1-MAT-260 Algebra 2

2. októbra 2012

Obsah

Kapitola 1

Úvod

Verzia: 2. októbra 2012

1.1 Predhovor

Cieľom tohoto textu nie je podať kompletné poznámky k prednáške. Na prednáške sa budeme pomerne dôsledne držať knihy [KGGS], čiže väčšinu odprednášaných vecí by ste mali nájsť tam. Niektoré časti tohoto textu sú, až na poradie skladania zobrazení, prakticky totožné s [Sl2].

Tento text by mal:

- slúžiť ako prehľad toho, čo sa odprednášalo (resp. čo plánujem odprednášať);
- v prípade potreby obsahovať niektore veci, ktoré chýbajú v [KGGS]; prípadne dôkazy, ktoré bude treba vysvetliť podrobnejšie než sú v [KGGS]; (a tiež tých pár drobností, v ktorých sa mierne odchýlim od [KGGS]);
- témy, pri prezentácii ktorých som sa z nejakého dôvodu odchýlil od [KGGS];
- obsahovať niektoré ďalšie súvisiace témy, na ktoré na prednáške nezvýši čas. (Môžete sa dozvedieť o rôznych veciach súvisiacich s tým, čo budeme preberať a prípadne aj o niektorých veciach, s ktorými sa neskôr stretnete na iných predmetoch.)
- Možno sa tu objavia aj nejaké riešené príklady.

Keď sa budem potrebovať odvolať na nejaké veci, čo by ste mali vedieť z minulého semestra alebo nižších ročníkov, tak použijem odkaz na [KGGS] alebo na príslušné tvrdenie zo súboru na stránke, kde budú zozbierané viaceré dôležité veci z Algebry 1. Takýto odkaz by mohol vyzerať napríklad takto: tvrdenie I-1.1.1, [KGGS, Veta 1.6.1]. (V princípe by takéto niečo nemalo byť nutné – veci, ktoré ste sa učili minulý semester by ste si ešte mohli pamätať – je to tu uvedené viacmenej len pre istotu, ak by ste si potrebovali zopakovať, čo presne príslušné tvrdenie hovorí.)

Ako som už spomenul, dám sem aj nejaké časti „navyše“ – neodznejú na prednáške, ale súvisia s učivom, ktoré tu preberáme a mohli by pre vás byť zaujímavé a pomôcť vám dať preberanú látku do súvisu s inými vecami. Dôležité je zvládnuť hlavne štandardné učivo; ak s ním nemáte problém, oplatí sa vám pozrieť aj na tieto rozširujúce veci. Pri niektorých asi úplne stačí, že ste sa o nich aspoň informatívne dozvedeli, a možno je lepšie vrátiť sa k nim neskôr – keď ich budete potrebovať a budete poznať aj niektoré ďalšie veci, s ktorými súvisia. Nepovinné časti budú buď označené menším písmom – napríklad poznámka 2.1.24; alebo bude príslušná časť mať na konci názvu hviezdičku – napríklad podkapitola 2.4 Existencia maximálnych ideálov*.

Za jednotlivými kapitolami nájdete aj rôzne úlohy a cvičenia. Spolu s úlohami z [KGGS] a s tými, ktoré budete riešiť na cvičeniach, by ste mali mať viac než dostatočné množstvo úloh na precvičenie materiálu, ktorý budeme preberať.

Označenie DU označuje časti dôkazu/príkladu, ktoré zostali na rozmyslenie čitateľovi. (Väčšinou ide o rôzne drobné detaily, ktorých zvládnutie by pre vás malo byť pomerne ľahké, ak ste preberanej látke porozumeli. A takisto obrátene, ak niečo ešte nemáte dostatočne zvládnuté, doplnenie detailov môže byť vhodným cvičením.)

1.2 Sylaby a literatúra

Sylaby predmetu: Definície okruhov, oborov integrity telies a polí. Podokruhy a ideály. Vzťahy medzi ideálmi, homomorfizmami a okruhovými kongruenciami. Konštrukcia podielového poľa. Diferenčný (faktorový) okruh.

Definícia okruhu polynómov jednej neurčitej. Okruh polynomických funkcií. Najväčší spoločný deliteľ polynómov. Rozklad polynómu na súčin ireducibilných polynómov. Hornerova schéma, Taylorov rozvoj polynómu. Korene polynómu a rozklad polynómu na súčin koreňových činiteľov. Polynómy viacerých neurčitých, symetrické polynómy. Algebraické rozširovanie polí. Riešenia niektorých algebraických rovníc.

Literatúra: Základnou literatúrou pre tento kurz je [KGGS]. Ďalšia literatúra, ktorú som použil pri príprave poznámok (a mohla by byť pre vás zaujímavá): [DF, P]. Cvičenia som vyberal napríklad aj z [CH, DF, K]. Viaceré z uvedených príkladov navrhla cvičiaca K. Kováčiková.

1.3 Základné označenia

Pre číselné obory budeme používať nasledujúce označenia:
$\mathbb{N} = \{0, 1, 2, \ldots\}$ = množina prirodzených čísel (Teda nulu považujeme za prirodzené číslo.)
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ = množina celých čísel
$\mathbb{Z}^+ = \mathbb{N} \setminus \{0\} = \{1, 2, 3, \ldots\}$ = množina kladných celých čísel
$\mathbb{Q}$=racionálne čísla, $\mathbb{R}$=reálne čísla, $\mathbb{C}$=komplexné čísla
$\mathbb{R}^+ = \{x \in \mathbb{R}; x > 0\}$
$\mathbb{R}_0^+ = \{x \in \mathbb{R}; x \geq 0\}$
$\mathbb{R}^- = \{x \in \mathbb{R}; x < 0\}$
$\mathbb{R}_0^- = \{x \in \mathbb{R}; x \leq 0\}$

Identické zobrazenie na množine A označujem $id_A \colon A \to A$, nie I_A ako v [KGGS].

Kapitola 2

Okruhy a polia

2.1 Okruhy (a súvisiace pojmy)

Definícia 2.1.1. 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 $\{0\}$. Pozri lemu 2.1.6.
Z minulého semestra vieme, že jednotka v okruhu musí byť jednoznačne určená – tvrdenie I-1.1.1, [KGGS, Veta 1.6.1].
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 2.1.2. 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 $n \in \mathbb{N} \setminus \{0\}$).

V rámci tejto prednášky sa stretneme s mnohými príkladmi okruhov. Veľmi často budeme pracovať s okruhmi, rôznymi číselnými okruhmi; t.j. s takými okruhmi $(R, +, \cdot)$, kde R je nejaká podmnožina $\mathbb{C}$ a operácie $+$ a $\cdot$ sú obvyklé sčitovanie a násobenie komplexných čísel zúžené na túto podmnožinu.

Príklad 2.1.3. $(\mathbb{Z}, +, \cdot)$ – 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. DU Rozmyslite si, že $(\mathbb{Z}_n, \oplus, \odot)$ je naozaj okruh.

Príklad 2.1.4. Príklad komutatívneho okruhu, ktorý nemá jednotku: $(2\mathbb{Z}, +, \cdot)$.

Príklad 2.1.5. Nech $(G, +)$ je komutatívna grupa, ktorej neutrálny prvok označíme 0. Definujme $a \cdot b = 0$ pre $a, b \in G$. Potom $(G, +, \cdot)$ je komutatívny okruh. (Nie je to okruh s jednotkou.)

{okr:LMNULA}

Lema 2.1.6. *Nech $(R, +, \cdot)$ je okruh, $a, b \in R$. Potom platí*

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

Dôkaz. DU □

Podobne ako pri grupách, budeme vidieť viacero spôsobov ako z nejakých okruhov vytvoriť nové okruhy.

{okr:PRZxZ}

Príklad 2.1.7. 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:

{okr:PRSUCIN}

Príklad 2.1.8. 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] $\prod_{i\in I} R_i = \{f\colon I \to \bigcup_{i\in I} R_i \mid (\forall i \in I)(if \in R_i)\}$ tvorí s operáciami definovanými po zložkách

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

okruh. Tento okruh sa nazýva *priamy súčin* okruhov R_i, $i \in I$.

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.

Pomerne dôležité sú i maticové okruhy. Navyše ich vlastnosti by ste pomerne dobre mohli poznať z lineárnej algebry.

Príklad 2.1.9. 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, viete z lineárnej algebry. Tento okruh má jednotku, je ňou jednotková matica I. Tento okruh nie je komutatívny.

Podobne ako pri grupách sme často pracovali s podgrupami (=podmnožiny, ktoré tiež tvoria s tou istou operáciou grupu), v tomto kontexte budú mať podobnú úlohu podokruhy.

Definícia 2.1.10. 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 2.1.11. *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 2.1.12. $2\mathbb{Z}$ je podokruh $(\mathbb{Z}, +, \cdot)$.

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

{okr:PRC01}

Príklad 2.1.13. 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 $C(0, 1)$.

{okr:POZNJEDNPODOKR}

Poznámka 2.1.14. V niektorých knihách autori používajú konvenciu, že pracujú iba s okruhmi s jednotkou. (Teda keď napíšu okruh, myslia tým automaticky okruh s jednotkou.) V takomto prípade je obvyklé požadovať, aby podokruh obsahoval jednotku okruhu R.

My budeme používať tú definíciu, ktorú sme uviedli. Viacero príkladov ilustrujúcich to, že okruh a podokruh môžu mať rôzne jednotky, nájdete v úlohe 2.1.9.

[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.

Definícia 2.1.15. 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 2.1.7. Dokonca ľubovoľný okruh tvaru $R_1 \times R_2$ (pozri príklad 2.1.8), 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: {okr:TVROIKRATENIE}

Tvrdenie 2.1.16. *Nech R je okruh bez deliteľov nuly a $a, b, c \in R$. Ak $a \neq 0$ a platí $ab = ac$, tak $b = c$.*

Dôkaz. DU □

{okr:DEFTEL}

Definícia 2.1.17. 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 2.1.18. *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 2.1.17 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. Z prvého ročníka už 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].

Urobme ešte stručný prehľad definícií, ktoré sme tu uviedli. Všetky z nich požadujú aby $(R, +)$ bola komutatívna grupa a aby platila distributívnosť. Líšia sa len podmienkami na operáciu $\cdot$. V prípade okruhu požadujeme, aby $(R, \cdot)$ bola pologrupa. Pozrime sa na to, aké podmienky pribudnú v ostatných prípadoch:

R je komutatívny okruh	$(R, \cdot)$ je komutatívna pologrupa
R je okruh s jednotkou	$(R, \cdot)$ je monoid (a $1 \neq 0$)
R je okruh bez deliteľov nuly	$\cdot$ je binárna operácia na $R \setminus \{0\}$
R je teleso	$(R \setminus \{0\}, \cdot)$ je grupa
R je pole	$(R \setminus \{0\}, \cdot)$ je komutatívna grupa

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

2.1.1 Podokruh generovaný danou množinou

Pomerne ľahko sa ukáže, že prienik ľubovoľného systému podokruhov je opäť podokruh – úloha 2.2.3.

