatívnu grupu, v tomto prípade sú ľavé a pravé stranslácie totožné.)

V tomto prípade pre $a \in \mathbb{Z}$ máme zobrazenie $f_a \colon \mathbb{Z} \to \mathbb{Z}$

$$f_a(x) = a + x,$$

ktoré je očividne bijektívne, čiže $f_a \in S(\mathbb{Z})$. Takisto sa ľahko overí, že $f_{a+b} = f_a \circ f_b$, z čoho vidíme, že $a \mapsto f_a$ je homomorfizmus. Fakt, že tento homomorfizmus je injektívny, môžeme overiť podobne ako v dôkaze Cayleyho vety.

Príklad 2.6.11. Skúsme sa pozrieť na reprezentáciu grupy $(S, \cdot)$, kde $S = \{z \in \mathbb{C}; |z| = 1\}$ pomocou Cayleyho vety.

V tomto prípade máme $f_z(x) = zx$. Z Moivrovej vety vieme, že vynásobenie komplexných číslom z s jednotkovou veľkosťou presne zodpovedá otočeniu bodu v komplexnej rovine okolo počiatku o uhol φ taký, že $z = \cos\varphi + i \sin\varphi$. Čiže v tomto prípade tvoria grupu transformácií z Cayleyho vety všetky otočenia kružnice okolo nuly.

Poznámka 2.6.12. Ďalšou zaujímavou oblasťou, ktorá súvisí s grupami transformácií sú grupy symetrií rovinných útvarov alebo telies. V prípade, že by Vás táto téma zaujímala, môžete si o nej niečo prečítať napríklad v [KGGS, Kapitola 3.1].

Cvičenia

Úloha 2.6.1.

Izomorfizmus grupy G na samú seba voláme *automorfizmus.* Dokážte, že:
a) Množina $\operatorname{Aut} G$ všetkých automorfizmov grupy G je grupou transformácií.
b) Definujeme pre ľubovoľné $a \in G$ zobrazenie $f_a \colon G \to G$ ako $f_a(g) = aga^{-1}$. Potom platí $f_{ab} = f_a \circ f_b$ pre ľubovoľné $a, b \in G$.
c) Pre každé $a \in G$ je zobrazenie f_a automorfizmus grupy G (takýto automorfizmus nazveme vnútorný).
d) Množina $\operatorname{VAut} G$ všetkých vnútorných automorfizmov grupy G je grupou transformácií.
e) Grupa G je komutatívna práve vtedy, keď množina $\operatorname{VAut} G$ všetkých jej vnútorných automorfizmov je jednoprvková.
f) Zobrazenie $a \mapsto f_a$ je surjektívny homomorfizmus z G na $\operatorname{VAut} G$. Nájdite jadro tohoto automorfizmu.

Kapitola 3

Faktorizácia

3.1 Relácie ekvivalencie a rozklady

So základnými vlastnosťami ekvivalencií a rozkladov a s ich vzájomným súvisom ste sa už stretli na iných prednáškach (pozri [OŠ]), napriek tomu tu však zopakujeme niektoré ich základné vlastnosti.

Definícia 3.1.1. *Relácia ekvivalencie* je relácia R na množine A, ktorá je reflexívna, symetrická a tranzitívna; t.j. pre všetky $a, b, c \in A$ platí:

$$aRa$$
$$aRb \Rightarrow bRa$$
$$aRb \wedge bRc \Rightarrow aRc$$

Množina $\{b \in A; aRb\}$ sa nazýva *triedou ekvivalencie s reprezentantom* a a označuje sa $[a]_R$, prípadne len $[a]$.

Definícia 3.1.2. *Rozklad množiny* A je taká množina $\mathcal{A} = \{A_i; i \in I\}$ neprázdnych podmnožín množiny A, že platí:

(i) Pre všetky $i, j \in I$ platí buď $A_i = A_j$ alebo $A_i \cap A_j = \emptyset$.

(ii) $\bigcup_{i \in I} A_i = A$.

Pred hlavnými výsledkami týkajúcimi sa rozkladov a ekvivalencií uvedieme si ešte jednu lemu:

Lema 3.1.3. *Nech R je relácia ekvivalencie. Potom*

$$aRb \Leftrightarrow [a]_R = [b]_R.$$

Veta 3.1.4. *Ak R je relácia ekvivalencie na A, tak množina všetkých tried ekvivalencie tvorí rozklad množiny A.*

Veta 3.1.5. *Ak $\mathcal{A} = \{A_i; i \in I\}$ je rozklad množiny A, tak relácia R definovaná tak, že*

$$aRb \qquad \Leftrightarrow \qquad (\exists i \in I) a \in A_i \wedge b \in A_i$$

je relácia ekvivalencie. (*Definícia relácie R vlastne hovorí, že dva prvky sú v relácii R práve vtedy, keď ležia v tej istej množine rozkladu $\mathcal{A}$.*)

Dôkaz týchto viet môžete nájsť napríklad v [OŠ].

Videli sme, že relácii ekvivalencie na množina A môžeme priradiť rozklad množiny A a opačne. Chceli by sme ukázať, že táto korešpondencia medzi reláciami ekvivalencie a rozkladmi je jednojednoznačná; čiže relácie ekvivalencie a rozklady sú vlastne len 2 rôzne pohľady na tú istú vec.

Označme rozklad prislúchajúci relácii ekvivalencie R ako $\mathcal{A}_R$ a reláciu ekvivalencie danú rozkladom $\mathcal{A}$ ako $R_{\mathcal{A}}$. My vlastne chceme ukázať, že tieto 2 priradenia sú navzájom inverzné, čiže $R_{\mathcal{A}_R} = R$ a $\mathcal{A}_{R_{\mathcal{A}}} = \mathcal{A}$.

(Tu je tiež dôležité si uvedomiť, čo znamená že 2 relácie resp. 2 rozklady sú rovnaké. Relácie chápeme ako podmnožiny $A \times A$, 2 relácie sa R a R' sa rovnajú práve vtedy, keď platí $aRb \Leftrightarrow aR'b$ pre všetky $a, b \in A$. Rovnosť pre rozklady takisto chápeme ako rovnosť množín – to znamená, že rovnaké rozklady pozostávajú z tých istých podmnožín.)

Z lemy 3.1.3 vidíme, že ak priradíme relácii ekvivalencie rozklad, tak v rovnakých podmnožinách budú práve tie prvky, ktoré sú v relácii R, a teda skutočne platí $R_{\mathcal{A}_R} = R$. Platnosť rovnosti $\mathcal{A}_{R_{\mathcal{A}}} = \mathcal{A}$ pre ľubovoľný rozklad sa tiež ukáže pomerne jednoducho (úloha 3.1.2 – dá sa opäť použiť lema 3.1.3).

Cvičenia

Úloha 3.1.1. Dokážte lemu 3.1.3.

Úloha 3.1.2. Dokážte, že pre ľubovoľný rozklad $\mathcal{A}$ platí $\mathcal{A}_{R_{\mathcal{A}}} = \mathcal{A}$.

Úloha 3.1.3. a) Nech $f\colon A \to B$ je surjektívne zobrazenie. Dokážte, že relácia R na množine A určená predpisom $aRa' \Leftrightarrow f(a) = f(a')$ je relácia ekvivalencie a triedy rozkladu sú množiny $f^{-1}(\{b\}) = f^{-1}(b)$ pre $b \in B$.
b) Nech R je relácia ekvivalencie na množine A a nech B je množina všetkých tried ekvivalencie. Dokážte, že zobrazenie $f\colon A \to B$, ktoré každému prvku priradí jeho triedu ekvivalencie (teda $f\colon a \mapsto [a]$) je surjektívne.
c) V predchádzajúcej časti sme každému surjektívnemu zobrazeniu priradili reláciu ekvivalencie a obrátene. Dokážte, že tieto dve priradenia sú navzájom inverzné.

Úloha 3.1.4. Dokážte, že relácia $R_1 = A \times A$ na A je relácia ekvivalencie. Dokážte, že $R_2 = \{(a, a); a \in A\}$ je relácia ekvivalencie na A.

Úloha 3.1.5. Ak R_1, R_2 sú relácie ekvivalencie na A, tak aj $R_1 \cap R_2$ je relácia ekvivalencie na A.

Úloha 3.1.6. a) Relácia R na množine S_n taká, že $\varphi R \tau$ práve vtedy, keď permutácie φ a τ majú rovnaký počet inverzií;
b) relácia R na množine $\mathbb{Z}$ definovaná ako $xRy \Leftrightarrow x$ a y majú rovnaký ciferný súčet;
c) relácia R na množine $\mathbb{Z}$ definovaná predpisom $xRy \Leftrightarrow x + y$ je párne;
d) pre ľubovoľnú (konečnú) množinu M relácia R na množine $\mathcal{P}(M)$ definovaná ako $ARB \Leftrightarrow |A| = |B|$. (Pod označením $|A|$ rozumieme buď počet prvkov – v prípade, že M je konečná, alebo mohutnosť množiny.)

Úloha 3.1.7. Dokážte, že nasledujúce relácie sú relácie ekvivalencie:
a) relácia R na množine $\mathbb{R}$ definovaná ako $(x, y, z)R(x', y', z') \Leftrightarrow x + y + z = x' + y' + z'$,
b) relácia R na množine S_n definovaná ako $\varphi R \tau \Leftrightarrow \varphi$ a τ majú rovnakú paritu,
c) relácia R na množine $\mathbb{Z}$ definovaná ako $xRy \Leftrightarrow 5 \mid x - y$
d) pre ľubovoľnú maticu typu $m \times n$ nad poľom F je relácia $\vec{\alpha}R\vec{\beta} \Leftrightarrow A\vec{\alpha}^T = A\vec{\beta}^T$ relácia ekvivalencie na množine F^n;

e) relácia R na množine $\mathbb{R}$ definovaná tak, že $xRy \Leftrightarrow x = y \vee x = -y$;
f) relácia R na množine $\mathbb{R}^{\mathbb{R}}$ všetkých zobrazení z $\mathbb{R}$ do $\mathbb{R}$ definovaná ako $fRg \Leftrightarrow f(0) = g(0)$.

Úloha 3.1.8. Nech R je relácia ekvivalencie na množine X a S je relácia ekvivalencie na množine Y. Potom relácia T určená ako $(x, y)T(x', y') \Leftrightarrow xRx' \wedge ySy'$ je relácia ekvivalencie na množine $X \times Y$.

Úloha 3.1.9. Nech $f\colon X \to Y$ je surjektívne zobrazenie.
a) Ak R je relácia ekvivalencie na X, tak relácia S na Y daná predpisom $ySy' \Leftrightarrow$ existujú $x, x' \in X$ také, že $f(x) = y$, $f(x') = y'$ a xRx' je tiež relácia ekvivalencie.
b) Ak S je relácia ekvivalencie na množine Y tak relácia R na X daná predpisom $xRx' \Leftrightarrow f(x)Sf(x')$ je tiež relácia ekvivalencie. (Ako špeciálny prípad dostaneme tvrdenie z úlohy 3.1.3b).)

3.2 Rozklad grupy podľa podgrupy

Najprv si zadefinujeme jeden pomocný pojem – násobenie podmnožín grupy.

Definícia 3.2.1. Nech G je grupa a $A, B \subseteq G$ sú jej ľubovoľné podmnožiny. Potom definujeme *súčin AB podmnožín A, B* ako

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

V prípade, že jedna z množín je jednoprvková, budeme používať stručnejší zápis aB namiesto $\{a\}B$ a Ab namiesto $A\{b\}$.

Niektoré užitočné vlastnosti násobenia podmnožín zhrnieme v nasledujúcej leme:

Lema 3.2.2. *Nech G je grupa.*

(i) *Násobenie podmnožín je asociatívne, t.j. $A(BC) = (AB)C$ pre ľubovoľné podmnožiny $A, B, C \subseteq G$.*

(ii) *Pre ľubovoľnú podmnožinu $A \subset G$ platí $eA = Ae = A$.*

(iii) *Ak H je podgrupa grupy G a $h \in H$, tak $hH = H$.*

(iv) *Ak H je podgrupa grupy G, tak $H^2 = H.H = H$.*

(v) *Pre ľubovoľnú podmnožinu $A \subseteq G$ platí $(A^{-1})^{-1} = A$, kde používame označenie $A^{-1} = \{a^{-1}; a \in A\}$.*

(vi) *Ak H je podgrupa grupy G, tak $H^{-1} = \{h^{-1}; h \in H\} = H$.*

(vii) *Pre ľubovoľné podmnožiny $A, B \subseteq G$ platí $(AB)^{-1} = B^{-1}.A^{-1}$.*

(viii) *Ak K, H sú podgrupy grupy G, tak $(HK)^{-1} = K^{-1}.H^{-1} = KH$.*

Označenie H^{-1} v predchádzajúcej leme neznamená, že by táto množina bola inverzným prvkom ku H v $\mathcal{P}(G) \setminus \{\emptyset\}$ s operáciou násobenia podmnožín – H^{-1} jednoducho len označuje množinu inverzných prvkov ku prvkom z H.

Nebudeme dokazovať všetky časti tejto lemy – väčšinu z nich ponecháme ako cvičenie (úloha 3.2.1). Na ukážku si dokážme (v).

Dôkaz. (v): Pretože $(a^{-1})^{-1} = a$, každý prvok z A patrí aj do $(A^{-1})^{-1}$, čiže $A \subseteq (A^{-1})^{-1}$.

Obrátene, ak $b \in (A^{-1})^{-1}$, tak $b = (a^{-1})^{-1}$ pre nejaké $a \in A$, ale $(a^{-1})^{-1} = a$, teda $b = a \in A$. Ukázali sme aj inklúziu $(A^{-1})^{-1} \subseteq A$. □

Násobenie podmnožín vo všeobecnosti nemusí byť komutatívne (ako kontrapríklad stačí zobrať v nekomutatívnej grupe 2 jednoprvkové množiny $\{a\}$ a $\{b\}$ pre prvky a a b, ktoré nekomutujú). Samozrejme, pre komutatívnu grupu je aj násobenie podmnožín komutatívne.

Definícia 3.2.3. Ak H je podgrupa grupy G, tak označíme pre $a \in G$

$$aH = \{ah; h \in H\},$$
$$Ha = \{ha; h \in H\}.$$

Množiny aH nazývame *ľavé triedy grupy G podľa H* (alebo ľavé triedy grupy G modulo H), množiny Ha sú *pravé triedy grupy G podľa H*.

Ako sme už spomenuli, násobenie podmnožín vo všeobecnosti nemusí byť komutatívne, takisto ani nemusí vo všeobecnosti platiť $aH = Ha$. V ďalšej časti uvidíme, že podgrupy, ktoré majú túto vlastnosť sú z istého hľadiska zaujímavé. Je zrejmé, že táto rovnosť platí ak G je komutatívna.

Začali by sme však s tým, že ukážeme, že ľavé triedy G podľa H tvoria rozklad G (a podobne to platí pre pravé triedy).

Príklad 3.2.4. Triedy $\mathbb{Z}$ podľa $3\mathbb{Z}$ sú $\{3k; k \in \mathbb{Z}\}$, $\{3k+1; k \in \mathbb{Z}\}$ a $\{3k+2; k \in \mathbb{Z}\}$. Je zrejmé, že tvoria rozklad množiny $\mathbb{Z}$ – každé celé číslo je buď tvaru $3k$, $3k+1$ alebo $3k+2$. (V tomto prípade ide o komutatívnu grupu, preto sú ľavé a pravé triedy totožné.)

Lema 3.2.5. *Nech H je podgrupa G a $a, b \in G$. Potom $aH = bH$ práve vtedy, keď $b^{-1}a \in H$.*

Podobne platí $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Dôkaz. $\boxed{\Rightarrow}$ Ak $aH = bH$, tak $a \in bH$, čiže $a = bh$ pre nejaké $h \in H$. Z toho $b^{-1}a = h \in H$.

$\boxed{\Leftarrow}$ Ak $b^{-1}a \in H$, tak $b^{-1}aH = H$, a teda $bH = b(b^{-1}aH) = (bb^{-1})aH = eaH = aH$.

Dôkaz druhej časti tejto lemy je analogický. □

Tvrdenie 3.2.6. *Ľavé triedy grupy G podľa jej podgrupy H tvoria rozklad G. (Inak: $\{aH; a \in G\}$ je rozklad množiny G.)*

Pravé triedy grupy G podľa jej podgrupy H tvoria rozklad G.

Dôkaz. Každá trieda aH obsahuje prvok a, je teda neprázdna. Overme teda ešte ostatné dve podmienky z definície rozkladu.

Platí $\bigcup_{a \in G} aH \supseteq \bigcup_{a \in G} \{a\} = G$, teda zjednotenie všetkých ľavých tried je celé G.

Nech $a, b \in G$. Stačí ukázať, že ak $aH \cap bH \neq \emptyset$, tak $aH = bH$. Nech teda $x \in aH \cap bH$. To znamená, že $x = ah = bh'$ pre nejaké $h, h' \in H$. Z rovnosti $ah = bh'$ ľahko dostaneme $b^{-1}a = h'h^{-1}$, a teda $b^{-1}a \in H$. Podľa lemy 3.2.5 potom platí $aH = bH$

Dôkaz pre pravé triedy je skoro identický. □

Definícia 3.2.7. Nech G je grupa a H je podgrupa. Rozklad $\{aH; a \in G\}$ sa nazýva *ľavý rozklad G podľa H* a rozklad $\{Ha; a \in G\}$ sa nazýva *pravý rozklad G podľa H*.

Všimnime si, že $eH = He = H$, teda ako jedna z ľavých (pravých) tried sa vždy vyskytne podgrupa H.

Príklad 3.2.8. Uvažujme podgrupu $H = \{(x, x); x \in \mathbb{R}\}$ grupy $G = (\mathbb{R} \times \mathbb{R}, +)$. Ide o komutatívnu grupu, takže ľavý aj pravý rozklad sú rovnaké. Dva prvky $(a, b), (c, d) \in G$ ležia v tej istej triede rozkladu práve vtedy, keď $(a, b) - (c, d) = (a - b, c - d) \in H$, teda keď $a - b = c - d$. To znamená, že každá trieda rozkladu je určená rozdielom $r = a - b$. Inak povedané, jednotlivé triedy rozkladu sú práve množiny

$$\{(x, y) \in \mathbb{R}^2; x - y = r\}$$

pre $r \in \mathbb{R}$. Všimnime si, že rôznym r zodpovedajú triedy ekvivalencie, takže každú triedu ekvivalencie dostaneme takýmto spôsobom iba raz. Z každej triedy rozkladu by sme mohli vybrať napríklad reprezentanta tvaru $\{(r, 0); r \in \mathbb{R}\}$, t.j. triedy rozkladu môžeme zapísať ako

$$(r, 0) + H$$

pre $r \in \mathbb{R}$.

Uveďme ešte aspoň jeden príklad, kde G je konečná grupa.

Príklad 3.2.9. Nech $G = \mathbb{Z}_8$ a $H = 4\mathbb{Z}_8 = \{0, 4\}$. Opäť sú obe grupy komutatívne, takže ľavý a pravý rozklad sú totožné. Rozklad G podľa H obsahuje 4 triedy: $\{0, 4\}$, $\{1, 5\}$, $\{2, 6\}$, $\{3, 7\}$.

Teraz ukážeme nejaké tvrdenia hovoriace o počtoch (mohutnostiach) tried rozkladu G podľa H. (Môžete si ich podrobnejšie rozmyslieť na rozkladoch z príkladov 3.2.4, 3.2.8, 3.2.9.)

Lema 3.2.10. *Nech H je podgrupa grupy G a $a \in G$. Potom zobrazenie $\varphi\colon H \to aH$ definované ako*

$$\varphi\colon h \mapsto ah$$

je bijekcia.

Podobne zobrazenie $\psi\colon H \to Ha$, $\psi\colon h \mapsto ha$ je bijekcia.

Dôkaz. Zobrazenie φ je injekcia: $\varphi(h_1) = \varphi(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$ (podľa zákonov o krátení).

Priamo z definície množiny aH vyplýva, že φ je aj surjekcia.

Dôkaz pre zobrazenie ψ by bol analogický. □

Z predchádzajúcej lemy okamžite dostávame, že:

Veta 3.2.11. *Nech H je konečná podgrupa G. Potom počet prvkov každej ľavej triedy aH je rovnaký (a rovná sa počtu prvkov podgrupy H). Takisto sa rovná počtu prvkov ľubovoľnej pravej triedy Hb.*

Lema 3.2.12. *Nech H je podgrupa grupy G. Potom zobrazenie*

$$\varphi\colon aH \mapsto Ha^{-1}$$

je bijekcia medzi množinami tried $\{aH; a \in G\}$ a $\{Ha; a \in G\}$.

Dôkaz. Všimnime si, že platí $(aH)^{-1} = H^{-1}a^{-1} = Ha^{-1}$.

Z toho vyplýva, že zobrazenie φ je dobre definované. (Nezávisí od výberu reprezentanta triedy aH, keďže sme ukázali, že $\varphi(aH)$ je práve množina všetkých inverzných prvkov k prvkom z aH.)

Zobrazenie φ je zrejme surjekcia (vzorom pre triedu Hb je ľavá trieda $b^{-1}H$). Ukážeme ešte, že je to injekcia.

Na základe rovnosti $Ha^{-1} = (aH)^{-1}$ ďalej dostaneme $Ha^{-1} = Hb^{-1} \Leftrightarrow (aH)^{-1} = (bH)^{-1} \Leftrightarrow aH = bH$. (Využili sme lemu 3.2.2(v,vii).) □

Na základe predchádzajúcej vety, ktorá hovorí, že počet ľavých a pravých tried je rovnaký, má zmysel nasledujúca definícia.

Definícia 3.2.13. Nech H je podgrupa konečnej grupy. Potom $[G\colon H]$ je počet všetkých ľavých (pravých) tried rozkladu G podľa H. Toto číslo nazývame *indexom grupy G podľa H.*

Veta 3.2.14 (Lagrangeova veta). *Ak G je konečná grupa a H je jej podgrupa, tak platí*

$$|G| = |H|.[G\colon H].$$

Teda počet prvkov podgrupy H delí počet prvkov G.

Dôkaz. Máme rozklad množiny G na $[G\colon H]$ tried rovnakej veľkosti $|H|$. Potom $|G| = [G\colon H]|H|$.

Z toho je zrejmé aj to, že $|H| \mid |G|$ (počet prvkov H delí počet prvkov G). □

Na tomto mieste treba spomenúť, že neplatí obrátenie Lagrangeovej vety v tom zmysle, že pre každý deliteľ k čísla $|G|$ (počtu prvkov grupy G) by musela existovať k-prvková podgrupa. Pozri úlohu 3.3.3. (Pre cyklické grupy však toto tvrdenie platí, tam dokonca existuje jediná k-prvková podgrupa. Takéto tvrdenie – že by počtom prvkov bola podgrupa jednoznačne určená – takisto vo všeobecnosti neplatí.)

Nasledujúci výsledok by snáď mohol vysvetlovať, prečo namiesto počtu prvkov konečnej grupy niekedy používame aj termín *rád grupy.*

Dôsledok 3.2.15. *Ak G je konečná grupa, tak rád každého prvku delí rád grupy G (počet prvkov grupy G).*

Dôkaz. Stačí si uvedomiť, že rád prvku a je počet prvkov podgrupy $[a]$. □

Dôsledok 3.2.16. *Ak G je p-prvková grupa a p je prvočíslo, tak každý jej prvok okrem neutrálneho prvku je generátorom G (a teda G je cyklická).*

Dôkaz. Rád prvku $a \neq e$ nie je 1 a keďže je deliteľ prvočísla p, musí byť rovný p. Teda $[a]$ obsahuje p rôznych prvkov $e, a^1, a^2, \ldots, a^{p-1}$, čiže $[a] = G$. □

Dôsledok 3.2.17. *Každá 4-prvková grupa je izomorfná buď so $\mathbb{Z}_4$ alebo so $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Dôkaz. Nech G je 4-prvková grupa. Podľa dôsledku 3.2.15 rády jej prvkov môžu byť jedine 1, 2 alebo 4. Ak G obsahuje prvok rádu 4, tak tento prvok je jej generátor. V tomto prípade dostávame, že G je cyklická a $G \cong \mathbb{Z}_4$.

Druhá možnosť je, že všetky prvky s výnimkou neutrálneho majú rád 2, čiže pre každý prvok platí $a^2 = e$, kde e je neutrálny prvok G. Inak povedané, pre všetky $a \in G$ platí $a = a^{-1}$. Z toho dostávame aj to, že G je komutatívna: $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

Označme prvky tejto grupy e, a, b, c. Zatiaľ o nich vieme toto:

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

Podľa zákonov o krátení sa každý prvok vyskytne v ľubovoľnom riadku a v ľubovoľnom stĺpci tabuľky grupovej operácie práve raz. Tento fakt nám umožní jednoznačne doplniť prázdne miesta v tabuľke. Všimnime si napríklad, že prvok ab nemôže byť a, e ani b (inak by sme mali v niektorom riadku alebo stĺpci tento prvok dvakrát). Podobnú úvahu môžeme urobiť pre prvok ba. Dostávame:

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

Teraz už v každom riadku a stĺpci máme jediné voľné miesto, teda zostávajúci prvok je jednoznačne určený

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

Pretože aj $\mathbb{Z}_2 \times \mathbb{Z}_2$ má tú vlastnosť, že všetky prvky okrem neutrálneho majú rád 2, a práve sme ukázali, že touto podmienkou je grupa jednoznačne určená (až na označenie prvkov – čiže až na izomorfizmus), máme $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Cvičenia

Úloha 3.2.1. Dokážte zvyšné časti lemy 3.2.2.

Úloha 3.2.2. Ak G je konečná grupa, H je podgrupa G a K je podgrupa H, tak $[G : K] = [G : H][H : K]$.

Úloha 3.2.3. Dokážte, že každá grupa, ktorá má menej ako 6 prvkov, je komutatívna.

Úloha 3.2.4. Nájdite všetky ľavé (pravé) triedy grupy G podľa podgrupy H, ak
a) $G = (\mathbb{R}, +)$, $H = \mathbb{Z}$;
b) $G = (\mathbb{R} \times \mathbb{R}, +)$, $H = \{(x, y) \in \mathbb{R} \times \mathbb{R}; y = 3x\}$;
c) $G = (\mathbb{Z}_6, \oplus)$, $H = 2\mathbb{Z}_3$;
d) $G = S_n$, $H = A_n$;
e) $G = S_3$, $H = [(12)]$;
f) $G = (\mathbb{Z}, +)$, $H = 3\mathbb{Z}$.
(Pod „nájdite všetky triedy“ sa rozumie to, že pre každú triedu vyberieme jedného reprezentanta, v prípade, že ide o konečné množiny ich môžeme aj vypísať.)

Úloha 3.2.5. Dokážte, že každá 8-prvková grupa obsahuje dvojprvkovú podgrupu.

Úloha 3.2.6. Ak G má p^2 prvkov, kde p je prvočíslo, tak každá vlastná podgrupa G je cyklická.

Úloha 3.2.7. Ak p je prvočíslo a $k \geq 1$ prirodzené číslo, tak každá p^k-prvková grupa má p-prvkovú podgrupu.

Úloha 3.2.8. Nech S_i je podgrupa G a $t_i \in G$ pre každé $i \in I$. Označme $D = \bigcap_{i \in I} S_i$. Dokážte, že buď $\bigcap_{i \in I} S_i t_i = \emptyset$ alebo existuje $g \in G$ také, že $\bigcap_{i \in I} S_i t_i = Dg$. (T.j. prienik pravých tried $S_i t_i$ je buď prázdna množina alebo niektorá pravá trieda rozkladu podľa D.)

Úloha 3.2.9. Dokážte, že v každej grupe s nepárnym počtom prvkov je ľubovoľný prvok štvorcom nejakého (a navyše jednoznačne určeného) prvku tejto grupy.

Úloha 3.2.10. Nech H je podgrupa G. Ukážte, že systém $\{HaH; a \in G\}$ je rozklad množiny G.

3.3 Normálne podgrupy

Dostali sme teda rozklad G podľa ľavých tried a rozklad G podľa pravých tried. Tieto 2 rozklady môžu byť vo všeobecnosti rôzne – my sa budeme snažiť nájsť podmienky, kedy sú rovnaké.

Tvrdenie 3.3.1. *Nech H je podgrupa grupy G. Ak $aH = Hb$, tak $Ha = Hb$. (Takisto za týchto predpokladov platí $aH = bH$.)*

Dôkaz. Ak $aH = Hb$, tak $a \in Hb$, čiže $a = hb$ pre nejaké $h \in H$. Potom $h = ab^{-1} \in H$ a podľa lemy 3.2.5 máme $Ha = Hb$.

Dôkaz druhej časti tvrdenia je analogický. □

Veta 3.3.2. *Nech H je podgrupa G. Nasledujúce podmienky sú ekvivalentné:*

(i) $aH = Ha$ *pre všetky* $a \in G$,

(ii) $aH \subseteq Ha$ *pre všetky* $a \in G$,

(iii) $Ha \subseteq aH$ *pre všetky* $a \in G$,

(iv) $aHa^{-1} \subseteq H$ *pre všetky* $a \in G$,

(v) $H \subseteq aHa^{-1}$ *pre všetky* $a \in G$,

(vi) $aHa^{-1} = H$ *pre všetky* $a \in G$,

(vii) $\{aH; a \in G\} = \{Hb; b \in G\}$.

Všimnime si, že podmienku (v) môžeme zapísať aj tak, že platí $aha^{-1} \in H$ pre všetky $h \in H$ a $a \in G$, čiže

$$h \in H \qquad \Rightarrow \qquad aha^{-1} \in H. \tag{3.1}$$

V nasledujúcom dôkaze budeme využívať vlastnosti násobenia podmnožín sformulované v leme 3.2.2 ako aj pomerne ľahko dokázateľný fakt, že násobenie podmnožín zachováva inklúzie. (Vlastne nám bude stačiť implikácia $B \subseteq C \Rightarrow aB \subseteq aC$.)

Dôkaz. Zrejmé: (i) ⇒ (ii), (i) ⇒ (iii)

(ii) ⇒ (iv): Ak platí $aH \subseteq Ha$, tak platí aj

$$aHa^{-1} \subseteq (Ha)a^{-1} = H(aa^{-1}) = He = H.$$

Podobne sa ukáže (iii) ⇒ (iv): Máme $Ha^{-1} \subseteq a^{-1}H$, preto

$$aHa^{-1} \subseteq aa^{-1}H = H.$$

(iv) ⇒ (v): Použitím (iv) pre prvok a^{-1} dostaneme $a^{-1}Ha \subseteq H$. Keď túto inklúziu vynásobíme zľava a a sprava a^{-1}, tak máme

$$H = a(a^{-1}Ha)a^{-1} \subseteq aHa^{-1}.$$

(v) ⇒ (vi): Stačí v skutočnosti ukázať, že (v) ⇒ (iv), pretože z (v) a (iv) okamžite vyplýva (vi). Dôkaz implikácie (v) ⇒ (iv) je takmer rovnaký ako dôkaz predchádzajúcej implikácie. Ak použijeme (v) pre prvok a^{-1}, dostaneme $a^{-1}Ha \subseteq H$. Keď túto inklúziu vynásobíme zľava a a sprava a^{-1}, tak máme

$$H = a(a^{-1}Ha)a^{-1} \subseteq aHa^{-1}.$$

(vi) ⇒ (i): Ak $H = aHa^{-1}$, tak $Ha = (aHa^{-1})a = aH(a^{-1}a) = a(He) = aH$.

Takisto implikácia (i) ⇒ (vii) je zrejmá. Opačná implikácia (vii) ⇒ (i) vyplýva z tvrdenia 3.3.1. Z rovnosti $\{aH; a \in G\} = \{Hb; b \in G\}$ totiž vyplýva, že každé aH sa musí rovnať nejakému Hb, ale potom podľa tvrdenia 3.3.1 platí aj $aH = Ha$.

Dokázali sme:
(i) ⇒ (ii) ⇒ (iv) ⇒ (v) ⇒ (vi) ⇒ (i),
(i) ⇒ (iii) ⇒ (iv) ⇒ (v) ⇒ (vi) ⇒ (i),
(i) ⇔ (vii),
z čoho vyplýva, že všetky uvedené podmienky sú ekvivalentné. □

Definícia 3.3.3. Podgrupa H grupy G sa nazýva *normálna* (*invariantná*) *podgrupa,* ak spĺňa niektorú z ekvivalentných podmienok uvedených vo vete 3.3.2. Označujeme $H \triangleleft G$.

Ak G je komutatívna grupa, tak každá jej podgrupa je invariantná.

Z vety 3.3.2 vidíme, že pre invariantnú podgrupu ľavé a pravé triedy rozkladu sú totožné.

Príklad 3.3.4. Pre každú grupu G sú jej podgrupy G a $\{e\}$ normálnymi podgrupami.

Pretože v komutatívnej grupe je každá podgrupa normálna, úloha zistiť, či nejaká podgrupa je normálna, je zaujímavá len v nekomutatívnom prípade.

Príklad 3.3.5. Preskúmajme, ktoré podgrupy S_3 sú normálne. Zostavme najprv tabuľku grupovej operácie. (Do riadku φ a stĺpca τ zapisujeme $\varphi \circ \tau$.)

	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(132)	(123)	(23)	(13)
(13)	(13)	(123)	id	(132)	(12)	(23)
(23)	(23)	(132)	(123)	id	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	id
(132)	(132)	(23)	(12)	(13)	id	(123)

Teraz skúsme nájsť všetky podgrupy grupy S_3. Z Lagrangeovej vety 3.2.14 vieme, že (okrem podgrúp $\{e\}$ a S_3) stačí hladať podgrupy rádu 2 a 3. Podľa dôsledku 3.2.16 ide o cyklické grupy, teda nám stačí nájsť všetky prvky rádu 2 resp. 3.

Prvky rádu 2 sú práve cykly dĺžky 2. Tie vygenerujú podgrupy $H_1 = \{id, (12)\}$, $H_2 = \{id, (13)\}$ a $H_3 = \{id, (23)\}$.

Napríklad pre podgrupu $H_1 = \{id, (12)\}$ máme $(13)H_1 = \{(13), (123)\}$ a $H_1(13) = \{(13), (132)\}$. Keďže sme dostali pre ten istý prvok inú ľavú a pravú triedu, podgrupa H_1 nespĺňa podmienku (i) z vety 3.3.2, a teda nie je normálna.

Podobným spôsobom môžeme overiť, že ani ostatné 2-prvkové podgrupy nie sú normálne.

Prvky rádu 3 sú trojcykly (123) a (132). Obe generujú tú istú 3-prvkovú podgrupu $A_3 = \{id, (123), (132)\}$ pozostávajúcu z párnych permutácií množiny $\{1, 2, 3\}$. Vidíme, že pravý i ľavý rozklad je rovnaký, jeho triedy sú množina A_3 (párne permutácie) a jej doplnok $S_3 \setminus A_3$ (nepárne permutácie). Teda A_3 spĺňa podmienku (vii) z vety 3.3.2, čiže je normálna. (Na zdôvodnenie toho, že H_4 je normálna sme mohli použiť aj všeobecnejší fakt, že každá podgrupa indexu 2 je normálna – úloha 3.3.2.)

Cvičenia

Úloha 3.3.1. Dokážte, že prienik (ľubovoľného systému) normálnych podgrúp danej grupy G je opäť normálna podgrupa G.

Úloha 3.3.2. Ak H je podgrupa G a $[G : H] = 2$, tak H je normálna podgrupa. Navyše, pre každý prvok $x \in G$ platí $x^2 \in H$.

Úloha 3.3.3*. Dokážte, že grupa A_4 párnych permutácií 4-prvkovej množiny nemá žiadnu 6-prvkovú podgrupu.