{okr:DEFGENER}

Definícia 2.1.19. Nech R je okruh a $A \subseteq R$. Potom prienik všetkých podokruhov okruhu R, ktoré obsahujú množinu A, budeme nazývať *podokruh generovaný množinou* A a označujeme ho $[A]$.

Všimnime si, že systém všetkých podokruhov okruhu R je neprázdny – obsahuje celý okruh R. Teda predošlá definícia má zmysel[5] a vidíme, že podokruh $[A]$ existuje pre ľubovoľnú podmnožinu $A \subseteq R$. Je to presne najmenší podokruh (vzhľadom na inklúziu), ktorý obsahuje množinu A.

Niekedy sa nám však bude hodiť o niečo presnejší popis tohoto podokruhu.

{okr:LMGENER}

Lema 2.1.20. *Nech R je okruh a $A \subseteq R$. Potom podokruh $[A]$ pozostáva zo všetkých konečných súčtov prvkov tvaru $\pm a_1 a_2 \dots a_n$, kde $n \in \mathbb{N}$, $a_i \in A$.*

Dôkaz. Označme S množinu všetkých konečných súčtov prvkov tvaru $a_1 a_2 \dots a_n$, kde $n \in \mathbb{N}$, $a_i \in A$.

Je zrejmé, že každý podokruh obsahujúci A musí obsahovať všetky takéto prvky. Teda $S \subseteq [A]$.

Nie je ťažké uvedomiť si, že množina S je uzavretá na rozdiel a súčin. DU Teda ide o podokruh okruhu R. Takisto je zrejmé, že $A \subseteq S$. Priamo z definície podokruhu $[A]$ potom máme $[A] \subseteq S$. □

{okr:VTOKRAU}

Veta 2.1.21. *Nech R je komutatívny okruh s jednotkou a nech A je podokruh obsahujúci jednotku. Nech $u \in R$. Potom $[A \cup \{u\}]$ je rovný množine*

$$A[u] := \{a_n u^n + a_{n-1} u^{n-1} + \dots + a_0; n \in \mathbb{N}, a_0, \dots, a_n \in A\}.$$

Dôkaz. Vyplýva z lemy 2.1.20, treba si len uvedomiť, že vďaka komutatívnosti môžeme prvky vystupujúce v tejto leme vhodne prepísať. Pozri aj [KGGS, Veta 4.3.5]. □

Okrem podokruhov, budeme pracovať niekedy s podpoľami, resp. podtelesami. (Ide o podokruh, ktorý je poľom, resp. telesom.) Opäť sa pomerne ľahko ukáže, že prienik podtelies je podteleso.

Ak $A \subseteq R$, kde R je teleso, tak *podteleso generované množinou* A označíme $[[A]]$. Pre nás bude dôležitý hlavne komutatívny prípad, vtedy hovoríme o *podpoli generovanom množinou* A.

{okr:LMPOLEGENER}

Lema 2.1.22. *Nech F je pole, $A \neq \{0\}$ je podokruh F. Potom najmenšie podpole obsahujúce množinu A je*

$$[[A]] = \{\frac{a}{b}; a, b \in A, b \neq 0\}.$$

Dôkaz je podobný, ako v leme 2.1.20. Treba overiť, že uvedená množina tvorí podpole a takisto, že každé podpole obsahujúce A musí obsahovať všetky takéto prvky. DU

[5] Pripomeňme, že prienik systému množín môžeme robiť, len ak tento systém je neprázdny.

{:VTPOLEGENER}

Veta 2.1.23. *Nech F je podpole poľa L. Nech $u \in L$. Potom $[[F \cup \{u\}]]$ je rovné množine*

$$F(u) = \left\{ \frac{a_n u^n + a_{n-1}u^{n-1} + \cdots + a_0}{b_m u^m + b_{m-1}u^{m-1} + \cdots + b_0}; n, m \in \mathbb{N}, a_i, b_j \in F, b_m u^m + b_{m-1}u^{m-1} + \cdots + b_0 \neq 0 \right\}.$$

Dôkaz. Vyplýva z lemy 2.1.22. □

Azda sa oplatí na tomto mieste zastaviť a uvedomiť si, že toto je podobná situácia s akou ste sa už viackrát stretli.[6]

{okr:POZNTOPDOWN}

Poznámka 2.1.24. Podokruh generovaný množinou A sme práve popísali dvoma spôsobmi. Je to prienik všetkých podokruhov obsahujúcich A – takýto prístup budeme nazývať zhora-nadol; lebo ide o popis pomocou systému všetkých nadokruhov $[A]$. Súčasne sme popísali ako vyzerajú prvky patriace do $[A]$. Ide o prístup zdola-nahor, použili sme tu prvky, ktoré sú obsiahnuté v množine A.

Do rovnakej schémy zapadajú viaceré pojmy s ktorými ste sa už stretli (alebo stretnete):

- Vo vektorových priestoroch: lineárny obal – podpriestor generovaný danou množinou
- V grupách: podgrupa generovaná danou množinou. (Špeciálne cyklické podgrupy – generované jediným prvkom.)
- Ideál v okruhu generovaný danými prvkami – poznámka 3.3.20.
- Tranzitívny uzáver relácie, t.j. najmenšia relácia, ktoré obsahuje danú reláciu a je tranzitívna. (Podobne existujú napríklad reflexívny či symetrický uzáver.)
- Uzáver množiny v topologickom priestore je najmenšia uzavretá množina, ktorá ju obsahuje.
- Konvexný obal danej množiny.

Obvykle sa hodí mať pre objekty, s ktorými chceme pracovať, popis zhora-nadol aj zdola-nahor. V závislosti od toho, na čo ich chceme použiť, môže byť jeden z nich vhodnejší. Napríklad to, že z $A \subseteq B$ vyplýva $[A] \subseteq [B]$ vidno okamžite z popisu $[A]$ ako prieniku, t.j. použitím prístupu zhora-nadol. Keď ale napríklad chceme ukázať, že $[A]$ obsahuje nejaký konkrétny prvok, pravdepodobne sa nám skôr bude hodiť prístup zdola-nahor.

Všetky uvedené príklady sú špeciálnymi prípadmi operátorov uzáveru[7] a uzáverových systémov, pozri napríklad [Gr, Section 3.12], [KLŠZ, podkapitola 2.4].

Cvičenia

Úloha 2.1.1. Zistite (a svoje tvrdenie zdôvodnite) ktoré z uvedených vlastností sa z okruhu R prenesú na uvedené konštrukcie: [8]

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

Úloha 2.1.2. Je každý podokruh poľa okruh bez deliteľov nuly? Je každý podokruh poľa obsahujúci 1 oborom integrity?

{okrcvic:ULOSQRT2}

Úloha 2.1.3. 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) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$

[6] Pekne je to popísané napríklad tu: `http://math.stackexchange.com/a/54334/`

[7] closure operator

[8] Označenie R/I označuje faktorový okruh okruhu R podľa ideálu I. O faktorových okruhoch sa dozviete v nasledujúcej podkapitole, čiže tento stĺpec zatiaľ nechajte nevyplnený a vráťte sa k nemu neskôr.

Úloha 2.1.4. 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 2.1.5. Dokážte: Ak R je obor integrity a $x^2 = 1$, tak $x = 1$ alebo $x = -1$.

Úloha 2.1.6. Ak R je okruh bez deliteľov nuly a $ab = 1$, tak aj $ba = 1$.

Úloha 2.1.7. Nech $(R, +, \cdot)$ je okruh. Definujme binárnu operáciu $*$ ako $a * b = b \cdot a$. Dokážte, že aj $(R, +, *)$ je okruh.

Úloha 2.1.8. Dokážte, že $\{(r, r); r \in R\}$ je podokruh okruhu $R \times R$. Je tento podokruh izomorfný s okruhom R?

{okrcvic:ULOPODOKJEDN}

Úloha 2.1.9. Zistite, či S je podokruhom R, a tiež či v okruhoch S a R existuje jednotka (a ak áno, tak či je v oboch prípadoch rovnaká).
a) $R = \mathbb{Z}_6$, $S = 2\mathbb{Z}_3 = \{0, 2, 4\}$.
b) $R = A \times A$ a $S = A \times \{0\}$, kde A je ľubovoľný okruh s jednotkou.
c) $R = M_{2,2}(\mathbb{R})$, t.j. reálne matice rozmerov 2×2 a $S = \{\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right); a \in \mathbb{R}\}$.
d) $R = \mathbb{Z} \times \mathbb{Z}$, $S = \mathbb{Z} \times \{0\}$.
e) $R = \mathbb{Z} \times \mathbb{Z}$, $S = \{(x, x); x \in \mathbb{Z}\}$.

Úloha 2.1.10. Nech S je podokruh okruhu R, pričom oba okruhy sú okruhy s jednotkou a R je obor integrity. Je aj S obor integrity? Je jednotka v okruhu R rovnaká ako v S?

{idecvic:BINOM}

Úloha 2.1.11. 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 2.1.12. Nech R je okruh. Centrom okruhu R nazveme množinu $Z = \{z \in R; (\forall r \in R) zr = rz\}$. Ukážte, že:
a) Z je podokruh R.
b) Ak R má jednotku, tak $1 \in Z$.
c) Centrum telesa je pole.

Úloha 2.1.13*. Nech $(R, +, \cdot)$ je okruh s jednotkou. Ak existuje inverzný prvok vzhľadom na operáciu $\cdot$ k $1 - ab$, tak existuje aj inverzný prvok k $1 - ba$.

Úloha 2.1.14*. Nech R je okruh, $Z(R) = \{a \in R; (\forall x \in R) ax = xa\}$ je *centrum* okruhu R. Ukážte, že ak platí $r^2 - r$ pre všetky $r \in R$, tak R je komutatívny.

Úloha 2.1.15. Uvažujme grupu $(\mathbb{Z}_6, \oplus)$. Koľkými spôsobmi môžeme zvoliť operáciu $*$, tak aby $(\mathbb{Z}_6, \oplus, *)$ bol okruh? Koľko z týchto okruhov bude izomorfných?

Úloha 2.1.16. Dokážte: Konečná pologrupa s krátením je grupa. Konečný obor integrity je pole.

2.2 Homomorfizmy, ideály a faktorové okruhy

Definícia 2.2.1. Nech $(R,+,\cdot)$, $(S,+,\cdot)$ sú okruhy. Zobrazenie $f\colon R\to S$ nazývame *homomorfizmus,* ak platí

$$(a+b)f = af+bf,$$
$$(ab)f = af\cdot bf.$$

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 2.2.2. *Zloženie homomorfizmov je homomorfizmus. Zloženie izomorfizmov je izomorfizmus.*

Príklad 2.2.3. 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.

{ide:PRKOMPLMAT}

Príklad 2.2.4. 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

$$\begin{pmatrix} a & b\\ -b & a\end{pmatrix}\begin{pmatrix} c & d\\ -d & c\end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc\\ -(ad+bc) & ac-bd\end{pmatrix}, \tag{2.1}$$

{ide:EQKOMPLMAT}

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 (2.1) vidíme, že pre $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in S$ máme

$$(AB)f = (ac - bd) + (ad + bc)i = (a + bi)(c + di) = (Af)(Bf).$$

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 ju niekto povedal, alebo aby sme ju „uhádli“.

Skúsme sa, pre dané komplexné číslo $z = a + bi$ pozrieť na zobrazenie $g_z \colon \mathbb{C} \to \mathbb{C}$, $g_z \colon x \mapsto xz$ (toto je presne zobrazenie, ktoré sme priradili komplexnému číslu v Cayleyho vete I-1.2.8, pozri tiež príklad I-1.2.11). 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 $(0, 1)$ 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 2.2.5. 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 $xf = x^2$, xgx, $xh = 1$ máme $(xg + xh)f = (x + 1)^2 = x^2 + 2x + 1$, zatiaľčo $xgf + xhf = x^2 + 1$, čiže

$$(g + h) \circ f \neq g \circ f + h \circ f.$$

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 2.2.6. 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 2.2.7. 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 2.2.8. Ak R je komutatívny okruh a $a \in R$, tak množina

$$(a) = \{ax; x \in R\}$$

je ideálom v R (úloha 2.2.6). Ideály takéhoto tvaru voláme *hlavné ideály.*

Nasledujúce pozorovanie je veľmi jednoduché, sformulujeme ho však do lemy, aby sme sa naň neskôr mohli odkazovať.

{ide:LMID1}

Lema 2.2.9. *Nech R je okruh s jednotkou a I je ideál v R. Potom $I = R$ práve vtedy, keď $1 \in I$.*

Dôkaz. DU □

Dôsledok 2.2.10. *Ak R je pole, tak jediné ideály v R sú $\{0\}$ a R.*

Dôkaz. DU □

Prvý krok na ceste k tomu, aby sme ukázali, že ideály majú pre okruhy podobnú úlohu ako normálne podgrupy pre grupy, je nasledujúca lema.

{ide:LMKER}

Lema 2.2.11. *Ak $\varphi\colon R \to S$ je homomorfizmus okruhov, tak jeho jadro* $\operatorname{Ker}\varphi$ *je ideál v R.*

Dôkaz. DU □

Podobne ako pri grupách sme pre invariantné podgrupy boli schopní zadefinovať faktorovú grupu aj v tomto prípade vieme definovať faktorový okruh.

Ak na chvíľu zabudneme na operáciu $\cdot$, tak máme komutatívnu grupu $(R, +)$ a I je jej podgrupa. Pretože každá podgrupa komutatívnej podgrupy je normálna, máme potom faktorovú grupu $(R/I, +)$. Dôkaz nasledujúcej vety v podstate spočíva v overení, že sa dá pridať

operácia $\cdot$ a že tak dostaneme okruh. Overenie týchto podmienok je vlastne jednoduchým mechanickým výpočtom, pričom používame iba definíciu ideálu a podmienku

$$a + I = b + I \qquad \Leftrightarrow \qquad a - b \in I,$$

ktorú poznáme z lemy I-2.2.4. Takisto v ďalších výsledkoch o faktorových okruhoch sa budeme často odvolávať na to, čo už vieme o faktorových grupách; potom zostane overiť niektoré vlastnosti operácie $\cdot$.

Veta 2.2.12. *Nech $(R, +, \cdot)$ je ľubovoľný okruh a I je ideál v R. Ak na prvkoch faktorovej*[9] *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 I-2.2.4), 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

$$\begin{aligned}
(a + I)((b + I)(c + I)) &= a(bc) + I = (ab)c + I = ((a + I)(b + I))(c + I) \\
(a + I)((b + I) + (c + I)) &= a(b + c) + I = (ab + ac) + I = (ab + I) + (ac + I) \\
((b + c) + I)(a + I) &= (b + c)a + I = (ba + ca) + I = (ba + I) + (ca + I)
\end{aligned}$$

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.

{ide:VTIZOMOKR}

Veta 2.2.13 (Veta o izomorfizme)**.** *Ak $f\colon R \to R'$ je homomorfizmus okruhov, tak* Ker f *je ideál v okruhu R a faktorový okruh $R/\operatorname{Ker} f$ je izomorfný s podokruhom* Im f *okruhu R'.*

Dôkaz. Z lemy 2.2.11 vieme, že 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

$$\varphi\colon a + I \mapsto f(a)$$

[9] Grupa $(R, +)$ je komutatívna, takže jej podgrupa I je invariantná. Má teda zmysel hovoriť o faktorovej grupe.

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:

$$(ab + I)\varphi = (ab)f = (af)(bf) = (a + I)\varphi(b + I)\varphi.$$

□

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 2.2.14. 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.

Napríklad $I = 3\mathbb{Z}$ je prvoideál v $\mathbb{Z}$, zatiaľčo $4\mathbb{Z}$ prvoideálom nie je. (Podobne to v $\mathbb{Z}$ funguje pre všetký prvočísla a zložené čísla. DU)

{ide:VTOIPRV}

Veta 2.2.15. *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 $\varphi\colon R \to R/I$; $a\varphi = a + I$. Z toho vyplýva, že ak $ab \in I$, tak

$$(ab)\varphi = (a\varphi)(b\varphi) = 0.$$

Pretože R/I je obor integrity, z predchádzajúcej rovnosti vyplýva, že $a\varphi = 0$ alebo $b\varphi = 0$, čiže $a \in I = \operatorname{Ker}\varphi$ alebo $b \in I = \operatorname{Ker}\varphi$.

$\boxed{\Leftarrow}$ Podobne ako v prvej časti využijeme surjektívny homomorfizmus $\varphi\colon R \to R/I$; $(a\varphi) = a + I$. Ak $x, y \in R/I$ sú také, že $xy = 0$ a $x = a\varphi$, $y = b\varphi$ (zo surjektívnosti vyplýva, že také $a, b \in R$ existujú) tak máme

$$(ab)\varphi = (a\varphi)(b\varphi) = xy = 0,$$

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

$$x = a\varphi = 0 \qquad \vee \qquad y = b\varphi = 0.$$

□

Definícia 2.2.16. 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 2.2.17. Bez dôkazu spomeňme, že pre každý ideál I taký, že $I \neq R$ existuje maximálny ideál M obsahujúci I, t.j. $I \subseteq M$.

{ide:VTPOLEMA

Veta 2.2.18. *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 2.2.9).

$\boxed{\Leftarrow}$ 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:

{ide:DOSMAXJEPRV}

Dôsledok 2.2.19. *V komutatívnom okruhu s jednotkou je každý maximálny ideál prvoideál.*

Opäť, podobne ako v prípade grúp a normálnych podgrúp, zodpovedajú ideály kongruenciám na okruhu R (pozri úlohy 2.2.25, 2.2.26).

{ide:DEFKONG}

Definícia 2.2.20. 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

{idecvic:ULOSYMDIF}

Úloha 2.2.1. 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 2.2.2. Nech F je pole a $I \neq \emptyset$. Dokážte, že v okruhu F^I (príklad 2.1.8) 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 2.2.18.)

{c:ULOPRIENIK}

Úloha 2.2.3. Prienik ľubovoľného systému podokruhov je podokruh. Prienik ľubovoľného systému ideálov je ideál.

Úloha 2.2.4. Nájdite príklad podokruhu, ktorý nie je ideálom.

Úloha 2.2.5. Nech $f\colon R_1 \to R_2$ je homomorfizmus okruhov. Nech S_1 je podokruh R_1 a S_2 je podokruh R_2. Ukážte, že $f[R_1]$ a $f^{-1}(R_2)$ sú podokruhy. Platia podobné tvrdenia pre ideály?

{idecvic:ULOHI}

Úloha 2.2.6. Overte, že $(a) = \{ax; x \in R\}$ je ideál v komutatívnom okruhu R (teda hlavné ideály sú skutočne ideály.)

{idecvic:HOMSUCIN}

Úloha 2.2.7. Dokážte, že zobrazenie $f_1\colon R_1 \times R_2 \to R_1$ určené predpisom $(r_1, r_2)f_1 = r_1$ je homomorfizmus.

Dokážte, že pre každé $i \in I$ je zobrazenie $f_i\colon R^I \to R$ dané predpisom $gf_i = ig$ (pre ľubovoľné $g\colon I \to R$) je homomorfizmus.

Úloha 2.2.8. Nech $R \neq \{0\}$ je komutatívny okruh s jednotkou taký, že jediné ideály v R sú $\{0\}$ a R. Dokážte, že R je pole.

Úloha 2.2.9. 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 2.2.10. 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 2.2.11. 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?

{idecvic:ULOZJEDINCR}

Úloha 2.2.12. 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 2.2.13. 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 2.2.1.)

Úloha 2.2.14. Dokážte, že okruhy $(2\mathbb{Z}, +, \cdot)$ a $(3\mathbb{Z}, +, \cdot)$ nie sú izomorfné.

Úloha 2.2.15. Nájdite všetky homomorfné obrazy okruhu $\mathbb{Z}$.

Úloha 2.2.16. Nájdite všetky homomorfizmy zo $\mathbb{Z}$ do $\mathbb{Z}_{30}$.

Úloha 2.2.17. 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 2.1.3.)

Úloha 2.2.18. Nájdite všetky homomorfizmy $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$.

Úloha 2.2.19. 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 2.2.20. 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 2.2.21. Zistite, s akými okruhmi sú izomorfné okruhy $\mathbb{Z}_{60}/(15)$, $\mathbb{Z}_{60}/(20)$, $\mathbb{Z}_{60}/(12)$.

Úloha 2.2.22. 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 2.2.23*. a) Dokážte, že v okruhu $C(0, 1)$ (príklad 2.1.13) 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 2.2.24. 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.

{idecvic:KONGRNG}

Úloha 2.2.25$^+$. 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 2.2.20).

Obrátene ak E je ľubovoľná kongruencia na R, tak trieda ekvivalencie $[0]_E$ je ideál v R.

{idecvic:KONGHOM}

Úloha 2.2.26$^+$. Nech $(R, +, \cdot)$ je okruh.
a) Ak $f\colon R \to S$ je homomorfizmus, tak relácia E na množine R daná predpisom $xEy \Leftrightarrow xf = yf$ je kongruencia (pozri úlohu 2.1.1).
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 $[0]$.

2.3 Vety o izomorfizme*

Podobne ako v prípade grúp, aj pri okruhoch sa veta 2.2.13, ktorú sme uviedli pod názvom veta o izomorfizme, dosť často zvykne volať prvá veta o izomorfizme. Často sú užitočné i ďalšie vety o faktorových okruhoch, ktoré sa zvyknú nazývať vety o izomorfizme.