Úloha 3.3.4. Pre všetky $n \in \mathbb{N}$ je A_n normálna podgrupa grupy S_n.

Úloha 3.3.5. Dokážte, že ľubovoľná normálna podgrupa A_n pre $n \geq 5$, ktorá obsahuje aspoň jeden cyklus dĺžky 3 je celá grupa A_n.

Úloha 3.3.6. Nájdite všetky normálne podgrupy v grupe: a) $(\mathbb{Z}_5, \oplus)$, b) $(\mathbb{Z}_6, \oplus)$, c) $(\mathbb{Z}_4, \oplus)$, d) $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$, e) $(\mathbb{Z}_{12}, \oplus)$, f) $(\mathbb{Z}_p, \oplus)$, kde p je prvočíslo, g*) $(A_4, \circ)$, h*) $(S_4, \circ)$.

Úloha 3.3.7. Dokážte, že ak H je normálna podgrupa G a $[G : H] = n$, tak $x^n \in H$ pre ľubovoľné $x \in G$. Ukážte na príklade, že toto tvrdenie nemusí platiť, ak H nie je normálna.

Úloha 3.3.8. Dokážte, že každá jednoduchá podgrupa grupy S_n, ktorá má viac ako 2 prvky, je obsiahnutá v grupe A_n. (Grupa sa nazýva jednoduchá, ak nemá žiadne normálne podgrupy okrem seba samej a triviálnej podgrupy.)

Úloha 3.3.9. Centrom grupy G nazývame množinu $Z(G) = \{g \in G; (\forall h \in G)gh = hg\}$ takých prvkov, ktoré komutujú so všetkými prvkami G. Ukážte, že $Z(G)$ je normálna podgrupa grupy G.

Úloha 3.3.10. Ak A a B sú normálne podgrupy G, $a \in A$ a $b \in B$, tak $aba^{-1}b^{-1} \in A \cap B$.

Úloha 3.3.11. Ak H a H' sú normálne podgrupy G také, že $H \cap H' = \{e\}$, tak $hh' = h'h$ pre ľubovoľné $h \in H$ a $h' \in H'$ (ľubovoľný prvok H komutuje s ľubovoľným prvkom H'.)

Úloha 3.3.12. Uvažujme grupu G všetkých zhodných izometrií[1] roviny nemeniacich orientáciu. Inak povedané, sú to všetky zobrazenia, ktoré môžeme dostať ako zloženie posunutia o nejaký vektor $\vec{u}$ a otočenia o nejaký uhol α, čiže zobrazenia dané predpisom $(x, y) \mapsto (c + x\cos\alpha + y\sin\alpha, d - x\sin\alpha + y\cos\alpha)$. Sú nasledujúce grupy normálnymi podgrupami grupy G?
a) $H =$ všetky posunutia;
b) $H =$ rotácie okolo počiatku súradnicovej sústavy;
c) $H_x =$ všetky zobrazenia z G také, že $f(x) = x$, pričom $x \in \mathbb{R}^2$ je nejaký pevne zvolený bod roviny.

3.4 Faktorové grupy

Veta 3.4.1. *Ak G je grupa a H je jej invariantná podgrupa, tak na množine všetkých tried G podľa H môžeme definovať operáciu $\cdot$ ako*

$$(aH) \cdot (bH) = (ab)H.$$

Táto operácia je dobre definovaná (nezávisí od výberu reprezentanta triedy) a množina všetkých tried G podľa H s touto operáciou tvorí grupu. Túto grupu označujeme G/H a nazývame faktorová grupa *grupy G podľa H.*

Je dôležité si uvedomiť, že faktorovú grupu môžeme definovať iba pre invariantnú podgrupu.

[1] izometria=zobrazenie zachovávajúce vzdialenosti; zhodné = zachovávajú aj orientáciu

Dôkaz. Všetky tvrdenia vety vlastne vyplývajú z toho, že takto definované násobenie je to isté ako násobenie podmnožín grupy G. Platí totiž

$$(aH)(bH) = (aH)(Hb) = a(HH)b = aHb = a(Hb) = a(bH) = (ab)H.$$

Z toho vyplýva, že operácia, ktorú sme definovali je dobre definovaná a takisto, že je asociatívna.

Pretože $eH = H$ a $HH = H$, trieda eH je neutrálny prvok.

Inverzný prvok k aH je $a^{-1}H$, pretože $(aH)(a^{-1}H) = (aa^{-1})H = eH = H$. □

Príklad 3.4.2. Ak $G = \mathbb{Z}$ a $H = 3\mathbb{Z}$ tak G/H obsahuje 3 triedy H, $1 + H$ a $2 + H$ (príklad 3.2.4).

	H	$1+H$	$2+H$
H	H	$1+H$	$2+H$
$1+H$	$1+H$	$2+H$	H
$2+H$	$2+H$	H	$1+H$

Z predchádzajúcej tabuľky vidíme, že $H \mapsto 0$, $1 + H \mapsto 1$, $2 + H \mapsto 2$ je izomorfizmus medzi G/H a $(\mathbb{Z}_3, \oplus)$, čiže v tomto prípade je faktorová grupa izomorfná s grupou $\mathbb{Z}_3$.

Príklad 3.4.3. Nech $G = (\mathbb{R} \times \mathbb{R}, +)$ a $H = \{(x, x); x \in \mathbb{R}\}$.

V príklade 3.2.8 sme videli, že každú triedu rozkladu môžeme reprezentovať ako $(r, 0)+H$ (a navyše takto dostaneme každú triedu práve raz). Z toho pomerne ľahko vidno, že zobrazenie

$$(r, 0) + H \mapsto R$$

je izomorfizmus medzi grupami G/H a $(\mathbb{R}, +)$, čiže $G/H \cong \mathbb{R}$.

Podobne môžeme vidieť, že pre $G = \mathbb{Z}_8$ a $H = 4\mathbb{Z}_8$ máme $G/H \cong \mathbb{Z}_4$. V ďalšej podkapitole dokážeme vetu, ktorá nám umožní takéto vlastnosti dokazovať pomerne jednoducho a elegantne.

3.5 Vety o izomorfizme

V úlohe 3.1.3 sme videli jednojednoznačný vzťah medzi surjektívnymi zobrazeniami a reláciami ekvivalencie. V prípade, že na danej množine máme navyše grupovú štruktúru, surjektívne homomorfizmy budú podobným spôsobom zodpovedať normálnym podgrupám (a navyše, ako uvidíme v cvičeniach za touto časťou, istým špeciálnym reláciam ekvivalencie, ktoré voláme kongruencie).

Veta 3.5.1 (Kanonický homomorfizmus). *Ak G je grupa a H je normálna podgrupa G, tak zobrazenie $f\colon G \to G/H$ dané predpisom*

$$f\colon a \mapsto aH$$

je surjektívny homomorfizmus. Tento homomorfizmus voláme kanonický homomorfizmus.

Navyše, jadro kanonického homomorfizmu je práve podgrupa H.

Dôkaz. Z vlastností násobenia podmnožín grupy (lema 3.2.2) a z toho, že H je normálna podgrupa dostaneme

$$f(a)f(b) = (aH)(bH) = a(Hb)H = a(bH)H = (ab)H^2 = (ab)H = f(ab).$$

Teda toto zobrazenie je skutočne homomorfizmus.

Surjektívnosť vyplýva priamo z definície.

Pretože neutrálny prvok faktorovej grupy G/H je $eH = H$, jadro zobrazenia f je množina tých $a \in G$, pre ktoré platí $aH = eH$, čo je presne podgrupa H (vyplýva to napríklad z lemy 3.2.5, ľahko to však môžeme overiť aj priamo.) □

Vidíme teda, že pre každú faktorovú grupu máme surjektívny homomorfizmus. Obrátené tvrdenie dáva nasledujúca veta:

Veta 3.5.2 (Veta o izomorfizme). *Ak $f\colon G \to G'$ je homomorfizmus grúp, tak* $\operatorname{Ker} f$ *je normálna podgrupa grupy G a faktorová grupa $G/\operatorname{Ker} f$ je izomorfná s podgrupou* $\operatorname{Im} f$ *grupy G'.*

Dôkaz. Označme $H = \operatorname{Ker} f$ a neutrálny prvok grupy G' označme ako e'. Z dôsledku 2.3.10 vieme, že H je podgrupa G. Ukážeme, že táto podgrupa je normálna. Skutočne, ak $h \in \operatorname{Ker} f$, t.j. $f(h) = e'$, tak aj

$$f(aha^{-1}) = f(a)f(h)f(a)^{-1} = f(a)e'f(a)^{-1} = f(a)f(a)^{-1} = e'$$

a $aha^{-1} \in \operatorname{Ker} f = H$.

Definujme zobrazenie $\varphi\colon G/H \to \operatorname{Im} f$ ako

$$\varphi\colon aH \mapsto f(a).$$

Najprv ukážeme, že toto zobrazenie je dobre definované (nezávisí od výberu reprezentanta ľavej triedy aH). Skutočne, ak $aH = bH$, tak $b^{-1}a \in H = \operatorname{Ker} f$, čiže $f(b^{-1}a) = e'$. Potom

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

Zostáva dokázať, že takto definované zobrazenie je bijektívny homomorfizmus. Máme

$$\varphi(abH) = f(ab) = f(a)f(b) = \varphi(aH)\varphi(bH),$$

teda φ je homomorfizmus.

Surjektívnosť vyplýva z toho, že za obor hodnôt sme zobrali $\operatorname{Im} f$. Aby sme ukázali, že homomorfizmus φ je injektívny, stačí ukázať, že $\operatorname{Ker}\varphi$ obsahuje iba neutrálny prvok (úloha 2.3.6). Skutočne, ak $\varphi(aH) = e'$, znamená to, že $f(a) = e'$ a $a \in \operatorname{Ker} f = H$, teda $aH = H$. □

Dôsledok 3.5.3. *Ak $f\colon G \to H$ je surjektívny homomorfizmus grúp, tak grupa H je izomorfná s faktorovou grupou $G/\operatorname{Ker} f$.*

Vety 3.5.1 a 3.5.2 nám hovoria, že normálne podgrupy sú práve jadrá homomorfizmov. (Jadro každého homomorfizmu je normálna podgrupa a obrátene, pre každú normálnu podgrupu máme epimorfizmus na faktorovú grupu, ktorého jadrom je práve táto podgrupa.)

Z vety o izomorfizme okamžite dostaneme nasledujúce jednoduché dôsledky.

Príklad 3.5.4. Použime vetu o izomorfizme pre homomorfizmy $f\colon G \to H$, $f(x) = e$ (kde G, H sú ľubovoľné grupy a e označuje neutrálny prvok grupy H) a $id_G\colon G \to G$. Platí $\operatorname{Ker} f = G$ a $\operatorname{Ker} id_G = \{e\}$, z čoho vyplýva na základe vety 3.5.2 $G/G \cong \{e\}$ a $G/\{e\} \cong G$.

V predchádzajúcej podkapitole sme uviedli niekoľko príkladov faktorových grúp pričom sme spomenuli, že sú izomorfné s niektorými známymi grupami. Predchádzajúca veta je jednoduchým prostriedkom ako ukázať, že ide skutočne o izomorfné grupy.

Príklad 3.5.5. Z príkladu 3.2.4 vieme, že rozklad grupy $\mathbb{Z}$ podľa podgrupy $3\mathbb{Z}$ má 3 prvky. Z toho je jasné, že faktorová grupa $\mathbb{Z}/3\mathbb{Z}$ je izomorfná s grupou $(\mathbb{Z}_3, \oplus)$. (Z dôsledku 3.2.16 a vety 2.4.11 vyplýva, že $\mathbb{Z}_3$ je, až na izomorfizmus, jediná trojprvková grupa.)

Skúsme však tento fakt odvodiť na základe vety 3.5.2. Na to stačí nájsť surjektívny homomorfizmus so $\mathbb{Z}$ na $\mathbb{Z}_3$, ktorého jadro je práve $3\mathbb{Z}$. Takýmto homomorfizmom je zobrazenie $f\colon \mathbb{Z} \to \mathbb{Z}_3$ dané predpisom

$$f\colon n \mapsto n \bmod 3,$$

t.j. každému prvku priradí zvyšok po delení 3.

Príklad 3.5.6. Uvažujme situáciu z príkladu 3.2.8, t.j. grupu $G = (\mathbb{R}\times\mathbb{R}, +)$ a jej podgrupu $H = \{(x, x); x \in \mathbb{R}\}$. Jednoducho možno overiť, že zobrazenie $f\colon (G, +) \to (\mathbb{R}, +)$

$$f\colon (x, y) \mapsto x - y$$

je epimorfizmus a $\operatorname{Ker} f = H$. Z toho vyplýva, že $G/H \cong (\mathbb{R}, +)$.

Príklad 3.5.7. V príklade 3.2.9 sme mali $G = \mathbb{Z}_8$ a $H = 4\mathbb{Z}_8 = \{0, 4\}$. V tomto prípade máme surjektívny homomorfizmus $f\colon \mathbb{Z}_8 \to \mathbb{Z}_4$

$$f\colon n \mapsto n \bmod 4$$

a faktorová grupa G/H je izomorfná s grupou $(\mathbb{Z}_4, \oplus)$.

Príklad 3.5.8. V príklade 3.3.5 sme videli, že jedinou normálnou podgrupou grupy S_3 je podgrupa A_3 všetkých nepárnych permutácií. Zobrazenie $f\colon S_3 \to \mathbb{Z}_2$, ktoré priradí párnym permutáciam 0 a nepárnym 1 je surjektívny homomorfizmus taký, že $\operatorname{Ker} f = A_3$.

Dôkaz nasledujúceho tvrdenia je veľmi podobný tej časti dôkazu vety 3.5.2, v ktorej sme dokazovali, že ide o homomorfizmus.

Lema 3.5.9. *Nech $f\colon G \to G'$ je grupový homomorfizmus. Nech H je normálna podgrupa G taká, že $H \subseteq \operatorname{Ker} f$. Potom zobrazenie $\varphi\colon G/H \to G'$ dané predpisom*

$$\varphi(aH) = f(a)$$

je dobre definované a je to grupový homomorfizmus.

Navyše, ak f je epimorfizmus, tak aj φ je epimorfizmus.

Dôkaz. Najprv ukážeme, že φ je dobre definované. Ak máme 2 rôznych reprezentantov tej istej triedy, t.j. $aH = bH$, tak platí $b^{-1}a \in H \subseteq \operatorname{Ker} f$. To znamená, že $f(b^{-1}a) = e'$, a teda

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

Overíme teraz, že φ je homomorfizmus.

$$\varphi(abH) = f(ab) = f(a)f(b) = \varphi(aH)\varphi(bH).$$

Ak f je surjektívne zobrazenie, tak pre každé $b \in G'$ existuje $a \in G$ také, že $f(a) = b$. Potom platí $\varphi(aH) = b$, teda aH je vzor b v zobrazení φ. Z toho vyplýva, že aj zobrazenie φ je surjektívne. □

Ak túto lemu použijeme na kanonický homomorfizmus $\varphi\colon G \to G/K$, dostaneme:

Dôsledok 3.5.10. *Ak H, K sú normálne podgrupy grupy G a $H \subseteq K$, tak zobrazenie* $f\colon G/H \to G/K$

$$f\colon aH \mapsto aK$$

je surjektívny homomorfizmus.

Pomocou predchádzajúcej vety môžeme odvodiť výsledok, ktorý pripomína „krátenie“ pre faktorové grupy. Dôležité je uvedomiť si, že ak H, K sú normálne podgrupy G a $H \subseteq K$, tak H je normálna podgrupa K. Navyše K/H je podmnožina G/H tvorená triedami aH pre ktoré $a \in K$.

Veta 3.5.11 (Tretia veta o izomorfizme). *Ak H, K sú normálne podgrupy G, pričom $H \subseteq K \subseteq G$, tak K/H je normálna podgrupa G/H a platí*

$$G/K \cong (G/H)/(K/H).$$

Dôkaz. Pretože $H \subseteq K$, dostávame z dôsledku 3.5.10, že zobrazenie $\psi\colon G/H \to G/K$ určené predpisom

$$\psi\colon aH \mapsto aK$$

je surjektívny homomorfizmus. Potom podľa vety 3.5.2 je grupa G/K izomorfná s grupou $(G/H)/(\operatorname{Ker}\psi)$. Pokúsme sa teda určiť jadro homomorfizmu ψ.

Do $\operatorname{Ker}\psi$ patria tie ľavé triedy aH grupy G/H, ktoré sa zobrazia na neutrálny prvok grupy G/K, čiže na $eK = K$. Teda $aH \in \operatorname{Ker}\psi$ platí práve vtedy, keď $aK = K$, čiže $a \in K$. To znamená, že $\operatorname{Ker}\psi = K/H$ (keďže $\operatorname{Ker}\psi$ pozostáva práve z tých ľavých tried aH, pre ktoré $a \in K$). Vďaka tomu vidíme z vety o izomorfizme, že $K/H = \operatorname{Ker}\psi$ je normálna podgrupa a

$$(G/H)/(K/H) \cong G/K.$$

□

Dôkaz predchádzajúcej vety opäť ilustruje užitočnosť vety 3.5.2. Keby sme namiesto použitia tejto vety robili priamy dôkaz, museli by sme pracovať s prvkami grupy $(G/H)/(K/H)$, čo sú triedy rozkladu faktorovej grupy G/H podľa jej podgrupy K/H, ktorých reprezentantmi sú opäť triedy rozkladu, tentokrát rozkladu K podľa H. Zdá sa, že prístup využívajúci vetu o izomorfizme je prehľadnejší.

Ukážeme si ešte jeden výsledok o faktorových grupách.

Veta 3.5.12. *Nech G je grupa, H je normálna podgrupa G a S je podgrupa G. Potom množina SN tvorí podgrupu grupy G, N je normálna podgrupa SN, $S \cap N$ je normálna podgrupa S a platí*

$$S/(S \cap N) \cong SN/N.$$

Dôkaz. Najprv overme, že $SN = \{ab; a \in S, b \in N\}$ je podgrupa G. Z toho, že N je normálna, máme $gN = Ng$ pre každé $g \in G$, teda pre ľubovoľné $g \in G$ a $n \in N$ existuje $n' \in \mathbb{N}$ také, že $gn = n'g$. Pomocou tejto vlastnosti už ľahko overíme kritérium podgrupy.

Ak máme 2 prvky z SN tvaru a_1b_1, a_2b_2, kde $a_{1,2} \in S$ a $b_{1,2} \in S$, tak ich súčin môžeme vyjadriť ako

$$a_1b_1a_2b_2 = a_1a_2b_1'b_2$$

pre nejaké $b_1' \in N$. Keďže $a_1a_2 \in S$ a $b_1'b_2 \in N$, vidíme, že uvedený súčin patrí do SN.

Ak máme prvok z SN tvaru ab, pričom $a \in S$, $b \in N$, tak tento prvok môžeme prepísať ako $b'a$ pre vhodné $b \in N$. Potom inverzný prvok

$$(b'a)^{-1} = a^{-1}b'^{-1}$$

je opäť z SN.

Z toho, že $N \subseteq SN$ dostaneme, že N je podgrupa SN. Fakt, že $N \triangleleft SN$, t.j. ide o normálnu podgrupu, overíme použitím podmienky (vi) z vety 3.3.2. Skutočne, pre ľubovoľné $a \in S$, $b \in N$ máme

$$(ab)N(ab)^{-1} = (ab)N(b^{-1}a^{-1}) = a(bNb^{-1})a^{-1} = aNa^{-1} = N.$$

Na dôkaz ostatných častí tvrdenia použijeme kanonický homomorfizmus

$$f\colon a \mapsto aN,$$
$$f\colon G \to G/N.$$

Aj jeho zúženie $f|_S\colon S \to G/N$ na množinu S je homomorfizmus. Pokúsme sa zistiť, čomu sa rovná jeho jadro.

Máme

$$\operatorname{Ker} f|_S = \{a \in S; aN = N\} = \{a \in S; a \in N\} = S \cap N.$$

Podľa vety o izomorfizme je $S \cap N$ normálna podgrupa S a platí

$$S/(S \cap N) \cong \operatorname{Im} f|_S.$$

Stačí nám už teda len dokázať, že $\operatorname{Im} f|_S = SN/N$.

Množina $\operatorname{Im} f|_S$ pozostáva práve z tých tried aN, pre ktoré $a \in S$;

$$\operatorname{Im} f|_S = \{aN; a \in S\}.$$

Súčasne však máme

$$SN/N = \{abN; a \in S, b \in N\} = \{aN; a \in S\},$$

teda skutočne platí rovnosť $\operatorname{Im} f|_S = SN/N$. □

Videli sme, že normálne podgrupy zodpovedajú homomorfizmom – zobrazeniam, ktoré rešpektujú grupovú operáciu. V úlohách 3.5.11 a 3.5.12 môžeme vidieť, ako súvisia s reláciami, ktoré rešpektujú grupovú operáciu. Takéto relácie nazývame kongruenciami.

Definícia 3.5.13. Nech $(G, *)$ je grupa. Relácia ekvivalencie R na množine G sa nazýva *kongruencia,* ak platí

$$(a_1, b_1) \in R, (a_2, b_2) \in R \quad \Rightarrow \quad (a_1 * b_1, a_2 * b_2) \in R.$$

Napríklad všetky relácie ekvivalencie z úlohy 3.1.7 sú kongruencie.

Cvičenia

Úloha 3.5.1. Overte, či H je normálna podgrupa grupy G a opíšte faktorovú grupu G/H (aké má triedy, vybrať z každej triedy práve jedného reprezentanta, zistiť, či je izomorfná s nejakou známou grupou).

a) $G = (\mathbb{R} \times \mathbb{R}, +)$, $H = \{(x, y); x + 2y = 0\}$
b) $G = (\mathbb{R} \times \mathbb{R}, +)$, $H = \{(x, 3x); x \in \mathbb{R}\}$
c) $G = (\mathbb{C}, +)$, $H = \mathbb{R}$
d) $G = (\mathbb{C} \setminus \{0\}, \cdot)$, $H = \mathbb{R} \setminus \{0\}$
e) $G = (\mathbb{C} \setminus \{0\}, \cdot)$, $H = \mathbb{R}^+ = \{x \in \mathbb{R}; x > 0\}$
f) $G = (\mathbb{Z}, +)$, $H = 4\mathbb{Z} = \{4z; z \in \mathbb{Z}\}$

g) $G = (\mathbb{Z}_4 \times \mathbb{Z}_6, +)$, $H = [(2,2)]$
h) $G = (\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}, +)$, $H = \{(n,m,0); n,m \in \mathbb{Z}\}$
i) $G = (\{c \in \mathbb{C}; c^{12} = 1\}, \cdot)$, $H = \{c \in \mathbb{C}; c^4 = 1\}$
j) $G = (S_n, \circ)$, $H = A_n$
k) $G = (\mathbb{Z}, +)$, $H = n\mathbb{Z}$
l) $G = (\mathbb{C} \setminus \{0\}, \cdot)$, $H = \{c \in \mathbb{C}; c^6 \in \mathbb{R} \setminus \{0\}\}$
m) $G = (\mathbb{C} \setminus \{0\}, \cdot)$, $H = \{c \in \mathbb{C}; c^n \in \mathbb{R} \setminus \{0\}\}$

Úloha 3.5.2. Zistite, či dané grupy sú izomorfné. V celom cvičení budeme ako S označovať grupu $(\{c \in \mathbb{C}; |c| = 1\}, \cdot)$ (prípadne množinu prvkov tejto grupy) a $C_n = (\{c \in \mathbb{C}; c^n = 1\}, \cdot)$
a) $(\mathbb{C} \setminus \{0\}, \cdot)/\{c \in \mathbb{C}; c^n \in \mathbb{R} \setminus \{0\}\}$, $(\mathbb{C} \setminus \{0\}, \cdot)/\mathbb{R}^+$ (pod $\mathbb{R}^+$ tu myslíme kladné reálne čísla, čiže $0 \notin \mathbb{R}^+$), S
b) $(\mathbb{R}, +)/\mathbb{Z}$, $S/\mathbb{C}_n$, S
c) $(C \setminus \{0\}, \cdot)$, $(C \setminus \{0\}, \cdot)/C_n$
d) $(\{c \in \mathbb{C}; c^n \in \mathbb{R} \setminus \{0\}\}, \cdot)/\mathbb{R}^+$, C_n
e) $(\{c \in \mathbb{C}; c^n \in \mathbb{R} \setminus \{0\}\}, \cdot)/C_n$, $\mathbb{R}^+$
f) C_{12}/C_4, $\mathbb{Z}_3$
g) $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)/(\mathbb{Z}_2 \times \{0\})$, $\mathbb{Z}_3$
h) $S_3/[(123)]$, $(\mathbb{Z}_2, +)$

Úloha 3.5.3. Nech G je grupa všetkých regulárnych matíc typu $n \times n$ (s operáciou násobenia matíc). Ako H označme tie z nich, ktoré majú determinant $|A| = 1$. Dokážte, že H je invariantná podgrupa G! Vedeli by ste nájsť grupu izomorfnú s G/H?

Úloha 3.5.4. Nech $S = \{z \in \mathbb{C}; |z| = 1\}$ (jednotková kružnica v komplexnej rovine). Ukážte, že zobrazenie $\varphi\colon \mathbb{R} \to \mathbb{C}$ definované ako $\varphi(x) = e^{2\pi x i} = \cos 2\pi x + i \sin 2\pi x$ je surjektívny homomorfizmus. Nájdite $\operatorname{Ker}\varphi$. Aká faktorová grupa je potom izomorfná s kružnicou?

Úloha 3.5.5. Je podgrupa $\{id, (12)(34), (13)(24), (14)(23)\}$ normálna podgrupa A_4?

Úloha 3.5.6. Ukážte, že $\mathbb{Q}/\mathbb{Z}$ (obe grupy berieme so sčitovaním) je nekonečná grupa, v ktorej má každý prvok konečný rád.

Úloha 3.5.7. Nech $\varphi\colon G \to G/H$ je kanonický homomorfizmus a $X \subset G$. Dokážte: Ak $\varphi[X]$ generuje G/H, tak $H \cup X$ generuje G.

Úloha 3.5.8. Ukážte na príklade, že ak H je normálna podgrupa G, tak G nemusí obsahovať podgrupu izomorfnú s G/H.

Úloha 3.5.9. Nech G je množina všetkých matíc tvaru $\left(\begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix}\right)$, kde $a, b \in \mathbb{R}$ a $a \neq 0$. Dokážte:
a) G s násobením matíc tvorí grupu.
b) Zobrazenia $f\colon G \to (\mathbb{R}, \cdot)$ a $g\colon G \to (\mathbb{R}, +)$ dané ako $f\colon \left(\begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix}\right) \mapsto a$; $g\colon \left(\begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix}\right) \mapsto b$ sú homomorfizmy.
c) Izomorfizmus akých grúp dostatneme podľa časti b) na základe vety o izomorfizme?
d) Popíšte lineárne zobrazenia zodpovedajúce maticiam z $\operatorname{Ker} f$, $\operatorname{Ker} g$ a G.

Úloha 3.5.10. V úlohe 3.3.9 sme videli, že centrum grupy G, t.j. množina $Z(G) = \{g \in G; (\forall h \in G) gh = hg\}$, je normálna podgrupa G. Dokážte, že faktorová grupa $G/Z(G)$ je izomorfná s grupou $\operatorname{VAut} G$ všetkých vnútorných automorfizmov grupy G (pozri úlohu 2.6.1).

Úloha 3.5.11$^+$. Nech G je grupa.
a) Pre normálnu podgrupu H definujme reláciu R ako $aRb \Leftrightarrow a^{-1}b \in H$. Dokážte, že táto

relácia je kongruencia (definícia 3.5.13). Dokážte, že rozklad zodpovedajúci relácii R je práve rozklad G podľa podgrupy H.
b) Dokážte, že ak R je kongruencia na G, tak $[e]_R$ je normálna podgrupa G. Navyše, rozklad určený reláciou ekvivalencie R je práve rozklad G podľa tejto podgrupy.
c) Overte, že priradenia medzi normálnymi podgrupami G a kongrueniami na G z predchádzajúcich častí úlohy sú navzájom inverzné.

Úloha 3.5.12$^+$. Nech $(G, *)$ je grupa.
a) Ak $f\colon G \to H$ je homomorfizmus, tak relácia R na množine G daná predpisom $xRy \Leftrightarrow f(x) = f(y)$ je kongruencia (pozri úlohu 3.1.3).
b) Ak R je kongruencia na G, tak na množine G/R tried ekvivalencie predpis $[a] * [b] = [a * b]$ dobre definuje binárnu operáciu a G/R s touto binárnou operáciou tvorí grupu. Navyše, zobrazenie $a \mapsto [a]$ je surjektívny homomorfizmus z G do G/R a jeho jadro je $[e]$.

3.6 Komutátor a komutant*

Skúsme sa pozrieť na problém, kedy je faktorová grupa komutatívna. Ľahko dostaneme nasledujúce kritérium.

Lema 3.6.1. *Ak G je grupa a H je jej normálna podgrupa, tak G/H je komutatívna práve vtedy, keď pre ľubovoľné $a, b \in G$ platí*

$$a^{-1}b^{-1}ab \in H.$$

Dôkaz. Grupa G/H je normálna práve vtedy, keď pre ľubovoľné $a, b \in G$ platí $(ab)H = (ba)H$. Podľa lemy 3.2.5 je to ekvivalentné s podmienkou

$$(ba)^{-1}ab = a^{-1}b^{-1}ab \in H.$$

□

Definícia 3.6.2. Nech G je grupa. Pre $a, b \in G$ nazývame prvok

$$[a, b] = a^{-1}b^{-1}ab$$

sa *komutátor* prvkov a a b.

Podgrupa generovaná všetkými komutátormi sa nazýva *komutant* grupy G a označuje sa ako $[G, G]$.

Poznamenajme, že množina všetkých komutátorov ešte nemusí tvoriť podgrupu, hoci nie je celkom ľahké nájsť kontrapríklad. (Najmenší možný kontrapríklad je 96-prvková grupa [Rot, Exercise 2.43]).

Ukážeme, že komutant je vždy normálna podgrupa. Na to sa nám bude hodiť explicitný popis podgrupy generovanej danou množinou.

Lema 3.6.3. *Ak G je grupa a $A \subseteq G$, tak podgrupa $[A]$ generovaná množinou A pozostáva práve z prvkov tvaru*

$$a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n}$$

pre $n \in \mathbb{N}$, $a_i \in A$ a $\varepsilon_i \in \{\pm 1\}$. (V prípade, že $n = 0$, pod týmto súčinom chápeme neutrálny prvok.)

Dôkaz. □

Tvrdenie 3.6.4. *Nech G je grupa. Jej podgrupa $[G, G]$ je normálna.*

Dôkaz. □

3.7 Faktorové vektorové priestory *

Keď sme zvládli faktorové grupy, môžeme si uvedomiť, že podobná konštrukcia bude fungovať aj pre vektorové priestory.

Definícia 3.7.1. Nech $(V, +, \cdot)$ je vektorový priestor nad poľom F a S je jeho podpriestor. Triedy rozkladu grupy $(V, +)$ podľa podgrupy S budeme v tomto prípade označovať ako $\vec{\alpha}+S$ pre $\vec{\alpha} \in V$. Potom $(V/S, +)$ s operáciou $(\vec{\alpha} + S) + (\vec{\beta} + S) = (\vec{\alpha} + \vec{\beta}) + S$ tvorí komutatívnu grupu. Ukážeme, že aj násobenie dané predpisom

$$c.(\vec{\alpha} + S) = (c.\vec{\alpha}) + S$$

pre $c \in F$ a $\vec{\alpha} \in V$ je dobre definované a V/S spolu s týmito operáciami tvorí vektorový priestor nad poľom F. Tento vektorový priestor nazývame *faktorový vektorový priestor* V podľa S.

Dôkazy faktov, ktoré sme spomínali v predchádzajúcej definícii sú pomerne jednoduché a mohli by sme ich ponechať ako cvičenie, pre úplnosť ich však aspoň naznačíme.

Dôkaz. Operácia $\cdot : F \times V/S \to V/S$ *je dobre definovaná.* Ak $\vec{\alpha} + S = \vec{\beta} + S$, tak $\vec{\alpha} - \vec{\beta} \in S$. Pretože S je podpriestor, platí potom aj $c(\vec{\alpha} - \vec{\beta}) = c\vec{\alpha} - c\vec{\beta} \in S$, čiže

$$c\vec{\alpha} + S = c\vec{\beta} + S.$$

V/S s uvedenými operáciami tvorí vektorový priestor nad F. Vieme, že V/S je komutatívna grupa.

Z ostatných podmienok vystupujúcich v definícii vektorového priestoru overme na ukážku jednu, všetky ostatné sa overia veľmi podobne.

Nech napríklad $\vec{\alpha}, \vec{\beta} \in V$ a $c \in F$. Potom

$$c[(\vec{\alpha} + S) + (\vec{\beta} + S)] = c[(\vec{\alpha} + \vec{\beta}) + S] = c(\vec{\alpha} + \vec{\beta}) + S = (c\vec{\alpha} + c\vec{\beta}) + S = (c\vec{\alpha} + S) + (c\vec{\beta} + S).$$

□

Príklad 3.4.3, t.j. faktorová grupa grupy $G = (\mathbb{R} \times \mathbb{R}, +)$ podľa podgrupy $H = \{(x, x); x \in \mathbb{R}\}$ je súčasne aj príkladom faktorového vektorového priestoru (keďže G je súčasne vektorový priestor a H je jeho podpriestor).

Kapitola 4

Okruhy a polia

4.1 Okruhy (a súvisiace pojmy)

Definícia 4.1.1. Trojicu $(R, +, \cdot)$ nazývame *okruh* ak $+$ a $\cdot$ sú binárne operácie na množine R také, že

(i) $(R, +)$ je komutatívna grupa,

(ii) operácia $\cdot$ je asociatívna[1]

$$(\forall a, b, c \in R) \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(iii) pre operácie $+$ a $\cdot$ platia *distributívne zákony*

$$(\forall a, b, c \in R) \qquad a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(\forall a, b, c \in R) \qquad (b + c) \cdot a = b \cdot a + c \cdot a$$

Neutrálny prvok operácie $+$ budeme označovať 0. Podobne ako sme to robili pre polia, inverzný prvok k prvku a vzhľadom na operáciu $+$ budeme označovať $-a$. Označenie $b - a$ bude znamenať $b + (-a)$.

Ak je navyše operácia $\cdot$ komutatívna, t.j.

$$(\forall a, b \in R) \qquad a \cdot b = b \cdot a,$$

tak $(R, +, \cdot)$ voláme *komutatívny okruh.*

Ak existuje neutrálny prvok e operácie $\cdot$ a súčasne $e \neq 0$ (ako sme sa dohodli, 0 označuje neutrálny prvok operácie $+$), tak tento neutrálny prvok označujeme 1 a hovoríme že, že $(R, +, \cdot)$ je (*komutatívny*) *okruh s jednotkou.*[2]

[1] t.j. $(R, \cdot)$ je pologrupa

[2] Prípad, že neutrálny prvok oboch operácií je ten istý, ktorý sme z tejto definície vylúčili, nastane iba pre jednoprvkový okruh $\{0\}$.
Z minulého semestra vieme, že jednotka v okruhu musí byť jednoznačne určená – tvrdenie I-3.1.7.
V niektorých učebniciach sa v definícii okruhu s jednotkou nepožaduje podmienka $1 \neq 0$, potom sa však táto podmienka objaví ako jeden z predpokladov vo väčšine viet, ktoré o okruhoch s jednotkou dokazujeme, preto sme tu zvolili túto formu definície.