Dôkazy sú veľmi podobné ako pri grupách a formálny dôkaz je v podstate len precvičenie manipulácie s definíciou faktorového okruhu. Skôr je dôležité uvedomiť si, čo tieto vety hovoria. (Asi je vhodné začať s tým, že si človek premyslíte platnosť podobných tvrdení pre

rozklady, t.j. keď na daných množinách nemáme dodatočnú grupovú či okruhovú štruktúru). A tiež je užitočné naučiť sa ich používať.[10]

Veta 2.3.1 (Druhá veta o izomorfizme)**.** *Nech R je okruh, S je podokruh R a I je ideál v R. Potom*

(i) *$S + I$ je podokruh R;*

(ii) *$S \cap I$ je ideál v S;*

(iii) *$S/(S \cap I) \cong (S + I)/I$.*

Dôkaz. Prvé dve časti sa overia priamo z definície.

V tretej časti môžeme postupovať rovnako ako v dôkaze druhej vety o izomorfizme pre grupy.[11] Vieme, že kanonický homomorfizmus $f\colon R \to R/I$ je homomorfizmus okruhov. Jeho zúžením na podmnožinu S dostaneme nový homomorfizmus $f|_S\colon S \to R/I$. V dôkaze pre grupy sme ukázali, že $\operatorname{Ker} f|_S = S \cap I$ a $\operatorname{Im} f|_S = S + I$. Podľa vety 2.2.13 máme teda $S/(S \cap I) \cong (S + I)/I$. □

Veta 2.3.2 (Tretia veta o izomorfizme)**.** *Nech R je okruh a $I \subseteq J$ sú ideály v R. Potom*

$$R/I \cong (R/J)/(I/J).$$

Dôkaz. TODO □

Veta 2.3.3 (Štvrtá veta o izomorfizme)**.** *Nech R je okruh a I je ideál v R. Potom priradenie*

$$S \mapsto S/I$$

je bijektívna korešpondencia medzi podokruhmi okruhu R obsahujúcimi ideál I a podokruhmi okruhu R/I.

Dôkaz. TODO □

Cvičenia

Úloha 2.3.1. Vedeli by ste vety 2.2.15 a 2.2.18 dokázať pomocou viet o izomorfizme?

2.4 Existencia maximálnych ideálov*

{maxid:SECTZORN}

Už aj vety 2.2.15 a 2.2.18 by vás mohli presvedčiť, že prvoideály a maximálne ideály sú pomerne dôležité. Ešte viac sa o tom presvedčíte ak sa budete neskôr venovať algebraickej geometrii a komutatívnej algebre.

Na tomto mieste by sme chceli dokázať dôležitý fakt, že každý okruh obsahuje maximálny ideál, dokonca každý vlastný ideál je obsiahnutý v nejakom maximálnom ideále. Dôkaz tohoto faktu využíva Zornovu lemu. O Zornovej leme ste možno už počuli v prvom ročníku na diskrétnej matematike. Pravdepodobne sa s ňou stretnete i na funkcionálnej analýze pri dôkaze Hahn-Banachovej vety. Viac sa o nej dozviete neskôr, napríklad na predmete Teória množín a matematická logika. Pokiaľ by vás zaujímal vzťah medzi axiómou výberu a Zornovou

[10] Čiže táto podkapitola by bola oveľa užitočnejšia, keby tu bolo viacero cvičení – ak niekedy zvýši čas, skúsim nejaké pridať.

[11] Dôkaz je podrobne uvedený napríklad v [Sl2].

lemou, iné aplikácie Zornovej lemy a ďalšie veci súvisace s touto témou, môžete sa o nich dočítať napríklad v [BŠ], [Sl3], [Z].

Na tomto mieste ale úplne stačí, ak Zornovej leme uveríte a naučíte sa ju používať. To je práve jeden z dôvodov, prečo som sem zaradil dôkaz o existencii maximálnych ideálov.

Uveďme najprv znenie Zornovej lemy. Pripomeňme, že *reťazec* v čiastočne usporiadanej množine $(P, \leq)$, je taká podmnožina $C \subseteq P$, že $(R, \leq)$ je lineárne usporiadaná, t.j. ľubovoľné dva prvky množiny C sú porovnateľné.

{maxid:VTZORN}

Veta 2.4.1 (Zornova lema)**.** *Ak každý reťazec v čiastočne usporiadanej množine $(P, \leq)$ má horné ohraničenie, tak $(P, \leq)$ má maximálny prvok.*

Pomocou Zornovej lemy teraz dokážeme:

{maxid:VTEXMAX}

Veta 2.4.2. *Nech R je okruh s jednotkou. Nech I je vlastný ideál v R. Potom existuje maximálny ideál J v okruhu R taký, že $I \subseteq J$.*

Dôkaz. Nech

$$P = \{K \subseteq R; K \text{ je ideál}, I \subseteq K \neq R\}.$$

Pretože $I \in P$, množina P je neprázdna. Budeme pracovať s čiastočne usporiadanou množinou $(P, \subseteq)$.

Chceme overiť, že $(P, \subseteq)$ spĺňa predpoklady Zornovej lemy. Nech teda $C \subseteq P$ je reťazec v P. Tvrdíme, že potom aj množina

$$H = \bigcup C = \bigcup_{K \in C} K$$

patrí do P. Je evidentné, že $I \subseteq H$. Keďže pre každý ideál $K \in C$ platí $1 \notin K$, máme $1 \notin H$.

Zostáva ukázať, že H je ideál. Nech teda $x, y \in H$. To znamená, že existujú $K_{1,2} \in C$ také, že $x \in K_1$ a $y \in K_2$. Keďže ide o reťazec, platí $K_1 \subseteq K_2$ alebo $K_2 \subseteq K_1$, bez ujmy na všeobecnosti predpokladajme, že platí prvá možnosť. Potom máme $x, y \in K_2$. Pretože K_2 je ideál, dostávame $x - y \in K_2 \subseteq H$. Ešte jednoduchšie sa ukáže, že ak $x \in H$, $z \in R$, tak aj $xz \in H$. DU (Môžete si všimnúť, že táto časť dôkazu je veľmi podobná na úlohu 2.2.12, s tým rozdielom, že tam nešlo o ľubovoľný reťazec.)

Podľa Zornovej lemy existuje prvok maximálny prvok J množiny $(P, \subseteq)$. Tento prvok je maximálny ideál v okruhu R, pre ktorý platí $I \subseteq J$. □

Viacero ďalších zaujímavých aplikácií Zornovej lemy v algebre môžete nájsť v [C2].[12]

{maxidcvic:ULOBEZMAX}

Cvičenia

Úloha 2.4.1*. Nájdite príklad okruhu, ktorý nemá žiadne maximálne ideály. (Z vety 2.4.2 viete, že to nemôže byť okruh s jednotkou.)

Úloha 2.4.2. Dokážte, že prienik reťazca prvoideálov je prvoideál. Na základe toho pomocou Zornovej lemy ukážte, že každý prvoideál obsahuje minimálny prvoideál. (Minimálny = minimálny vzhľadom na inklúziu.) Ako vyzerajú minimálne ideály v okruhu bez deliteľov nuly?

[12] Stránku `http://www.math.uconn.edu/~kconrad/blurbs/` odporúčam do vašej pozornosti – je tam veľa zaujímavých a užitočných vecí spísaných pomerne prístupným spôsobom.

2.5 Rád prvku, charakteristika okruhu

2.5.1 Rád prvku

V okruhu budeme rádom prvku $a \in R$ nazývať rád prvku a v komutatívnej grupe $(R, +)$.

Definícia 2.5.1. Ak $a \in R$, tak *rád* prvku a je najmenšie kladné celé číslo k také, že

$$k \times a = 0,$$

t.j. $\min\{k \in \mathbb{Z}^+; k \times a = 0\}$.

Ak také číslo neexistuje, tak rád prvku a je nekonečno. (Inak povedané, definitoricky kladieme $\min \emptyset = \infty$.)

Ľahko vidno, že rád nuly je vždy 1.

{radchar:VTROVNRAD}

Veta 2.5.2. *Ak R je okruh bez deliteľov nuly, tak ľubovoľné dva nenulové prvky okruhu R majú rovnaký rád.*

Dôkaz. [KGGS, Veta 4.4.1] Základná myšlienka dôkazu: $k \times a = 0 \Leftrightarrow k \times (ab) = b(k \times a) = a(k \times b) = 0 \Leftrightarrow k \times b = 0$ □

2.5.2 Charakteristika okruhu

Definícia 2.5.3. Nech R je okruh. *Charakteristika okruhu R* je najmenšie nezáporné celé číslo také, že $k \times a = 0$ platí pre všetky $a \in R$. Ak také, číslo neexistuje, tak charakteristika okruhu R je ∞.

$$\mathrm{char}(R) = \min\{k \in \mathbb{Z}^+; (\forall a \in R) k \times a = 0\}.$$

Poznámka 2.5.4. V mnohých textoch nájdete pomenovanie *okruh charakteristiky* 0 pre to isté, čo mi voláme okruh charakteristiky ∞. Takáto definícia by bola presne tá istá, ako keby sme definovali charakteristiku okruhu R ako minimálny prvok množiny $\{k \in \mathbb{Z}^+; (\forall a \in R) k \times a = 0\}$, pričom by sme ale hľadali minimálny prvok vzhľadom na čiastočné usporiadanie $|$ namiesto obvyklého usporiadania $\leq$. Iný pohľad, prečo by mohlo dávať zmysel hovoriť o okruhu charakteristiky 0, poskytuje aj úloha 2.5.1.

Veta 2.5.5. *Charakteristika okruhu bez deliteľov nuly je ∞ alebo prvočíslo.*

Dôkaz. [KGGS, Veta 4.4.2] □

2.5.3 Polia $\mathbb{Z}_p$ a $\mathbb{Q}$

Z minulého semestra vieme, že každá cyklická grupa je izomorfná buď so $(\mathbb{Z}, +)$ alebo $(\mathbb{Z}_n, \oplus)$.

Veta 2.5.6. *Nech R je okruh s jednotkou, ktorý nemá deliteľov nuly. Ak* $\mathrm{char}(R) = \infty$*, tak* $[1] \cong \mathbb{Z}$ *a ak* $\mathrm{char}\, R = p$*, tak* $[1] \cong \mathbb{Z}_p$.

V súlade s definíciou 2.1.19 by bol správnejší zápis $[\{1\}]$; potobne ako pri grupách však v prípade jednoprvkovej množiny $A = \{a\}$ budeme písať $[a]$ namiesto $[\{a\}]$.

Dôkaz. Využije sa homomorfizmus $\varphi\colon \mathbb{Z} \to R$, $\varphi\colon n \mapsto n \times 1$. Potom si stačí uvedomiť, že v uvedených dvoch prípadoch máme $\mathrm{Ker}\, \varphi = \{0\}$ resp. $\mathrm{Ker}\, \varphi = (p)$ a využiť vetu o izomorfizme. [KGGS, Veta 4.4.3] □

{radchar:VTQZP}

Veta 2.5.7. *Nech F je pole. Ak* $\mathrm{char}(F) = \infty$*, tak* $[[1]] \cong \mathbb{Q}$ *a ak* $\mathrm{char}(F) = p$*, tak* $[[1]] = \mathbb{Z}_p$.