Poznámka 4.1.2. Označenie pre operáciu $\cdot$ obvykle vynechávame, čiže namiesto $a \cdot b$ častejšie budeme používať označenie ab.

Takisto, keď budú uvažované binárne operácie jasné z kontextu, budeme písať stručne R namiesto $(R, +, \cdot)$.

Pri grupách sme spomínali aditívny a multiplikatívny zápis – v okruhu vždy pre operáciu $+$ používame aditívny a pre operáciu $\cdot$ multiplikatívny zápis. Teda použitie operácie viackrát na ten istý prvok označíme ako $n \times a$ pre operáciu $+$ a a^n pre operáciu $\cdot$ (kde $n \in \mathbb{N} \setminus \{0\}$).

Príklad 4.1.3. $(\mathbb{Z}, +, \cdot)$ – celé čísla s obvyklým sčitovaním a násobením tvoria komutatívny okruh s jednotkou.
$(\mathbb{Z}_n, \oplus, \odot)$ – množina $\mathbb{Z}_n = 0, 1, \ldots, n-1$ so sčitovaním modulo n tvorí komutatívny okruh s jednotkou.

Príklad 4.1.4. Príklad komutatívneho okruhu, ktorý nemá jednotku: $(2\mathbb{Z}, +, \cdot)$.

Dôkaz nasledujúcej lemy ponechávame ako cvičenie, keďže je veľmi podobný dôkazom, ktoré sme robili pre polia.

Lema 4.1.5. *Nech $(R, +, \cdot)$ je okruh, $a, b \in R$. Potom platí*

$$0a = a0 = 0$$
$$a(-b) = -ab = (-a)b$$
$$(-a)(-b) = ab$$

Príklad 4.1.6. Na množine $\mathbb{Z} \times \mathbb{Z}$ definujeme operácie $+$ a $\cdot$ ako sčitovanie a násobenie po zložkách, t.j.

$$(a, b) + (a', b') = (a + a', b + b'),$$
$$(a, b)(a', b') = (aa', bb').$$

Potom $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ je komutatívny okruh s jednotkou. (Jednotka je dvojica $(1, 1)$, nula je dvojica $(0, 0) = 0$.)

Všimnime si, že $(1, 0) \cdot (0, 1) = (0, 0)$, teda v okruhu môže byť súčin nenulových prvkov rovný nule.

Predchádzajúci príklad možno jednoducho zovšeobecniť:

Príklad 4.1.7. Ak $(R_1, +, \cdot)$ a $(R_2, +, \cdot)$ sú okruhy, tak $R_1 \times R_2$ tvorí s operáciami definovanými po zložkách

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2)$$

tiež okruh.

Podobne, ak pre každé $i \in I$ je $(R_i, +, \cdot)$ okruh, tak aj množina[3] $\prod_{i \in I} R_i = \{f \colon I \to \bigcup_{i \in I} R_i \mid (\forall i \in I)(f(i) \in R_i)\}$ tvorí s operáciami definovanými po zložkách

$$(f + g)(i) = f(i) + g(i)$$
$$(f \cdot g)(i) = f(i) \cdot g(i)$$

[3]Takto sa definuje karteziánsky súčin pre ľubovoľný (teda nie len konečný) počet množín. V prípade, že ste to nemali na žiadnom inom predmete, bude asi jednoduchšie, keď túto definíciu budete čítať tak, ako keby $R_i = R$ pre všetky $i \in I$ – pozri poznámku na konci tohoto príkladu.

okruh.

V prípade, že všetky použité okruhy sú rovnaké, t.j. $R_i = R$ pre každé $i \in I$, budeme používať označenie R^I. Okruh R^I pozostáva zo všetkých zobrazení z I do R.

Príklad 4.1.8. Dôležitý príklad okruhu tvoria matice $M_{n,n}(F)$ typu $n \times n$ nad poľom F spolu s násobením matíc. To, že sčitovanie a násobenie matíc spĺňajú podmienky z definície okruhu, sme ukázali v minulom semestri. Tento okruh má jednotku, je ňou jednotková matica I. Tento okruh nie je komutatívny.

Definícia 4.1.9. Nech $(R, +, \cdot)$ je okruh a $S \subseteq R$ je neprázdna podmnožina množiny R. Hovoríme, že S je *podokruh* okruhu R, ak pre ľubovoľné $a, b \in S$ platí $a - b \in S$, $ab \in S$.

$$a, b \in S \qquad \Rightarrow \qquad a - b \in S, ab \in S$$

Inými slovami, podokruh je podgrupa grupy $(R, +)$, ktorá je navyše uzavretá vzhľadom na násobenie.

Pomerne jednoducho sa dá overiť, že platí

Tvrdenie 4.1.10. *Nech $(R, +, \cdot)$ je okruh a $S \subseteq R$, $S \neq \emptyset$. Množina S je podokruh okruhu $(R, +, \cdot)$ práve vtedy, keď S s operáciami $+$ a $\cdot$ zúženými na množinu S tvorí okruh.*

Príklad 4.1.11. $2\mathbb{Z}$ je podokruh $(\mathbb{Z}, +, \cdot)$.

$\mathbb{N}$ nie je podokruh $(\mathbb{Z}, +, \cdot)$ (je uzavretý na násobenie a súčet, nie však na rozdiel).

Príklad 4.1.12. Uvažujme zobrazenia z uzavretého intervalu $\langle 0, 1\rangle$ do $\mathbb{R}$. Z matematickej analýzy vieme, že rozdiel a súčin spojitých funkcií je opäť spojitá funkcia. Vďaka tomu spojité funkcie $f\colon \langle 0, 1\rangle \to \mathbb{R}$ tvoria, so sčitovaním a násobením funkcií po bodoch, podokruh okruhu $\mathbb{R}^{\langle 0,1\rangle}$. Tento okruh označujeme $C(0, 1)$.

Definícia 4.1.13. Ak v okruhu $(R, +, \cdot)$ neexistujú prvky a, b také, že $a, b \neq 0$ a

$$ab = 0,$$

tak hovoríme, že R je *okruh bez deliteľov nuly* (alebo tiež, že R nemá delitele nuly).

Ak $(R, +, \cdot)$ je komutatívny okruh s jednotkou bez deliteľov nuly, hovoríme, že $(R, +, \cdot)$ je *obor integrity.*

Fakt, že R je okruh bez deliteľov nuly môžeme vyjadriť pomocou nasledovnej implikácie[4]

$$(\forall a, b \in R) \qquad ab = 0 \Rightarrow a = 0 \vee b = 0.$$

Príklad okruhu, ktorý nie je oborom integrity, je okruh $\mathbb{Z} \times \mathbb{Z}$ z príkladu 4.1.6. Dokonca ľubovoľný okruh tvaru $R_1 \times R_2$ (pozri príklad 4.1.7), kde ani jeden z okruhov R_1, R_2 nie je nulový, nám dáva takýto príklad.

Ľahko sa overí, že v okruhu bez deliteľov nuly môžeme krátiť nenulovými prvkami:

Tvrdenie 4.1.14. *Nech R je okruh bez deliteľov 0 a $a, b, c \in R$. Ak $a \neq 0$ a platí $ab = ac$, tak $b = c$.*

Dôkaz. Z rovnosti $ab = ac$ dostaneme pomocou distributívnosti $a(b - c) = 0$. Keďže $a \neq 0$, máme $b - c = 0$, a teda $b = c$. □

[4] Je to negácia výroku $(\exists a, b \in \mathbb{R})\ \ ab = 0 \wedge (a \neq 0 \wedge b \neq 0)$.

Definícia 4.1.15. Okruh R s jednotkou nazývame *telesom,* ak ku každému nenulovému prvku $a \in R \setminus \{0\}$ existuje inverzný prvok vzhľadom na násobenie, t.j.

$$(\forall a \in R \setminus \{0\})(\exists b \in R) \qquad ab = ba = 1$$

Komutatívne teleso voláme *pole.*

Tvrdenie 4.1.16. *Každé teleso je okruh bez deliteľov nuly.*
Každé pole je oborom integrity.

Dôkaz. Nech R je teleso a pre $a, b \in R$ platí $ab = 0$. Predpokladajme, že $a \neq 0$. Potom existuje $c \in R$ taký, že $ca = 1$. Z toho dostaneme

$$b = 1b = cab = c0 = 0,$$

čiže $b = 0$. Podobne, z predpokladu $b \neq 0$ by sme dostali $a = 0$.
Druhá časť tvrdenia ľahko vyplýva z prvej časti. □

Definícia 4.1.15 vlastne hovorí, že ak $(R, +, \cdot)$ je okruh a navyše $(R \setminus \{0\}, \cdot)$ je grupa, ide o teleso. Ak je to komutatívna grupa, ide o pole. Táto definícia poľa je teda ekvivalentná s definíciou I-3.3.1, ktorú sme uviedli v minulom semestri. Z minulého poznáme veľa príkladov polí – $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ s obvyklým sčitovaním a násobením, $(\mathbb{Z}_p, \oplus, \odot)$ pre ľubovoľné prvočíslo p.

Príkladom telesa, ktoré nie je poľom (t.j. nekomutatívneho telesa) sú kvaternióny. Viac sa o nich môžete dozvedieť v [KGGS, Kapitola 4.7].

Cvičenia

Úloha 4.1.1. Zistite (a svoje tvrdenie zdôvodnite) ktoré z uvedených vlastností sa z okruhu R prenesú na uvedené konštrukcie:

	$R \times R$	R/I	R^I	podokruh
pole				
obor integrity				
nemá delitele nuly				
má delitele nuly				
komutatívny okruh				
okruh s jednotkou				

Úloha 4.1.2. Je každý podokruh poľa okruh bez deliteľov nuly? Je každý podokruh poľa obsahujúci 1 oborom integrity?

Úloha 4.1.3. Zistite, či nasledujúce množiny tvoria podokruhy poľa $(\mathbb{C}, +, \cdot)$. Zistite, ktoré z nich sú navyše poliami.
a) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$
b) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$

Úloha 4.1.4. Zistite, či nasledujúce množiny tvoria podokruhy poľa $(\mathbb{Q}, +, \cdot)$. Sú niektoré z nich polia?
a) Všetky zlomky také, že v základnom tvare je menovateľ nepárne číslo.
b) Všetky zlomky také, že v základnom tvare je menovateľ párne číslo.
c) Všetky zlomky také, že v základnom tvare je čitateľ nepárne číslo.
d) Všetky zlomky také, že v základnom tvare je čitateľ párne číslo.
e) Všetky druhé mocniny racionálnych čísel.

Úloha 4.1.5. Dokážte: Ak R je obor integrity a $x^2 = 1$, tak $x = 1$ alebo $x = -1$.

Úloha 4.1.6. Ak R je okruh bez deliteľov nuly a $ab = 1$, tak aj $ba = 1$.

Úloha 4.1.7. Dokážte, že $\{(r, r); r \in R\}$ je podokruh okruhu $R \times R$. Je tento podokruh izomorfný s okruhom R?

4.2 Homomorfizmy, ideály a faktorové okruhy

Definícia 4.2.1. Nech $(R, +, \cdot)$, $(S, +, \cdot)$ sú okruhy. Zobrazenie $f\colon R \to S$ nazývame *homomorfizmus,* ak platí

$$f(a + b) = f(a) + f(b),$$
$$f(ab) = f(a)f(b).$$

Surjektívny homomorfizmus nazývame *epimorfizmus,* injektívny homomorfizmus nazývame *monomorfizmus* a bijektívny homomorfizmus nazývame *izomorfizmus.* Ak existuje izomorfizmus medzi $(R, +, \cdot)$ a $(S, +, \cdot)$, hovoríme, že okruhy R a S sú izomorfné a píšeme $R \cong S$.

Pretože oba tieto pojmy používame aj pre grupy, občas sa vyskytne situácia, že budeme potrebovať rozlíšiť, či hovoríme o homomorfizme (izomorfizme) grúp alebo okruhov. V takomto prípadne použijeme termín *grupový homomorfizmus* (*izomorfizmus*) alebo *okruhový homomorfizmus* (*izomorfizmus*).

Dôkaz nasledujúceho tvrdenia vynechávame – je skoro identický s dôkazom analogického tvrdenia pre grupy.

Tvrdenie 4.2.2. *Zloženie homomorfizmov je homomorfizmus. Zloženie izomorfizmov je izomorfizmus.*

Príklad 4.2.3. Jednoduché príklady homomorfizmov:
$f\colon \mathbb{Z} \to \mathbb{Z}_n$, $f\colon k \mapsto k \bmod n$
$g\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $g\colon (a, b) \mapsto a$
$h\colon \mathbb{C} \to \mathbb{C}$, $h\colon a + bi \mapsto a - bi$

Opäť, podobne ako pri grupách, existencia izomorfizmu medzi dvoma okruhmi znamená, že tieto okruhy sú z hľadiska teórie okruhov rovnaké – nie sú rozlíšiteľné pomocou pojmov definovaných pre ľubovoľné okruhy. (Obe operácie pracujú rovnako, len prvky sú inak pomenované a izomorfizmus je bijektívne zobrazenie, ktoré poskytuje „slovník“ na preklad medzi týmito dvoma pomenovaniami.)

Túto myšlienku je možné použiť aj keď chceme ukázať, že nejaká množina s danými binárnymi operáciami tvorí okruh – nájdeme bijekciu medzi touto množinou a nejakým známym okruhom, ktorá zachováva operácie.

Príklad 4.2.4. Uvažujme podmnožinu S okruhu $M_{2,2}(\mathbb{R})$ tvorenú maticami tvaru

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

kde $a, b \in \mathbb{R}$.

Overme najprv, že ide o podokruh. Zrejme rozdiel 2 matíc takéhoto tvaru má opäť uvedený tvar. Pre súčin máme

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}, \tag{4.1}$$

čiže súčin matíc z S opäť patrí do S.

Definujme teraz zobrazenie $f\colon S \to \mathbb{C}$ predpisom

$$f\colon \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi.$$

Z rovnosti (4.1) vidíme, že pre $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in S$ máme

$$f(AB) = (ac - bd) + (ad + bc)i = (a + bi)(c + di) = f(A)f(B).$$

Overenie, že f zachováva súčty je jednoduché, takže ide o okruhový homomorfizmus.

Navyše, f je bijekcia, je to teda izomorfizmus medzi okruhom A a poľom komplexných čísel.

Toto zobrazenie by sme mohli použiť napríklad na dôkaz, že komplexné čísla tvoria okruh; alebo tiež na dôkaz, že A je podokruh (ak by sme už mali dokázané, že $\mathbb{C}$ je okruh; t.j. stačilo by nám overiť, že sa zachovávajú operácie). Vďaka tomu, že sme našli izomorfizmus medzi uvedenými dvoma okruhmi, hneď vieme, že A je pole – aj bez toho, že by sme to museli overovať priamym výpočtom.

Môžeme si položiť otázku, či sa na túto maticovú reprezentáciu komplexných čísel dá príjsť aj nejakým priamočiarym spôsobom, bez toho, aby nám ho niekto povedal, alebo aby sme ho „uhádli“.

Skúsme sa, pre dané komplexné číslo $z = a + bi$ pozrieť na zobrazenie $f_z\colon \mathbb{C} \to \mathbb{C}$, $f_z\colon x \mapsto zx$ (toto je presne zobrazenie, ktoré sme priradili komplexnému číslu v Cayleyho vete 2.6.8, pozri tiež príklad 2.6.11). Ak komplexné číslo z vyjadríme v goniometrickom tvare ako $z = r(\cos\varphi + i\sin\varphi)$ tak z Moivrovej vety vieme, že násobenie číslom z znamená otočenie bodu (komplexné čísla chápeme ako body v rovine) okolo bodu 0 o uhol φ a potom jeho r-násobné zväčšenie.

Obidve tieto zobrazenia – otočenie aj natiahnutie – sú lineárne zobrazenia. Skúsme sa pozrieť na maticu takéhoto zobrazenia – nato stačí vedieť kam sa zobrazia vektory $(1, 0)$ a $(0, 1)$. Vektor $(1, 0)$ sa zobrazí otočením o uhol φ na $(\cos\varphi, \sin\varphi)$ a vektor $(1, 0)$ na $(-\sin\varphi, \cos\varphi)$. To znamená, že otočeniu zodpovedá matica

$$\begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}$$

Ak ešte použijeme natiahnutie s koeficientom r, dostaneme maticu

$$\begin{pmatrix} r\cos\varphi & r\sin\varphi \\ -r\sin\varphi & r\cos\varphi \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

čiže presne tú, ktorú sme použili v našom izomorfizme.

Príklad 4.2.5. Uvažujme lineárne zobrazenia z F^n do F^n. Označme množinu všetkých takýchto zobrazení A. Ukážeme, že $(A, +, \circ)$ je okruh s jednotkou ($+$ znamená obvyklé sčitovanie funkcií a $\circ$) je skladanie funkcií.

Namiesto toho, aby sme priamo overovali definíciu okruhu, uvažujme zobrazenie $f\colon A \to M_{n,n}(F)$, ktoré každému zobrazeniu priradí jeho maticu. Toto zobrazenie je bijektívne a navyše, keď ho berieme ako zobrazenie medzi $(A, +, \circ)$ a okruhom $(M_{n,n}(F), +, \cdot)$ rešpektuje binárne operácie (matica súčtu zobrazení je súčet matíc, matica súčinu zobrazení je súčin matíc). Keďže už vieme, že matice typu $n \times n$ tvoria okruh, vyplýva z toho, že aj $(A, +, \circ)$ je okruh. (Samozrejme, nie je ťažké overiť vlastnosti okruhu aj priamo, bez toho, aby sme si pomáhali maticami.)

Môžeme si ešte všimnúť, že podobné tvrdenie už neplatí, ak vezmeme ľubovoľné zobrazenia (t.j. nielen lineárne). Napríklad pre $F^n = \mathbb{R}^1$ a zobrazenia $f(x) = x^2$, $g(x) = x$, $h(x) = 1$ máme $f(g(x) + h(x)) = (x+1)^2 = x^2 + 2x + 1$, zatiaľčo $f(g(x)) + f(h(x)) = x^2 + 1$, čiže

$$f \circ (g + h) \neq f \circ g + f \circ h.$$

Ľahko sa dá ukázať, že jadro a obraz homomorfizmu musia byť podokruhy. Pri grupách sme videli, že nie každá podgrupa danej grupy môže byť jadrom nejakého homomorfizmu – túto vlastnosť mali len invariantné podgrupy. V prípade okruhov je zodpovedajúcim pojmom pojem ideálu.

Definícia 4.2.6. Nech R je okruh. Neprázdna podmnožina $I \subseteq R$ je *ideál* v okruhu R, ak platí

$$\begin{aligned} (\forall a, b \in I) \qquad & a - b \in I \\ (\forall a \in I)(\forall r \in R) \qquad & ar \in I, ra \in I \end{aligned}$$

t.j. ak je táto množina uzavretá vzhľadom na sčitovanie (prvkov z I) a násobenie ľubovoľným prvkom z R.

Inak povedané, ideál je taký podokruh, ktorý je uzavretý vzhľadom na násobenie všetkými prvkami z R.

Príklad 4.2.7. V každom okruhu máme ideály $\{0\}$ a R. Ideály I také, že $I \neq R$ voláme *vlastné.*

Pre ľubovoľné $k \in \mathbb{Z}$ je podmnožina $k\mathbb{Z} = \{kz; z \in \mathbb{Z}\}$ ideálom v okruhu $(\mathbb{Z}, +, \cdot)$.

V okruhu $R_1 \times R_2$ tvoria podmnožiny $R_1 \times \{0\}$ aj $\{0\} \times R_2$ ideály.

Príkladom podokruhu, ktorý nie je ideálom, je napríklad $\mathbb{Z}$ v $(\mathbb{R}, +, \cdot)$.

Často sa budú vyskytovať ideály určené jediným prvkom.

Definícia 4.2.8. Ak R je komutatívny okruh a $a \in R$, tak množina

$$(a) = \{ax; x \in R\}$$

je ideálom v R (úloha 4.2.4). Ideály takéhoto tvaru voláme *hlavné ideály.*

Nasledujúce pozorovanie je veľmi jednoduché, sformulujeme ho však do lemy, aby sme sa naň neskôr mohli odkazovať.

Lema 4.2.9. *Nech R je okruh s jednotkou a I je ideál v R. Potom $I = R$ práve vtedy, keď $1 \in I$.*

Dôkaz. Implikácia $\Rightarrow$ je úplne triviálna. Na dôkaz opačnej implikácie si stačí všimnúť, že pre ľubovoľné $c \in R$ máme

$$c = c.1$$

a ak $1 \in I$, tak aj $c.1$ patrí do ideálu I. □

Dôsledok 4.2.10. *Ak R je pole, tak jediné ideály v R sú $\{0\}$ a R.*

Dôkaz. Ak ideál I obsahuje prvok $a \neq 0$, tak k prvku a existuje inverzný prvok b, t.j. taký prvok, že $ba = 1$. Potom ale priamo z definície ideálu vyplýva, že aj $1 = ba \in I$, a teda $I = R$. □

Prvý krok na ceste k tomu, aby sme ukázali, že ideály majú pre okruhy podobnú úlohu ako normálne podgrupy pre grupy, je nasledujúca lema.

Lema 4.2.11. *Ak $\varphi\colon R \to S$ je homomorfizmus okruhov, tak jeho jadro* $\operatorname{Ker}\varphi$ *je ideál v R.*

Dôkaz. Ak $a \in \operatorname{Ker}\varphi$, znamená to, že $\varphi(a) = 0$. Potom pre ľubovoľné $x \in R$ máme

$$\varphi(ax) = \varphi(a)\varphi(x) = 0\varphi(x) = 0$$
$$\varphi(xa) = \varphi(x)\varphi(a) = \varphi(x)0 = 0$$

čiže aj $ax, xa \in \operatorname{Ker}\varphi$. □

Podobne ako pri grupách sme pre invariantné podgrupy boli schopní zadefinovať faktorovú grupu aj v tomto prípade vieme definovať faktorový okruh.

Veta 4.2.12. *Nech $(R, +, \cdot)$ je ľubovoľný okruh a I je ideál v R. Ak na prvkoch faktorovej*[5] *grupy $(R, +)$ podľa podgrupy I*

$$R/I = \{a + I; a \in R\}$$

definujeme binárnu operáciu $\cdot$ ako

$$(a + I) \cdot (b + I) = (a \cdot b) + I,$$

tak je táto binárna operácia dobre definovaná a $(R/I, +, \cdot)$ je okruh. Tento okruh voláme faktorový okruh *R podľa I.*

Ak je okruh R komutatívny, tak aj R/I je komutatívny. Ak R je okruh s jednotkou a $I \neq R$, tak $1 + I$ je jednotka faktorového okruhu R/I.

Dôkaz. Najprv ukážeme, že uvedená operácia je dobre definovaná. T.j. potrebujeme dokázať, že ak $a + I = a' + I$ a $b + I = b' + I$, tak aj $ab + I = a'b' + I$. Rovnosť $a + I = a' + I$ je však ekvivalentná s tým, že $a - a' \in I$ (lema 3.2.5), podobne druhú podmienku môžeme nahradiť podmienkou $b - b' \in I$.

Ak $a - a' \in I$, $b - b' \in I$, tak $ab - a'b' = a(b - b') + b'(a - a') \in I$. (Máme $a(b - b') \in I$, lebo $b - b' \in I$, podobne $b'(a - a') \in I$ lebo $a - a' \in I$, uvedený prvok je teda súčet dvoch prvkov z I.) Z $ab - a'b' \in I$ už vyplýva, že $ab + I = a'b' + I$.

Keď už vieme, že uvedený predpis definuje binárnu operáciu na R/I, zostáva overiť podmienky z definície okruhu. Vieme, že $(R/I, +)$ je grupa, navyše je aj komutatívna (lebo grupa R je komutatívna). Zostáva overiť asociatívnosť a distributívnosť. Máme

$$(a + I)((b + I)(c + I)) = a(bc) + I = (ab)c + I = ((a + I)(b + I))(c + I)$$
$$(a + I)((b + I) + (c + I)) = a(b + c) + I = (ab + ac) + I = (ab + I) + (ac + I)$$
$$((b + c) + I)(a + I) = (b + c)a + I = (ba + ca) + I = (ba + I) + (ca + I)$$

Úplne rovnako sa dokáže komutatívnosť R/I v prípade, že R je komutatívny a takisto, že $1 + I$ je neutrálny prvok operácie $\cdot$. Podmienka $I \neq R$ zabezpečí, že $1 = 1 - 0 \notin I$, t.j. $1 + I \neq 0 + I$ (v okruhu s jednotkou požadujeme aj aby $1 \neq 0$.) □

Aj pre faktorové okruhy platí veta o izomorfizme.

Veta 4.2.13 (Veta o izomorfizme). *Ak $f\colon R \to R'$ je homomorfizmus okruhov, tak* $\operatorname{Ker} f$ *je ideál v okruhu R a faktorový okruh $R/\operatorname{Ker} f$ je izomorfný s podokruhom* $\operatorname{Im} f$ *okruhu R'.*

[5] Grupa $(R, +)$ je komutatívna, takže jej podgrupa I je invariantná. Má teda zmysel hovoriť o faktorovej grupe.

Dôkaz. Z lemy 4.2.11 vieme, že $\operatorname{Ker} f$ je ideál.

Označme $I = \operatorname{Ker} f$. Pretože $(R, +)$ je komutatívna grupa, preto jej podgrupa I je invariantná podgrupa. Potom (podľa vety o izomorfizme pre grupy) je zobrazenie $\varphi\colon R/I \to R'$ určené predpisom

$$\varphi\colon a + I \mapsto f(a)$$

dobre definované a je to injektívny grupový homomorfizmus. Zostáva teda len dokázať, že je to aj okruhový homomorfizmus, t.j. že zachováva aj operáciu $\cdot$. To však ľahko vyplýva z toho, že f je okruhový homomorfizmus:

$$\varphi(ab + I) = f(ab) = f(a)f(b) = \varphi(a + I)\varphi(b + I).$$

□

Postupom z predchádzajúceho dôkazu sa dá ukázať, že pre každý ideál I je zobrazenie $\varphi\colon R \to R/I$ určené predpisom

$$\varphi\colon a \mapsto a + I$$

okruhový homomorfizmus. Toto zobrazenie voláme *kanonický homomorfizmus.* Pre kanonický homomorfizmus platí $I = \operatorname{Ker} \varphi$.

Videli sme, že faktorový okruh komutatívneho okruhu je opäť komutatívny okruh a (s výnimkou prípadu $I = R$) dostaneme aj z okruhu s jednotkou znovu okruh s jednotkou. Otázka, či sa na faktorový okruh prenesie aj vlastnosť „byť oborom integrity“ alebo „byť poľom“ je o čosi komplikovanejšia.

Definícia 4.2.14. Ideál I v okruhu R sa nazýva prvoideál, ak pre ľubovoľné $a, b \in R$ také, že $a \cdot b \in I$ aspoň jeden z prvkov a, b patrí do I čiže ak platí

$$a \cdot b \in I \qquad \Rightarrow \qquad a \in I \vee b \in I.$$

Môžeme si všimnúť, že $\{0\}$ je prvoideál v R práve vtedy, keď R nemá delitele nuly.

Veta 4.2.15. *Nech R je komutatívny okruh s jednotkou a I je ideál v R. Potom faktorový okruh R/I je oborom integrity práve vtedy, keď I je vlastný prvoideál.*

Dôkaz. $\boxed{\Rightarrow}$ Nech R/I je obor integrity. Z toho hneď vyplýva $1 + I \neq 0 + I$, a teda ideál I je vlastný. Využijeme fakt, že $I = \operatorname{Ker} \varphi$ pre kanonický homomorfizmus $\varphi\colon R \to R/I$; $\varphi(a) = a + I$. Z toho vyplýva, že ak $ab \in I$, tak

$$\varphi(ab) = \varphi(a)\varphi(b) = 0.$$

Pretože R/I je obor integrity, z predchádzajúce rovnosti vyplýva, že $\varphi(a) = 0$ alebo $\varphi(b) = 0$, čiže $a \in I = \operatorname{Ker} \varphi$ alebo $b \in I = \operatorname{Ker} \varphi$.

$\boxed{\Leftarrow}$ Podobne ako v prvej časti využijeme surjektívny homomorfizmus $\varphi\colon R \to R/I$; $\varphi(a) = a + I$. Ak $x, y \in R/I$ sú také, že $xy = 0$ a $x = \varphi(a)$, $y = \varphi(b)$ (zo surjektívnosti vyplýva, že také $a, b \in R$ existujú) tak máme

$$\varphi(ab) = \varphi(a)\varphi(b) = xy = 0,$$

čiže $ab \in \operatorname{Ker} \varphi = I$. Pretože I je prvoideál, tak z toho vyplýva $a \in I = \operatorname{Ker} \varphi$ alebo $b \in I = \operatorname{Ker} \varphi$, čo však znamená, že

$$x = \varphi(a) = 0 \qquad \vee \qquad y = \varphi(b) = 0.$$

□

Definícia 4.2.16. Ideál I v okruhu R nazývame *maximálny,* ak $I \neq R$ a súčasne pre každý ideál J s vlastnosťnou $I \subseteq J \subseteq R$ platí $I = J$ alebo $J = R$.

Predchádzajúca definícia vlastne hovorí, že maximálne ideály sú práve maximálne prvky množiny vlastných ideálov okruhu R vzhľadom na usporiadanie $\subseteq$.

Poznámka 4.2.17. Bez dôkazu spomeňme, že pre každý ideál I taký, že $I \neq R$ existuje maximálny ideál M obsahujúci I, t.j. $I \subseteq M$.

Veta 4.2.18. *Nech R je komutatívny okruh s jednotkou a I je ideál v R. Potom faktorový okruh R/I je pole práve vtedy, keď I je maximálny ideál.*

Dôkaz. $\boxed{\Rightarrow}$ Predpokladajme, že R/I je pole. Potom musí platiť $0 + I \neq 1 + I$, čiže $1 \notin I$ a I je vlastný ideál.

Ďalej nech $I \subseteq J \subseteq R$. Predpokladajme, že $I \neq J$, teda existuje prvok $a \in J$ taký, že $a \notin I$. Potom $a + I \neq 0 + I$, čiže k $a + I$ existuje v poli R/I inverzný prvok. To znamená, že existuje $c \in R$ také, že

$$(ac) + I = 1 + I,$$

čiže $1 - ac \in I \subseteq J$. Potom z toho, že $ac \in J$ (lebo $a \in J$) a $1 - ac \in J$ vyplýva $1 \in J$ a $J = R$ (lema 4.2.9).

$\boxed{\Leftarrow}$ Nech I je maximálny ideál. Ak $a \notin I$ (čiže $a + I \neq 0 + I$), chceme ukázať, že k $a + I$ existuje v R/I inverzný prvok. Definujme

$$J = \{j + ca; j \in I, c \in R\}.$$

Overme najprv, že J je ideál. Skutočne, $(j + ca) - (j' + c'a) = (j - j') + (c - c')a$ a $j - j' \in I$, $c - c' \in R$ pre $j, j' \in J$, $c, c' \in R$. Ďalej $(j + ca).(j' + c'a) = jj' + a(cj' + jc' + cc'a)$ a opäť $jj' \in I$, $cj' + jc' + cc'a \in R$ pre $j, j' \in I$, $c, c' \in R$.

Navyše, pre ideál J platí $I \subsetneqq J \subset R$. Pretože I je maximálny ideál, máme potom $J = R$, a teda $1 \in J$. To znamená, že existujú $c \in R$, $j \in I$ také, že $j + ca = 1$. Potom máme

$$ca - 1 \in I,$$
$$ca + I = 1 + I,$$

čiže $c + I$ je inverzný prvok vzhľadom na násobenie k $a + I$ v okruhu R/I. □

Pretože každé pole je oborom integrity, dokázali sme súčasne:

Dôsledok 4.2.19. *Každý maximálny ideál je prvoideál.*

Opäť, podobne ako v prípade grúp a normálnych podgrúp, zodpovedajú ideály kongruenciám na okruhu R (pozri úlohy 4.2.23, 4.2.24).

Definícia 4.2.20. Nech $(R, +, \cdot)$ je okruh. Relácia ekvivalencie E na R sa nazýva *kongruencia*, ak platí

$$aEa', bEb' \qquad \Rightarrow \qquad (a + b)E(a' + b'), (ab)E(a'b')$$

Cvičenia

Úloha 4.2.1. Nech $X \neq \emptyset$ je ľubovoľná neprázdna množina. Dokážte, že potenčná množina $(P(X), \triangle, \cap)$ s operáciami $\triangle$ (symetrická diferencia množín) a $\cap$ (prienik množín) tvorí okruh. Nájdite izomorfizmus medzi týmto okruhom a okruhom $\mathbb{Z}_2^X$. (Poznámka: Bijekcia, ktorú nájdete v druhej časti, by sa dala použiť aj na dôkaz tvrdenia uvedeného v prvej časti.)

Úloha 4.2.2. Nech F je pole a $I \neq \emptyset$. Dokážte, že v okruhu F^I (príklad 4.1.7) je každý ideál tvaru $M_p = \{f \in F^I; f(p) = 0\}$, kde p je nejaký prvok z I, maximálny. (Hint: Dá sa využiť veta 4.2.18.)

Úloha 4.2.3. Prienik ľubovoľného systému podokruhov je podokruh. Prienik ľubovoľného systému ideálov je ideál.

Úloha 4.2.4. Overte, že $(a) = \{ax; x \in R\}$ je ideál v okruhu R (teda hlavné ideály sú skutočne ideály.)

Úloha 4.2.5. Dokážte, že zobrazenie $f_1 \colon R_1 \times R_2 \to R_1$ určené predpisom $f_1(r_1, r_2) = r_1$ je homomorfizmus.

Dokážte, že pre každé $i \in I$ je zobrazenie $f_i \colon R^I \to R$ dané predpisom $f_i(g) = g(i)$ (pre ľubovoľné $g \colon I \to R$) je homomorfizmus.

Úloha 4.2.6. Ak I_1 je ideál v okruhu R_1 a I_2 je ideál v okruhu R_2, tak podmnožina $I_1 \times I_2$ je ideál v okruhu $R_1 \times R_2$.

Úloha 4.2.7. Ak I_1, I_2 sú ideály v komutatívnom okruhu $(R, +, \cdot)$, tak aj
a) $I_1 + I_2 = \{a + b; a \in I_1, b \in I_2\}$ je ideál v R.
b) $I_1.I_2 = \{a_1b_1 + \cdots + a_nb_n; n \in \mathbb{N}, a_i \in I_1, b_i \in I_2\}$ je ideál v R.

Úloha 4.2.8. Nech $(G, *)$ je cyklická grupa, a je jej generátor, t.j. $G = [a]$. Ak definujeme operáciu $\cdot$ ako $a^k \cdot a^l = a^{k.l}$ (pre ľubovoľné $k, l \in \mathbb{Z}$), tak $(G, *, \cdot)$ je okruh. Viete povedať (v závislosti od rádu generátora a) s akým okruhom je tento okruh izomorfný?

Úloha 4.2.9. Ak pre každé $n \in \mathbb{N}$ je I_n ideál v okruhu R a navyše platí $I_n \subseteq I_{n+1}$, tak aj zjednotenie $\bigcup_{i=1}^{\infty} I_i$ je ideál v R.

Úloha 4.2.10. Okruh R sa volá boolovský okruh, ak pre každé $a \in R$ platí $a^2 = a$. Dokážte, že každý boolovský okruh je komutatívny. (Boolovským okruhom je napríklad okruh z úlohy 4.2.1.)

Úloha 4.2.11. Dokážte, že okruhy $(2\mathbb{Z}, +, \cdot)$ a $(3\mathbb{Z}, +, \cdot)$ nie sú izomorfné.

Úloha 4.2.12. Nájdite všetky homomorfné obrazy okruhu $\mathbb{Z}$.