Dôkaz. [KGGS, Veta 4.4.4] □

Nasledujúce tvrdenie má veľmi jednoduchý dôkaz a už ste sa s ním pravdepodobne viackrát stretli. Uviedli sme ho sem hlavne preto, že je pomerne často užitočné, takže si ho nezaškodí pripomenúť.

{radchar:LMPODPOLEVPR}

Lema 2.5.8. *Nech L je pole a $F \subseteq L$ je jeho podpole. Potom L je vektorový priestor nad F. (Pričom sčitovanie vo vektorom priestore L a násobenie skalárom $\cdot\colon F \times L \to L$ je obvyklé sčitovanie a násobenie z poľa L.)*

Dôkaz. DU □

Veta 2.5.9. *Počet prvkov konečného poľa je mocninou jeho charakteristiky.*

Dôkaz. Pozri [KGGS, Veta 4.4.5]. V podstate si stačí uvedomiť, že ak F je konečné pole charakteristiky p, tak obsahuje podpole izomorfné so $\mathbb{Z}_p$. Teda F je vektorový priestor nad $\mathbb{Z}_p$ podľa lemy 2.5.8. Keďže F je konečné, musí to byť konečnorozmerný priestor. □

Z tejto vety vidíme, že počet prvkov konečného poľa môže byť len tvaru p^n, kde p je prvočíslo. Neskôr ukážeme, že pre každé číslo tvaru p^n existuje konečné pole, ktoré má p^n prvkov. Navyše je takéto pole jediné až na izomorfizmus.

{radchar:VTXNAQJEQ}

Veta 2.5.10. *Ak počet prvkov konečného poľa F je q, tak pre každý prvok $a \in F$ platí $a^q = a$.*

Dôkaz. Stačí si uvedomiť, že rád prvku $a \neq 0$ v multiplikatívnej grupe poľa F je deliteľ $q-1$, z čoho vyplýva $a^{q-1} = 1$. [KGGS, Veta 4.4.6] □

Cvičenia

{radcvic:ULOCHAR0}

Úloha 2.5.1. Nech R je obor integrity. Ukážte, že:
a) Existuje práve jeden okruhový homomorfizmus $f\colon \mathbb{Z} \to R$, taký, že $1f = 1$.
b) $\mathrm{char}(R) = p$ práve vtedy, keď $\mathrm{Ker}\, f = (p)$.
Posledná uvedená rovnosť vysvetľuje prečo sa niekedy používa terminológia *okruh charakteristiky* 0. Prípad, ktorý my označujeme $\mathrm{char}(R) = \infty$, zodpovedá prípadu $\mathrm{Ker}\, f = (0)$. (Teda používať 0 namiesto ∞ tiež dáva zmysel.)

{radcvic:ULODREAM}

Úloha 2.5.2. Nech R je komutatívny okruh s jednotkou a $\mathrm{char}(R) = p$, kde p je prvočíslo. Ukážte potom, že v takomto okruhu platí $(x+y)^p = x^p + y^p$. (Môže pritom pomôcť úloha 2.1.11)

2.6 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 nuly – boli by deliteľmi nuly aj v jeho nadpoli.

Táto otázka má teda zmysel hlavne pre obory integrity. V nasledujúcej vete dokážeme, že každý obor integrity je podokruhom nejakého poľa.

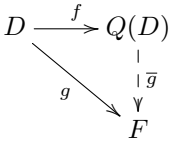
Poznámka 2.6.1. Konštrukcia podielového poľa obsahujúceho daný obor integrity je veľmi podobná na konštrukciu grupy z pologrupy s krátením. Tento výsledok poznáte z minulého semestra – pozri vetu I-3.2.1.

Definícia 2.6.2. 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'.

{podielove:VTQD}

Veta 2.6.3. *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 práve jedno vnorenie $\overline{g}\colon Q(D) \to F$ také, že $f \circ \overline{g} = g$.*



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.)

DU Rozmyslite si, že podmienka z vety určuje $Q(D)$ jednoznačne až na izomorfizmus.

Dôkaz vety 2.6.3 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 2.6.4. *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 2.6.3.) 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 relácia $\equiv$ je reflexívna a symetrická je úplne priamočiary. DU

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 2.6.5. *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

$$[(ad+bc, bd)] = [(a'd+b'c, b'd)]$$
$$[(ac, bd)] = [(a'c, b'd)]$$

čiže $[(a,b)] + [(c,d)] = [(a',b')] + [(c,d)]$ a $[(a,b)] \cdot [(c,d)] = [(a',b')] \cdot [(c,d)]$.

$(Q(D), +)$ *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 2.6.6. *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 práve jeden injektívny homomorfizmus $\overline{g}\colon Q(D) \to F$ s vlastnosťou $f \circ \overline{g} = g$.

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

$$\overline{g}\colon [(a,b)] \mapsto (ag)(bg)^{-1}.$$

(Pretože g je injektívny homomorfizmus, máme $\operatorname{Ker} g = \{0\}$, čiže $bg \neq 0$ pre každé $b \in D \setminus \{0\}$. Uvedený predpis teda skutočne má zmysel. Navyše je jasné, že toto je jediná možnosť ako definovať $\overline{g}$, pretože toto zobrazenie musí spĺňať $([a,1])\overline{g} = ag$ a $([1,b])\overline{g} = (bg)^{-1}$.)

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)

$$(ag)(dg) = (bg)(cg)$$

Po vynásobení tejto rovnosti $(bg)^{-1}(dg)^{-1}$ máme

$$(ag)(bg)^{-1} = (cg)(dg)^{-1}.$$

Čiže hodnota $\overline{g}$ skutočne nezávisí od výberu reprezentanta.

Zobrazenie $\overline{g}$ je homomorfizmus. Zachováva sčitovanie:

$$\begin{aligned}[(a,b)] + [(c,d)] = [(ad+bc,bd)] \mapsto (ad+bc)g((bd)g)^{-1} = ((ad)g + (bd)g)((bd)g)^{-1} = \\ = (ag)(dg)(bg)^{-1}(dg)^{-1} + (bg)(cg)(bg)^{-1}(dg)^{-1} = \\ = (ag)(bg)^{-1} + (cg)(dg)^{-1} = [(a,b)]\overline{g} + [(c,d)]\overline{g}\end{aligned}$$

Zachováva násobenie:

$$\begin{aligned}[(a,b)] \cdot [(c,d)] = [(ac,bd)] \mapsto (ac)g((bd)g)^{-1} = \\ = (ag)(bg)^{-1}(cg)(dg)^{-1} = [(a,b)]\overline{g} \cdot [(c,d)]\overline{g}\end{aligned}$$

Homomorfizmus $\overline{g}$ je injektívny. Stačí overiť, že $\operatorname{Ker}\overline{g} = \{0\}$. Ak $ag(bg)^{-1} = 0$, znamená to, že $ag = 0$ (lebo prvok $(bg)^{-1} \in F \setminus \{0\}$ 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 2.6.3.

{podielove:POZLOKAL}

Poznámka 2.6.7. 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 2.6.3 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 2.6.8. 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 2.6.1. Dokážte, že každý komutatívny okruh možno vložiť do komutatívneho okruhu s jednotkou.

Úloha 2.6.2. Ukážte, že $D_1 \cong D_2 \Rightarrow Q(D_1) \cong Q(D_2)$.

Úloha 2.6.3. Dokážte, že podielové pole je vlastnosťami uvedenými vo vete 2.6.3 určené jednoznačne až na izomorfizmus.

Úloha 2.6.4. Dokážte, že $\mathrm{char}(Q(D)) = \mathrm{char}(D)$.

Úloha 2.6.5. Nech D je podokruh poľa F a $1 \in D$. Dokážte, že:[13]
a) Existuje podpole K poľa F, ktoré obsahuje D a je to najmenšie (vzhľadom na inklúziu) podpole F s touto vlastnosťou.
b) $K \cong Q(D)$.

Úloha 2.6.6. Dokážte: Ak $D \subseteq D' \subseteq Q(D)$ pričom D' aj D sú obory integrity a podokruhy poľa $Q(D)$, tak $Q(D') = Q(D)$.

Úloha 2.6.7. Vysvetlite, ako vyplýva veta 2.5.7 z toho, čo sme dokázali o podielovom poli.

Úloha 2.6.8. Nájdite podielové pole pre daný okruh. (Vo všetkých prípadoch ide o podokruh poľa $\mathbb{C}$, čiže je to obor integrity.)
a) $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$
b) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$
c) $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt{2} + c\sqrt[3]{2}; a, b, c \in \mathbb{Z}\}$
Zdôvodnite, že ide skutočne o podielové pole daného okruhu.

Úloha 2.6.9. Aká je kardinalita podielového poľa $Q(D)$ v závislosti od kardinality D?

Úloha 2.6.10. Nájdite príklad oborov integrity D_1, D_2 takých, že $Q(D_1) \cong Q(D_2)$, ale $D_1 \ncong D_2$, $D_1 \ncong Q(D_1)$, $D_2 \ncong Q(D_2)$.

[13] Toto cvičenie je pomerne jednoduché. Je však užitočné uvedomiť si, že poskytuje podobný popis podielového poľa o akom sme hovorili v poznámke 2.1.24.

Kapitola 3

Celé čísla, polynómy a euklidovské okruhy

Naším cieľom v tejto kapitole je dokázať viaceré užitočné vlastnosti euklidovských okruhov. Typickým príkladom týchto okruhov sú okruh $(\mathbb{Z}, +, \cdot)$ celých čísel a okruh $(F[x], +, \cdot)$ polynómov nad poľom F. Začneme tým, že uvedieme niektoré vlastnosti týchto dvoch okruhov a potom sa budeme snažiť niektoré ich vlastnosti zovšeobecniť.

3.1 Celé čísla

{celeZ:SECTCELE}

Neskôr by sme sa chceli dostať k niektorým špeciálnym vlastnostiam okruhov, ktoré sú typické pre okruh $(\mathbb{Z}, +, \cdot)$ celých čísel a okruhy polynómov $(F[x], +, \cdot)$. Skúsime začať tým, že ich pripomenieme pre celé čísla (pre tento prípad by ste ich už mali poznať) a aj pre okruhy polynómov. Neskôr sa dostaneme k spoločnému zovšeobecneniu. (Pretože viaceré veci plánujeme neskôr dokázať všeobecnejšie, mnohé z nich tu uvedieme bez dôkazov alebo dôkazy preskočíme na prednáške.)

3.1.1 Deliteľnosť celých čísel

Pripomenieme si niektoré základné vlastnosti deliteľnosti pre celé čísla. Súčasne si môžeme rozmyslieť, ktoré z týchto vlastností platia vo všeobecnosti v oboroch integrity.

{celeZ:DEFDELI}

Definícia 3.1.1. Nech R je obor integrity. Hovoríme, že a *delí* b, označujeme $a \mid b$, ak existuje $c \in R$ také, že $b = ca$.

V opačnom prípade hovorím, že a *nedelí* b, označujeme $a \nmid b$.

Špeciálne pre celé čísla máme napríklad $3 \mid 9$ ale $3 \nmid 7$.

{celeZ:LMDELIZ}

Lema 3.1.2. *Pre ľubovoľné* $a, b, c, d \in \mathbb{Z}$, $a_i, r_i \in \mathbb{Z}$ *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. DU Skúste si pri dokazovaní týchto vlastností rozmyslieť i to, či by váš dôkaz fungoval v ľubovoľnom obore integrity. Neskôr sa k vlastnostiam deliteľnosti vrátime vo všeobecnejšom prípade – pozri lemu 3.3.2. □

V niektorých dôkazoch o deliteľnosti sa nám bude hodiť veta o delení so zvyškom, ktorú by ste mali poznať z prvého ročníka.

{celeZ:VTLONGDIV}

Veta 3.1.3 (Veta o delení so zvyškom)**.** *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.

Číslo r z predchádzajúcej vety sa nazýva *zvyšok p po delení číslom q* a označuje sa $p \bmod q$.

DU Dôkaz tejto vety ste už videli (s veľkou pravdepodobnosťou dokonca viackrát). Pokúste sa ju dokázať samostatne skôr než si prečítate nasledujúci dôkaz.

Dôkaz. Existencia: Množina $\{k \in \mathbb{Z}; kq \leq p\}$ je neprázdna a 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 $n = n'$, $r = r'$. □

Dôležitý pojem, s ktorým budeme často pracovať, je pojem najväčší spoločný deliteľ.

{celeZ:DEFGCD}

Definícia 3.1.4. *Najväčší spoločný deliteľ* čísel $a, b \in \mathbb{Z}$ je také $c \in \mathbb{Z}$, pre ktoré platí

(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 $\gcd(a, b)$.

V súvislosti s touto definíciou si môžeme položiť viacero otázok:

- Je $\gcd(a, b)$ určený jednoznačne?
- Existuje $\gcd(a, b)$ pre ľubovoľné $a, b \in \mathbb{Z}$?
- Prečo je táto definícia iná, než tá, na akú som zvyknutý? (Ak to tak je.)

Postupne sa pokúsime zodpovedať všetky tieto otázky.

Príklad 3.1.5. Skúsme sa pozrieť na konkrétny príklad, nájdime $\gcd(6,9)$. Ľahko sa dá overiť, že číslo 3 spĺňa definíciu najväčšieho spoločného deliteľa. To isté však platí aj o čísle -3. (Stačí si uvedomiť, že $a \mid b \Leftrightarrow (-a) \mid b$.)

Vidíme teda, že najväčší spoločný deliteľ v $\mathbb{Z}$ nie je určený jednoznačne.

DU Rozmyslite si, že $\gcd(a,b)$ pre $a,b \in \mathbb{Z}$ je určený jednoznačne *až na znamienko.* Možno vám pomôže dokázať najprv, že v $\mathbb{Z}$ platí $a \mid b \wedge b \mid a \Rightarrow a = \pm b$.

V prípade celých čísel by sme všetky problémy s nejednoznačnosťou vyriešiť jednoducho – vieme, že $\gcd(a,b)$ je jednoznačný až na znamienko, takže by sme sa mohli napríklad dohodnúť, že z dvoch možností vyberieme vždy tú nezápornú. Neskôr však budeme niečo podobné robiť všeobecnejšie v ďalších okruhoch, nie vždy sa dá nejako vybrať z viacerých možností pre n.s.d. jeden kanonický reprezentant.

Poznámka 3.1.6. Často budeme používať zápisy ako $d = \gcd(a,b)$, $3 = \gcd(6,9)$, $-3 = \gcd(6,9)$ či dokonca $\pm 3 = \gcd(6,9)$. Dalo by sa namietať, že tento zápis nie je úplne korektný – píšeme znamienko rovnosti medzi dve veci pričom na jednej strane máme číslo a na druhej strane niečo, čo nie je určené jednoznačne. Táto námietka je do istej miery oprávnená, azda však nespôsobí veľký problém keď zápis $d = \gcd(a,b)$ budeme chápať ako skratku pre „d je najväčší spoločný deliteľ a a b“. (Keby sme chceli byť veľmi presní, možno by sme zaviedli symbol $\gcd(a,b)$ pre množinu všetkých najväčších spoločných deliteľov a a b a používali zápis $d \in \gcd(a,b)$, takýto zápis však rozhodne nie je obvyklý. Iná možnosť by bola používať zápis $d \sim \gcd(a,b)$ ako v [KGGS], zatiaľ sme však nezaviedli symbol $\sim$; pozri definíciu 3.3.5.)

Takáto situácia nie je pre vás úplne nová s „nepresnosťou“ podobného typu ste sa už zvykli. Napríklad ste zvyknutí písať

$$\lim_{n\to\infty}(x_n + y_n) = \lim_{n\to\infty} x_n + \lim_{n\to\infty} y_n,$$

pričom uvedený zápis nepredstavuje úplne presne rovnosť, ale je skratkou pre tvrdenie: Ak existujú obe limity na pravej strane tejto rovnosti, tak existuje aj limita na ľavej strane a platí uvedená rovnosť. (Snáď sa to aspoň trochu podobá na situáciu, ktorú tu máme v súvislosti s n.s.d.)

Príklad 3.1.7. Ešte si všimnime jeden dôležitý špeciálny prípad: Pre ľubovoľné $a \in \mathbb{Z}$ platí $\gcd(a,0) = a$.

{celeZ:LMGCDLINKOM}

Lema 3.1.8. *Nech $a,b \in \mathbb{Z}$, pričom $a,b \neq 0$.*

Označme

$$M_{a,b} = \{n \in \mathbb{Z}; n > 0, (\exists x,y \in \mathbb{Z}) n = ax + by\},$$

čiže množinu všetkých kladných celočíselných kombinácií čísel a, b. Nech

$$c = \min M_{a,b}.$$

Potom $d = \gcd(a,b)$.

Dôkaz. Máme vlastne overiť, že dané číslo c spĺňa predpoklady z definície 3.1.4.

Najprv ukážme, že $c \mid a$ a $c \mid b$. Podľa vety 3.1.3 existujú q a r také, že $a = cq + r$, $0 \leq r < c$. Ak by platilo $r > 0$, tak dostaneme $r = a - cq = a(1 - cu) - bv \in M$, čo je v spore s tým, že c je najmenší prvok množiny $M_{a,b}$. Preto musí platiť $r = 0$, z čoho dostaneme $a = cq$ a $c \mid a$. Podobne sa overí $c \mid b$.

Predpokladajme, že $d \mid a,b$. Pre každé takéto číslo platí aj $d \mid ax + by$ pre ľubovoľné celé čísla x, y. Špeciálne platí $d \mid c$. □

Keďže každá podmnožina $\mathbb{N}$ má najmenší prvok, z predchádzajúcej lemy vyplýva existencia $\gcd(a,b)$ v prípade, že $a,b \neq 0$. Už vieme, že $\gcd(a,0)=0$. Vyriešili sme teda otázku existencie najväčšieho spoločného deliteľa a súčasne sme našli aj jeho celkom užitočnú charakterizáciu, ktorú sformulujeme ako samostatné tvrdenie – veta 3.1.10.

DU Využívame fakt, že každá podmnožina prirodzených čísel má najmenší prvok. Skúste si pripomenúť, ako tento fakt súvisí s princípom matematickej indukcie. (Diskrétna matematika, prvý ročník.)

Poznámka 3.1.9. Keby sme v predchádzajúcu lemu sformulovali tak, že by sme hovorili o minimálnom (najmenšom) prvku v čiastočne usporiadanej množine $(\mathbb{N},|)$, mohli by sme ju sformulovať tak, aby zahŕňala i prípady $a=0$ a $b=0$. Na dôkaz je ale asi vhodnejšia formulácia s $(\mathbb{Z}^+,\leq)$, pretože existencia minimálneho prvku je tu očividnejšia.

Z predchádzajúcej lemy dostaneme:

{celeZ:VTGCDLINKOM}

Veta 3.1.10 (Bézoutova identita)**.** *Nech $d=\gcd(a,b)$ pre $a,b\in\mathbb{Z}$. Potom existujú čísla $u,v\in\mathbb{Z}$ také, že*

$$d=au+bv.$$

Navyše pre $a,b\neq 0$ d je najmenšie nezáporné celé číslo, ktoré možno zapísať v takomto tvare.

DU Rozmyslite si, že veta platí aj v prípade, že niektoré z čísel a, b je nula.

{celeZ:DOSDELIGCD}

Dôsledok 3.1.11. *Nech $a,b,x\in\mathbb{Z}$. Ak $c=\gcd(a,b)$ a platí $x\mid a$, $x\mid b$, tak platí aj $x\mid c$.*

Poznámka 3.1.12. Možno ste zo strednej školy a z nižších ročníkov zvyknutí na trochu inú definíciu najväčšieho spoločného deliteľa. Konkrétne v druhej časti definície ste mohli použiť namiesto $d\mid c$ podmienku $|d|\leq|c|$. (Alebo $d\leq c$, ak ste pracovali s $\mathbb{N}$ namiesto $\mathbb{Z}$.) Je táto definícia ekvivalentná s tou, ktorú sme uviedli?

Všimnime si nasledujúcu vlastnosť: Ak $a\mid b$ a $b\neq 0$, tak $|a|\leq|b|$. DU

V oboch definíciach hľadáme istý prvok množiny $D_{a,b}=\{d\in\mathbb{Z}; d\mid a, d\mid b\}$. V jednej je to najväčší prvok vzhľadom na reláciu (kváziusporiadanie) $|$. (Všimnite si, že je reflexívna a tranzitívna $\mathbb{Z}$. Nie je však antisymetrická, čiže to nie je čiastočné usporiadanie. Takáto relácia sa zvykne nazývať kváziusporiadanie.[1]) V druhej definícii je to prvok, ktorý je najväčší v absolútnej hodnote.

Prepokladajme, že aspoň jeden z prvkov a, b je nenulový. Nech $c=\gcd(a,b)$ (podľa našej definície, t.j. najväčší prvok vzhľadom na $|$). Podľa dôsledku 3.1.11 potom $x\mid c$ pre všetky $x\in D_{a,b}$. Keďže $x,c\neq 0$, máme potom aj $|x|\leq|c|$. Teda c je prvok množiny $D_{a,b}$, ktorý je najväčší v absolútnej hodnote.

Vidíme teda, že tieto dve definície sú okrem prípadu $a=0$, $b=0$ ekvivalentné.

3.1.2 Rozšírený Euklidov algoritmus

{celeZ:SSECTEUKLID}

Už vieme, že najväčší spoločný deliteľ dvoch čísel sa dá vyjadriť ako ich celočíselná kombinácia $d=au+bv$. Skúsme sa pozrieť na to, či pre dané $a,b\in\mathbb{Z}$ by sme vedeli nájsť koeficienty u, v.