Úloha 4.2.13. Nájdite všetky homomorfizmy zo $\mathbb{Z}$ do $\mathbb{Z}_{30}$.

Úloha 4.2.14. Nájdite všetky homomorfizmy:
a) zo $\mathbb{Z}[\sqrt{2}]$ do $\mathbb{Z}[\sqrt{2}]$,
b) z $\mathbb{Q}[\sqrt{2}]$ d $\mathbb{Q}[\sqrt{2}]$.
(Tieto okruhy sú definované v úlohe 4.1.3.)

Úloha 4.2.15. Nájdite všetky homomorfizmy $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$.

Úloha 4.2.16. Zistite, ktoré z nasledujúcich zobrazení sú homomorfizmy medzi okruhom A všetkých matíc typu 2×2 s celočíselnými koeficientami a okruhom $\mathbb{Z}$.
a) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a$
b) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d$ (*stopa* matice)
c) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$ (determinant matice)

Úloha 4.2.17. Zistite, či tieto množiny tvoria ideály v okruhu $\mathbb{Z} \times \mathbb{Z}$:
a) $\{(a, a); a \in \mathbb{Z}\}$
b) $\{(2a, 2b); a, b \in \mathbb{Z}\}$
c) $\{(2a, 0); a \in \mathbb{Z}\}$
d) $\{(a, -a); a \in \mathbb{Z}\}$

Úloha 4.2.18. Zistite, s akými okruhmi sú izomorfné okruhy $\mathbb{Z}_{60}/(15)$, $\mathbb{Z}_{60}/(20)$, $\mathbb{Z}_{60}/(12)$.

Úloha 4.2.19. Zistite, či dané ideály v okruhu $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ sú maximálne ideály/prvoideály.
a) $(1 + i) = \{(1 + i)z; z \in \mathbb{Z}[i]\}$
b) $(2) = \{2z; z \in \mathbb{Z}[i]\}$
c*) $(2 + i) = \{(2 + i)z; z \in \mathbb{Z}[i]\}$

Úloha 4.2.20. Nech R je komutatívny okruh s jednotkou. Dokážte, že v ňom platí binomická veta

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} \times a^k b^{n-k}.$$

Úloha 4.2.21*. a) Dokážte, že v okruhu $C(0, 1)$ (príklad 4.1.12) je každý ideál tvaru $M_p = \{f \in C(0, 1); f(p) = 0\}$ pre $p \in \langle 0, 1\rangle$ maximálny.
b) Dokážte, že všetky maximálne ideály v $C(0, 1)$ majú takýto tvar.

Úloha 4.2.22. Nájdite príklad takých okruhov $(R, +, \cdot)$, $(S, +, \cdot)$ a zobrazenie $f\colon R \to S$, že f je grupový homomorfizmus (medzi grupami $(R, +)$ a $(S, +)$), ale nie je to okruhový homomorfizmus.

Úloha 4.2.23+. Nech R je okruh, I je ideál v R. Definujeme reláciu E na R ako $aEb \Leftrightarrow a - b \in I$. Dokážte, že E je (okruhová) kongruencia (definícia 4.2.20).

Obrátene ak E je ľubovoľná kongruencia na R, tak trieda ekvivalencie $[0]_E$ je ideál v R.

Úloha 4.2.24+. Nech $(R, +, \cdot)$ je okruh.
a) Ak $f\colon R \to S$ je homomorfizmus, tak relácia E na množine R daná predpisom $xEy \Leftrightarrow f(x) = f(y)$ je kongruencia (pozri úlohu 3.1.3).
b) Ak E je kongruencia na R, tak na množine R/E tried ekvivalencie tejto relácie predpisy $[a]+[b] = [a+b]$, $[a]\cdot[b] = [ab]$ dobre definuje binárne operácie $+, \cdot$ a R/E s týmito binárnymi operáciami tvorí grupu. Navyše, zobrazenie $a \mapsto [a]$ je surjektívny homomorfizmus z R do R/E a jeho jadro je $[0]$.

4.3 Okruhy polynómov – definícia a delenie so zvyškom

Na strednej škole ste strávili veľa času s kvadratickými rovnicami $ax^2+bx+c = 0$. Venovali ste sa aj všeobecnejším rovniciam vyššieho stupňa. Tieto rovnice súvisia s funkciami $f\colon \mathbb{R} \to \mathbb{R}$

tvaru

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Takéto funkcie budeme volať polynomické funkcie.

V tejto časti by sme chceli zaviesť podobný pojem pre ľubovoľný okruh. V minulom semestri sme pracovali s polynomickými funkciami nad $\mathbb{R}$ ako s prvkami vektorového priestoru $\mathbb{R}^{\mathbb{R}}$ všetkých zobrazení z $\mathbb{R}$ do $\mathbb{R}$. Vtedy sme často používali fakt, že polynomická funkcia $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ sa rovná nulovej funkcii (t.j. v každom bode nadobúda hodnotu 0) práve vtedy, keď všetky koeficienty sú nulové, t.j.

$$a_n = a_{n-1} = \ldots = a_0 = 0.$$

(Ako uvidíme, táto vlastnosť neplatí pre všetky polia, v prípade poľa $\mathbb{R}$ však platí, ukážeme to v tvrdení 4.3.13.)

Práve toto je vlastnosť, ktorú budeme požadovať od pojmu polynómu, ktorý teraz ideme definovať.

4.3.1 Definícia okruhu polynómov

Definícia 4.3.1. Nech R je komutatívny okruh s jednotkou. Potom formálne zápisy tvaru

$$p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

kde n je prirodzené číslo a $a_i \in R$ pre $i = 0, \ldots, n$ nazývame *polynómy* v premennej x nad okruhom R.

Namiesto zápisu $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ budeme obvykle používať stručnejší zápis

$$p = \sum_{i=0}^{n} a_i x^i.$$

Prvky $a_n, a_{n-1}, \ldots, a_0 \in R$ voláme *koeficienty* polynómu p.

Ak navyše $a_n \neq 0$, tak n voláme *stupeň polynómu* p, označujeme $\operatorname{st} p = n$. V prípade nulového polynómu (všetky koeficienty sú nulové) definujeme $\operatorname{st} p = -\infty$. (Všimnite si, že s výnimkou nulového polynómu je možné také n zvoliť, t.j. stupeň je definovaný pre každý polynóm.) Polynómy stupňa menšieho ako 1 voláme *konštantné polynómy.*

Koeficient $a_n \neq 0$ pre $n = \operatorname{st} p$ voláme *vedúci koeficient* polynómu p.

Dva polynómy považujeme za rovnaké, ak majú rovnaké koeficienty, t.j. ak $p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $q = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ a $n \geq m$, tak $p = q$ práve vtedy, keď

$$a_i = b_i \qquad \text{pre } i = 0, 1, \ldots, m$$

a $a_i = 0$ pre $i = m+1, \ldots, n$.

V tejto definícii môže byť trochu nejasné, čo je x a prečo sa volá premenná. Ešte sa tohoto problému dotkneme na konci tejto časti, je to však možné jednoducho brať tak, že doplnenie symbolov x^i je len spôsob zápisu – polynóm je jednoznačne určený svojími koeficientami.

Príklad 4.3.2. Napríklad $0x^3 + 1x^2 + 2x + 1 = 1x^2 + 2x + 1$ chápeme ako dva rôzne zápisy toho istého polynómu z $\mathbb{R}[x]$.

Vidíme teda, že pridanie alebo odobranie nulových koeficientov polynóm tento polynóm nemení.

Ďalej by sme radi rozumným spôsobom zadefinovali sčitovanie a násobenie polynómov. „Rozumný“ spôsob by mal spĺňať prinajmenšom to, že nejakým spôsobom bude rešpektovať násobenie v okruhu R a tiež by bolo vhodné, aby výsledný okruh bol komutatívny.

Pritom polynóm budeme chápať ako súčet výrazov $a_i x^i$. To vlastne jednoznačne určuje sčitovanie, napríklad pre $p = x^2 + 2x + 1$ a $q = 2x + 1$ máme

$$p + q = (x^2 + 2x + 1) + (2x + 1) = x^2 + 2x + 2x + 1 + 1 = x^2 + 4x + 2.$$

(Využili sme iba to, že polynóm vieme rozložiť na jednotlivé členy a distributívnosť.)

Tieto požiadavky (t.j. vlastnosti komutatívneho okruhu a to, že koeficienty sa násobia rovnako ako v R) už takmer určujú násobenie. Ak chceme napríklad vynásobiť polynómy $p = x^2 + 2x + 1$ a $q = 2x + 1$ v $\mathbb{Z}[x]$, tak z distributívnosti dostaneme

$$(x^2 + 2x + 1)(2x + 1) = x^2.2x + 2x.2x + 1.2x + x^2.1 + 2x.1 + 1.1.$$

Na základe komutatívnosti dostaneme

$$(x^2 + 2x + 1)(2x + 1) = 2x^2.x + 4x.x + 2.x + 1x^2 + 2x + 1.$$

Predpokladajme, že násobenie výrazov obsahujúcich iba x^k funguje takým spôsobom, že $x^m.x^n = x^{m+n}$. Potom predchádzajúci výraz môžeme upraviť na tvar

$$(x^2 + 2x + 1)(2x + 1) = 2x^3 + 4x^2 + 2x + 1x^2 + 2x + 1.$$

Opäť z distributívnosti dostaneme

$$(x^2 + 2x + 1)(2x + 1) = 2x^3 + 5x^2 + 4x + 1.$$

Možno sa tento jednoduchý výpočet zdá rozpísaný zbytočne priveľmi podrobne, cieľom však bolo ukázať, aké vlastnosti potrebujeme, keď chceme niečo podobné definovať nad ľubovoľným komutatívnym okruhom s jednotkou. Zopakovaním rovnakej úvahy pre všeobecný prípad dostaneme:

Definícia 4.3.3. Nech R je komutatívny okruh s jednotkou. Nech $p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ a $q = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$ sú ľubovoľné polynómy nad R. (Tým, že u oboch polynómov predpokladáme rovnaký počet koeficientov sme sa nijako neobmedzili – v príade potreby je možné niektorý polynóm doplniť nulami.)

Potom *súčet polynómov* p a q je

$$p + q = \sum_{i=0}^{n} (a_i + b_i) x^i.$$

Súčin polynómov p a q je polynóm $r = \sum_{i=0}^{n} c_i x^i$, kde

$$c_k = \sum_{j=0}^{k} a_j b_{k-j}.$$

Teda obe operácie sme definovali rovnako ako v predchádzajúcom príklade – pri sčitovaní sa jednoducho sčítajú koeficienty a pri násobení sú koeficienty výsledného polynómu práve tie výrazy, ktoré by sme dostali roznásobením (koeficient c_k je súčet všetkých možných $a_s b_l$ pre $s + l = k$, čo sú presne všetky možnosti, ako môžeme dostať $x^k = x^s.x^l$).

Definíciu súčtu by sme mohli ekvivalentne prepísať ako

$$c_k = \sum_{m+n=k} a_m b_n.$$

Z tejto ekvivalentnej definície vidno, že pre násobenie polynómov platí asociatívnosť: pre $p = \sum_{i=0}^{n} a_i x^i$, $q = \sum_{i=0}^{n} b_i x^i$, $r = \sum_{i=0}^{n} c_i x^i$ dostaneme $(pq)r = \sum_{i=0}^{n} d_i x^i$, kde koeficienty d_k majú hodnoty

$$d_k = \sum_{m+n=k} a_m \sum_{s+t=n} b_s c_t = \sum_{m+s+t=k} a_m b_s c_t.$$

Vďaka tomu dostaneme, že

Tvrdenie 4.3.4. *Nech R je komutatívny okruh s jednotkou. Množina všetkých polynómov nad R s násobením a sčitovaním definovaným v predchádzajúcej definícii tvorí komutatívny okruh s jednotkou. Tento okruh označujeme $R[x]$ a voláme ho* okruh polynómov nad R.

Sčitovanie a násobenie polynómov sme vlastne definovali tak, aby akákoľvek rovnosť, ktorá platí pre polynómy platila aj keď namiesto x napíšeme akýkoľvek prvok okruhu R (alebo nejakého nadokruhu, ktorý obsahuje R). To zdôvodňuje použitie názvu premenná – namiesto x môžeme napísať (dosadiť) hocijaký prvok, čiže sa môže meniť. (Aj dosadzovaniu do polynómov sa budeme ešte venovať.)

Dohoda. V ďalšom budeme polynómy zapisovať ako $p(x)$, $q(x)$ atď., čím označíme o polynóm v akej premennej ide. (Ak budeme niekde hovoriť súčasne o polynómoch aj o funkciách, tak opäť použijeme radšej jednopísmenkové označenie p, q; aby nemohlo dôjsť k omylu, že máme na mysli nejakú funkciu resp. jej funkčnú hodnotu.)

Poznámka 4.3.5. Všimnime si, že sčitovanie a násobenie konštantných polynómov funguje rovnako ako násobenie v okruhu R. To znamená, že keď prvky okruhu R stotožníme s im prislúchajúcimi konštantnými polynómami, môžeme R chápať ako podokruh okruhu $R[x]$. (Formálne by sme tento fakt sformulovali tak, že zobrazenie, ktoré prvku $a \in R$ priradí konštantný polynóm $a \in R[x]$ je okruhový homomorfizmus, ktorý je navyše injektívny.) V ďalšom budeme toto stotožnenie často používať (aj bez toho, že by sme na to výslovne upozornili.) To znamená, že R budeme chápať priamo ako podmnožinu $R[x]$.

Všimnime si ešte, že vlastnosť „byť oborom integrity“ sa prenesie z okruhu R na okruh $R[x]$ polynómov nad týmto okruhom.

Tvrdenie 4.3.6. *Ak R je obor integrity, tak pre ľubovoľné nenulové polynómy $f, g \in R[x]$ platí*

$$\operatorname{st}(fg) = \operatorname{st}(f) + \operatorname{st}(g)$$

a okruh $R[x]$ polynómov nad okruhom R je obor integrity.

Dôkaz. Ak f a g sú nenulové polynómy, môžeme ich zapísať ako

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$
$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0,$$

pričom $n = \operatorname{st} f$, $m = \operatorname{st} g$. Vyrátajme, aký bude koeficient c_{n+m} polynómu $f.g$ pri x^{n+m}. Priamo z definície máme, že

$$c_{n+m} = a_n b_m,$$

a pretože R je obor integrity, dostávame $c_{n+m} \neq 0$. To znamená, že polynóm $f.g$ je nenulový (teda $R[x]$ je obor integrity) a tiež, že

$$\operatorname{st}(fg) = m + n = \operatorname{st}(f) + \operatorname{st}(g).$$

□

4.3.2 Delenie so zvyškom

Pre nás bude dôležitý hlavne prípad keď okruh R je pole. Ako sme už ukázali, v tomto prípade platí

$$\mathrm{st}(pq) = \mathrm{st}\, p + \mathrm{st}\, q.$$

Neskôr bude pre nás dôležitá nasledujúca veta:

Veta 4.3.7 (Veta o delení so zvyškom). *Nech F je pole, $f(x), g(x) \in F[x]$ a $g(x) \neq 0$. Potom existujú $q(x), r(x) \in F[x]$ také, že*

$$f(x) = q(x).g(x) + r(x)$$

a $\mathrm{st}\, r(x) < \mathrm{st}\, g(x)$.

Navyše, $q(x)$ a $r(x)$ sú týmito podmienkami jednoznačne určené.

Definícia 4.3.8. Polynómy $q(x)$ a $r(x)$ jednoznačne určené podmienkami z vety 4.3.7 sa nazývajú *podiel* a *zvyšok po delení* polynómu $f(x)$ polynómom $g(x)$. Zvyšok po delení označujeme $f(x) \bmod g(x)$.

Dôkaz. Existencia. Matematickou indukciou vzhľadom na $n = \mathrm{st}(f)$.

1° Ak $\mathrm{st}\, f(x) < \mathrm{st}\, g(x)$, stačí položiť $q(x) = 0$ a $r(x) = f(x)$.

2° Nech $n = \mathrm{st}\, f(x) \geq \mathrm{st}\, g(x)$ a každý polynóm stupňa menej ako n sa dá vydeliť so zvyškom polynómom $g(x)$ (indukčný predpoklad).

Označme $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ pričom $a_n, b_m \neq 0$. Položme $h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$. Koeficient pri x^n v polynóme $h(x)$ je $a_n - a_n b_m^{-1} b_m = 0$. Teda $\mathrm{st}(h) < \mathrm{st}(f)$, čiže pre polynóm h (podľa indukčného predpokladu) existujú $s(x), r(x) \in F[x]$ také, že

$$h(x) = s(x)g(x) + r(x)$$

a $\mathrm{st}(r) < \mathrm{st}(g)$. Potom

$$f(x) = (s(x) + a_n b_m^{-1} x^{n-m})g(x) + r(x).$$

Jednoznačnosť. Nech platí

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x),$$

pričom $\mathrm{st}(r_1) < \mathrm{st}(g)$, $\mathrm{st}(r_2) < \mathrm{st}(g)$. Potom máme

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x).$$

Na pravej strane je polynóm stupňa menšieho ako $\mathrm{st}(g)$. Ak by platilo $q_1(x) - q_2(x) \neq 0$, tak na ľavej strane tejto rovnosti dostaneme polynóm stupňa aspoň $\mathrm{st}(g)$, čo je spor. Preto musí platiť $q_1(x) - q_2(x) = 0$ a $q_1(x) = q_2(x)$.

Z toho potom dostávame aj $r_1(x) - r_2(x) = 0$ a $r_1(x) = r_2(x)$. □

Všimnime si, že dôkaz predchádzajúcej vety nám súčasne dáva návod, ako rátať pre dané polynómy ich podiel a zvyšok.

Príklad 4.3.9. Vydeľme so zvyškom polynóm $f(x) = x^4 + 6x^3 + 12x^2 + 12x + 10$ polynómom $g(x) = x^2 + x + 1$. Podľa návodu z dôkazu by sme sa mali pozrieť najprv na vedúce členy – vidíme, že $x^4 = x^2.x^2$. Vypočítame teda

$$f(x) - x^2 g(x) = (x^4 + 6x^3 + 12x^2 + 12x + 10) - x^2(x^2 + x + 1) = 5x^3 + 11x^2 + 12x + 10.$$

Výsledok by sme opäť mali deliť polynómom $g(x)$ a postup opakovať, až kým nedostaneme polynóm stupňa menšieho ako $g(x)$.

$$5x^3 + 11x^2 + 12x + 10 - 5x(x^2 + x + 1) = 6x^2 + 7x + 10$$
$$6x^2 + 7x + 10 - 6(x^2 + x + 1) = x + 4$$

Celkovo sme dostali, že $f(x) - (x^2 + 5x + 6)g(x) = x + 4$, čiže

$$f(x) = (x^2 + 5x + 6)g(x) + (x + 4),$$

teda podiel je $x^2 + 5x + 6$ a zvyšok po delení je $x + 4$.

V prípade, že je polynóm $g(x)$ (=stupňa 1) môžeme podiel vyrátať jednoduchším spôsobom, ktorý sa naučíme v časti 4.5.1.

Neskôr bude pre nás užitočný fakt, že analogická veta platí aj v okruhu $(\mathbb{Z}, +, \cdot)$. Dala by sa dokazovať podobným spôsobom ako predchádzajúca veta , tu si ukážeme o trochu iný dôkaz.

Veta 4.3.10. *Nech p, q sú celé čísla, $q > 0$. Potom existujú celé čísla n a r také, že*

$$p = n.q + r \qquad a \qquad 0 \leq r < q.$$

Navyše, n a r sú týmito podmienkami jednoznačne určené.

Definícia 4.3.11. Číslo r z predchádzajúcej vety sa nazýva *zvyšok p po delení q* a označuje sa $p \mod q$.

Dôkaz. Existencia: Množina $\{k; kq \leq p\}$ je zhora ohraničená. Preto existuje $n := \max\{k; kq \leq p\}$. Položme $r = p - nq$. Očividne $r \geq 0$.

Tvrdíme, že $r < q$. Nech by to tak nebolo. Z nerovnosti $r \geq q$ dostaneme $p \geq (n + 1)q$, čo je spor s definíciou čísla n.

Jednoznačnosť: Predpokladajme, že $p = n.q + r = n'.q + r'$, kde $0 \leq r, r' < q$. Potom

$$(n - n').q = r' - r.$$

Predpokladajme, že by $|n - n'| > 0$. Potom $|r - r'| \geq q$, čo je spor s tým, že $0 \leq r, r' < q$.

Preto platí

$$(n - n').q = r - r' = 0,$$

a $n = n'$, $r = r'$. □

4.3.3 Polynómy a polynomické funkcie

V tomto článku budeme polynómy vždy označovať ako $p, q, \ldots$ (t.j. jedným písmenom).

Definícia 4.3.12. Nech R je komutatívny okruh s jednotkou. *Polynomickou funkciou* nad R budeme rozumieť ľubovoľnú funkciu $f\colon R \to R$ určenú predpisom

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

pre nejaké $n \in \mathbb{N}$ a $a_1 \ldots a_n \in R$.

Množina všetkých polynomických funkcií s obvyklým násobením a sčitovaním funkcií opäť tvorí okruh (je to podokruh okruhu R^R – úloha 4.3.1), tento okruh budeme označovať $R\langle x\rangle$.

Pri zavedení polynómov sme spomínali polynomické funkcie nad poľom $\mathbb{R}$. Zaujíma nás, aký je vo všeobecnosti vzťah medzi okruhmi $F[x]$ a $F\langle x\rangle$, ak F je ľubovoľné pole.

Máme prirodzené priradenie medzi polynómami a polynomickými funkciami $\varphi\colon F[x] \to F\langle x\rangle$, ktoré polynómu $p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ priradí funkciu danú predpisom $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Dá sa overiť, že toto zobrazenie je surjektívny homomorfizmus z okruhu $F[x]$ na okruh $F\langle x\rangle$.

V prípade, že homomorfizmus φ je injektívny, tak je to izomorfizmus. Čiže na to, aby sme zistili, či sú tieto dva okruhy izomorfné, stačí zistiť, ako vyzerá $\operatorname{Ker}\varphi$. Ukážeme, že pre nekonečné polia sú okruhy $F[x]$ a $F\langle x\rangle$ izomorfné, zatiaľčo pre konečné polia to platiť nemusí.

Tvrdenie 4.3.13. *Ak F je nekonečné pole tak polynomická funkcia $f\colon F \to F$*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

sa rovná nulovej funkcii práve vtedy, keď $a_0 = a_1 = \cdots = a_n = 0$, t.j. vtedy, keď sú všetky koeficienty nulové.

Náčrt dôkazu. Vyberme $n+1$ navzájom rôznych prvkov $x_0, \ldots, x_n$ poľa F. Potom koeficienty $a_0, \ldots, a_n$ spĺňajú sústavu $n+1$ lineárnych rovníc

$$\begin{aligned} a_n x_0^n + a_{n-1}x_0^{n-1} + \cdots + a_0 &= 0 \\ a_n x_1^n + a_{n-1}x_1^{n-1} + \cdots + a_0 &= 0 \\ &\cdots \\ a_n x_n^n + a_{n-1}x_n^{n-1} + \cdots + a_0 &= 0 \end{aligned}$$

Z úlohy I-6.5.7 (pozri tiež napríklad [K, Príklad 6.2.17(2)], [KGGS, s.114/7]) vieme, že determinant matice tejto sústavy je

$$\begin{vmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_x^n \end{vmatrix} = \prod_{0 \le i < j \le n} (x_j - x_i)$$

čiže ak prvky x_i sú navzájom rôzne, je nenulový. To znamená, že táto matica je regulárna a uvedenej sústave rovníc vyhovuje iba nulové riešenie.

Teda $\operatorname{Ker} f$ v tomto prípade pozostáva iba z nulového polynómu (všetky koeficienty sú nuly). □

Príklad 4.3.14. Homomorfizmus $\varphi\colon \mathbb{Z}_2[x] \to \mathbb{Z}_2\langle x\rangle$, ktorý polynómu priraďuje zodpovedajúcu polynomickú funkciu, nie je injektívny.

Stačí si všimnúť, že pre každé $x \in \mathbb{Z}_2$ platí $x^2 + x = 0$, teda polynomická funkcia $x^2 + x$ je nulová a

$$x^2 + x \in \operatorname{Ker}\varphi.$$

Homomorfizmus $\varphi\colon R[x] \to R\langle x\rangle$ nám súčasne dáva možnosť „dosadzovať“ do polynómov. Ak totiž máme daný prvok $b \in R$ a nejaký polynóm $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R(x)$, tak mu vieme priradiť funkciu $\varphi(f)\colon R \to R$. Potom môžeme a dosadiť do tejto funkcie, čiže dostaneme

$$\varphi(f)(b) = a_n b^n + a_{n-1}b^{n-1} + \cdots + a_0.$$

Navyše, zobrazenie $f_b\colon R[x] \to R$ určené predpisom

$$f_b\colon f \mapsto a_n b^n + a_{n-1}b^{n-1} + \cdots + a_0$$

je okruhový homomorfizmus taký, že $f(x) = b$ (t.j. polynóm x sa zobrazí na prvok b.)

To, že f_b je skutočne homomorfizmus možno vidieť napríklad z toho, že $f_b = g_b \circ \varphi$, kde $g_b\colon R^R \to R$ je homomorfizmus daný predpisom $g_b(f) = f(b)$ (úloha 4.2.5).

Definícia 4.3.15. Ak R je komutatívny okruh a $b \in R$, tak homomorfizmus $f_b\colon R[x] \to R$ daný predpisom

$$f_b\colon f \mapsto a_n b^n + a_{n-1}b^{n-1} + \cdots + a_0$$

voláme *dosadzovací homomorfizmus.*

4.3.4 Iné možnosti, ako definovať okruh polynómov

Keďže považujeme izomorfné okruhy za rovnaké (z toho dôvodu, že sú nerozlíšiteľné pomocou pojmov definovaných „v jazyku okruhov“, t.j. nemožno ich odlíšiť žiadnou vlastnosťou sformulovanou len s použitím sčitovania a násobenia v okruhu), je jasné, že akákoľvek iná definícia okruhov, ktorá by ako výsledok poskytla okruh izomorfný s okruhom $R[x]$, by bola rovnako dobrá.

Pomerne jednoduchá definícia, s ktorou by sa nám dobre pracovalo a ktorej by sme intuitívne celkom dobre rozumeli, by bola definícia okruhu $R[x]$ ako okruhu všetkých polynomických funkcií. Ako sme už videli, takto okruh $R[x]$ nemôžeme definovať, pretože pre konečné polia by sme takto zadefinovali niečo úplne iné než chceme.

Iná možná definícia okruhu polynómov nad okruhom R by bola nasledovná (takto sa definujú okruhy polynómov v [KGGS]):

Definícia 4.3.16. Nech R je komutatívny okruh s jednotkou. Predpokladajme, že R je podokruh nejakého komutatívneho okruhu R' a existuje prvok $x \in R'$ taký, že rovnosť

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

pre $a_1, \ldots, a_n \in R$ platí práve vtedy, keď $a_1 = \cdots = a_n = 0$. Potom prvok x voláme *transcendentný prvok* nad R.

Podokruh

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0; n \in \mathbb{N}, a_1, \ldots, a_n \in R\}$$

okruhu R' potom voláme *okruhom polynómov* v premennej x nad R.

Overiť, že množina $R[x]$ zadefinovaná v predchádzajúcej definícii je skutočne podokruhom R' je jednoduché – dá sa dokonca ukázať, že je to najmenší podokruh obsahujúci $R \cup \{x\}$. Z toho vyplýva výhoda tejto definície – automaticky vidíme, že $R[x]$ je okruh, z toho, že ide o podokruh okruhu R'. (V našej definícii sme to museli dokazovať.)

Táto definícia si vyžaduje istú prácu navyše – aby sme mohli definovať $R[x]$ pre ľubovoľný komutatívny okruh R s jednotkou, treba dokázať, že pre každý takýto okruh R existuje vhodný nadokruh R', t.j. existuje nadokruh obsahujúci aspoň jeden transcendentný prvok. O chvíľu sa dozvieme, ako sa dá dokázať takéto niečo.

Ďalej pri použití takejto definície musíme ukázať aj to, že bez ohľadu na voľbu nadokruhu R' a transcendentného prvku $x \in R'$ dostaneme vždy (až na izomorfizmus) to isté.

Skúsme sa ešte na chvíľu pozrieť na našu definíciu 4.3.1. K nej by sme mohli mať jednu vážnu výhradu – kedysi v minulom semestri sme tvrdili, že pre nás bude pojem množiny základným pojmom, ktorý síce nedefinujeme (iba popíšeme niektoré jeho vlastnosti), pomocou

množín a operácii s nimi už však budeme schopní vystavať celú potrebnú teóriu, teda všetky ďalšie pojmy budeme schopný preformulovať v jazyku množín.

V tejto definícii sme použili „symbol x“ a „formálne zápisy tvaru“ $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ – čo rozhodne nesedí s našou koncepciou definovať všetko pomocou množín. (Čo je symbol? Čo znamená *formálny zápis*?)

Ukážeme si, ako to môžeme zachrániť – t.j. zadefinujeme okruh polynómov tak, aby naša definícia bola „množinová“. Súčasne nám táto definícia poskytne aj riešenie jedného z problémov s definíciiou 4.3.16 – existenciu nadokruhu, ktorý obsahuje transcendentný prvok.

Napriek tomu sa však menej formálna definícia 4.3.1 zdá byť lepšia – pretože pri nej s prvkami okruhu $R[x]$ pracujeme rovnako ako s výrazmi obsahujúcimi nejaké prvky okruhu R. Násobenie, ako sme ho definovali v tejto definícii je teda veľmi prirodzené. V nasledujúcej definícii bude o niečo komplikovanejšie a striktné používanie tejto definície by viedlo k zložitejším zápisom polynómov.

Definícia 4.3.17. Nech R je ľubovoľný komutatívny okruh s jednotkou. Ako $R[x]$ označíme množinu všetkých postupností prvkov z R takých, že iba konečne veľa členov tejto postupnosti je nenulových. Ďalej zadefinujeme sčitovanie dvoch postupností ako

$$(a_n)_{n=1}^{\infty} + (b_n)_{n=1}^{\infty} = (a_n + b_n)_{n=1}^{\infty}$$

a súčin postupností $(a_n)_{n=1}^{\infty}$, $(b_n)_{n=1}^{\infty}$ definujeme ako postupnosť $(c_n)_{n=1}^{\infty}$, ktorej členy sú určené predpisom

$$c_k = \sum_{j=0}^{k} a_j b_{k-j} = \sum_{m+n=k} a_m b_n.$$

Táto množina postupností s uvedeným sčitovaním a násobením tvorí okruh, ktorý voláme *okruh polynómov* nad R.

Táto definícia v istom zmysle presne zodpovedá definícii 4.3.1 – postupnosti sú tiež jednoznačne určené svojími členmi, takisto ako dva polynómy sme v definícii 4.3.1 prehlásili za rovnaké, ak mali rovnaké koeficienty.

Dôkaz, že takýmto spôsobom dostaneme okruh je takmer totožný s dôkazom tvrdenia 4.3.4.

Polynóm $3x^2 - 1x + 0$ v tejto definícii zodpovedá postupnosti $(0, -1, 3, 0, 0, \ldots)$. Prvky z R môžeme stotožniť s postupnosťami tvaru $(a, 0, 0, 0, \ldots)$, kde $a \in R$. Všimnime si, že polynóm x zodpovedá postupnosti $(0, 1, 0, 0, \ldots)$ a dá sa ukázať, že v okruhu $R[x]$ (chápanom ako postupnosti, čiže ako v poslednej uvedenej definícii) je tento prvok transcendentným prvkom nad R.

Cvičenia

Úloha 4.3.1. Dokážte, že polynomické funkcie (definícia 4.3.12) tvoria podokruh okruhu F^F.

4.4 Deliteľnosť v okruhoch

V tejto časti sa budeme zaoberať deliteľnosťou v okruhoch. Najdôležitejšími príkladmi budú pre nás okruh $(\mathbb{Z}, +, \cdot)$ celých čísel a okruh $(F[x], +, \cdot)$ polynómov nad poľom F.

V celej podkapitole budeme predpokladať, že okruh, s ktorým pracujeme, je obor integrity. Nasledujúcu vlastnosť oborov integrity budeme často používať, preto ju sformulujeme ako samostatnú lemu.

Lema 4.4.1. *Nech R je obor integrity, $a, b \in R$. Ak platí $ab = a$ pre $a \neq 0$, tak $b = 1$.*

Dôkaz. Z rovnosti $ab = a = a1$ vyplýva

$$ab - a1 = a(b-1) = 0,$$

čiže v obore integrity pre $a \neq 0$ máme $b - 1 = 0$, čiže $b = 1$. □

Definícia 4.4.2. Nech R je obor integrity. Hovoríme, že a *delí* b, označujeme $a \mid b$, ak existuje $c \in R$ také, že $b = ca$.

Lema 4.4.3. *Nech R je obor integrity. Potom pre ľubovoľné $a, b, c, d \in R$, $a_i, r_i \in R$ platí*

(i) $a \mid a$

(ii) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

(iii) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$

(iv) $a \mid 0$, $1 \mid a$

(v) $0 \mid a \Leftrightarrow a = 0$

(vi) $ac \mid bc \wedge c \neq 0 \Rightarrow a \mid b$

(vii) $a \mid a_i$ *pre* $i = 1, \ldots n \Rightarrow a \mid a_1 r_1 + \cdots + a_n r_n$

Dôkaz. Jednoduchý – ponecháme ako cvičenie. □

Príklad 4.4.4. V prípade okruhu $\mathbb{Z}$ je relácia $\mid$ tá istá relácia deliteľnosti, ktorú poznáte zo strednej školy, t.j. napríklad $3 \mid 12$, lebo $12 = 3.4$, zatiaľčo $3 \nmid 7$.

Všimnime si, že $a \mid b$ znamená to isté, ako že zvyšok čísla b po delení číslom a je 0.

Príklad 4.4.5. V okruhoch $\mathbb{Z}[x]$, $\mathbb{R}[x]$ platí $x - 1 \mid x^2 - 1$, pretože $x^2 - 1 = (x-1)(x+1)$.

Pritom si môžeme všimnúť, že v $\mathbb{R}[x]$ platí aj $2x - 2 \mid x^2 - 1$ (lebo $x^2 - 1 = (2x-2)(\frac{1}{2}x + \frac{1}{2})$), ale v okruhu $\mathbb{Z}[x]$ už táto relácia neplatí. Deliteľnosť polynómov, ak ich chápeme ako polynómy nad $\mathbb{Z}$ a nad $\mathbb{R}$, sú rôzne pojmy, hoci $\mathbb{R}$ je nadpoľom $\mathbb{Z}$.

Všimnime si, že aj v okruhoch $F[x]$ platí $f(x) \mid g(x)$ práve vtedy, keď zvyšok polynómu $g(x)$ po delení $f(x)$ je 0. (neskôr si to zdôvodníme podrobnejšie vo všeobecnejšom prípade)

Definícia 4.4.6. Ak $a, b \in R$, kde R je obor integrity, hovoríme, že prvky a a b sú *asociované,* označujeme $a \sim b$, ak $a \mid b$ a súčasne $b \mid a$

$$a \mid b \ \wedge \ b \mid a \Leftrightarrow a \sim b$$

Lema 4.4.7. *Nech R je obor integrity. Pre ľubovoľné $a, b, c, d \in R$ platí*

(i) $a \sim b \wedge b \sim c \Rightarrow a \sim c$

(ii) $a \sim a$

(iii) $a \sim b \Rightarrow b \sim a$

(iv) $a \sim b \wedge c \sim d \Rightarrow ac \sim bd$

Dôkaz lemy 4.4.7 pre jednoduchosť vynechávame. Môžeme si všimnúť, že prvé tri vlastnosti nám hovoria, že relácia „byť asociovaný“ je relácia ekvivalencie. (Podobným spôsobom môžeme dostať z ľubovoľného čiastočného usporiadania reláciu ekvivalencie – úloha 4.4.2.) Posledná podmienka hovorí, že relácia $\sim$ sa správa rozumne vzhľadom na násobenie.