To sa dá robiť pomocou rozšíreného Euklidovho algoritmu, ktorého základom je nasledujúce jednoduché pozorovanie:

[1] V angličtine quasiorder alebo preorder. Najväčší a najmenší prvok môžeme pre kváziusporiadanie definovať rovnakým spôsobom ako pre čiastočné usporiadanie; rozdiel je ten, že pri kváziusporiadaní môžeme mať viacero najväčších prvkov.

{:LMEUKLIDGCD}

Lema 3.1.13. *Pre ľubovoľné $a, b, x \in \mathbb{Z}$, platí*

$$\gcd(a, b) = \gcd(a + bx, b).$$

Toto tvrdenie dokážeme neskôr v trochu všeobecnejšej formulácii – lema 3.3.24. Dôkaz je však vcelku jednoduchý, takže si ho môžete skúsiť rozmyslieť aspoň pre celé čísla. DU

{celeZ:PREUKLID}

Príklad 3.1.14. Chceme vyrátať $d = \gcd(89, 16)$ a vyjadriť ho v tvare $89u + 16v$.

Keď použijeme viackrát vetu o delení so zvyškom, tak dostaneme:

$$\begin{aligned} 89 &= 5.16 + 9 & 9 &= 89 - 5.16 \\ 16 &= 1.9 + 7 & 7 &= 16 - 9 = 6.16 - 89 \\ 9 &= 1.7 + 2 & 2 &= 9 - 7 = 2.89 - 11.16 \\ 7 &= 3.2 + 1 & 1 &= 7 - 3.2 = 39.16 - 7.89 \\ 2 &= 2.1 + 0 \end{aligned}$$

Z lemy 3.1.13 potom vidíme, že $\gcd(89, 16) = \gcd(16, 9) = \gcd(9, 7) = \gcd(7, 2) = \gcd(2, 1) = 1$. V pravom stĺpci sme dostali hľadané vyjadrenie

$$1 = 39.16 - 7.89.$$

Tento postup môžeme prehľadne zapísať aj do tabuľky.

89	1	0	
16	0	1	
9	1	-5	`1r-5*2r`
7	-1	6	`3r-4r`
2	2	-11	`4r-5r`
1	-7	39	`4r-3*5r`

Tento postup do istej miery pripomína riadkové úpravy na matici. V každom riadku máme koeficienty, pomocou ktorých vieme číslo z prvého stĺpca vyjadriť ako celočíselnú kombináciu čísel 89 a 16.

Posledný stĺpec tabuľky sme doplnili len na to, aby bolo vidno, aké úpravy sme robili. Môže to byť užitočné pri hľadaní prípadnej chyby – tento stĺpec ale v podstate nie je nutný. Postupovali sme presne podľa vety o delení so zvyškom. Ak rátate niečo takéto ručne, pri malých číslach si občas môžete všimnúť aj nejaké veci, ktoré vám trochu urýchlia výpočet. Napríklad ak si všimnete, že $2 = 2.9 - 16$, ušetríte jeden riadok. (Treba si ale dávať pozor, či zrýchlený postup je správny – v podstate si stačí pamätať lemu 3.1.13 a postupovať podľa nej.)

89	1	0	
16	0	1	
9	1	-5	`1r-5*2r`
2	2	-11	`2*4r-3r`
1	-7	39	`3r-4*4r`

V predošlom príklade sme našli jednu dvojicu (u, v) takú, že $89u + 16v = 1$. Je to jediná možnosť? Vedeli by ste nájsť všetky ostatné také dvojice? DU*

{celeZ:PRINVZ

Príklad 3.1.15. 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; prípadne použitím malej Fermatovej vety. 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

$$1 = -5 \odot 5 = 8 \odot 5,$$

ktorá platí v $\mathbb{Z}_{13}$. Teda v $\mathbb{Z}_{13}$ platí $5^{-1} = 8$.

Opäť ten istý postup by sme mohli zapísať tabuľkou:

13	1	0	
5	0	1	
3	1	-2	`1r-2*2r`
2	-1	3	`2r-3r`
1	2	-5	`2r-3r`

3.1.3 Kanonický rozklad

Pre prirodzené čísla poznáme kanonický rozklad na súčin prvočísel. Keby sme ho chceli sformulovať pre celé čísla, mohol by vyzerať napríklad takto:

Tvrdenie 3.1.16. *Pre každé celé číslo $z \in \mathbb{Z} \setminus \{0\}$ existuje práve jeden rozklad na prvočísla*

$$z = \pm p_1 \dots p_k,$$

pričom tento rozklad je jednoznačný až na poradie činiteľov.

Číslo $z = 1$ môžeme chápať ako prázdny súčin, t.j. $k = 0$.

Cvičenia

{celeZcvic:CUMRE}

Úloha 3.1.1. Ukážte, že $(\mathbb{N}, |)$ je čiastočne usporiadaná množina.

Úloha 3.1.2. Nech $(A, \leq)$ je kváziusporiadaná množina, t.j. $\leq$ je tranzitívna a reflexívna relácia na množine A. Definujme reláciu $\sim$ na množine A ako

$$a \sim b \Leftrightarrow a \leq b \wedge b \leq a.$$

Ukážte, že $\sim$ je relácia ekvivalencie na A. Ukážte, že predpis

$$[a] \preceq [b] \Leftrightarrow a \leq b$$

určuje dobre definovanú reláciu na množine $A/\sim$ tried ekvivalencie a táto relácia je čiastočným usporiadaním.

Úloha 3.1.3. Nech a, b, z sú celé čísla.
a) Ukážte, že ak existujú $x, y \in \mathbb{Z}$ také, že $ax + by = 1$, tak $\gcd(a, b) = 1$.
b) Ukážte, že $\gcd(za, zb) = z \gcd(a, b)$.

Úloha 3.1.4. Pre dané čísla a, b nájdite $d = \gcd(a, b)$. Nájdite tiež aspoň jednu dvojicu celých čísel x, y takú, že $ax + by = d$.
a) $a = 129$, $b = 43$;
b) $a = 221$, $b = 84$;
c) $a = 102$, $b = 147$;
d) $a = 348$, $b = 207$;
e) $a = 957$, $b = 609$;
f) $a = 4411$, $b = 2486$.

Úloha 3.1.5. Nájdite inverzný prvok k prvku a vzhľadom na násobenie modulo n (ak existuje); t.j. hľadáme inverzný prvok v okruhu $(\mathbb{Z}_n, \oplus, \odot)$:
a) $a = 6$, $n = 13$;
b) $a = 5$, $n = 23$;
c) $a = 5$, $n = 8$;
d) $a = 4$, $n = 15$;
e) $a = 9$, $n = 24$.

Úloha 3.1.6. Zistite, či existujú celé čísla x, y tak, aby platila uvedená rovnosť a ak áno, tak nájdite aspoň jednu takú dvojicu.
a) $\frac{1}{63} = \frac{x}{9} + \frac{y}{7}$
b) $\frac{29}{210} = \frac{x}{10} + \frac{b}{21}$

Úloha 3.1.7. Pre dané celé čísla a, b, c nájdite $d = \gcd(a, b, c)$ a nájdite aspoň jednu trojicu celých čísel x, y, z takú, že $d = ax + by + cz$.
a) $a = 6$, $b = 10$, $c = 15$;
b) $a = 156$, $b = 123$, $c = 114$;
c) $a = 952$, $b = 700$, $c = 546$.

Úloha 3.1.8. Ak máme nádoby s objemom 25l a 16l, dá sa pomocou nich odmerať 3l vody?

Úloha 3.1.9. Fibonacciho postupnosť je určená rekurentným predpisom $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$ pre $n \in \mathbb{N}$, $n \geq 1$. Ukážte, že $\gcd(F_n, F_{n+1}) = 1$. Koľko krokov (delení so zvyškom) je potrebných v Euklidovom algoritme pre čísla F_n a F_{n+1}? Vedeli by ste nájsť x, y také, že $xF_n + yF_{n+1} = 1$?

3.2 Okruhy polynómov – definícia, základné vlastnosti

Okrem okruhu celých čísel $(\mathbb{Z}, +, \cdot)$ budeme často pracovať aj s okruhmi polynómov.

Definícia 3.2.1. Nech R a komutatívny okruh s jednotkou a súčasne nech R je podokruh komutatívneho okruhu B, pričom oba okruhy majú tú istú jednotku. Prvok $x \in B \setminus R$ sa nazýva *neurčitá* nad R, ak pre ľubovoľné $a_n, a_{n-1}, \ldots, a_0 \in R$ platí

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0 \qquad \Rightarrow \qquad a_0 = \cdots = a_{n-1} = a_n = 0; \tag{3.1}$$ {polyndef:EQNEUR1}

t.j. výraz tvaru $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ sa rovná nule jedine v prípade, že všetky a_k sú nulové.

Definícia 3.2.2. Ak x je neurčitá nad okruhom R, tak prvky okruhu $R[x]$ nazývame *polynómy* v neurčitej x nad okruhom R a $R[x]$ voláme *okruh polynómov* nad R.

Z vety 2.1.21 vieme, že prvky $R[x]$ sú práve prvky tvaru $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 = \sum_{k=0}^{n} a_kx^k$ pre $n \in \mathbb{N}$, $a_0, \ldots, a_n \in R$.

Polynómy budeme obvykle označovať $f(x)$, $g(x)$, $p(x)$ a pod., kde písmeno x označuje neurčitú, ktorú používame, t.j. budeme používať zápis

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 = \sum_{k=0}^{n} a_kx^k.$$

Každému polynómu $f(x)$ môžeme priradiť nekonečnú postupnosť

$$(a_0, a_1, \ldots, a_{n-1}, a_n, 0, 0, \ldots)$$

prvkov okruhu R. Prvky $a_0, \ldots, a_n$ nazývame *koeficienty* polynómu $f(x)$.

Nie je ťažké si uvedomiť, že ak $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ a $g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_0$ sú dva polynómy z $R[x]$, tak

{polyndef:EQNEUR2}
$$f(x) = g(x) \qquad \Leftrightarrow \qquad (a_0, \ldots, a_n, 0, 0, \ldots) = (b_1, \ldots, b_m, 0, 0, \ldots), \tag{3.2}$$

čiže dva polynómy sa rovnajú práve vtedy, keď sa rovnajú ich postupnosti koeficientov. Podmienku (3.2) by sme dokonca mohli použiť priamo v definícii neurčitej namiesto (3.1) a dostali by sme tak ekvivalentnú definíciu. DU

Ďalej sa dohodneme, že posledný nenulový člen postupnosti koeficientov budeme nazývať *vedúci koeficient* polynómu. Inak povedané, ak $f(x) = \sum_{k=0}^{n} a_kx^k$ a $a_n \neq 0$, tak a_n je vedúci koeficient polynómu $f(x)$. Člen a_nx^n budeme nazývať *vedúci člen* polynómu $f(x)$ a číslo n budeme volať *stupeň polynómu p,* označujeme $\operatorname{st} f(x) = n$.

Všetky uvedené pojmy sme vlastne zatiaľ zadefinovali iba pre $f(x) \neq 0$, pretože pre nulový polynóm nemám žiadny nenulový koeficient. V takomto prípade kladieme definitoricky $\operatorname{st} f(x) = -\infty$.