Definícia 4.4.8. Ak okruh R má jednotku a $ab = 1$, hovoríme, že a je deliteľ jednotky. Množinu všetkých deliteľov jednotky budeme označovať $U(R)$.

Tvrdenie 4.4.9. *Nech R je obor integrity. Potom*

(i) *Delitele jednotky s operáciou násobenia tvoria grupu, t.j. $(U(R), \cdot)$ je grupa.*

(ii) *$a \sim b$ práve vtedy, keď existuje deliteľ jednotky u taký, že $a = bu$.*

Dôkaz. (i) Uzavretosť na násobenie: Ak $a, b \in U(R)$, znamená to existenciu $c, d \in R$ takých, že $ac = 1$, $bd = 1$. Potom $acbd = (ab)(cd) = 1$, čiže aj ab je deliteľ jednotky.

Asociatívnosť máme priamo z definície okruhu, neutrálny prvok je 1.

Existencia inverzného prvku: Ak a je deliteľ jednotky, znamená to, že existuje $b \in R$ také, že $ab = 1$. To znamená, že $b \in U(R)$ a tento prvok je inverzný k a vzhľadom na násobenie.

(ii) Ľahko vidno, že $a \sim 0$ platí práve vtedy, keď $a = 0$ (z lemy 4.4.3 vieme, že $0 \mid a$ iba pre $a = 0$). Samozrejme, $u0 = 0$ pre ľubovoľné $u \in U(R)$.

Zostáva nám teda dokázať tvrdenie pre prípade $a \neq 0$.

Ak $a \mid b$ a $b \mid a$, tak existujú $c, d \in R$ také, že $ac = b$ a $bd = a$. Potom máme

$$a = bd = (ac)d = a(cd)$$

a z lemy 4.4.1 dostaneme $cd = 1$, čiže c aj d sú delitele jednotky. □

Príklad 4.4.10. Ľahko sa dá overiť, že ± 1 sú delitele jednotky v $\mathbb{Z}$ a všetky nenulové konštantné polynómu sú delitele jednotky v $F[x]$. (Tento fakt vyplýva aj z lemy 4.4.14, ktorú o chvíľu dokážeme.)

Takisto nie je ťažké ukázať, že iné delitele jednotky tam už nie sú. Skutočne, ak $ab = 1$ v $\mathbb{Z}$, tak $a, b \neq 0$, z čoho máme $|a| \geq 1$, $|ab| = |a||b| \geq 1$. Aby v predchádzajúcej rovnosti nastala rovnosť, musí byť $|a| = 1$, čiže $a = \pm 1$.

Ak $f(x)$ je deliteľ jednotky v $F[x]$, tak máme $f(x)g(x) = 1$. Pritom $g(x) \neq 0$ (lebo potom by sme dostali $f(x)g(x) = 0$), preto $\operatorname{st} g \geq 0$. Potom (tvrdenie 4.3.6) $\operatorname{st}(fg) = \operatorname{st} f + \operatorname{st} g \geq \operatorname{st} f$. Súčasne vieme $\operatorname{st}(fg) = \operatorname{st} 1 = 0$, preto aj $\operatorname{st} f = 0$ a $f(x)$ je konštantný polynóm. (Nemôže platiť $f(x) = 0$; zdôvodniť to môžeme rovnako ako sme to spravili pre polynóm $g(x)$.)

4.4.1 Euklidovské okruhy

Veta 4.3.7 o delení so zvyškom je dôležitou vlastnosťou okruhu $F[x]$ polynómov nad poľom F. Veta 4.3.10 nám hovorí, že analogickú vlastnosť má aj okruh celých čísel $(\mathbb{Z}, +, \cdot)$.

Na základe tejto vety môžeme odvodiť mnohé vlastnosti, ktoré sú spoločné pre oba spomínané okruhy – najjednoduchšie bude odvodiť ich všeobecne pre oba spomínané okruhy.

Definícia 4.4.11. Obor integrity R sa nazýva *euklidovský okruh,* ak existuje funkcia $N \colon R \to \mathbb{N}$ taká, že pre ľubovoľné $a, b \in R$, $b \neq 0$ existujú $c, d \in R$ také, že $a = bc + d$ a buď $d = 0$ alebo $N(d) < N(b)$.

Funkciu N budeme nazývať *norma.*

Okruh je euklidovský, ak existuje funkcia N s uvedenými vlastnosťami. Samozrejme, ako uvidíme aj v nasledujúcom príklade, pre nejaký euklidovský okruh môže existovať viacero noriem.

Poznámka 4.4.12. Niektorí autori v definícii euklidovského okruhu navyše požadujú, aby norma spĺňala podmienku $N(a) \leq N(ab)$. V skutočnosti sú tieto 2 definície ekvivalentné, t.j. ak na obore integrity existuje norma s vlastnosťami z definície 4.4.11, tak existuje aj taká norma, ktorá navyše spĺňa $N(a) \leq N(ab)$ (pozri napríklad [Rog]).

Príklad 4.4.13. Okruh $\mathbb{Z}$ je euklidovský okruh. Ako normu môžeme zvoliť absolútnu hodnotu čísla z, čiže $N(z) = |z|$. Takisto norma $N(z) = |z| - 1$ vyhovuje definícii euklidovského okruhu.

Okruh $F[x]$, kde F je ľubovoľné pole, je euklidovský okruh. Za normu môžeme zvoliť stupeň polynómu (ten je pre každý nenulový polynóm definovaný ako prirodzené číslo).

Ľahko si môžeme všimnúť, že

Lema 4.4.14. *Ak R je euklidovský okruh, $u \neq 0$ a $N(u) = 0$, tak u je deliteľ jednotky.*

Dôkaz. Priamo z definície máme, že $1 = u.c + d$, pričom $N(d) < 0$ alebo $d = 0$. Pretože prípad $N(d) < 0$ nemôže nastať, máme $d = 0$. □

4.4.2 Okruhy hlavných ideálov

Ďalším typom okruhov, ktorý bude pre nás užitočný sú okruhy hlavných ideálov.

Definícia 4.4.15. Ak R je obor integrity, hovoríme, že R je okruh hlavných ideálov, ak každý ideál v R je hlavný, t.j. ak je tvaru

$$I = (a) = \{ax; x \in R\}$$

pre nejaké $a \in R$.

Tvrdenie 4.4.16. *Každý euklidovský okruh je okruh hlavných ideálov.*

Dôkaz. Nech R je euklidovský okruh, $I \neq \emptyset$ je ideál v R.

Ak $I = \{0\}$, tak $I = (0)$. Môžeme teda predpokladať, že I obsahuje aspoň jeden nenulový prvok.

Ak by všetky nenulové prvky v I mali nulovú normu, tak sú deliteľmi jednotky (podľa lemy 4.4.14). To by ale znamenalo, že $I = R = (1)$. V ďalšej časti dôkazu teda môžeme predpokladať, že v I existuje nenulový prvok s nenulovou normou.

Nech b je prvok z I s najmenšou nenulovou normou. (Taký prvok existuje, lebo $\{N(b); b \in I \setminus \{0\}\}$ je neprázdna podmnožina prirodzených čísel. Každá neprázdna podmnožina prirodzených čísel má najmenší prvok – princíp dobrého usporiadania.)

Tvrdíme, že $I = (b)$. Pre každý prvok $a \in I$ máme $a = b.c + d$. Pritom $d = b.c - a \in I$, čiže opäť nemôže nastať možnosť $N(d) < N(b)$. Teda $d = 0$ a $a = b.c$. Tým sme ukázali, že $I \subseteq (b)$. Inklúzia $(b) \subseteq I$ je zrejmá. □

Obrátené tvrdenie neplatí, ale príklad, ktorý to ukazuje nie je úplne jednoduchý.

Príklad 4.4.17. Z predchádzajúceho tvrdenia špeciálne dostávame, že $\mathbb{Z}$ a $F[x]$ sú okruhy hlavných ideálov, teda v $\mathbb{Z}$ neexistujú iné ideály ako ideály tvaru $(k) = k\mathbb{Z}$ a takisto v $F[x]$ každý ideál pozostáva z násobkov nejakého polynómu $f(x)$.

Príklad 4.4.18. Okruh $\mathbb{Z}[x]$ je príklad oboru integrity, ktorý nie je okruhom hlavných ideálov. Ak uvažujeme ideál

$$(2, x) = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]; a_0 \in \mathbb{Z}, a_i \in 2\mathbb{Z} \text{ pre } i \geq 1\}$$

v okruhu $\mathbb{Z}[x]$ (t.j. ideál generovaný polynómom x a konštantným polynómom 2; pozri poznámku 4.4.20), tak tento ideál nie je hlavný.

Ak by bol totiž generovaný jediným polynómom, musel by to byť polynóm stupňa 0. (V ideále $(f(x))$ generovanom polynómom $f(x)$ majú všetky polynómy stupeň väčší alebo

rovný st f – vyplýva to z tvrdenia 4.3.6.) Generátorom by teda musel byť nejaký konštantný polynóm c. Potom však c musí byť párne (lebo iné konštantné polynómy v ideále $(2, x)$ nie sú.) V hlavnom ideále (c) generovanom nejakou párnou konštantou však nevyhnutne musia mať všetky polynómy iba párne koeficienty, čiže nedostali by sme tak všetky polynómy patriace do $(2, x)$.

Špeciálne, keďže sme ukázali, že $\mathbb{Z}[x]$ nie je okruh hlavných ideálov, vyplýva z tvrdenia 4.4.16, že to nie ani euklidovský okruh.

V dôsledku 4.2.19 sme ukázali, že každý maximálny ideál je prvoideál. V okruhu hlavných ideálov platí aj obrátená implikácia:

Tvrdenie 4.4.19. *Ak $I = (m)$, $I \neq \{0\}$, je prvoideál v OHI R, tak I je maximálny.*

Dôkaz. Nech $I \subseteq J \subseteq R$. Pretože R je OHI existuje prvok $a \in R$ taký, že $J = (a)$. Zrejme $a \neq 0$ (inak by platilo $I \subseteq (0)$, teda I by bol nulový ideál). Máme teda $(m) \subseteq (a)$, čiže $m = a.c$ pre nejaké $c \in R$. Potom buď $a \in I$ a $I = (a)$ alebo $c \in I$, čiže $c = m.d$ a $m = a.c = m(ad)$. Z toho máme $ad = 1$ (pretože R je OI), čiže a je deliteľ jednotky a $(a) = R$. □

Deliteľnosť v okruhoch hlavných ideálov

Všimnime si, že v OHI platí nasledovný vzťah medzi deliteľnosťou v okruhu a hlavnými ideálmi:

$$a \mid b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a). \tag{4.2}$$

(Vyplýva to priamo z definície deliteľnosti a z definície hlavného ideálu.)

V súvislosti s hlavnými ideálmi si tiež môžeme všimnúť, že $(a) = R$ práve vtedy, keď a je deliteľ jednotky. (Pozri lemu 4.2.9.)

Poznámka 4.4.20. Podobne, ako (a) označuje ideál generovaný prvkom a, znakom $(a_1, \ldots, a_n)$ budeme označovať najmenší ideál obsahujúci všetky prvky $a_1, \ldots, a_n$. Ľahko sa dá overiť, že v komutatívnom okruhu s jednotkou

$$(a_1, \ldots, a_n) = \{\sum_{i=1}^{n} x_i a_i; x_i \in R\}$$

(Je zjavné, že táto množina obsahuje prvky $a_1, \ldots, a_n$. Stačí teda overiť, že to je ideál – to ide ľahko z definície ideálu.)

Špeciálne máme

$$(a, b) = \{ax + by; x, y \in R\}.$$

Podobne ako pre celé čísla, aj v oboroch integrity vieme definovať pojem najväčší spoločný deliteľ.

Definícia 4.4.21. *Najväčší spoločný deliteľ* prvkov $a, b \in R$ je taký prvok $c \in R$, že

(i) $c \mid a$, $c \mid b$,

(ii) pre ľubovoľný prvok $d \in R$ taký, že $d \mid a$ a $d \mid b$ platí aj $d \mid c$.

Označujeme ho $\gcd(a, b)$.

Inak povedané, $\gcd(a, b)$ je najväčší (vzhľadom na usporiadanie $|$) prvok z množiny čísel, ktoré súčasne delia a aj b (=spoločné delitele čísel a, b).

Priamo z definície vidno, že najväčší spoločný deliteľ (ak existuje) je určený jednoznačne až na asociovanosť.

Tvrdenie 4.4.22. *Ak R je okruh hlavných ideálov, tak pre ľubovoľné $a, b \neq 0$ existuje v R najväčší spoločný deliteľ $c = \gcd(a, b)$.*

Navyše, existujú také $x, y \in R$, že

$$c = xa + yb.$$

Dôkaz. Vieme, že $(a, b) = \{ax + by; x, y \in R\}$ je ideál v R. Pretože R je okruh hlavných ideálov, existuje $c \in R$ také, že $(c) = (a, b)$. Z toho špeciálne máme $a, b \in (c)$, čiže $c \mid a$, $c \mid b$.

Navyše, pretože $c \in (a, b)$, máme zaručenú existenciu $x, y \in R$ s vlastnosťou $ax + by = c$.

Z toho potom dostávame, že pre ľubovoľné $d \in R$ také, že $d \mid a$, $d \mid b$, platí

$$d \mid ax + by = c.$$

□

Z predchádzajúceho tvrdenia dostávame nasledujúci dôsledok, ktorý je často užitočný.

Dôsledok 4.4.23. *Nech R je okruh hlavných ideálov, $a, b, c \in R$, $a, b \neq 0$. Ak $\gcd(a, b) = 1$ a $a \mid bc$, tak $a \mid c$.*

$$\gcd(a, b) = 1 \quad \wedge \quad a \mid bc \qquad \Rightarrow \qquad a \mid c$$

Dôkaz. Z tvrdenia 4.4.22 máme existenciu $x, y \in R$ takých, že

$$ax + by = 1.$$

Potom

$$a \mid ac.x + bc.y = (ax + by).c = c.$$

□

Tvrdenie 4.4.22 hovorí o existencii najväčšieho spoločného deliteľa čísel a, b a o existencii $x, y \in R$ s vlastnosťou $\gcd(a, b) = xa + yb$, nehovorí však, ako by sme $\gcd(a, b)$, x a y vedeli vyrátať.

V prípade, že vieme v našom obore integrity (algoritmicky) deliť so zvyškom, dá sa to urobiť pomocou *Euklidovho algoritmu.*

Základom Euklidovho algoritmu je nasledujúca lema:

Lema 4.4.24. *Ak R je obor integrity a $a, b \in R$, tak*

$$\gcd(a, b) = \gcd(a + bx, b)$$

pre ľubovoľné $x \in R$.

Dôkaz. Keďže najväčší spoločný deliteľ je generátor ideálu (a, b), stačí dokazovať rovnosť ideálov $(a, b) = (a + bx, b)$.

Priamo z definície ideálu máme $bx \in (a, b)$, teda aj $a + bx \in (a, b)$ a $(a + bx, b) \subseteq (a, b)$.

Podobne sa ukáže $a = (a + bx) - bx \in (a + bx, bx)$ a $(a, b) \subseteq (a + bx, b)$. □

Ak postupne počítame zvyšky po delení, vieme ich vyjadriť ako kombináciu čísel a, b.

$$\begin{aligned}
a &= q_1.b + r_1 && N(r) < N(b) && r_1 = a - q_1.b \\
b &= q_2.r_1 + r_2 && N(r_2) < N(r_1) && r_2 = b - q_2.r_1 = (1 + q_1q_2)b - q_2a \\
r_1 &= q_3.r_2 + r_3 && N(r_3) < N(r_2) && r_3 = r_2 - q_3.r_2 = \cdots = x_3a + y_3b \\
&\vdots && && \vdots \\
r_{l-2} &= q_l.r_{l-1} + r_l && N(r_l) < N(r_{l-1}) && r_l = r_{l-2} - q_l.r_{l-1} = \cdots = x_la + y_lb \\
r_{l-1} &= q_{l+1}.r_l && \text{zvyšok } 0
\end{aligned}$$

Pretože v každom kroku norma zvyše klesá, po istom čase sa algoritmus musí zastaviť a dostaneme nulový zvyšok. Navyše, z predchádzajúcej lemy vidíme, že v každom kroku platí $(r_k, r_{k-1}) = (a, b)$, preto na konci platí $(a, b) = (r_{l-1}, r_l) = (q_{l+1}r_l, r_l) = r_l$. Ďalej každý zvyšok sme vedeli vyjadriť v tvare $r_k = x_k a + y_k b$, kde $x_k, y_k \in R$, čiže týmto algoritmom vieme získať takéto vyjadrenie pre $\gcd(a, b)$.

Príklad 4.4.25. Konkrétne príklady (v okruhoch $\mathbb{Z}$, $F[x]$) si ukážeme na cvičeniach.

Ukážeme si tento postup na konkrétnych príkladoch – najprv v $\mathbb{Z}$. (Najväčší spoločný deliteľ v $\mathbb{Z}$ viete zo strednej školy rátať pomocou rozkladu na prvočísla – niečo podobné platí všeobecne, ako uvidíme v tvrdení 4.4.39. Takýto postup nám však neposkytuje najväčší spoločný deliteľ ako kombináciu daných čísel – v nasledujúcom príklade uvidíme, že to môže byť užitočná úvaha. Navyše to predpokladá, že poznáme rozklad na ireducibilné prvky – čo zatiaľ v $F[x]$ nevieme robiť vôbec, v $\mathbb{Z}$ to vieme robiť pre malé čísla. Pre veľké čísla je výpočtovo efektívnejší Euklidov algoritmus.)

Príklad 4.4.26. Inverzné prvky v poli $\mathbb{Z}_p$ (kde p je prvočíslo) sme zatiaľ vedeli počítať iba takým spôsobom, že sme postupne skúšali všetky prvky poľa. Euklidov algoritmus, ktorý sme sa teraz naučili, môžeme využiť na ten istý účel.

Pokúsme sa vypočítať 5^{-1} v $\mathbb{Z}_{13}$. Pretože 13 je prvočíslo platí $\gcd(5, 13) = 1$, čiže vieme nájsť čísla $x, y \in \mathbb{Z}$ také, že $1 = 5x + 13y$.

Postupným delením dostaneme

$$\begin{aligned} 13 &= 2.5 + 3 & 3 &= 1.13 - 2.5 \\ 5 &= 1.3 + 2 & 2 &= 5 - 3 = 3.5 - 1.13 \\ 3 &= 1.2 + 1 & 1 &= 3 - 2 = 2.13 - 5.5 \end{aligned}$$

Ak pre všetky čísla v rovnosti $1 = 2.13 - 5.5$ urobíme zvyšok po delení 13, dostaneme rovnosť

$$1 = -5.5 = 8.5,$$

ktorá platí v $\mathbb{Z}_{13}$. Teda v $\mathbb{Z}_{13}$ platí $5^{-1} = 8$.

Vyskúšajme si aspoň jeden konkrétny príklad v $\mathbb{Q}[x]$. Vieme, že najväčší spoločný deliteľ je určený jednoznačne až na asociovanosť – čiže v tomto prípade až na vynásobenie konštantou. Dohodnime sa, že si vyberieme ten, ktorý má vedúci koeficient 1 (tzv. normovaný polynóm) – potom už je najvúčší spoločný deliteľ určený jednoznačne.

Príklad 4.4.27. Vypočítajte $d(x) = \gcd(f(x), g(x))$ a vyjadrite ho v tvare $d(x) = u(x)f(x) + v(x)g(x)$ pre polynómy $f(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$, $g(x) = 3x^4 - 4x^3 - x^2 - x - 2$.

Podobne ako v predchádzajúcom príklade, budeme polynómy postupne deliť so zvyškom a zvyšok si v každom kroku vyjadríme ako kombináciu $f(x)$ a $g(x)$.

Kvôli prehľadnosti som zapísal zvlášť delenie polynómov a zvlášť vyjadrenie zvyšku v tvare kombinácie $f(x)$ a $g(x)$.

$$\begin{aligned} 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6 &= (x + 3)(3x^4 - 4x^3 - x^2 - x - 2) - 3x^3 - 2x^2 \\ 3x^4 - 4x^3 - x^2 - x - 2 &= (-3x^3 - 2x^2)(-x + 2) + 3x^2 - x - 2 \\ -3x^3 - 2x^2 &= (3x^2 - x - 2)(-x - 1) + (-3x - 2) \end{aligned}$$

Vieme, že posledný nenulový zvyšok $-3x - 2$ v Euklidovom algoritme je hľadaný najväčší spoločný deliteľ. Pretože chceme dostať normovaný polynóm, vydelíme ho ešte vedúcim koeficientom -3.

$$\gcd(f(x), g(x)) = x + \frac{2}{3}$$

Zvyšky v jednotlivých deleniach vyjadríme pomocou $f(x)$ a $g(x)$ takto

$$-3x^3 - 2x^2 = f(x) - g(x)(x+3)$$

$$\begin{aligned} 3x^2 - x - 2 = g(x) - (-3x^3 - 2x^2)(-x+2) = \\ g(x) - (f(x) - g(x)(x+3))(-x+2) = \\ f(x)(x-2) + [1 - (x-2)(x+3)g(x)] = \\ (x-2)f(x) - (x^2 + x - 7)g(x) \end{aligned}$$

$$\begin{aligned} -3x - 2 = -3x^3 - 2x^2 - (3x^2 - x - 2)(-x-1) = \\ f(x) - g(x)(x+3) + [(x-2)f(x) - (x^2 + x - 7)g(x)](x+1) = \\ f(x)[1 + (x-2)(x+1)] - g(x)[(x+3) + (x+1)(x^2 + x - 7)] = \\ f(x)(x^2 - x - 1) - g(x)(x^3 + 2x^2 - 5x - 4) \end{aligned}$$

Po vydelení poslednej rovnosti číslom -3 dostávame

$$\gcd(f(x), g(x)) = x + \frac{2}{3} = -f(x)\frac{x^2 - x - 1}{3} + g(x)\frac{x^3 + 2x^2 - 5x - 4}{3}$$

Pri výpočtoch takého typu ako sme robili v predchádzajúcom príklade sa celkom ľahko dá pomýliť – preto je užitočné občas (povedzme po každom kroku) vyskúšať, či rovnosti, ktoré sme dostali pre polynómy skutočne platí aj po dosadení nejakých čísel. (Je rozumné skúšať malé, čísla, napríklad 0, ± 1 – aby sa nám ľahko počítali hodnoty polynómu v týchto číslach.) Pri takejto čiastočnej skúške správnosti máme veľkú šancu prípadnú chybu odhaliť. (Samozrejme, dá sa urobiť skúška aj tak, že kombináciu $f(x)$ a $g(x)$, ktorú sme dostali, skutočne poroznásobujeme a zistíme, či vyjde rovnaký polynóm ako na druhej strane rovnosti – čo je však o dosť prácnejšie.)

Podobne ako pri počítaní racionálnych koreňov, ak v priebehu výpočtu nám vyjde ako jeden zo zvyškov polynóm, v ktorom všetky koeficienty sú násobkom toho istého celého čísla, môžeme polynóm týmto číslom vydeliť – dostaneme opäť polynóm s celočíselnými koeficientami (teda sa nám s ním bude dobre počítať) a neovplyvníme hodnotu najväčšieho spoločného deliteľa (v okruhu $F[x]$ sme tento polynóm zmenili len o deliteľ jednotky). Je ale dôležité pri vyjadrovaní najväčšieho spoločného deliteľa pomocou $f(x)$ a $g(x)$ nezabudnúť zarátať aj toto vydelenie.

4.4.3 Gaussove okruhy

Pojem analogický k pojmu prvočísla je v okruhu pojem ireducibilného prvku.

Definícia 4.4.28. Prvok $a \neq 0$ okruhu R sa nazýva *ireducibilný,* ak a je nenulový, nie je to deliteľ jednotky a ak z rovnosti $a = b.c$ vyplýva, že niektorý z prvkov b, c je deliteľ jednotky v R.

Inými slovami, ireducibilný prvok sa (až na asociovanosť) nedá zapísať ako súčin dvoch prvkov z R inak ako $1.a$.

Príklad 4.4.29. Vieme, že prvočísla boli definované tak, že ich rozklad na súčin $p = a.b$ je možný iba vtedy, ak niektoré z čísel a, b je rovné 1. Z toho vidno, že ireducibilné prvky v $\mathbb{Z}$ sú práve čísla tvaru $\pm p$, kde p je prvočíslo.

Ireducibilnými prvkami v okruhu $F[x]$ (volajú sa ireducibilné polynómy) sa budeme zaoberať neskôr.

Naším najbližším cieľom je dokázať, že v okruhoch hlavných ideálov platí tvrdenie zodpovedajúce rozkladu prirodzených (celých) čísel na súčin prvočísel.

Definícia 4.4.30. *Okruh s jednoznačným rozkladom* (alebo tiež *Gaussov okruh*) je obor integrity, v ktorom pre každý prvok $x \in R$, ktorý je nenulový a nie je deliteľom jednotky, existuje rozklad

$$x = p_1 \dots p_k$$

na súčin ireducibilných prvkov a navyše je tento rozklad jednoznačný až na asociovanosť a poradie.

Tvrdenie 4.4.31. *Ak ideál (p) v obore integrity R je vlastný prvoideál a $p \neq 0$, tak p je ireducibilný v R.*

Dôkaz. Ak (p) je prvoideál a $ab = p$, tak jeden prvok z dvojice a, b musí byť násobkom p. Bez ujmy na všeobecnosti, nech $a = kp$. Potom $p = ab = (kb)p$, z čoho $kb = 1$ (lema 4.4.1), čiže b je deliteľ jednotky.

Keďže ideál p je vlastný, p nie je deliteľ jednotky. □

V OHI platí aj obrátená implikácia.

Tvrdenie 4.4.32. *Ak p je ireducibilný prvok v OHI R, tak (p) je prvoideál.*

Dôkaz. Nech p je ireducibilný. Ukážeme, že ideál p je maximálny (a teda je to prvoideál). Nech by $(p) \subseteq (m)$. Z toho vyplýva $p = m.c$. Potom buď m je asociovaný s p a $(p) = (m)$, alebo m je invertibilný a $(m) = R$. □

Z toho dostávame (pomocou (4.2)) nasledujúci veľmi dôležitý vzťah.

Dôsledok 4.4.33. *V OHI pre ľubovoľný ireducibilný prvok p platí implikácia*

$$p \mid ab \qquad \Rightarrow \qquad p \mid a \vee p \mid b.$$

Teraz už sme schopný vysloviť a dokázať tvrdenie o rozklade na súčin ireducibilných prvkov.

Tvrdenie 4.4.34. *Každý okruh hlavných ideálov je okruhom s jednoznačným rozkladom.*

Dôkaz. Chceme dokázať existenciu a jednoznačnosť rozkladu na súčin ireducibilných prvkov. Jednoznačnosť vyplýva z dôsledku 4.4.33.

Existencia. Sporom. Nech by x bol taký prvok, ktorý sa nedá v R rozložiť na súčin ireducibilných prvkov (pričom $x \neq 0$, x nie je deliteľ jednotky). Pretože x nie je ireducibilný, vieme ho zapísať ako $x = r_1.q_1$. Keby obidva prvky r_1 aj q_1 boli ireducibilné, máme rozklad x. Teda jeden z nich nie je ireducibilný, bez ujmy na všeobecnosti nech je to q_1. Potom $q_1 = r_2.q_2$ pre nejaké $r_2, q_2 \in R$. Takýmto spôsobom indukciou zostrojíme nekonečnú postupnosť prvkov $r_n \in R$ takú, že nasledujúci vždy delí predchádzajúci, teda $r_{n+1} \mid r_n$. To je ekvivalentné s tým,

že $(r_n) \subseteq (r_{n+1})$ a takto dostávame nekonečnú postupnosť ideálov $I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_n \subsetneq \ldots$, kde I_k označuje ideál (r_k). Ukážeme, že v OHI takáto postupnosť nemôže existovať, čím dostaneme požadovaný spor.

Skutočne, ak by sme mali takýto rastúci reťazec ideálov. Potom aj $I = \bigcup_{n=1}^{\infty} I_n$ je ideál. Pretože R je OHI, existuje $a \in R$ také, že $(a) = I$. Lenže z toho, že $a \in \bigcup_{n=1}^{\infty} I_n$ vyplýva existencia čísla n_0 s vlastnosťou $a \in I_{n_0}$. Potom pre všetky $n > n_0$ máme $(a) \subseteq I_{n_0} \subseteq I_n \subseteq I$, čiže od n_0 počnúc sa už všetky ideály I_n rovnajú. □

Poznamenajme, že okruhy, ktoré spĺňajú podmienku, že v nich neexistuje nekonečný rastúci reťazec ideálov, sa nazývajú *noetherovské*.

Z predchádzajúceho tvrdenia špeciálne dostávame, že každé prirodzené číslo vieme napísať ako súčin prvočísel jednoznačne až na poradie. (A po pridaní deliteľov jednotky ± 1 dostaneme všetky prvé čísla.)

Analogickému tvrdeniu pre okruh polynómov $F[x]$ sa budeme venovať v nasledujúcej kapitole.

Skúsme nájsť príklad oboru integrity, ktorý nie je okruh s jednoznačným rozkladom.

Príklad 4.4.35. Budeme pracovať v okruhu $\mathbb{Z}[2i] = \{a + 2bi; a, b \in \mathbb{Z}\}$. Zrejme ide o obor integrity (je to podokruh poľa $\mathbb{C}$). Jediné delitele jednotky v tomto okruhu sú ± 1. Pozrime sa na rozklad $4 = 2.2 = (2i)(-2i)$.

Prvky 2 aj $\pm 2i$ sú ireducibilné. Ak totiž máme $2 = ab$, tak platí aj $2 = |a|.|b|$, pričom $|a| = |b|$ sú celé čísla. Potom pre niektoré z čísel a, b musí platiť, že má veľkosť 1. Takéto prvky v $\mathbb{Z}[i]$ sú však iba ± 1, zistili sme teda, že niektoré z čísel a, b je deliteľ jednotky. Tým sme overili, že 2 je ireducibilný prvok, zdôvodnenie pre $\pm 2i$ je presne rovnaké, opäť využijeme, že $|\pm 2i| = 2$.

Súčasne 2 je asociovaný iba s prvkami ± 2. Našli sme teda dva rozklady čísla 4 na súčin ireducibilných prvkov, ktoré sa nelíšia iba asociovanosťou. Teda $\mathbb{Z}[2i]$ nie je okruh s jednoznačným rozkladom.

Príklad 4.4.36. Ďalším takýmto príkladom je $\mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i; a, b \in \mathbb{Z}\}$. V tomto okruhu máme rozklady

$$6 = 2.3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i).$$

Vidno, že 2 nedelí žiaden z činiteľov na pravej strane. Ak ukážeme, že 2 je ireducibilný prvok, tak z dôsledku 4.4.33 vyplýva, že to nie je okruh s jednoznačným rozkladom.

Nech $2 = x.y$, kde $x, y \in \mathbb{Z}[\sqrt{5}i]$. Potom $|x| \leq 2$ aj $|y| \leq 2$, lebo všetky prvky tohoto okruhu majú vlastnosť $|x| \geq 1$. Ak $x = a + \sqrt{5}i$, tak sme dostali

$$|x|^2 = a^2 + 5b^2 \leq 4,$$

čo je možné jedine v prípade $b = 0$. Rozklad $2 = x.y$ je teda v skutočnosti rozklad na súčin dvoch celých čísel. V takomto rozklade musí byť nevyhnutne niektorý z činiteľov rovné ± 1.

Poznamenajme, že podobný spôsobom sa dá ukázať, že aj 3 a $1 \pm \sqrt{5}i$ sú ireducibilné.

Príklad 4.4.37. Dá sa dokázať, že ak R je okruh s jednoznačným rozkladom, tak aj okruh polynómov $R[x]$ je okruh s jednoznačným rozkladom. (Pozri napríklad [KGGS, Lema 7.4], [DF, Corollary 9.6]). Ak sme ochotní uveriť tomuto tvrdeniu, tak máme $\mathbb{Z}[x]$ ako príklad Gaussovho okruhu, ktorý nie je okruh hlavných ideálov. (Pozri príklad 4.4.18.)

V prípade, že máme rozklad prvkov a, b Gaussovho okruhu R, môžeme z neho zistiť, či $a \mid b$ ako aj určiť rozklad ich najväčšieho spoločného deliteľa $\gcd(a, b)$.

Lema 4.4.38. *Nech R je Gaussov okruh a $a, b \in R$. Ak $a = p_1 \dots p_n$ a $b = q_1 \dots q_m$ sú rozklady týchto prvkov na súčin ireducibilných činiteľov, tak $a \mid b$ práve vtedy, keď existuje injekcia $f\colon \{1, 2, \dots, n\} \to \{1, 2, \dots, m\}$ s vlastnosťou $q_{f(m)} \sim p_m$.*

(*Toto tvrdenie je len formálny zápis faktu, že všetky ireducibilné prvky z rozkladu a sa musia vyskytnúť aj v rozklade b, pričom ak sa tam vyskytuje viackrát prvok z tej istej triedy asociovanosti, tak sa toľkokrát musí vyskytnúť aj v rozklade b.*)

Dôkaz. □

Tvrdenie 4.4.39. *Nech R je Gaussov okruh, $a, b \in R \setminus \{0\}$. Majme tieto prvky vyjadrené v tvare $a = up_1^{k_1} \dots p_n^{k_n}$ a $b = u'p_1^{l_1} \dots p_n^{l_n}$, kde $u, u' \in U(R)$ a $p_1, \dots, p_n$ sú po dvoch neasociované ireducibilné prvky v R. Potom*

$$d = p_1^{m_1} \dots p_n^{m_n},$$

kde $m_i = \min\{k_i, l_i\}$ pre $i = 1, \dots, n$ je ich najväčší spoločný deliteľ.

Dôkaz. □

Cvičenia

Úloha 4.4.1. Ak u je deliteľ jednotky v okruhu R, tak aj $-u$ je deliteľ jednotky.

Úloha 4.4.2.

4.5 Okruhy polynómov II

V tejto časti sa budeme zaoberať polynómami, pričom často budeme využívať niektoré fakty, ktoré sme dokázali v predchádzajúcej podkapitole pre euklidovské okruhy, resp. pre okruhy s jednoznačným rozkladom. (Vieme, že $R[x]$ je euklidovský okruh, ak R je pole. Bez dôkazu sme si spolmenuli, že ak R je Gaussov okruh, tak aj $R[x]$ je Gaussov okruh.)

4.5.1 Korene polynómov

Do polynómu $f(x) \in F[x]$ môžeme dosadiť ľubovoľný prvok c poľa F a vypočítať hodnotu polynómu v tomto prvku. (Zobrazenie, ktoré polynómu priradilo jeho hodnotu v c sme nazvali dosadzovací homomorfizmus – definícia 4.3.15.)

Definícia 4.5.1. Nech F je pole a F' je jeho nadpole. Prvok $c \in F'$ nazývame *koreňom* polynómu $f(x) \in F[x] \subset F'[x]$, ak $f(c) = 0$ (t.j. po dosadení c do polynómu F dostaneme 0.)

V predchádzjúcej definícii dosadzujeme do polynómu z $F[x]$ prvok z nadpoľa F'. To však nie je problém – keďže koeficienty polynómu $f(x)$ sú z $F \subseteq F'[x]$, tento polynóm súčasne patrí do $F'[x]$.

Príklad 4.5.2. Číslo i je koreňom polynómu $x^2 + 1$, lebo $i^2 + 1 = 0$.

Všimnime si, aký je vzťah medzi koreňmi polynómu a deliteľnosťou lineárnymi polynómami.

Lema 4.5.3. *Ak $f(x) \in F[x]$, kde F je pole, a $c \in F$, tak zvyšok polynómu $f(x)$ po delení polynómom $x - c$ je rovný $f(c)$, t.j. existuje polynóm $g(x) \in F[x]$ taký, že*

$$f(x) = (x - c)g(x) + f(c). \tag{4.3}$$

Dôkaz. Z vety o delení so zvyškom vieme

$$f(x) = g(x)(x-c) + r,$$

pričom zvyšok je polynóm stupňa menšieho ako 1, preto je to nejaká konštanta $r \in F$.

Ak do predošlej rovnosti dosadíme c za x, tak máme

$$f(c) = g(c)(c-c) + r = r,$$

čiže táto konštanta musí byť rovná práve $f(c)$, t.j. hodnote polynómu f v bode c. □

Z predchádzajúcej lemy už ľahko dostaneme

Lema 4.5.4. *Nech F je pole a F' je jeho nadpole. Nech $f(x) \in F[x]$. Potom $c \in F'$ je koreňom $f(x)$ práve vtedy, keď $x - c \mid f(x)$ v $F'[x]$, t.j. existuje polynóm $g(x) \in F'[x]$ taký, že $f(x) = g(x)(x-c)$.*

Dôkaz. Podľa (4.5.3) máme $f(x) = (x-c)g(x)+f(c)$, čiže ak $f(c) = 0$, tak $f(x) = (x-c)g(x)$, čiže $x - c \mid f(x)$.

Obrátene, ak $x - c \mid f(x)$, tak zvyšok po delení polynómu $f(x)$ polynómom $x - c$ je 0, čiže (opäť z lemy 4.5.3) $f(c) = 0$ a c je koreň polynómu f. □

Definícia 4.5.5. Nech F' je nadpole poľa F, $f(x) \in F[x]$ a c je koreň $f(x)$. Hovoríme, že *násobnosť* koreňa c je k (alebo tiež, že c je k-násobný koreň $f(x)$), ak $(x-c)^k \mid f(x)$ (t.j. ak existuje polynóm $g(x) \in F'[x]$ taký, že $f(x) = g(x)(x-c)^k$) a súčasne $(x-c)^{k+1} \nmid f(x)$.

Pre $k = 1$ voláme k-násobný koreň *jednoduchý koreň* polynómu $f(x)$, ak $k > 1$ tak hovoríme o násobnom koreni.

Príklad 4.5.6. Čísla ± 1 sú dvojnásobné korene polynómu $x^4 - 2x^2 + 1$, lebo $x^4 - 2x^2 + 1 = (x^2-1)^2 = (x-1)^2(x+1)^2$

Jednoduchý spôsob ako ručne spočítať hodnotu polynómu v danom čísle (a tým zistiť, či toto číslo je koreňom polynómu) je použitie Hornerovej schémy.

Základná idea Hornerovej schémy je, že hodnotu polynómu môžeme vyjadriť ako

$$a_n c^n + a_{n-1}c^{n-1} + \cdots + a_0 = \left(a_n c^{n-1} + \cdots + a_1\right) c + a_0 = \\ ((\ldots(a_n c + a_{n-1})c + \ldots)c + a_1)c + a_0$$

Stačí nám teda postupne počítať čísla a_n, $a_n c + a_{n-1}$, $(a_n c + a_{n-1})c + a_{n-2}$ atď., t.j. predchádzajúci výsledok vždy vynásobíme číslom c a pripočítame k nemu nasledujúci koeficient.

Príklad 4.5.7. Vypočítajte hodnotu polynómu $f(x) = x^4 - 3x^3 + 2x - 1$ nad poľom $\mathbb{R}$ v bode $c = 2$.

Do tabuľky si zapíšeme koeficienty polynómu (dôležité je nezabudnúť na nulový koeficient pochádzajúci z člena $0x^2$) a postupujeme postupom, ktorý sme naznačili.

	1	-3	0	2	-1
2		2	-2	-4	-4
	1	-1	-2	-2	$\boxed{-5}$

Všimnime sme, že súčasne sme vypočítali, že

$$x^4 - 3x^3 + 2x - 1 = (x^3 - x^2 - 2x - 2)(x-2) - 5.$$

(Stačí si uvedomiť, že pri Hornerovej schéme vlastne robíme to isté, čo pri algoritme na delenie polynómov.)

Aby sme si uvedomili, čo vlastne v Hornerovej schéme počítame, pokúsme sa ju zapísať o čosi všeobecnejšie (kvôli šírke rozdelené na 2 tabuľky)

	a_n	a_{n-1}	a_{n-2}	$\dots$
c		a_nc	$(a_nc+a_{n-1})c$	$\dots$
	a_n	a_nc+a_{n-1}	$a_nc^2+a_{n-1}c+a_{n-2}$	$\dots$

$\dots$	a_1	a_0
$\dots$	$\dots$	$(a_nc^{n-1}+a_{n-1}c^{n-2}+\cdots+a_1)c$
$\dots$	$a_nc^{n-1}+a_{n-1}c^{n-2}+\cdots+a_1$	$a_nc^n+a_{n-1}c^{n-1}+\cdots+a_1c+a_0=f(c)$

Príklad 4.5.8. Overte, že 1 je koreňom polynómu $f(x)=x^4-3x^3+3x-1\in\mathbb{R}[x]$. Zistite násobnosť tohoto koreňa.

Budeme postupovať pomocou Hornerovej schémy – pri vypočítaní hodnoty $f(1)$ súčasne nájdeme polynóm $g(x)$ taký, že $f(x)=g(x)(x-1)+f(1)$. Ak $f(1)=0$, na zistenie, či ide násobnosť tohoto koreňa je aspoň 2, stačí overiť, či aj $g(1)=0$. Analogicky postupujeme ďalej, až kým nedostaneme nenulový zvyšok.

	1	-3	0	3	-1
1		1	-2	-2	1
	1	-2	-2	1	$\boxed{0}$
1		1	-1	-3	
	1	-1	-3	$\boxed{-2}$	

Zistili sme, že 1 je jednoduchým (jednonásobným) koreňom polynómu $f(x)$ a že

$$f(x)=(x-1)(x^3-2x^2-2x+1),$$

pričom $x-1\nmid x^3-2x^2-2x+1$.

Rátať korene polynómov je vo všeobecnosti ťažká úloha. Zo strednej školy poznáte vzorec na hľadanie koreňov polynómov druhého stupňa – kvadratických polynómov. (Podobné vzorce, aj keď zložitejšie, sa dajú nájsť aj pre rovnice tretieho a štvrtého stupňa. Vo všeobecnosti však také vzorce neexistujú.) Okrem nich vieme ešte v komplexných číslach riešiť binomické rovnice, t.j. rovnice tvaru $x^n=a$, kde $a\in\mathbb{C}$ (pozri I-B.3.2 alebo [KGGS, kapitola 6.1]).

Povieme si, ako pre polynóm s celočíselnými koeficientami vieme nájsť všetky korene, ktoré sú racionálnymi číslami (t.j. všetky korene daného polynómu ležiace v poli $\mathbb{Q}$).

4.5.2 Racionálne korene polynómu s celočíselnými koeficientami

Tvrdenie 4.5.9. *Ak $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in\mathbb{Z}[x]$ je polynóm s celočíselnými koeficientami a racionálne číslo $c=\frac{p}{q}$ je koreň $f(x)$ (pričom $\gcd(p,q)=1$, t.j. racionálne číslo c je zapísané v základnom tvare), tak*

$$p\mid a_0 \qquad a \qquad q\mid a_n.$$

Dôkaz. Ak $c=\frac{p}{q}$ je koreň $f(x)$, tak máme rovnosť

$$f(c)=a_n\frac{p^n}{q^n}+a_{n-1}\frac{p^{n-1}}{q^{n-1}}+\cdots+a_1\frac{p}{q}+a_0=0.$$

Ak túto rovnosť vynásobíme q^n, dostaneme

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0.$$

(Všimnime si, že v predchádzajúcej rovnosti vystupujú iba celé čísla.)

Túto rovnosť môžeme upraviť ako

$$-a_n p^n = (a_{n-1} p^{n-1} + \cdots + a_1 p q^{n-2} + a_0 q^{n-1}) q,$$

čo znamená, že $q \mid a_n p^n$. Pretože $\gcd(p, q) = 1$ (p a q sú nesúdeliteľné), vyplýva z toho $q \mid a_n$ (dôsledok 4.4.23).

Pri dôkaze toho, že $p \mid a_0$ postupujeme takmer rovnako. Máme

$$-a_0 q^n = (a_n p^{n-1} + a_{n-1} p^{n-2} q + \cdots + a_1 q^{n-1}) p,$$

čiže $p \mid a_0 q^n$, a teda (na základe nesúdeliteľnosti) $p \mid a_0$. □

Predchádzajúce tvrdenie môžeme použiť na nájdenie všetkých racionálnych koreňov daného polynómu zo $\mathbb{Z}[x]$. Predchádzajúce tvrdenie nám poskytuje obmedzenie na všetkých možných kandidátov na korene. Postupným vyskúšaním nájdeme všetky korene.

Ďalšie obmedzenie, ktoré nám môže pomôcť pri skúšaní jednotlivých možností, nám poskytne nasledujúce pozorovanie (ktorého špeciálnym prípadom je tvrdenie 4.5.9).

Tvrdenie 4.5.10. *Nech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ je polynóm s celočíselnými koeficientami a racionálne číslo $c = \frac{p}{q}$ je koreň $f(x)$ (pričom $\gcd(p, q) = 1$, t.j. racionálne číslo c je zapísané v základnom tvare). Nech $g(x) = b_{n-1} x^{n-1} + \cdots + b_0$ je polynóm z $\mathbb{Q}[x]$ taký, že*

$$f(x) = g(x) \left(x - \frac{p}{q} \right).$$

Potom aj $g(x) \in \mathbb{Z}[x]$, t.j. koeficienty polynómu $g(x)$ sú celočíselné.

Dôkaz. Indukciou vzhľadom na k dokážeme, že pre $k = 0, \ldots, n-1$ je číslo b_k celé a je navyše deliteľné číslom q.

Pre $k = 0$ táto vlastnosť vyplýva z rovnosti $a_0 = -b_0 \frac{p}{q}$. Pretože a_0 je celé číslo, musí platiť $p \mid q$. Pritom $\gcd(p, q) = 1$, teda $q \mid b_0$ (dôsledok 4.4.23).

Predpokladajme, že b_{k-1} je celé číslo deliteľné q. Z predpokladov máme

$$a_k = b_{k-1} - b_k \frac{p}{q}.$$

Potom

$$b_k \frac{p}{q} = a_k - b_{k-1}$$

je celé číslo (rozdiel dvoch celých čísel), preto $q \mid b_k p$. Opäť, z toho, že $\gcd(p, q) = 1$, vyplýva $q \mid b_k$. □

Z predchádzajúceho tvrdenia vyplýva, že ak overujeme, či nejaké racionálne číslo je koreňom polynómu s celočíselnými koeficientami, v okamihu, keď nám v priebehu výpočtu vyjde v spodnom riadku zlomok, už nemusíme rátať ďalej. (Vieme totiž, že čísla v spodnom riadku Hornerovej schémy sú presne koeficienty polynómu $g(x)$, teda ak je dané racionálne číslo koreňom, musia všetky tieto koeficienty podľa predchádzajúceho tvrdenia byť celé čísla.)

Ukážme si teda hľadanie racionálnych koreňov daného polynómu zo $\mathbb{Z}[x]$ na konkrétnom príklade.

Príklad 4.5.11. Nájdite racionálne korene polynómu $f(x) = 24x^5+10x^4-x^3-19x^2-5x+6$ (aj s násobnosťami).

Podľa tvrdenia 4.5.9 má platiť $p \mid 6$, $q \mid 24$. Dostávame teda možnosti:
$p \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$
$q \in \{1, 2, 3, 4, 6, 8, 12, 24\}$
$\frac{p}{q} \in \{\pm 1, \pm \frac{1}{2}, \pm \frac{1}{3}, \dots\}$
(Pre q nám stačí skúšať kladné hodnoty, pretože voľba znamienok pre číslo p nám zabezpečí obidve možnosti – kladné aj záporné korene.)

Začnime najprv skúšať tých kandidátov na korene, kde čitateľ je ± 1.

	24	10	-1	-19	-5	6
1		24	34	33	14	9
	24	34	33	14	9	15

	24	10	-1	-19	-5	6
-1		-24	14	-13	32	-27
	24	-14	13	-32	27	-21

	24	10	-1	-19	-5	6
$\frac{1}{2}$		12	11	5	-7	-6
	24	22	10	-14	-12	0
$\frac{1}{2}$		12	17	$\frac{27}{2}$		
	24	34	27	$-\frac{1}{2}$	$\neq 0$	

Zistili sme, že $\frac{1}{2}$ je jednoduchý koreň polynómu $f(x)$. (V podslednom výpočte sme nerátali do konca – zastavili sme sa pri zlomku $-\frac{1}{2}$.)

Mohli by sme pokračovať v skúšaní možností ďalej, trochu nám však zjednoduší prácu, ak si uvedomíme, že všetky ďalšie korene musia byť koreňmi polynómu $g(x) = 24x^4 + 22x^3 + 10x^2 - 14x - 12$. (Tento polynóm je podiel polynómu $f(x)$ a polynómu $x - \frac{1}{2}$, jeho koeficienty vieme vyčítať z predchádzajúcej Hornerovej schémy.)

Každý koeficient tohoto polynómu je párny – môžeme teda celý polynóm vydeliť číslom 2 a dostaneme polynóm $12x^4 + 11x^3 + 5x^2 - 7x - 6$, ktorý má tiež celočíselné koeficienty a má rovnaké korene ako $g(x)$. Keď hľadáme racionálne korene tohoto polynómu, dostávame pre čitateľ a menovateľ podmienky $p \mid 6$, $q \mid 12$, čiže
$p \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$
$q \in \{1, 2, 3, 4, 6, 12\}$
$\frac{p}{q} \in \{\pm 1, \pm \frac{1}{2}, \pm \frac{1}{3} \pm \frac{1}{4}, \dots\}$
Pritom samozrejme čísla, ktoré sme už vyskúšali pre $f(x)$, pre polynóm $g(x)$ skúšať nemusíme. Získali sme teda dve zjednodušenia – budeme pracovať s polynómom nižšieho stupňa a máme menej možností, ktoré treba vyskúšať.

	12	11	5	-7	-6
$-\frac{1}{2}$		-6	$-\frac{5}{2}$		
	12	5	$\frac{5}{2}$		$\neq 0$

	12	11	5	-7	-6
$\frac{1}{3}$		4	5	$\frac{10}{3}$	
	12	15	10	$\frac{-11}{3}$	$\neq 0$

	12	11	5	-7	-6
$-\frac{1}{3}$		-4	$-\frac{7}{3}$		
	12	7	$-\frac{28}{3}$		$\neq 0$

	12	11	5	-7	-6
$\frac{1}{4}$		3	$\frac{14}{4}$		
	12	14			$\neq 0$

	12	11	5	-7	-6
$-\frac{1}{4}$		-2	$\frac{9}{4}$		
	12	9			$\neq 0$

	12	11	5	-7	-6
$\frac{1}{6}$		2	$\frac{13}{6}$		
	12	13			$\neq 0$

	12	11	5	-7	-6
$-\frac{1}{6}$		-2	$\frac{9}{6}$		
	12	9			$\neq 0$

	12	11	5	-7	-6
2		24	70	150	286
	12	35	75	143	$\boxed{280}$

	12	11	5	-7	-6
-2		-24	26	-62	138
	12	-13	31	-69	$\boxed{132}$

	12	11	5	-7	-6
$\frac{2}{3}$		8	$\frac{38}{3}$		
	12	19			$\neq 0$

	12	11	5	-7	-6
$-\frac{2}{3}$		-8	-2	-2	6
	12	3	3	-9	$\boxed{0}$
$-\frac{2}{3}$		-8	$\frac{10}{3}$		
	12	-5		$\neq 0$	

Dostali sme ďalší jednoduchý koreň $-\frac{2}{3}$. Nový polynóm, s ktorým budeme pracovať, je $h(x) = 12x^3+3x^2+3x-9$. Po vydelení koeficientov číslom 3 dostaneme jednoduchší polynóm $4x^3 + x^2 + x - 3$ a podmienky pre korene $p \mid 3$, $q \mid 4$, čiže
$p \in \{\pm 1, \pm 3\}$
$q \in \{1, 2, 4\}$
$\frac{p}{q} \in \{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm 3, \pm\frac{3}{2} \pm \frac{3}{4}\}$

	4	1	1	-3
3		12	39	120
	4	13	40	$\boxed{117}$

	4	1	1	-3
-3		-12	33	-102
	4	-11	34	$\boxed{-105}$

$$\begin{array}{c|cccc} & 4 & 1 & 1 & -3 \\ \frac{3}{2} & & 6 & \frac{21}{2} & \\ \hline & 4 & 7 & & \neq 0 \end{array}$$

$$\begin{array}{c|cccc} & 4 & 1 & 1 & -3 \\ -\frac{3}{2} & & -6 & -\frac{15}{2} & \\ \hline & 4 & -5 & & \neq 0 \end{array}$$

$$\begin{array}{c|cccc} & 4 & 1 & 1 & -3 \\ \frac{3}{4} & & 3 & 3 & 3 \\ \hline & 4 & 4 & 4 & \boxed{0} \\ \frac{3}{4} & & 3 & \frac{21}{4} & \\ \hline & 4 & 7 & \neq 0 & \end{array}$$

Našli sme ďalší jednoduchý koreň $\frac{3}{4}$

Ďalej môžeme pracovať s polynómom $x^2 + x + 1$. Tu sú však jediní možní kandidáti na korene čísla ± 1 a tie sme už vyskúšali.

Záver: Daný polynóm má tieto 3 racionálne korene: $\frac{1}{2}$, $-\frac{2}{3}$, $\frac{3}{4}$; násobnosť každého z nich je 1.

Všimnime si, že sme vlastne súčasne dostali, že

$$f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6 = 24(x - \frac{1}{2})(x + \frac{2}{3})(x - \frac{3}{4})(x^2 + x + 1).$$

(Pri poslednom delení nám vyšiel podiel $4(x^2 + x + 1)$ a v priebehu výpočtu sme polynóm vydelili raz číslom 2 a raz číslom 3.) Predchádzajúcu rovnosť môžeme tiež prepísať ako

$$f(x) = (2x - 1)(3x + 2)(4x - 3)(x^2 + x + 1).$$

4.5.3 Algebraicky uzavreté polia

Definícia 4.5.12. Pole F sa nazýva *algebraicky uzavreté,* ak každý polynóm $f(x) \in F[x]$ stupňa aspoň jedna má v poli F aspoň jeden koreň.

V prípade, že $f(x)$ má koreň c, môžeme ho vydeliť koreňovým činiteľom $x - c$ a dostaneme jeho deliteľ nižšieho stupňa. Ten opäť musí mať nejaký koreň (ak nie je konštatný), preto takýmto spôsobom postupne dostaneme rozklad polynómu $f(x)$ na koreňové činitele. Dostávame:

Tvrdenie 4.5.13. *Ak F je algebraicky uzavreté pole, tak každý polynóm $f(x)$ je v $F[x]$ rozložiteľný na koreňové činitele.*

Z toho ďalej vidno, že ak F je algebraicky uzavreté pole, tak súčet násobností koreňov polynómu $f(x)$ je rovný jeho stupňu. (Toto tvrdenie sa zvyčajne formuluje tak, že polynóm stupňa n má práve n koreňov, ak zarátame aj ich násobnosti.)

Vieme, že pole komplexných čísel $\mathbb{C}$ má túto vlastnosť (aj keď dôkaz tejto vety nie je jednoduchý).

Veta 4.5.14 (Základná veta algebry). *Pole komplexných čísel $\mathbb{C}$ je algebraicky uzavreté.*

Spomeňme (opäť bez dôkazu), že ku každému poľu sa dá zostrojiť nadpole, v ktorom už každý polynóm z $F[x]$ bude mať koreň. Dokonca platí:

Veta 4.5.15 (Steinitz). *Pre každé pole F existuje algebraicky uzavreté nadpole F'.*

Všimnime si ešte jednu užitočnú vlastnosť komplexných koreňov polynómov s reálnymi koeficientami.

Tvrdenie 4.5.16. *Ak $f(x) \in \mathbb{R}[x]$ je polynóm s reálnymi koeficientami a $z = a + bi \in \mathbb{C}$ je koreň polynómu $f(x)$, tak aj komplexne združené číslo $\overline{z} = a - bi$ je koreňom polynómu $f(x)$. Pritom násobnosť koreňa $\overline{z}$ je rovnaká ako násobnosť z.*

Dôkaz. Stačí si všimnúť, že zobrazenie $z \mapsto \overline{z}$ je homomorfizmus (súčet/súčin komplexne združených čísel je komplexne združené číslo k súčtu/súčinu) a že pre $z \in \mathbb{R}$ platí $\overline{z} = z$. Z toho potom dostávame rovnosť

$$\overline{f(z)} = \overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0} = a_n (\overline{z})^n + a_{n-1} (\overline{z})^{n-1} + \cdots + a_0 = f(\overline{z})$$

pre ľubovoľné $z \in \mathbb{C}$.

Z tejto rovnosti špeciálne vyplýva, že ak $f(z) = 0$, tak aj $f(\overline{z}) = 0$.

Druhá časť vyplýva z prvej použitej pre polynóm zapísaný v tvare $f(x) = g(x)(x - z)^k$, kde k je násobnosť koreňa z. □

Veľmi prirodzeným zovšeobecnením tohoto výsledku je tvrdenie sformulované v úlohe 4.5.1.

Dôsledok 4.5.17. *Každý polynóm $f(x) \in \mathbb{R}[x]$ nepárneho stupňa má aspoň 1 reálny koreň.*

Dôkaz. Ak by polynóm mal iba komplexné korene, tak môžeme popárovať dvojice komplexne združených koreňov. Komplexne združené korene majú podľa predchádzajúceho tvrdenia rovnakú násobnosť. Preto súčet násobností všetkých komplexných koreňov je párne číslo. Súčet násobností sa však rovná stupňu polynómu $f(x)$ (pretože $\mathbb{C}$ je algebraicky uzavreté pole). □

4.5.4 Ireducibilné polynómy

Definícia 4.5.18. Polynóm $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ sa nazýva *normovaný* (alebo tiež *monický,*) ak $a_n = 1$ (vedúci koeficient sa rovná 1).

Definícia 4.5.19. Ak R je obor integrity, tak ireducibilné prvky okruhu $R[x]$ nazývame *ireducibilné polynómy* v $R[x]$.

V prípade, že ide o pole, tak z predchádzajúcej kapitoly vieme, že $F[x]$ je euklidovský okruh (a teda je to aj okruh hlavných ideálov a okruh s jednoznačným rozkladom). Tento fakt nám umožní používať všetky výsledky z predchádzajúcej kapitoly aj pre polynómy nad nejakým poľom.

Veta 4.5.20 (Rozklad na ireducibilné polynómy). *Ak F je pole, tak každý polynóm $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ možno vyjadriť v tvare*

$$f(x) = a_n p_1(x) \dots p_n(x),$$

kde $p_1, \dots, p_n$ sú ireducibilné normované polynómy. Navyše, tento rozklad je (až na poradie činiteľov) jednoznačne určený.

Dôkaz. Pretože $F[x]$ je okruh s jednoznačným rozkladom, vieme, že každý polynóm sa dá rozložiť na súčin ireducibilných polynómov a ten rozklad je jednoznačný až na asociovanosť. V okruhu $F[x]$ sú dva prvky asociované práve vtedy, keď sa líšia iba konštantným násobkom. Tým, že vo vete požadujeme normované polynómy, sú teda už jednoznačne určené (z ľubovoľného polynómu dostaneme normovaný, keď ho vynásobíme b_m^{-1}, kde b_m je jeho vedúci koeficient; súčin vedúcich koeficientov sme dali pred súčin normovaných činiteľov – tento súčin sa rovná a_n). □

Zatiaľ však o ireducibilných polynómoch vieme iba to, že existujú – nevieme, ako overiť, či je daný polynóm ireducibilný ani ako rozklad na súčin ireducibilných polynómov hľadať.

Je zrejmé, že každý polynóm stupňa 1 je ireducibilný – nedá sa rozložiť na súčin polynómov nižších stupňov. Teda ak c je k-násobný koreň, v rozklade polynómu $f(x)$ sa musí vyskytnúť $(x-c)^k$. V prípade, že súčet násobností koreňov je rovný stupňu polynómu vieme teda ten polynóm rozložiť ako

$$f(x) = a_n(x-c_1)^{k_1}(x-c_2)^{k_2}\dots(x-c_m)^{k_m},$$

kde $c_1,\dots,c_m$ sú všetky korene $f(x)$ a $k_1,\dots,k_m$ sú ich násobnosti. Takýto rozklad (ak existuje) voláme rozklad na súčin *koreňových činiteľov.*

V niektorých prípadoch vieme o ireducibilite rozhodnúť, ak poznáme korene polynómu.

Tvrdenie 4.5.21. *Ak F je pole a $f(x) \in F[x]$ je polynóm stupňa 2 alebo 3, tak polynóm $f(x)$ je ireduciblný v F práve vtedy, keď $f(x)$ nemá koreň v F.*

Dôkaz. Stačí si všimnúť, že ak chceme polynóm stupňa 2 alebo 3 rozložiť ako súčin polynómov nižších stupňov, nevyhnutne sa tam musí vyskytnúť polynóm stupňa 1. Z lemy 4.5.4 vieme, ako súvisia lineárne delitele polynómu a jeho korene. □

Všimnime si, že ireducibilita polynómu závisí od toho, nad akým poľom ho uvažujeme (pretože polynóm nad poľom F môžeme súčasne chápať aj ako polynóm nad ľubovoľným nadpoľom $F' \supseteq F$).

Príklad 4.5.22. Uvažujme polynóm $f(x) = x^4+1$. Tento polynóm má celočíselné koeficienty, môžeme sa teda skúmať jeho ireducibilitu v okruhoch polynómov $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ aj $\mathbb{C}[x]$.

V poli $\mathbb{C}$ má tento polynóm 4 korene $\frac{\pm\sqrt{2}\pm\sqrt{2}i}{2}$ (vieme ich nájsť riešením binomickej rovnice $x^4 = -1$). Teda v $\mathbb{C}$ máme rozklad

$$x^4+1 = \left(x - \frac{\sqrt{2}+\sqrt{2}i}{2}\right)\left(x - \frac{\sqrt{2}-\sqrt{2}i}{2}\right)\left(x + \frac{\sqrt{2}+\sqrt{2}i}{2}\right)\left(x + \frac{\sqrt{2}-\sqrt{2}i}{2}\right)$$

Nad poľom $\mathbb{R}$ máme rozklad

$$x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1).$$

(Polynómy v rozklade môžeme získať napríklad ako súčin koreňových činiteľov pre komplexne združené korene. Alebo tento rozklad môžeme dostať tak, že si všimneme rovnosť $x^4+1 = (x^2+1)^2-(\sqrt{2}x)^2$.) Pritom oba polynómy $x^2 \pm \sqrt{2}x+1$ sú už nad $\mathbb{R}$ nerozložiteľné – pretože nemajú reálne korene.

Nad poľom $\mathbb{Q}$ je tento polynóm ireducibilný. Ak by sa totiž dal rozložiť na súčin nejakých polynómov, bol by súčasne aj súčinom týchto polynómov v $\mathbb{R}[x]$. Ako sme však videli, jediný (až na poradie a asociovanosť) rozklad na súčin polynómov nižšieho stupňa v $\mathbb{R}[x]$ je $x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$ a polynómy, ktoré vystupujú v tomto rozklade, nepatria do $\mathbb{Q}[x]$.

4.5.5 Ireducibilné polynómy nad $\mathbb{Q}$ a $\mathbb{R}$

Z toho, čo doteraz vieme, sme schopní aspoň v niektorých konkrétnych prípadoch nájsť rozklad daného polynómu na súčin ireducibilných polynómov.

Postupovať môžeme tak, že hľadáme korene polynómu – pomocou hľadania racionálnych koreňov, riešením kvadratickej alebo binomickej rovnice (prípadne iných typov rovníc, ktoré

vieme riešiť, ako sú reciproké rovnice, bikvadratické rovnice, kubické rovnice, rovnice štvrtého stupňa). Po nájdení koreňov môžeme polynóm vydeliť koreňovými činiteľmi (a znovu sa pokúsiť riešiť novú rovnicu nižšieho stupňa než bola pôvodná). V prípade, že by polynóm mal násobné korene, dá sa znížiť jeho stupeň použitím derivácie – o tom si ešte v tejto kapitole povieme.

V prípade, že po vydelení dostaneme polynóm dostatočne nízkeho stupňa, ktorý nemá korene, vieme už, že je ireducibilný.

Príklad 4.5.23. V príklade 4.5.11 sme zistili, že

$$f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6 = 24\left(x - \frac{1}{2}\right)\left(x + \frac{2}{3}\right)\left(x - \frac{3}{4}\right)(x^2 + x + 1).$$

Pretože polynóm $x^2 + x + 1$ nemá reálne korene (a je to polynóm druhého stupňa), je to rozklad na ireducibilné polynómy nad $\mathbb{R}$ (a tým pádom aj nad $\mathbb{Q}$). Rozklad nad $\mathbb{C}$ by sme získali, keby sme ešte $x^2 + x + 1$ rozložili na ireducibilné činitele.

Všimnime si, že sme vlastne dostali aj rozklad

$$f(x) = (2x - 1)(3x + 2)(4x - 3)(x^2 + x + 1)$$

v $\mathbb{Z}[x]$.

Viac o rozklade polynómov na ireducibilné činitele (a o algoritmoch používaných na jeho výpočet) sa môžete dozvedieť na predmete počítačová algebra, pozri napríklad [G1, G2].

4.5.6 Derivácia a Taylorov rozvoj polynómov

Definícia 4.5.24. *Formálna derivácia* polynómu $f(x) = \sum_{k=0}^{n} a_k x^k$ je polynóm $Df(x) = \sum_{k=1}^{n} k \times a_k x^{k-1}$.

V prípade, že pracujeme nad ľubovoľným poľom, môže sa stať, že nenulový polynóm má nulovú deriváciu.

Príklad 4.5.25. Pre $f(x) = x^p$ v $\mathbb{Z}_p[x]$ dostávame $Df(x) = p \times x^{p-1} = 0$.

Priamo z definície sa dá overiť, že takto definovaná formálna derivácia má podobné vlastnosti, na aké sme zvyknutí z analýzy.

Tvrdenie 4.5.26. *Nech F je pole. Pre ľubovoľné $c \in F$, $f(x), g(x) \in F[x]$ platí*

$$D(f(x) + g(x)) = Df(x) + Dg(x)$$
$$D(cf(x)) = cDf(x)$$
$$D(f(x)g(x)) = Df(x).g(x) + f(x).Dg(x)$$

Dôkaz. Overme iba tretiu rovnosť (prvé dve sú skutočne jedoduché). Koeficient pri x^n v polynóme na ľavej strane tejto rovnosti je $(n+1)$-násobok koeficientu polynómu $f(x).g(x)$ pri x^n.

Označme koeficienty polynómu $f(x)$ ako a_k, koeficienty polynómu $g(x)$ ako b_k. Pre koeficienty polynómu na ľavej strane rovnosti potom máme

$$l_n = (n+1) \times \sum_{k=0}^{n+1} a_k b_{n+1-k}$$

Na pravej strane rovnosti dostávame

$$p_n = \sum_{k=0}^{n}(k+1) \times a_{k+1}b_{n-k} + \sum_{k=0}^{n}(n+1-k) \times a_k b_{n+1-k}.$$

Zmenou sumačného indexu v prvej sume dostaneme vyjadrenie

$$p_n = \sum_{k=1}^{n+1} k \times a_k b_{n+1-k} + \sum_{k=0}^{n}(n+1-k) \times a_k b_{n+1-k} = \sum_{k=0}^{n+1}(n+1) \times a_k b_{n+1-k} = l_n$$

(aby sme uvedené členy mohli zlúčiť do jednej sumy, pridali sme dva nulové členy – v prvej sume pre $k = 0$ člen $0 \times a_0 b_{n+1}$ a v druhej sume pre $k = n+1$ člen $0 \times a_{n+1}b_0$). □

Uvedieme si dve tvrdenia, ktoré ukazujú, prečo je tento pojem užitočný – prvé z nich je vyjadrenie Taylorovho polynómu v nejakom $c \in F$; druhé z nich hovorí o tom, či nejaký polynóm má násobné korene.

Tvrdenie 4.5.27. *Nech F je pole, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$. Potom existujú jednoznačne určené $b_0, b_1, \ldots, b_n \in F$ také, že*

$$f(x) = b_n(x-c)^n + \cdots + b_1(x-c) + b_0. \tag{4.4}$$

Dôkaz. Indukciou vzhľadom na n. Ak $n = 0$, tak stačí položiť $a_0 = b_0$ (a inú možnosť očividne nemáme).

Predpokladajme, že uvedené tvrdenie platí pre polynómy stupňa nanajvýš $n-1$. Podľa lemy 4.5.3

$$f(x) = g(x)(x-c) + f(c). \tag{4.5}$$

Polynóm $g(x)$ je stupňa najviac $n-1$- Podľa indukčného predpokladu existujú $b_1, \ldots, b_n \in F$ také, že $g(x) = b_n(x-c)^{n-1} + \cdots + b_2(x-c) + b_1$. Položme $b_0 = f(c)$. Potom pre $f(x)$ platí

$$f(x) = (b_n(x-c)^{n-1} + \cdots + b_2(x-c) + b_1)(x-c) + b_0 = b_n(x-c)^n + \cdots + b_1(x-c) + b_0.$$

Tým máme dokázanú existenciu.

Ak dosadíme do rovnosti (4.4) $x = c$, tak vidíme, že $b_0 = f(c)$. Ďalej polynóm $g(x)$ z (4.5) je podľa vety o delení so zvyškom jednoznačne určený. K tomuto polynómu sú podľa indukčného predpokladu jednoznačne určené $b_1, b_2, \ldots, b_n \in F$. □

Tvrdenie 4.5.28. *Ak F je pole charakteristiky ∞, tak koeficienty $b_0, \ldots, b_n$ z tvrdenia* 4.5.27 *možno vyjadriť ako*

$$b_n = \frac{D^{(n)}f(c)}{n!},$$

kde znak $D^{(n)}$ znamená, že polynóm $f(x)$ zderivujeme n-krát.

Dôkaz. Toto tvrdenie dostaneme priamo z rovnosti (4.4) viacnásobným zderivovaním (resp. ho môžeme ukázať pomocou indukcie). □

Rozvoj v tvare (4.4) môžeme dostať aj pomocou Hornerovej schémy – teda Hornerova schéma nám poskytuje možnosť vypočítať hodnoty $D^{(n)}f(c)$ pre daný polynóm $f(x)$ a $c \in F$.

Pred dôkazom nasledujúceho tvrdenia si všimnime jednu dôležitú vlastnosť najväčšieho spoločného deliteľa – konkrétne fakt, že zostane taký istý, aj keď prejdeme k nejakému nadpoľu.

Poznámka 4.5.29. Už sme spomínali, že ak $f(x), g(x) \in F[x]$ a $F' \supseteq F$ je nadpole poľa F, tak polynómy $f(x)$ a $g(x)$ sú súčasne aj prvkami $F'[x]$. To znamená, že sa môžeme pýtať na najväčší spoločný deliteľ týchto 2 polynómov v okruhu $F[x]$ i v okruhu $F'[x]$. V obidvoch prípadoch je tento polynóm rovnaký.

Výplýva to z toho, že podiel a zvyšok pri delení dvoch polynómov z $F[x]$ vyjde rovnako, bez ohľadu na to, či delíme so zvyškom v $F[x]$ alebo v $F'[x]$. (V $F[x]$ sa dajú vydeliť tak, aby podiel i zvyšok mali koeficienty z F, podiel v $F'[x]$ je rovnaký, pretože vo vete o delení so zvyškom máme jednoznačnosť.)

Z toho vyplýva aj to, že relácia „delí“ nezávisí od toho, či sa na polynómy $f(x)$, $g(x)$ pozeráme ako na prvky $F[x]$ alebo ako na prvky $F'[x]$.

Tvrdenie 4.5.30. *Nech F je pole, $F' \supseteq F$ je jeho nadpole. Nech $f(x) \in F[x]$ je polynóm nad poľom F. Ak v nadpoli F' existuje násobný koreň polynómu $f(x)$, tak polynómy $f(x)$ a $Df(x)$ sú súdeliteľné, t.j.*

$$\mathrm{st}(\gcd(f(x), D(f(x)))) \geq 1.$$

Dôkaz. Ak c je násobný koreň $f(x)$, tak podľa definície 4.5.5 $f(x) = g(x)(x-c)^k$, kde $k > 1$. Potom

$$Df(x) = Dg(x)(x-c)^k + k \times g(x)(x-c)^{k-1} = (x-c)^{k-1}(Dg(x)(x-c) + k \times g(x)),$$

teda $x - c \mid Df(x)$. Keďže súčasne $x - c \mid f(x)$, máme

$$x - c \mid \gcd(f(x), Df(x))$$

a $\mathrm{st}(\gcd(f(x), D(f(x)))) \geq 1$. (Predchádzajúcu nerovnosť sme dokázali pre najväčší spoločný deliteľ v $F'[x]$. Na základe poznámky 4.5.29 je však najväčší spoločný deliteľ v $F[x]$ rovnaký.) □

Predchádzajúce tvrdenie nám umožní nájsť polynóm, ktorý má rovnaké korene ako daný polynóm, ale každý koreň má násobnosť 1. Pred uvedením tohoto výsledku však potrebujeme zaviesť pojem charakteristiky poľa.

Definícia 4.5.31. *Charakteristika poľa F* je najmenšie prirodzené číslo $k > 0$ s vlastnosťou $k \times 1 = 0$. Označujeme ju $\mathrm{char}(F)$. Ak neexistuje k s uvedenou vlastnosťou, tak definujeme $\mathrm{char}(F) = \infty$.

Ak $\mathrm{char}(F) = k$, tak pre každé $c \in F$ platí $k \times c = c.(k \times 1) = c.0 = 0$.

Tvrdenie 4.5.32. *Nech F je pole s nekonečnou charakteristikou. Nech $f(x) \in F[x]$ a $h(x)$ je najväčší spoločný deliteľ $f(x)$ a $Df(x)$. Potom existuje polynóm $g(x)$ s vlastnosťami*

(i) $f(x) = g(x).h(x)$,

(ii) *$g(x)$ má v každom nadpoli poľa F tie isté koreň ako $f(x)$,*

(iii) *násobnosť každého koreňa $g(x)$ je 1.*

Dôkaz. Pretože $\mathrm{char}(F) = \infty$, máme $Df(x) \neq 0$. (Vedúci koeficient $Df(x)$ je $n \times a_n$, kde a_n je vedúci koeficient $f(x)$. V poli s nekonečnou charakteristiokou z $a \neq 0$ vyplýva $n \times a \neq 0$.)

Potom aj $h(x)$ je nenulový polynóm. Navyše $h(x) \mid f(x)$, takže pri delení so zvyškom dostaneme

$$f(x) = g(x)h(x) + 0.$$

Ak c je násobný koreň $f(x)$ s násobnosťou k, tak platí $f(x) = (x-c)^k f_1(x)$, pričom c nie je koreňom $f_1(x)$. Z predchádzajúcej rovnosti dostaneme

$$Df(x) = Df_1(x)(x-c)^k + k \times f_1(x)(x-c)^{k-1} = (x-c)^{k-1}(Df_1(x)(x-c) + k \times f_1(x)).$$

Potom

$$h(x) = \gcd(f(x), Df(x)) = (x-c)^{k-1} \gcd((x-c)f_1(x), Df_1(x)(x-c) + k \times f_1(x)).$$

Pritom $x - c \nmid f_1(x)$, z čoho vyplýva $x - c \nmid Df_1(x)(x-c) + k \times f_1(x)$ a

$$x - c \nmid \gcd((x-c)f_1(x), Df_1(x)(x-c) + k \times f_1(x)).$$

Teda

$$(x-c)^k \nmid h(x)$$

(c je len $k-1$-násobným koreňom $h(x)$). T.j., ak vyjadríme $h(x)$ v tvare $h(x) = (x-c)^{k-1}h_1(x)$, tak $x - c \nmid h(x)$. Potom máme

$$(x-c)^k \mid g(x)h(x) = g(x)h_1(x)(x-c)^{k-1}$$
$$x - c \mid g(x)h_1(x)$$

Pretože $x - c$ je ireducibilný a $x - c \nmid h_1(x)$, vyplýva z toho už $x - c \mid g(x)$, čiže c je koreňom $g(x)$.

Navyše, c je iba jednoduchý koreň $g(x)$, v opačnom prípade by sme mali $(x-c)^2 \mid g(x)$, a teda

$$(x-c)^{k+1} \mid g(x)h_1(x-c)^{k-1} = g(x)h(x) = f(x).$$

To je spor s tým, že násobnosť koreňa c je k. □

Príklad 4.5.33. Majme polynóm $f(x) = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$. Potom $Df(x) = 4x^3 + 4x$ a ich normovaný najväčší spoločný deliteľ je

$$h(x) = \gcd(f(x), Df(x)) = x^2 + 1 = x^4 + 2x^2 + 1 - \frac{x}{4}(4x^3 + 4x).$$

Po vydelení $f(x)$ polynómom $h(x)$ dostaneme $g(x) = x^2 + 1$.

Skutočne, polynómy $f(x) = (x^2+1)^2$ a $g(x) = x^2 + 1$ majú v $\mathbb{C}$ tie isté korene $\pm i$, v prípade polynómu $g(x)$ sú to jednoduché korene.

Cvičenia

Úloha 4.5.1. Nech F je pole, F' je jeho nadpole a $\varphi\colon F' \to F'$ je homomorfizmus taký, že $\varphi(x) = x$ pre každé $x \in F$ (nemení prvky poľa F). Potom pre každý koreň c polynómu $f(x)$ je aj $\varphi(c)$ koreňom $f(x)$.

Úloha 4.5.2. Vedeli by ste dokázať dôsledok 4.5.17 na základe poznatkov, ktoré máte z analýzy?

Kapitola 5

Polia

5.1 Podielové pole

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.
(Celé čísla dal ľuďom dobrotivý Boh, všetko ostatné už je ľudským dielom.)
Leopold Kronecker

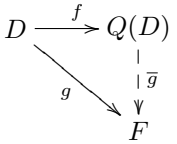
V tejto časti zodpovieme otázku, ktoré okruhy môžu byť podokruhmi polí. Je zrejmé, že podokruh poľa musí byť komutatívny okruh. Takisto nemôže obsahovať delitele jednotky – boli by deliteľmi jednotky už v jeho nadpoli.

Táto otázka má teda zmysel hlavne pre obory integrity. V nasledujúcej vete dokážeme, že každý obor integrity je podokruhom nejakého poľa.

Definícia 5.1.1. Hovoríme, že okruh R je *vnorený* do okruhu R' ak existuje injektívny homomorfizmus $f\colon R \to R'$. Injektívny homomorfizmus $f\colon R \to R'$ nazývame *vnorenie.*

Vnorenie je vlastne izomorfizmus na podokruh $\operatorname{Im} f$, to znamená, že okruh R môžeme chápať priamo ako podokruh R'.

Veta 5.1.2. *Pre každý obor integrity D existuje pole $Q(D)$ a vnorenie $f\colon D \to Q(D)$ s nasledujúcou vlastnosťou: Pre každé vnorenie $g\colon D \to F$ do poľa F existuje vnorenie $\overline{g}\colon Q(D) \to F$ také, že $\overline{g} \circ f = g$.*



Význam podmienky v predchádzajúcej vete je o trochu jasnejší, keď si uvedomíme, že injektívne zobrazenie f nám hovorí, že obor integrity D môžeme chápať ako podokruh $Q(D)$. V prípade, že stotožníme prvky z D s ich obrazmi nám teda táto podmienka vlastne hovorí, že každé vloženie $g\colon D \to F$ do nejakého poľa F možno rozšíriť na vloženie celého $Q(D)$. (Teda $Q(D)$ je v istom zmysle najmenšie pole obsahujúce D.)

Dôkaz vety 5.1.2 urobíme vo viacerých krokoch – najprv zadefinujeme, ako vyzerá pre daný obor integrity pole $Q(D)$, postupne overíme, že spĺňa vlastnosti z definície poľa aj vlastnosť uvedenú vo vete.

Lema 5.1.3. *Nech D je obor integrity. Na množine $D \times (D \setminus \{0\})$ definujeme reláciu $\equiv$ predpisom*

$$(a,b) \equiv (c,d) \qquad \overset{def}{\Leftrightarrow} \qquad ad = bc.$$

Potom táto relácia je reláciou ekvivalencie a jej triedy $[(a,b)]$ nazývame zlomkami *nad oborom integrity D.*

Všimnite si, že relácia ekvivalencie je definovaná rovnako ako rovnosť zlomkov predstavujúcich racionálne čísla – ako uvidíme, celá konštrukcia podielového poľa $Q(D)$, ktorá bude nasledovať, pripomína spôsob, ktorým z okruhu celých čísel $\mathbb{Z}$ dostaneme pole racionálnych čísel $\mathbb{Q}$. (Väčšina dôkazov je skoro rovnaká, ako keby sme overovali, že $\mathbb{Q}$ je pole a spĺňa vlastnosť uvedenú vo vete 5.1.2.) V mnohých učebniciach, aby sa zdôraznila podobnosť s konštrukciou racionálnych čísel, sa pre zlomky nad D používa priamo označenie $\frac{a}{b}$ namiesto nášho označenia $[(a,b)]$.

Dôkaz. Dôkaz, že ide relácia $\equiv$ je reflexívna a symetrická je úplne priamočiary – cvičenie.

Tranzitívnosť: Nech $(a,b) \equiv (c,d)$ a $(c,d) \equiv (e,f)$. To znamená, že $ad = bc$ a $cf = de$.

Ak prvú rovnosť vynásobíme prvkom f a druhú prvkom b, dostaneme $adf = bcf = bde$, čiže $d(af - be) = 0$. Pretože D je obor integrity a $d \neq 0$, máme $af - be = 0$, teda

$$af = be$$

a $(a,b) \equiv (e,f)$. □

Lema 5.1.4. *Označme $Q(D)$ množinu všetkých tried ekvivalencie $\equiv$ na množine $D \times (D \setminus \{0\})$ (čiže množinu všetkých zlomkov nad D). Na tejto množine definujeme operácie $+$ a $\cdot$ predpismi*

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)],$$
$$[(a,b)] \cdot [(c,d)] = [(ac, bd)].$$

Potom $+$ a $\cdot$ sú dobre definované a $(Q(D), +, \cdot)$ je pole.

Dôkaz. Najprv ukážeme, že obe operácie sú dobre definované, čiže nezávisia od výberu reprezentantov. Nech teda $(a,b) \equiv (a',b')$, čiže

$$ab' = a'b.$$

Potom máme

$$(ad + bc)b'd = ab'd^2 + bb'cd = a'bd^2 + bb'cd = (a'd + b'c)bd$$
$$acb'd = ab'cd = a'bcd = a'cbd$$

čo znamená

$$[(ad + bc, bd)] = [(a'd + b'c, b'd)]$$
$$[(ac, bd)] = [(a'c, b'd)]$$

$(Q(D), +)$ *je komutatívna grupa.* Komutatívnosť je zrejmá. Asociatívnosť overíme priamym výpočtom.

$$([(a,b)] + [(c,d)]) + [(e,f)] = [(ad + bc, bd)] + [(e,f)] = [(adf + bcf + bde, bdf)]$$
$$[(a,b)] + ([(c,d)] + [(e,f)]) = [(a,b)] + [(cf + ed, df)] = [(adf + bcf + bed, bdf)]$$

Neutrálny prvok pre sčitovanie je $[(0,1)]$, opačný prvok k triede $[(a,b)]$ je $[(-a,b)]$.

$(Q(D) \setminus \{0\}, \cdot)$ *je komutatívna grupa.* Komutatívnosť je zrejmá, asociatívnosť sa ľahko overí priamym výpočtom. Neutrálny prvok vzhľadom na násobenie je $[(1,1)]$. Všimnime si, že $[(a,b)] \neq [(0,1)]$ práve vtedy, keď $a \neq 0$. Preto každý nenulový prvok $[(a,b)]$ má inverzný prvok $[(b,a)]$.

Distributívnosť. Keďže ide o komutatívny okruh, stačí overovať iba jednu z podbmienok distributívnosti. Distributívnosť sa overí priamočiarym prepísaním z definície.

$$[(a,b)] \cdot ([(c,d)] + [(e,f)]) = [(a,b)] \cdot [(cf+de, df)] = [(a(cf+de), bdf)] =$$
$$= [(acf, bdf)] + [(ade, bdf)] = [(ac,bd)] + [(ae,bf)] = [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)]$$

□

Lema 5.1.5. *Zobrazenie* $f\colon D \to Q(D)$

$$f\colon a \mapsto [(a,1)]$$

je injektívny homomorfizmus okruhov.

Ďalej pre ľubovoľný injektívny homomorfizmus $g\colon D \to F$*, kde* F *je pole existuje homomorfizmus* $\overline{g}\colon Q(D) \to F$ *s vlastnosťou* $\overline{g} \circ f = g$*.*

Dôkaz. Zobrazenie f je homomorfizmus:

$$a + b \mapsto [(a+b,1)] = [(a,1)] + [(b,1)]$$
$$ab \mapsto [(ab,1)] = [(a,1)] \cdot [(b,1)]$$

Zobrazenie f je injektívne: rovnosť $[a,1] = [b,1]$ znamená, že $a.1 = b.1$, čiže $a = b$.

Ak $g\colon D \to F$ je injektívny homomorfizmus z D do nejakého poľa F, definujme $\overline{g}\colon Q(D) \to F$ predpisom

$$\overline{g}\colon [(a,b)] \mapsto g(a)g(b)^{-1}.$$

(Pretože g je injektívny homomorfizmus, máme $\operatorname{Ker} g = \{0\}$, čiže $g(b) \neq 0$ pre každé $b \in D \setminus \{0\}$. Uvedený predpis teda skutočne má zmysel.)

Zobrazenie $\overline{g}$ *je dobre definované.* Zobrazenie $\overline{g}$ sme definovali pomocou nejakého reprezentanta triedy $[(a,b)]$ – chceme ukázať, že výsledok zobrazenia nezávisí od výberu reprezentanta. Nech teda $(c,d) \equiv (a,b)$, čiže $ad = bc$. Potom dostávame (z toho, že g je homomorfizmus)

$$g(a)g(d) = g(b)g(c)$$

Po vynásobení tejto rovnosti $g(b)^{-1}g(d)^{-1}$ máme

$$g(a)g(b)^{-1} = g(c)g(d)^{-1}.$$

Čiže hodnota $\overline{g}$ skutočne nezávisí od výberu reprezentanta.

Zobrazenie $\overline{g}$ *je homomorfizmus.* Zachováva sčitovanie:

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)] \mapsto g(ad+bc)g(bd^{-1}) = (g(ad) + g(bd))g(bd)^{-1} =$$
$$= g(a)g(d)g(b)^{-1}g(d)^{-1} + g(b)g(c)g(b)^{-1}g(d)^{-1} =$$
$$= g(a)g(b)^{-1} + g(c)g(d)^{-1} = \overline{g}([(a,b)]) + \overline{g}([(c,d)])$$

Zachováva násobenie:

$$[(a,b)]\cdot[(c,d)] = [(ac,bd)] \mapsto g(ac)g(bd)^{-1} =$$
$$= g(a)g(b)^{-1}g(c)g(d)^{-1} = \overline{g}([(a,b)])\cdot\overline{g}([(c,d)])$$

Homomorfizmus $\overline{g}$ je injektívny. Stačí overiť, že $\operatorname{Ker}\overline{g} = \{0\}$. Ak $g(a)g(b)^{-1} = 0$, znamená to, že $g(a) = 0$ (lebo prvok $g(b)^{-1} \in F \setminus \{0\}$ je nenulový). Potom (keďže homomorfizmus g je injektívny) máme $a = 0$, čiže $[(a,b)] = [(0,b)] = [(0,1)]$ je nulový prvok poľa $Q(D)$. □

Predchádzajúce tri lemy už spolu dokazujú vetu 5.1.2.

Poznámka 5.1.6. Existuje o niečo všeobecnejšia konštrukcia, ktorá sa nazýva *okruh zlomkov* alebo *lokalizácia* (napríklad [DF, Section 15.4], [AM, Chapter 3]). V tomto prípade sa pracuje s komutatívnym okruhom R s jednotkou, vyberie sa nejaká podmnožina $U \subseteq R$, ktorej prvky budú predstavovať menovatele zlomkov. (Inak povedané, U sú tie prvky, ktoré budú po urobení tejto konštrukcie mať inverzy vzhľadom na násobenie. Treba vyžadovať, aby množina U bola uzavretá vzhľadom na násobenie. V prípade konštrukcie podielového poľa sme mali $U = D \setminus \{0\}$.) Konštrukcia okruhu zlomkov je veľmi podobná konštrukcii podielového poľa, má aj podobné vlastnosti. Dôležitý rozdiel je, že v tomto prípade už zobrazenia spomínané vo vete 5.1.2 nemusia byť (vo všeobecnosti) injektívne. (Od zobrazenia g sa požaduje, aby zobrazoval všetky prvky z U na delitele jednotky.) Táto konštrukcia je dôležitá napríklad v algebraickej geometrii a komutatívnej algebre.

Poznámka 5.1.7. Veľmi podobná konštrukcia ako vytvorenie podielového poľa z oboru integrity sa dá urobiť pre ľubovoľnú pologrupu s krátením (=pologrupa, v ktorej platia zákony o krátení). Dokážeme tak, že každú pologrupu s krátením možno vložiť do nejakej podgrupy (je podgrupou nejakej grupy.) Pozri úlohu 5.1.3.

Poznámka 5.1.8. Citát na začiatku tejto podkapitoly sa spája s konštrukciou reálnych čísel z celých čísel. My sme si ukázali, ako z celých čísel vytvoriť racionálne. Ďalším krokom by bolo pomocou racionálnych čísel nejakým spôsobom zaviesť reálne čísla. Existuje veľa ekvivalentných spôsobov ako to dosiahnuť (zúplnenie, Dedekinove rezy, reťazové zlomky, desatinné rozvoje...), viac sa o nich môžete dozvedieť napríklad v [Š]. Azda najčastejšie vyučovaným spôsobom je konštrukcia pomocou tried ekvivalencie cauchyovských postupností – zúplnenie racionálnych čísel – s ktorou by ste sa mohli stretnúť v niektorom pokročilejšom kurze analýzy. (Každý zo spomínaných spôsobov konštrukcie reálnych čísel nejakým spôsobom využíva pojem spojitosti.)

Cvičenia

Úloha 5.1.1. Dokážte, že každý komutatívny okruh možno vložiť do komutatívneho okruhu s jednotkou.

Úloha 5.1.2. Dokážte, že podielové pole je vlastnosťami uvedenými vo vete 5.1.2 určené jednoznačne až na izomorfizmus.

Úloha 5.1.3*. Dokážte, že každú komutatívnu pologrupu s krátením možno vložiť do grupy. (Teda ak S je komutatívna pologrupa, v ktorej platia zákony o krátení, tak existuje grupa G a prostý homomorfizmus $f\colon S \to G$; pričom pod homomorfizmom pologrúp sa rozumie zobrazenie zachovávajúce operáciu, podobne ako pri grupách.)

5.2 Charakteristika poľa

S charakteristikou poľa sme sa už stretli v tvrdení 4.5.32. Pripomenieme si jej definíciu a dokážeme si niektoré fakty o charakteristike poľa, ktoré budú pre nás v nasledujúcich častiach prednášky užitočné.

Definícia 5.2.1. *Charakteristika poľa F* je najmenšie prirodzené číslo $k > 0$ s vlastnosťou $k \times 1 = 0$. Označujeme ju $\mathrm{char}(F)$. Ak neexistuje k s uvedenou vlastnosťou, tak definujeme $\mathrm{char}(F) = \infty$.

Predchádzajúcu definíciu môžeme preformulovať aj nasledovne

$$\mathrm{char}\, F = \min\{k \in \mathbb{N}, k > 0; k \times 1 = 0\},$$

pričom minimum z prázdnej množiny chápeme ako nekonečno.

Charakteristiku možno definovať aj všeobecnejšie – pre ľubovoľný okruh, pozri napríklad [KGGS, Kapitola 4.4]. V prípade oboru integrity je táto všeobecnejšia definícia ekvivalentná s definíciou, ktorú sme tu uviedli pre polia. (My budeme charakteristiku potrebovať iba pre polia.)

Príklad 5.2.2. $\mathrm{char}(\mathbb{Z}_p) = p$, pretože $p \times 1 = 0$ (počítame modulo p) pre $0 < k < p$ platí v $\mathbb{Z}_p$ $k \times 1 = k \neq 0$.

$\mathrm{char}(\mathbb{Q}) = \infty$, pretože žiadny násobok jednotky $k \times 1$, pre kladné celé čísla k, nie je 0.

Lema 5.2.3. *Každé konečné pole F má konečnú charakteristiku.*

Dôkaz. Vyplýva z Dirichletovho princípu.

Uvažujme množinu $\{k \times 1; k \in \mathbb{N}, k > 0\}$. Táto množina je konečná (je to podmnožina konečnej množiny F). Preto (na základe Dirichletovho princípu) existujú rôzne prirodzené čísla $m, n > 0$ také, že

$$m \times 1 = n \times 1.$$

Bez ujmy na všeobecnosti, nech $m > n$. Potom pre $k = m - n$ máme

$$k \times 1 = (m - n) \times 1 = m \times 1 - n \times 1 = 0,$$

čiže množina $\{k \in \mathbb{N}, k > 0; k \times 1 = 0\}$ je neprázdna, teda charakteristika (najmenší prvok tejto množiny) je konečná. □

Poznámka 5.2.4. Existujú aj nekonečné polia s konečnou charakteristikou.

Tvrdenie 5.2.5. *Charakteristika ľubovoľného poľa F je prvočíslo alebo ∞.*

Dôkaz. Stačí ukázať, že v prípade, že ak je charakteristika konečná, nemôže byť zložené číslo.

Sporom. Predpokladajme, že charakteristika poľa F je zložené číslo m, teda $m = n.k$ pre nejaké prirodzené čísla $1 < n, k < m$. Potom platí

$$m \times 1 = (nk) \times 1 = (n \times 1)(k \times 1) = 0.$$

Každé pole je okruh bez deliteľov nuly, preto jeden z prvkov $n \times 1$, $k \times 1$ poľa F musí byť 0. Pritom $n, k < m$, čo je spor s tým, že m je (podľa definície charakteristiky) najmenšie kladné celé číslo s touto vlastnosťou. □

Nasledujúce tvrdenie budeme v ďalších kapitolách často využívať.

Tvrdenie 5.2.6. *Nech F, F' sú polia a zobrazenie $\varphi\colon F \to F'$ je okruhový homomorfizmus. Potom buď $\varphi[F] = \{0\}$, alebo $\varphi[F]$ je podpole F', ktoré je izomorfné s F. (Inými slovami: zobrazenie φ je buď nulové alebo injektívne; čiže vnorenie – izomorfizmus na svoj obraz.)*

Dôkaz. Vieme, že $\operatorname{Ker}\varphi$ je ideál v F. Jediné ideály v poli sú však $\{0\}$ a F. V prvom prípade je homomorfizmus φ injektívny, v druhom prípade sa každý prvok zobrazí na nulu. □

Pomocou predchádzajúceho tvrdenia môžeme ukázať, že (v závislosti od charakteristiky) každé pole obsahuje podpole (izomorfné s) $\mathbb{Q}$ alebo $\mathbb{Z}_p$.

Tvrdenie 5.2.7. *Ak* $\operatorname{char} F = \infty$*, tak existuje injektívny homomorfizmus z $\mathbb{Q}$ do F.*
Ak $\operatorname{char} F = p$ *pre nejaké prvočíslo p, tak existuje injektívny homomorfizmus zo $\mathbb{Z}_p$ do F.*

Dôkaz. Zobrazenie $\varphi\colon \mathbb{Z} \to F$

$$\varphi\colon z \mapsto z \times 1$$

je okruhový homomorfizmus, pričom $\operatorname{Ker}\varphi$ obsahuje práve tie celé čísla, ktoré sú násobky $\operatorname{char}(F)$ (a v prípade, že $\operatorname{char} F = \infty$ je $\operatorname{Ker}\varphi = \{0\}$).

Ak $\operatorname{char} F = p$, tak máme (na základe vety o faktorovom izomorfizme) izomorfizmus z $\mathbb{Z}/\operatorname{Ker}\varphi = \mathbb{Z}/(\operatorname{char}(F)) = \mathbb{Z}/(p) \cong \mathbb{Z}_p$ na $\operatorname{Im}\varphi$. Tým dostávame hľadaný injektívny homomorfizmus zo $\mathbb{Z}_p$ do F.

Ak $\operatorname{char} F = \infty$, tak $\operatorname{Ker} F = (0)$ a φ je injektívny homomorfizmus zo $\mathbb{Z}$ do F. Ten sa podľa vety 5.1.2 dá rozšíriť na injektívny homomorfizmus $\overline{\varphi}\colon Q(\mathbb{Z}) \to F$ z podielového poľa oboru integrity $\mathbb{Z}$ do F. Podielové pole $\mathbb{Z}$ je však práve pole racionálnych čísel. □

Nasledujúce tvrdenie má síce veľmi jednoduchý dôkaz, podarí sa nám však z neho odvodiť veľmi zaujímavé dôsledky.

Tvrdenie 5.2.8. *Nech K, F sú polia a $K \supseteq F$ (t.j. K je nadpole poľa F). Potom K je vektorový priestor nad poľom F (so sčitovaním a násobením skalárom rovnakým ako je sčitovanie a násobenie v K).*

Dôkaz. Jednoduchý – jednotlivé vlastnosti z definície vektorového priestoru po prepísaní na tento konkrétny príklad sú vlastne známe vlastnosti poľa ako distributívnosť, asociatívnosť násobenia atď. (Dôkaz je skoro identický s postupom použitým v úlohách I-4.1.10 a I-4.1.5) □

Ako sme už spomenuli, napriek jednoduchému dôkazu bude mať pohľad na nadpole ako na vektorový priestor nad daným poľom mnohé zaujímavé dôsledky. Ako prvý z nich si ukážeme, aký počet prvkov môže mať konečné pole.

Dôsledok 5.2.9. *Konečné pole charakteristiky p má p^n prvkov pre nejaké $n \in \mathbb{N}$.*

Dôkaz. Podľa tvrdenia 5.2.7 každé konečné pole F s $\operatorname{char}(F) = p$ obsahuje podpole (izomorfné so) $\mathbb{Z}_p$. Teda ho môžeme chápať ako vektorový priestor nad $\mathbb{Z}_p$. Keďže množina F je konečná, ide o konečnorozmerný vektorový priestor, teda F je (ako vektorový priestor) izomorfný s priestorom $(\mathbb{Z}_p)^n$ pre nejaké n (veta I-5.5.13). □

Z toho vyplýva, že počet prvkov konečného poľa musí byť mocnina prvočísla. Napríklad dostávame, že nemôže existovať 6-prvkové pole. (Platí aj obrátené tvrdenie, pre každú mocninu prvočísla $k = p^n$ existuje k-prvkové pole.)

Môžeme si všimnúť ešte jeden užitočný fakt súvisiaci s charakteristikou poľa.

Tvrdenie 5.2.10. *Nech* $\mathrm{char}(F) = p$ *(*p *je prvočíslo). Potom pre ľubovoľné* $a, b \in F$ *platí*

$$(a+b)^p = a^p + b^p$$
$$(ab)^p = a^p b^p$$

čiže zobrazenie $f\colon F \to F$, $f(x) = x^p$, *je izomorfizmus z* F *na* F *(automorfizmus poľa* F*).*

Dôkaz. Jediná netriviálna časť je rovnosť $(a+b)^p = a^p + b^p$. Použitím binomickej vety (ktorá platí v každom komutatívnom okruhu s jednotkou, úloha 4.2.20) máme

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} \times a^k b^{p-k}.$$

Chceme ukázať, že všetky sčítance s výnimkou prvého a posledného (t.j. $k = 0$ a $k = p$) sú nulové.

Na to nám stačí ukázať, že $p \mid \binom{p}{k}$ v $\mathbb{Z}$,keďže p je charakteristika poľa, s ktorým pracujeme. (Vieme, že binomický koeficient je vždy celé číslo.) Ak však p je prvočíslo, tak p delí čitateľ zlomku

$$\binom{p}{k} = \frac{p!}{k!(p-k!)}$$

pričom v menovateli sa (pre $k \neq 0, p$) vyskytnú len čísla ostro menšie ako p, t.j. žiadne z nich nie je deliteľné p. Z toho už vyplýva, že p delí toto číslo. □

5.3 Rozšírenia polí

Prezentácia výsledkov v tejto kapitole i v nasledujúcich kapitolách je podobná ako v [KGGS, Kapitola 8], [DF, Chapter 13].

Na začiatok začnime s definíciou pojmu rozšírenia poľa.

Definícia 5.3.1. Ak K, F sú polia a $K \supseteq F$, tak hovoríme, že K je *rozšírením* poľa F.

Vidíme, že rozšírenie poľa je vlastne len iné pomenovanie pre dvojicu pozostávajúcu z poľa F a jeho nadpoľa K (čiže vždy, keď hovoríme o rozšírení poľa, máme na mysli dve polia).

Ak K je rozšírenie poľa F, tak K môžeme chápať ako vektorový priestor nad F (tvrdenie 5.2.8). Pre nás bude zaujímavý hlavne ten prípad, keď je to konečnorozmerný vektorový priestor.

Definícia 5.3.2. Ak K je rozšírenie poľa F také, že K je konečnorozmerný vektorový priestor nad F, tak K nazývame *konečné rozšírenie* poľa F.

Dimenziu $d_F(K)$ poľa K ako vektorového priestoru nad F nazývame *stupeň rozšírenia* a označujeme $[K : F]$.

$$[K : F] = d_F(K)$$

Príklad 5.3.3. Pole $\mathbb{C}$ je rozšírením poľa $\mathbb{R}$. Všimnime si, že $\mathbb{C} = \{a + bi; a, b \in \mathbb{R}\}$, a teda 1, i tvoria bázu $\mathbb{C}$ ako vektorového priestoru nad $\mathbb{R}$. Preto $[\mathbb{C} : \mathbb{R}] = 2$.

Na $\mathbb{C}$ sa môžeme pozerať tak, že k poľu $\mathbb{R}$ sme pridali koreň polynómu $x^2 + 1$ (a aj všetky ďalšie prvky, ktoré si pridanie tohoto koreňa vynútilo, aby novovytvorená štruktúra bola opäť poľom). V poli $\mathbb{R}$ polynóm $x^2 + 1$ nemá koreň.

Príklad 5.3.4. Vieme, že $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2}; a, b \in \mathbb{Q}\}$ je pole (úloha I-3.3.2). Je to rozšírenie poľa $\mathbb{Q}$. Ak sa na $\mathbb{Q}[\sqrt{2}]$ pozrieme ako na vektorový priestor nad $\mathbb{Q}$, tak jeho bázu tvoria $1, \sqrt{2}$. (Rozmyslite si, prečo sú lineárne nezávislé nad $\mathbb{Q}$.) Teda $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

Aj v tomto prípade môžeme toto rozšírenie chápať tak, že k poľu $\mathbb{Q}$ sme pridali koreň polynómu $x^2 - 2$. (V poli $\mathbb{Q}$ tento polynóm nemá koreň.)

V predchádzajúcich dvoch príkladoch sme videli, že k ireducibilným polynómom $x^2 - 2 \in \mathbb{Q}[x]$, $x^2 + 1 \in \mathbb{R}[x]$ existujú konečné rozšírenia, v ktorých už tieto polynómy majú koreň. Ukážeme, že podobné tvrdenie platí pre ľubovoľný ireducibilný polynóm.

Veta 5.3.5. *Nech F je pole a $p(x)$ je ireducibilný polynóm v $F[x]$. Potom existuje rozšírenie poľa F, v ktorom $p(x)$ má koreň.*

Dôkaz. Keďže $p(x)$ je ireducibilný, $(p(x))$ je maximálny ideál v $F[x]$ (tvrdenia 4.4.19 a 4.4.32). Teda faktorový okruh $K = F[x]/(p(x))$ je pole. O tomto poli K ukážeme, že má požadované vlastnosti.

Máme kanonický homomorfizmus $\varphi\colon F[x] \to K$ taký, že $\operatorname{Ker}\varphi = (p(x))$. Súčasne F je podmnožinou $F[x]$, teda máme aj homomorfizmus $\varphi|_F\colon F \to K$ (zúženie homomorfizmu φ na podmnožinu F). Tento homomorfizmus je nenulový, keďže na nulu sa zobrazia iba prvky z $\operatorname{Ker}\varphi = (p(x))$, kam patria iba 0 a a polynómy stupňa aspoň $\operatorname{st} p(x) \geq 1$ (čiže žiadny nenulový konštantný polynóm – žiadny nenulový prvok poľa F). Podľa tvrdenia 5.2.6 je to teda injektívny homomorfizmus (vnorenie) a F môžeme chápať ako podpole K. Ide teda skutočne o rozšírenie poľa F.

Treba ešte dokázať, že $p(x)$ má v tomto poli koreň. Ukážeme, že koreňom je prvok $\varphi(x) = \underline{x+(p(x))}$. Kvôli zjednodušeniu zápisu budeme používať označenie $\varphi(x) = \overline{x}$, resp. $\varphi(f(x)) = \overline{f(x)}$ pre ľubovoľné $f(x) \in F[x]$.

Máme rovnosť

$$p(\overline{x}) \overset{(*)}{=} \overline{p(x)} = p(x) + (p(x)) = 0 + (p(x)),$$

ktorá znamená, že $\overline{x}$ je skutočne koreňom polynómu $p(x)$. (V predchádzajúcom odvodení bola najdôležitejším krokom rovnosť označená $(*)$, ktorá je založená na tom, že φ je homomorfizmus medzi komutatívnymi okruhmi, teda zachováva súčet, súčin a teda aj všetky polynomické výrazy). □

Teraz ukážeme, že rozšírenie K poľa F zostrojené v predchádzajúcej vete je konečným rozšírením.

Veta 5.3.6. *Nech $p(x) \in F[x]$ je ireducibilný polynóm a $K = F[x]/(p(x))$. Nech $n = \operatorname{st} p$. Označme $u = x + (p(x)) = \varphi(x)$ (kde $\varphi\colon F[x] \to K$ označuje kanonický homomorfizmus). Potom $1, u, \ldots, u^{n-1}$ je báza K ako vektorového priestoru nad F, čiže*

$$K = \{a_{n-1}u^{n-1} + \cdots + a_1 u + a_0; a_0, \ldots, a_{n-1} \in F\}.$$

Dôkaz. Máme surjektívny homomorfizmus $\varphi\colon F[x] \to K$, ktorý polynóm $f(x)$ zobrazí na triedu $f(x) + (p(x)) = f(u)$. (Teda každý prvok K možno vyjadriť ako $f(u)$ pre nejaké $f \in F[x]$.)

Ak $f(x)$ je ľubovoľný polynóm z $F[x]$, tak podľa vety o delení so zvyškom existujú $q(x)$ a $r(x)$ také, že

$$f(x) = q(x)p(x) + r(x),$$

pričom $\operatorname{st} r \leq \operatorname{st} p = n$ Potom máme

$$f(u) = f(x) + (p(x)) = r(x) + (p(x)) = r(u) = a_{n-1}u^{n-1} + \cdots + a_1 u + a_0.$$

Čiže každý prvok z K sa skutočne vyjadriť ako lineárna kombinácia $1, u, \ldots, u^{n-1}$ (t.j. vektory $1, u, \ldots, u^{n-1}$ generujú vektorový priestor K).

Ešte zostáva ukázať, že $1, u, \ldots, u^{n-1}$ sú lineárne nezávislé nad F. Predpokladajme, že pre nejaké $b_0, \ldots, b_{n-1}$ by platilo v $K = F[x]/(p(x))$

$$b_{n-1}u^{n-1} + \cdots + b_1 u + b_0 = 0.$$

Táto rovnosť vo faktorovom okruhu $F[x]/(p(x))$ znamená, že v okruhu $F[x]$ platí

$$b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in (p(x)).$$

Jediný polynóm v $(p(x))$, ktorý má stupeň menej ako n, je však nulový polynóm, preto $b_0 = b_1 = \cdots = b_{n-1} = 0$, čiže $1, u, \ldots, u^{n-1}$ sú skutočne lineárne nezávislé. □

Dôsledok 5.3.7. *Ak $p(x) \in F[x]$ je ireducibilný polynóm stupňa n, tak $K = F[x]/(p(x))$ je konečné rozšírenie F a stupeň rozšírenia $[K : F]$ je tiež rovný n.*

$$[K : F] = \operatorname{st} p(x)$$

Predchádzajúca veta nám hovorí, že každý prvok poľa $F[x]/(p(x))$ môžeme vyjadriť ako $a_{n-1}u^{n-1}+\cdots+a_1u+a_0$ pre nejaké $a_0, \ldots, a_{n-1} \in F$. V poli $F[x]/(p(x))$ vieme jednoduchým spôsobom sčitovať a násobiť – ide jednoducho o sčitovanie a násobenie modulo $p(x)$. Presnejšie ak máme 2 prvky vyjadrené ako $f(u)$ a $g(u)$ pre nejaké polynómy $f(x), g(x) \in F[x]$ stupňa menšieho ako n, tak ich súčet zodpovedá priamo súčtu polynómov $f(x) + g(x)$. Ich súčin dostaneme tak, že vypočítame súčin $f(x)g(x)$ a zistíme jeho zvyšok po delení $p(x)$. (Fakt, že sčitovanie a násobenie v poli $F[x]/(p(x))$ sa správa takýmto spôsobom, vyplýva priamo z definície faktorového okruhu.)

Príklad 5.3.8. Uvažujme polynóm $p(x) = x^2 + x + 1$ nad poľom $\mathbb{Z}_2$. Tento polynóm je ireducibilný, lebo ide o polynóm druhého stupňa, ktorý nemá v danom poli koreň (tvrdenie 4.5.21). Ak označíme ako u triedu polynómu x vo faktorovom okruhu $GF_4 = \mathbb{Z}_2[x]/(p(x))$, tak prvky poľa GF_4 sú $\{0, 1, u, u + 1\}$. Na základe predchádzajúcich úvah vieme vyplniť tabuľku násobenia a sčitovania v tomto poli:

$$(au + b) + (cu + d) = (a + b)u + (b + d)$$

$$(au + b)(cu + d) = acu^2 + (bc + ad)u + bd = ac(u + 1) + (bc + ad)u + bd = (ac + bc + ad)u + (ac + bd)$$

$+$	0	1	u	$u+1$
0	0	1	u	$u+1$
1	1	0	$u+1$	u
u	u	$u+1$	0	1
$u+1$	$u+1$	u	1	0

$\cdot$	0	1	u	$u+1$
0	0	0	0	0
1	0	1	u	$u+1$
u	0	u	$u+1$	1
$u+1$	0	$u+1$	1	u

Samozrejme, keďže polynóm x^2+x+1 je polynóm druhého stupňa a má v poli GF_4 koreň, musí sa dať rozložiť na lineárne činitele. Skutočne v GF_4 platí $x^2+x+1 = (x+u)(x+u+1)$.

Príklad 5.3.9. Polynóm $p(x) = x^2 + 1$ je ireducibilný nad $\mathbb{R}$. Uvažujme pole $\mathbb{R}[x]/(x^2 + 1)$. Pokúsme sa zistiť, čomu sa v tomu poli rovná súčin $(au + b)(cu + d)$. V $\mathbb{R}[x]$ máme rovnosť

$$(ax + b)(cx + d) = acx^2 + (cb + ad)x + bc = ac(x^2 + 1) + (cb + ad)x + (bd - ac).$$

Z toho dostávame rovnosť v poli $\mathbb{R}[x]/(x^2 + 1)$

$$(ax + b)(cx + d) + (p(x)) = (cb + ad)x + (bd - ac) + (p(x)),$$
$$(au + b)(cu + d) = (cb + ad)u + (bd - ac).$$

Vidíme, že predpis pre sčitovanie násobenie je rovnaký ako pre komplexné čísla, čiže sme takto (až na izomorfizmus) získali pole $\mathbb{C}$.

Definícia 5.3.10. Ak K je rozšírenie F a $u_1, \ldots, u_n \in K$, tak symbolom $F(u_1, \ldots, u_n)$ označujeme podpole generované množinou $F \cup \{u_1, \ldots, u_n\}$. (T.j. najmenšie podpole, ktoré obsahuje túto množinu, čiže prienik všetkých podpolí, ktoré ju obsahujú.)

V prípade, že existuje $u \in K$ také, že $K = F(u)$ hovoríme o *jednoduchom rozšírení.*

Vo vete 5.3.5 sme ukázali, že pre ireducibilný polynóm $p(x)$ existuje rozšírenie, v ktorom tento polynóm má koreň. Teraz ukážeme, že toto pole je jednoznačne určené až na izomorfizmus.

Veta 5.3.11. *Nech F je pole, $p(x) \in F[x]$ je ireducibilný polynóm nad F a K je rozšírenie F, ktoré obsahuje koreň u polynómu $p(x)$. Potom*

$$F(u) \cong F[x]/(p(x)).$$

Dôkaz. Máme dosadzovací homomorfizmus (definícia 4.3.15) $\varphi_u \colon F[x] \to F(u)$

$$\varphi_u \colon a(x) \mapsto a(u).$$

Keďže u je koreň $p(x)$, platí $p(x) \in \operatorname{Ker} \varphi_u$. Vďaka tomu je homomorfizmus $\overline{\varphi}_u \colon F[x]/(p(x)) \to F(u)$ určený ako

$$\overline{\varphi_u} \colon a(x) + (p(x)) \mapsto a(u)$$

dobre definovaný. (Ak $a(x)$ a $b(x)$ patria do tej istej triedy, tak $b(x) - a(x) = g(x)p(x)$, čiže $b(u) - a(u) = g(u)p(u) = 0$ a $b(u) = a(u)$. Teda definícia zobrazenia $\overline{\varphi}_u$ nezávisí od výberu reprezentanta.)

Zobrazenie $\overline{\varphi}_u$ je homomorfizmus polí. Je to nenulový homomorfizmus, lebo x sa zobrazí na $u \neq 0$. (Ak by 0 bol koreň f, znamenalo by to, že $p(x)$ má koreň v F, nebol by teda ireducibilný.) Z toho vyplýva, že tento homomorfizmus je injektívny (tvrdenie 5.2.6).

Navyše v tomto zobrazení sa každý prvok F zobrazí sám na seba a x sa zobrazí na u. Keďže $\operatorname{Im} \varphi_u$ je podpole K a obsahuje F aj u, musí obsahovať celé $F(u)$. Teda homomorfizmus φ_u je i surjektívny. □

Z predchádzajúcej vety vyplýva, že dva korene ireducibilného polynómu sú algebraicky nerozlíšiteľné v tom zmysle, že po ich pridaní k poľu F dostaneme izomorfné polia. Tento fakt o čosi zovšobecníme v nasledujúcej vete, kde nebudeme vychádzať z toho istého poľa ale z dvoch izomorfných polí.

Najprv si všimnime ako sa izomorfizmus medzi poľami dá rozšíriť na izomorfizmus medzi ich okruhmi polynómov.

Poznámka 5.3.12. Nech $\varphi \colon F \to F'$ je izomorfizmus, F aj F' sú polia. Potom môžeme definovať zobrazenie $\hat{\varphi} \colon F[x] \to F'[x]$, ktoré polynómu z $F[x]$ priradí polynóm rovnakého stupňa, ktorého koeficienty dostaneme ako obrazy koeficientov pôvodného polynómu v homomorfizme φ.

$$\hat{\varphi} \colon \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \varphi(a_i) x^i$$

Pomerne jednoducho sa overí, že ide opäť o izomorfizmus. Keďže ide o homorfizmus, toto zobrazenie musí zachovávať maximálne ideály, prvoideály, ireducibilné prvky (=ireducibilné polynómy) a mnohé ďalšie vlastnosti.

Všimnime si tiež, že tento izomorfizmus navyše zachováva aj stupne polynómov.

Veta 5.3.13. *Nech $\varphi\colon F \to F'$ je izomorfizmus polí. Nech $p(x)$ je ireducibilný polynóm nad F a $p'(x) \in F[x]$ je polynóm $\hat{\varphi}(p)$ (čiže polynóm, ktorý získame použitím izomorfizmu $\varphi\colon F \to F'$ na všetky koeficienty polynómu $f(x)$). Potom $p'(x)$ je tiež ireducibilný polynóm (nad F').*

Nech u je koreň $p(x)$ (v nejakom nadpoli F) a v je koreň $p'(x)$ (v nejakom nadpoli F'). Potom existuje izomorfizmus

$$\sigma\colon F(u) \to F'(v),$$

ktorý zobrazí u na v a rozširuje φ, t.j. $\sigma(u) = v$ a $\sigma|_F = \varphi$.

Dôkaz. Fakt, že $p'(x)$ je ireducibilný vyplýva priamo z existencie izomorfizmu $\hat{\varphi}\colon F[x] \to F'[x]$.

Podľa vety 5.3.11 je $F(u) \cong F[x]/(p(x))$ a $F'(v) \cong F'[x]/(p'(x))$ (pričom izomorfizmy medzi uvedenými poliami nemenia prvky z F, resp. prvky z F'). V skutočnosti nám teda stačí hľadať izomorfizmus (s požadovanými vlastnosťami) medzi $F[x]/(p(x))$ a $F'[x]/(p'(x))$.

Máme zobrazenie $\hat{\varphi}\colon F[x] \to F'[x]$. Definujme $\psi\colon F[x]/(p(x)) \to F'[x]/(p'(x))$ predpisom

$$\psi\colon f(x) + (p(x)) \mapsto \hat{\varphi}(f(x)) + (p'(x)).$$

Ukážeme, že toto zobrazenie je dobre definované a je to izomorfizmus s požadovanými vlastnosťami.

Ak $f(x) = g(x)p(x) + r(x)$, tak

$$\hat{\varphi}(f(x)) = \hat{\varphi}(g(x))p'(x) + \hat{\varphi}(r(x)).$$

(V ďalšom budeme namiesto $\hat{\varphi}(r(x))$ používať stručnejšie označenie $r'(x)$.) Keďže zobrazenie $\hat{\varphi}$ zachováva stupne polynómov, predchádzajúca rovnosť nám hovorí, že zachováva aj zvyšky po delení $p(x)$ a $p'(x)$. (T.j. zvyšok polynómu $f(x)$ po delení $p(x)$ sa zobrazí na zvyšok polynómu $\hat{\varphi}(f(x))$ po delení $p'(x)$.)

To špeciálne znamená, že ak dva polynómy $f_1(x), f_2(x) \in F[x]$ majú rovnaký zvyšok po delení $p(x)$ (=sú reprezentantmi tej istej triedy rozkladu v $F[x]/(p(x))$), tak aj ich obrazy budú mať rovnaký zvyšok po delení $p'(x)$. Z toho vidíme, že zobrazenie ψ je dobre definované.

Z predchádzajúcej úvahy vyplýva aj to, že ψ je homomorfizmus – zachováva operácie $+$ a $\cdot$. S operáciou $+$ nemáme žiadne problémy, pretože sčitovanie v $F[x]/(p(x))$ pracuje rovnako ako sčitovanie polynómov a vieme, že $\hat{\varphi}$ zachováva sčitovanie. Násobenie funguje ako násobenie v $F[x]$ (resp. v $F'[x]$) s tým rozdielom, že musíme ešte urobiť zvyšok po delení $p(x)$ (v druhom prípade $p'(x)$). Práve sme si ozrejmili, že $\hat{\varphi}$ zachováva zvyšky po delení.

Zobrazenie $\hat{\varphi}$ zobrazí polynóm x na polynóm x (lebo $\varphi(1) = 1$ pre ľubovoľný izomorfizmus polí). Z toho vyplýva, že koreň $x + (p(x))$ polynómu $p(x)$ sa zobrazí na koreň $x + (p'(x))$ polynómu $p'(x)$.

Zatiaľ teda vieme, že ψ je homomorfizmus polí a je nenulový (prvok $x + (p(x))$ sa zobrazí na $x + (p'(x))$, ktorý je nenulový). Podľa tvrdenia 5.2.6 je tento homomorfizmus injektívny. Navyše, pretože $\hat{\varphi}$ je surjektívne zobrazenie, priamo z definície ψ vyplýva, že aj zobrazenie ψ je surjektívne. Je to teda izomorfizmus.

Už sme videli, že $\hat{\varphi}$ zobrazí koreň $p(x)$ na koreň $p'(x)$. Z toho, že $\hat{\varphi}$ nemení prvky poľa F vyplýva, že rovnakú vlastnosť má aj ψ. □

5.4 Algebraické rozšírenia

Definícia 5.4.1. Nech K je rozšírenie poľa F. Nech $u \in K$. Hovoríme, že prvok u je *algebraický* nad F, ak existuje nenulový polynóm $f(x) \in F[x]$, ktorého koreňom je u.

Ak každý prvok rozšírenia K je algebraický, hovoríme, že K je *algebraické rozšírenie.*

Ak u je algebraický nad F, znamená to, že množina všetkých polynómov, ktorých koreňom je u, je neprázdna. Ľahko sa overí, že táto množina

$$\{f(x) \in F[x]; f(u) = 0\}$$

je ideál v $F[x]$. Keďže $F[x]$ je okruh hlavných ideálov, existuje polynóm, ktorý generuje tento ideál.

Definícia 5.4.2. Ak u je algebraický prvok nad F, tak *minimálny polynóm* prvku u je normovaný polynóm, ktorý generuje ideál $\{f(x) \in F[x]; f(u) = 0\}$. Označujeme ho $m_u(x)$.

Stupeň algebraického prvku definujeme ako stupeň jeho minimálneho polynómu. Označujeme ho $[u : F]$.

$$[u : F] = \operatorname{st} m_u(x)$$

Pretože v definícii máme požiadavku normovanosti, minimálny polynóm je určený jednoznačne. Je to nenulový normovaný polynóm najnižšieho možného stupňa, ktorý patrí do ideálu $\{f(x) \in F[x]; f(u) = 0\}$.

Algebraický prvok môže patriť do rôznych rozšírení poľa F (napríklad $\sqrt{3}$ je prvkom $\mathbb{R}$ i $\mathbb{C}$, obe sú rozšírenia $\mathbb{Q}$). Pretože jeho definícia používa len ideál v $F[x]$, minimálny polynóm nezávisí od toho, aké rozšírenie obsahujúce u uvažujeme.

Veta 5.4.3. *Ak u je algebraický prvok nad F a $m_u(x) \in F[x]$ je jeho minimálny polynóm. Potom $m_u(x)$ je ireducibilný polynóm nad F,*

$$F(u) \cong F[x]/(m_u(x))$$

a $[u : F] = [F(u) : F]$.

Dôkaz. Ak by bol polynóm $m_u(x)$ reducibilný, t.j. $m_u(x) = f(x)g(x)$ pre nejaké nekonštatné polynómy $f(x), g(x) \in F[x]$, tak z rovnosti $m_u(u) = f(u)g(u) = 0$ vyplýva $f(u) = 0$ alebo $g(u) = 0$. To znamená, že jeden z polynómov $f(x)$, $g(x)$ by patril do ideálu $(m_u(x))$ a súčasne by mal nižší stupeň ako $m_u(x)$, čo je spor.

Z vety 5.3.11 potom vyplýva $F(u) \cong F[x]/(m_u(x))$ a z dôsledku 5.3.7 máme $[F(u) : F] = \operatorname{st} m_u = [u : F]$. □

Veta 5.4.4. *Nech K je rozšírenie F a $u \in K$. Prvok u je algebraický nad F práve vtedy, keď $F(u)$ je konečné rozšírenie F.*

Dôkaz. Ak u je algebraický, tak $F(u) \cong F[x]/(m_u(x))$ podľa vety 5.4.3, čo je konečné rozšírenie podľa dôsledku 5.3.7.

Obrátene, nech $F(u)$ je konečné rozšírenie F. Označme jeho stupeň n. Potom $1, u, \ldots, u^n$ sú lineárne závislé v $F(u)$ (chápanom ako vektorový priestor nad F). Teda existujú c_0, c_1, c_n (nie všetky nulové) tak, že $c_n u^n + \cdots + c_1 u + c_0 = 0$. Čiže $c_n x^n + \cdots + c_1 x + c_0 \in F[x]$ je nenulový polynóm, ktorého koreňom je u. □

Dôsledok 5.4.5. *Každé konečné rozšírenie je algebraické.*

Dôkaz. Ak $u \in K$, kde K je konečné rozšírenie F, tak $F(u)$ je vektorový podpriestor priestoru K. Teda $F(u)$ je tiež konečnorozmerný priestor (konečné rozšírenie) a u je, na základe predchádzajúcej vety, algebraický prvok nad F. □

Tvrdenie 5.4.6. *Nech K je konečné rozšírenie poľa L a prvky $x_1, \ldots, x_n$ tvoria bázu K ako vektorového priestoru nad L. Nech L je konečné rozšírenie poľa F a prvky $y_1, \ldots, y_s$ tvoria bázu L ako vektorového priestoru nad F. Potom množina $\{x_i y_j; i = 1, \ldots, n, j = 1, \ldots, s\}$ tvorí bázu K ako vektorového priestoru nad F.*

Dôkaz. Podľa predpokladov každý prvok $k \in K$ možno vyjadriť ako

$$k = \sum_{i=1}^{n} c_i x_i$$

pre vhodné $c_1, \ldots, c_n \in L$. Ďalej každé $c_i \in L$ sa dá vyjadriť v tvare

$$c_i = \sum_{j=1}^{s} d_{ij} y_j,$$

kde $d_{ij} \in F$. Z týchto dvoch rovností dostávame vyjadrenie prvku x

$$x = \sum_{i=1}^{n} \sum_{j=1}^{s} d_{ij} x_i y_j$$

ako lineárnej kombinácie prvkov $x_i y_j$ s koeficientami z F.

Tým sme ukázali, že množina $\{x_i y_j; i = 1, \ldots, n, j = 1, \ldots, s\}$ generuje K ako vektorového priestoru nad F. Aby sme ukázali, že ide o bázu, stačí nám už len overiť jej lineárnu nezávislosť.

Predpokladajme teda, že

$$\sum_{i=1}^{n} \sum_{j=1}^{s} a_{ij} x_i y_j = 0.$$

Túto rovnosť môžeme prepísať do tvaru

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{s} a_{ij} y_j \right) x_i = 0.$$

Dostali sme, že lineárna kombinácia prvkov $x_1, \ldots, x_n$ (s koeficientami z L) je rovná 0, pretože $x_1, \ldots, x_n$ je báza, každý koeficient musí byť nulový, teda pre každé $i = 1, \ldots, n$ máme

$$\sum_{j=1}^{s} a_{ij} y_j = 0.$$

Použitím rovnakého argumentu, tentoraz pre bázu $y_1, \ldots, y_s$ priestoru L nad F, máme, že všetky koeficienty a_{ij} sú nulové. Teda uvedené vektory sú skutočne lineárne nezávislé (ako prvky vektorového priestoru K nad poľom F). □

Dôsledok 5.4.7. *Ak K je konečné rozšírenie poľa L a L je konečné rozšírenie poľa F, tak pre stupne rozšírení platí*

$$[L : F] = [L : K].[K : F].$$

Dôsledok 5.4.8. *Ak $u \in L$, kde L je konečné rozšírenie poľa F, tak*

$$[u : F] \mid [L : F].$$

Príklad 5.4.9. Uvažujme rozšírenie $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ poľa $\mathbb{Q}$, t.j. najmenšie podpole $\mathbb{C}$ obsahujúce $\mathbb{Q} \cup \{\sqrt{2}, \sqrt{3}\}$.

Vieme, že $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ a $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3}; a, b \in \mathbb{Q}\}$, čiže $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ aj $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

Pole $\mathbb{Q}(\sqrt{2},\sqrt{3})$ môžeme chápať ako rozšírenie poľa $\mathbb{Q}(\sqrt{2})$, konkrétne platí

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}).$$

(Na oboch stranách rovnosti je najmenšie pole obsahujúce $\mathbb{Q} \cup \{\sqrt{2},\sqrt{3}\}$.)

Vypočítajme stupeň $[\sqrt{3} : \mathbb{Q}(\sqrt{2})]$. Pretože $\sqrt{3}$ je koreň polynómu $x^2 - 3$ (s koeficientami z $\mathbb{Q}(\sqrt{2})$), jeho stupeň je najviac 2. Stupeň 1 by tento prvok mal iba ak by patril do $\mathbb{Q}(\sqrt{2})$. Z predpokladu $\sqrt{3} = a + b\sqrt{2}$ pre nejaké $a, b \in \mathbb{Q}$ však dostaneme

$$3 = a^2 + 2b + 2ab\sqrt{2}$$

a z tejto rovnosti:
a) pre $ab \neq 0$ vyplýva $\sqrt{2} \in \mathbb{Q}$, čo je spor;
b) pre $b = 0$ vyplýva $\sqrt{3} = \pm a \in \mathbb{Q}$, spor;
c) pre $a = 0$ vyplýva $\sqrt{3} = b\sqrt{2}$, čiže $\sqrt{6} = 2b \in \mathbb{Q}$, spor.

Teda platí $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = [\sqrt{3} : \mathbb{Q}(\sqrt{2})] = 2$, z čoho dostaneme na základe predchádzajúcej vety

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$$

a z báz $1, \sqrt{2}$ pre $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$ a $1, \sqrt{3}$ pre $\mathbb{Q}(\sqrt{2},\sqrt{3})$ nad $\mathbb{Q}(\sqrt{2})$ vieme vytvoriť bázu $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ pre $\mathbb{Q}(\sqrt{2},\sqrt{3})$ nad $\mathbb{Q}$, teda platí

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}.$$

Všimnime si, že

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}),$$

lebo každé nadpole $\mathbb{Q}$, ktoré obsahuje $u = \sqrt{2} + \sqrt{3}$, musí obsahovať aj

$$\frac{1}{u} = \frac{1}{\sqrt{2}+\sqrt{3}} \cdot \frac{\sqrt{3}-\sqrt{2}}{\sqrt{3}-\sqrt{2}} = \sqrt{3} - \sqrt{2},$$

a teda obsahuje aj prvky

$$\sqrt{3} = \frac{1}{2}(\sqrt{3}+\sqrt{2}) + \frac{1}{2}(\sqrt{3}-\sqrt{2}),$$
$$\sqrt{2} = \frac{1}{2}(\sqrt{3}+\sqrt{2}) - \frac{1}{2}(\sqrt{3}-\sqrt{2}).$$

Dá sa dokázať, že niečo podobné platí všeobecne – každé konečné rozšírenie $\mathbb{Q}$ je jednoduché. (Podobne pre ľubovoľné pole nekonečnej charakteristiky.)

Všimnime si, že mocniny prvku $\sqrt{2} + \sqrt{3}$ vieme vyjadriť ako lineárne kombinácie 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ obsahuje

$$(\sqrt{2}+\sqrt{3})^0 = 1$$
$$(\sqrt{2}+\sqrt{3})^1 = \sqrt{2}+\sqrt{3}$$
$$(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$$
$$(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}$$
$$(\sqrt{2}+\sqrt{3})^4 = 49+20\sqrt{6}$$

Máme teda 5 vektorov $(1,0,0,0)$, $(0,1,1,0)$, $(5,0,0,2)$, $(0,11,9,0)$, $(49,0,0,20)$ v priestore dimenzie 4 – sú teda lineárne závislé a riešením sústavy lineárnych rovníc vieme nájsť nenulové koeficienty také, že príslušná lineárna kombinácia týchto vektorov je 0.

Dostaneme tak $1 - 10u^2 + u^4 = 0$, čo znamená, že

$$x^4 - 10x^2 + 1$$

je minimálny polynóm prvku $u = \sqrt{2} + \sqrt{3}$. Teda

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cong \mathbb{Q}[x]/(x^4 - 10x^2 + 1).$$

Cvičenia

Úloha 5.4.1. Nech L je rozšírenie poľa F a $u \in L$. Dokážte, že ak $[F(u) : F] = 5$, tak $[F(u^2) : F] = 5$.

Úloha 5.4.2. V poli $\mathbb{Q}(\sqrt[3]{2})$ nájdite inverzný prvok ku $1 - 2\sqrt[3]{2} + \sqrt[3]{4}$ (treba ho vyjadriť ako $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ pre vhodné $a, b, c \in \mathbb{Q}$.)

Úloha 5.4.3. Nájdite minimálne polynómy týchto čísel nad $\mathbb{Q}$:
a) $\sqrt{2} + 1$; b) $2 - 3\sqrt{5}$; c) $\sqrt[3]{3} + \sqrt{3}$; d) $\sqrt{2} - \sqrt{3}$; e) $\sqrt[3]{2} + i$; f) $1 + \sqrt[3]{2} - \sqrt[3]{4}$; g) $\frac{1}{2-\sqrt[3]{2}} + \sqrt[3]{4}$; h) $\frac{3+\sqrt{7}}{1+2\sqrt{7}}$.

Úloha 5.4.4. Určite stupeň viacnásobného rozšírenia a nájdite bázu nad $\mathbb{Q}$:
a) $\mathbb{Q}(\sqrt{3}, \sqrt{5})$; b) $\mathbb{Q}(i, \sqrt{2})$; c) $\mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{25})$; d) $\mathbb{Q}(1 + \sqrt{2}, 1 - \sqrt{8})$

5.5 Rozkladové polia

Definícia 5.5.1. Nech F je pole, $f(x) \in F[x]$ je nekonštantný polynóm. Rozšírenie K poľa F nazývame *rozkladovým poľom polynómu $f(x)$ nad F,* ak existujú $c \in F$, $u_1, \ldots, u_n \in K$ také, že $L = F(u_1, \ldots, u_n)$ a f sa dá nad L rozložiť ako

$$f = c(x - u_1)(x - u_2)\ldots(x - u_n).$$

V príklade 5.3.8 sme vlastne zostrojili rozkladové pole polynómu $x^2 + x + 1$ nad $\mathbb{Z}_2$.

Veta 5.5.2. *Nech F je pole, $f(x) \in F[x]$ a* st $f = n > 0$. *Potom existuje rozšírenie K poľa F, ktoré je rozkladovým poľom polynómu $f(x)$.*

Dôkaz. Indukciou vzhľadom na n. Ak $n = 1$, tak je rozkladovým poľom priamo F.

Nech teraz $n > 1$ a tvrdenie platí pre všetky polynómy stupňa menšieho ako n nad ľubovoľným poľom. Podľa vety 5.3.5 existuje rozšírenie poľa F, v ktorom má f aspoň jeden koreň u. (Stačí vo vete 5.3.5 za $p(x)$ zobrať ktorýkoľvek ireducibilný polynóm deliaci $f(x)$.) Uvažujme pole $F(u)$. Polynóm $f(x)$ možno nad $F(u)$ rozložiť ako $(x-u)g(x)$, pričom st $g < n$. Nech $F(u)(u_2, \ldots, u_n)$ je rozkladové pole $g(x)$ nad $F(u)$. Ľahko vidíme, že $F(u)(u_2, \ldots, u_n) = F(u, u_2, \ldots, u_n)$ je rozkladové pole polynómu $f(x)$. (Polynóm $f(x)$ v ňom možno rozložiť na súčin koreňových činiteľov a toto pole je generované n koreňmi polynómu $f(x)$.) □

Predchádzajúca veta hovorí, že pre daný polynóm stupňa n existuje pole v ktorom tento polynóm má n koreňov. Steinitzova veta 4.5.15, ktorú sme si uviedli bez dôkazu, je podstatne silnejší výsledok – tam máme jediné pole, ktoré spĺňa túto vlastnosť pre všetky polynómy z $F[x]$.

Ďalej ukážeme že rozkladové pole polynómu $f(x)$ nad poľom F je určené jednoznačne až na izomorfizmus. (V dôkaze sme svedkami situácie, s ktorou sme sa už viackrát stretli – pri dôkaze indukciou je niekedy výhodnejšie dokazovať o niečo silnejšie tvrdenie, pretože potom nám silnejšie predpoklady môžu zjednodušiť dôkaz indukčného kroku.)

Veta 5.5.3. *Nech $\varphi\colon F \to F'$ je homomorfizmus polí, $f(x) \in F[x]$ a $f'(x) \in F'[x]$ je polynóm, ktorý získame z $f(x)$ aplikovaním φ na všetky koeficienty polynómu $f(x)$. (V označení z poznámky 5.3.12 to znamená $f'(x) = \hat{\varphi}(f(x))$.) Ak K je rozkladové pole polynómu $f(x)$ a L je rozkladové pole polynómu $f'(x)$, tak existuje izomorfizmus $\sigma\colon K \to L$, ktorý navyše rozširuje φ, t.j. $\sigma|_F = \varphi$.*

Dôkaz. Dôkaz urobíme indukciou vzhľadom na stupeň n polynómu $f(x)$.

1° Ak stupeň $f(x)$ je 1, tak jeho rozkladovým poľom je priamo pole F. Teda v tomto prípade tvrdenie platí.

2° Predpokladajme, že tvrdenie platí pre ľubovoľnú dvojicu izomorfných polí a ľubovoľný polynóm stupňa menšieho ako n. Nech $K = F(u_1 \dots u_n)$ je rozkladové pole polynómu $f(x)$ nad poľom F a nech $L = F'(v_1 \dots v_n)$ je rozkladové pole $f'(x)$ nad F'. Potom tieto polynómy môžeme rozložiť ako $f(x) = c(x-u_1)\dots(x-u_n)$ a $f'(x) = c'(x-v_1)\dots(x-v_n)$.

Súčasne máme $K = F(u_1)(u_2 \dots u_n)$ (t.j. K je rozkladové pole polynómu $f(x)$ nad $F(u_1)$) a takisto $L = F'(v_1)(v_2 \dots v_n)$. Navyše môžeme predpokladať, že u_1 a v_1 sú koreňmi navzájom si zodpovedajúcich ireducibilných faktorov polynómov $f(x)$ a $f'(x)$. (To sa dá dosiahnuť prípadnou výmenou koreňov.) Potom sú podľa vety 5.3.13 polia možno izomorfizmus φ rozšíriť na izomorfizmus $\sigma'\colon F(u_1) \to F'(v_1)$ taký, že $\sigma'|_F = \varphi$. Na základe indukčného predpokladu môžeme potom tento izomorfizmus rozšíriť na izomorfizmus $\sigma\colon K \to L$. □

Dôsledok 5.5.4. *Ľubovoľné dve rozkladové polia polynómu $f(x)$ nad F sú izomorfné.*

Predchádzajúci výsledok nám umožňuje dokázať úplnú charakterizáciu konečných polí. Vieme už, že počet prvkov konečného poľa musí byť mocninou prvočísla. Dokážeme, že pre každé $q = p^n$ (p je prvočíslo) existuje q-prvkové pole a je určené jednoznačne až na izomorfizmus.

Veta 5.5.5. *Nech $q = p^n$, kde p je prvočíslo a $n > 0$ je prirodzené číslo. Potom existuje (až na izomorfizmus jediné) q-prvkové pole. Je to rozkladové pole polynómu $x^q - x$ nad $\mathbb{Z}_p$.*

Dôkaz. Keďže pole s uvedenými vlastnosťami má charakteristiku p, obsahuje ako svoje podpole $\mathbb{Z}_p$.

Najprv si všimnime, že ak q-prvkové pole existuje, musí to byť skutočne rozkladové pole polynómu $x^q - x$ nad $\mathbb{Z}_p$. Vyplýva to z toho, že pre každé $x \neq 0$ platí $x^{q-1} = x$ (z Lagrangeovej vety). Teda skutočne každý prvok poľa F je koreňom polynómu $x^q - x$.

Stačí nám teda overiť, že rozkladové pole polynómu $x^q - x$ má práve q prvkov. Všimnime si, že v poli charakteristiky p platí $(a+b)^p = a^p + b^p$ (tvrdenie 5.2.10), a teda aj

$$(a+b)^q = a^q + b^q.$$

To znamená, že korene polynómu $x^q - x$ sú uzavreté vzhľadom na sčitovanie. Ľahko vidno, že sú uzavreté aj na rozdiel a násobenie. Teda samotné korene už tvoria pole – bude to rozkladové pole polynómu $x^q - x$, ktoré má práve q prvkov – q rôznych koreňov tohoto polynómu. □

Literatúra

[AM] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Adison-Wesley, Reading, 1969.

[Č] Juraj Činčura. Elementárna teória čísel. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/cvicenia/tc/`.

[DF] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Willey and Sons, 3rd edition, 2004.

[G1] Jaroslav Guričan. Faktorizácia polynómov I. *Obzory matematiky, fyziky a informatiky*.

[G2] Jaroslav Guričan. Faktorizácia polynómov II. *Obzory matematiky, fyziky a informatiky*. `http://thales.doa.fmph.uniba.sk/katc/pages/member.php?clen=gurican`.

[K] Július Korbaš. *Lineárna algebra a geometria I*. UK, Bratislava, 2003.

[KGGS] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, and Jaroslav Smítal. *Algebra a teoretická aritmetika 1*. UK, Bratislava, 2002.

[OŠ] Daniel Olejár and Martin Škoviera. *Úvod do teórie diskrétnych matematických štruktúr*. Univerzita Komenského, Bratislava, 2007. `http://www.dcs.fmph.uniba.sk/texty/dsmain.pdf`.

[Rog] Kenneth Rogers. The axioms for Euclidean domains. *Amer. Math. Monthly*, 78(10):1127–1128, 1971.

[Rot] Joseph J. Rotman. *An Introduction to the Theory of Groups*. Springer-Verlag, New York, 1995.

[Š] Tibor Šalát. *Reálne čísla*. Alfa, Bratislava, 1982.

[S] Martin Sleziak. Teória čísel. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[ŠHHK] T. Šalát, A. Haviar, T. Hecht, and T. Katriňák. *Algebra a teoretická aritmetika 2*. Alfa, Bratislava, 1986.

Register

Zoznam symbolov