Polynóm, ktorého vedúci člen je $a_n = 1$ budeme volať *monický polynóm.* Polynómy stupňa menšieho ako 1 voláme *konštantné polynómy.*

{polyndef:DOHONULKOEF}
Dohoda 3.2.3. Už sme si uvedomili, že polynómy sú rovnaké, ak majú rovnaké postupnosti koeficientov. Špeciálne napríklad polynómy $1+x+2x^2$ a je $1+x+2x^2+0x^3+0x^4$ sú rovnaké. Často sa nám bude hodiť to, že členy s nulovými koeficientami budeme môcť vynechávať alebo pridávať bez toho, aby sme zmenili polynóm.

Čiže napríklad ak budeme mať polynóm stupňa n v tvare $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$, tak niekedy budeme používať koeficienty a_m pre $m > n$, ktoré budeme automaticky chápať ako nulové. Niekedy sa nám dokonca bude hodiť pracovať i s koeficientami a_m pre $m < 0$, ktoré tiež budeme považovať za nulové.

{polyndef:POZNOTA}
Poznámka 3.2.4. Možno sa vám definícia okruhu polynómov tak, ako sme ju uviedli, zdá nejasná, či azda dokonca ťažkopádna. Ak je to tak, je úplne všetko v poriadku. Neskôr sa vrátime k otázke, či by sme okruh polynómov mohli definovať aj nejako inak a či by iné možné definície boli v nejakom zmysle „rovnako dobré“. Na to však budeme potrebovať najprv istú prípravu.

Zatiaľ sa pokúsime nejako zodpovedať aspoň tieto otázky:

- Ak by sme zobrali dve rôzne neurčité x, y nad R, dostaneme „rovnaké“ okruhy polynómov $R[x]$, $R[y]$? (Pod slovom „rovnaké“ tu budeme zrejme chápať *izomorfné.*)

- Existuje pre každý komutatívny okruh R s jednotkou nejaký okruh polynómov $R[x]$? Inak povedané: Dá sa pre každý okruh R nájsť nejaký nadokruh B a v ňom prvok x, ktorý je neurčitou nad R?

Azda po zodpovedaní týchto otázok a ukázaní iných možných definícií bude definícia okruhu polynómov jasnejšia.

Ešte predtým, než sa dostaneme k týmto otázkam, sa však pozrieme na to, ako funguje sčitovanie a násobenie polynómov a ukážeme si niektoré užitočné fakty o okruhoch polynómov.

Polynómy chápeme ako prvky $R[x]$. Pre ľubovoľný okruh tvaru $R[x]$ (aj ak by x nebola neurčitá nad R) sa dá overiť, že ak $f(x) = \sum_{k=0}^{n} a_k x^k$ a $g(x) = \sum_{k=0}^{m} b_k x^k$ tak ich súčet je tvaru

$$f(x) + g(x) = \sum_{k=1}^{l} (a_k + b_k) x^k,$$

kde $l = \max m, n$. (Podľa už spomenutej konvencie, ak nejaké koeficienty „chýbajú“ chápeme ich ako nulové – dohoda 3.2.3.) Súčin je o trochu komplikovanejší, ale dá sa ukázať, že

$$f(x) \cdot g(x) = \sum_{k=0}^{m+n} c_k,$$

kde

$$c_k = \sum_{i=1}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_{k-i}.$$

(Pri čítaní poslednej uvedenej sumy si opäť treba uvedomiť, že veľa v nej vystupujúcich koeficientov bude nulových – špeciálne všetky, kde sa objavuje niektorý koeficient pôvodného polynómu so záporným indexom.)

Formálny dôkaz predchádzajúcich rovností by bol len pomerne pracné cvičenie na indukciu a prácu s formálnymi zápismi súm. To sú pre študenta matematiky tiež nepochybne dôležité zručnosti, na tomto mieste ale asi bude užitočnejšie, ak si tieto dôkazy premyslíte len neformálne, ale zamyslíte sa nad tým, aké vlastnosti okruhu R a nadokruhu, z ktorého berieme neurčitú, sú tu dôležité. (Využíva sa niekde komutatívnosť okruhu B? Využívajú sa v dôkaze distributívne zákony? Využíva sa tam komutatívnosť sčitovania?) DU

Je dôležité, že sme si uvedomili, že polynómy môžeme sčitovať a násobiť a aj to, ako sčitovanie a násobenie polynómov funguje. Čiže slovo *okruh* v názve okruh polynómov je úplne oprávnené.

Keď už vieme, ako sa násobia polynómy pomerne ľahko z toho vieme ukázať, že

{polyndef:TVRRXJEOI}

Tvrdenie 3.2.5. *Ak R je obor integrity, tak pre ľubovoľné nenulové polynómy $f, g \in R[x]$ platí*

$$\mathrm{st}(fg) = \mathrm{st}(f) + \mathrm{st}(g)$$

a okruh $R[x]$ polynómov nad okruhom R je obor integrity.

Ak R je obor integrity a $f(x), g(x) \in R[x]$ sú polynómy, tak

$$\mathrm{st}(f(x)g(x)) = \mathrm{st}\, f(x) + \mathrm{st}\, g(x)$$

Dôkaz. Stačí si uvedomiť, že vedúci koeficient súčinu je súčin vedúcich koeficientov. Pozri aj [KGGS, Veta 5.2.1]. □

Keďže R je podokruh $R[x]$, platí aj obrátená implikácia: Ak $R[x]$ je obor integrity, tak aj R je obor integrity. DU

{polyndef:VTD

Veta 3.2.6. *Nech $A_{1,2}$ sú komutatívne okruhy s jednotkou, A_1 je podokruh B_1, A_2 je podokruh B_2. Nech $x \in B_1$ je neurčitá nad A_1 a nech $u \in B_2$. Nech $\varphi\colon A_1 \to A_2$ je homomorfizmus okruhov. Potom existuje práve jeden homomorfizmus $\tau\colon A_1[x] \to A_2[u]$ taký, že $\tau|_{A_1} = \varphi$ a $x\tau = u$.*

Dôkaz. [KGGS, Veta 5.2.2] □

{polyndef:DEFDOSHOM}

Definícia 3.2.7. Z vety 3.2.6 vyplýva, že ak máme polynóm $f(x)$ a $u \in R$, tak je jednoznačne určený homomorfizmus $\varphi\colon R[x] \to R$ podmienkami $x\varphi = u$, $a\varphi = a$ pre $a \in R$. Tento homomorfizmus budeme nazývať *dosadzovací homomorfizmus.*

Malo by byť jasné prečo používame názov dosadzovací homomorfizmus - vlastne sme do polynomického výrazu $f(x)$ za x všade dosadili u.

Dôsledok 3.2.8. *Ak $A_1 \cong A_2$, x je neurčitá nad A_1 a y je neurčitá nad A_2, tak $A_1[x] \cong A_2[y]$.*

Dôkaz. [KGGS, Dôsledok 2 vety 5.2.2] □

Predchádzajúca veta hovorí, že ak okruhy A_1, A_2 sú izomorfné, tak sú izomorfné aj okruhy polynómov nad týmito okruhmi. Tým je vlastne zodpovedná otázka o jednoznačnosti z poznámky 3.2.4, stále nám ale chýba odpoveď na otázku o existencii okruhov polynómov.

polyndef:POZNDOSADNADOK}

Poznámka 3.2.9. Všimnime si, že ak R je podokruh R', pričom oba sú komutatívne okruhy a majú rovnakú jednotku, tak neurčitá nad R' je súčasne neurčitou aj nad R. Preto okruh $R[x]$ môžeme chápať ako podokruh okruhu $R'[x]$.

Takisto ľahko vidno aj to, že do polynómu z $R[x]$ vieme dosadzovať aj hodnoty z ľubovoľného nadokruhu. Čiže pre ľubovoľný nadokruh R' okruhu R a ľubovoľné $u \in R'$ máme práve jeden homomorfizmus $\varphi\colon R[x] \to R'$ taký, že $x\varphi = u$, $a\varphi = a$ pre $a \in R$.

3.2.1 Existencia neurčitej

{polyndef:VTEXIST}

Veta 3.2.10. *Nech R je ľubovoľný komutatívny okruh s jednotkou. Potom existuje nadokruh B okruhu R a prvok $x \in B$, ktorý je neurčitou nad R.*

Dôkaz. Definujme B ako množinu všetkých postupností prvkov R, ktoré sú od istého členu nulové, t.j.

$$B = \{(a_0, \ldots, a_{n-1}, a_n, 0, 0, \ldots); a_n, a_{n-1}, \ldots, a_0 \in R\}.$$

Na tejto množine zadefinujeme operácie $+$ a $\cdot$ nasledovne: Pre postupnosti $a = (a_n)_{n=1}^{\infty}$, $b = (b_n)_{n=1}^{\infty}$ z B definujeme $a + b = c = (c_n)_{n=1}^{\infty}$ a $a \cdot b = d = (d_n)_{n=1}^{\infty}$

$$c_k = a_k + b_k$$

$$d_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}$$

Pomerne ľahko vidno, že takto dostaneme binárne operácie na množine B. Fakt, že $(B, +, \cdot)$ je okruh, sa dá overiť priamym výpočtom. (Síce pomerne pracne, ale skutočne nejde o nič iné ako mechanické overovanie identít.) DU

R je izomorfný s podokruhom B. Zobrazenie $f\colon R \to B$, $f\colon r \mapsto (r, 0, 0, \dots)$ je injektívny homomorfizmus. DU

B obsahuje neurčitú nad R. Nech $x = (0, 1, 0, 0, \dots)$. Potom $x^n = (\underbrace{0, 0, \dots, 0}_{n\text{-krát}}, 1, 0, 0, \dots)$ a

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (a_0, \dots, a_{n-1}, a_n, 0, 0, \dots).$$

Ak $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 = (0, 0, \dots)$, tak $a_0 = 0$, …, $a_{n-1} = 0$, $a_n = 0$. □

Poznámka 3.2.11. Keby sme podobne definovali násobenie na všetkých postupnostiach prvkov z R, dostali by sme okruh formálnych mocninových radov. S mocninovými radmi ste sa stretli na analýze, kde ste ich však skúmali ako funkcie iba v tých bodoch, kde daný rad konverguje. Formálne mocninové rady sú užitočné v kombinatorike, kde sa s nimi stretnete v podobe generujúcich funkcií.

3.2.2 Porovnanie rôznych definícií okruhu polynómov

Dá sa povedať, že to čo sme si doteraz povedali, dáva prinajmenšom dve možnosti, ako zaviesť okruh polynómov.

Najprv sme ho zaviedli pomocou pojmu neurčitej, čo bol prvok z nejakého nadokruhu. (Pričom sme ukázali jednoznačnosť až na izomorfizmus.) Pri tomto spôsobe sme mali zadarmo vlastnosť, že dostaneme okruh; problém bol s tým, že sme nevedeli zaručiť, či neurčitá vôbec existuje.

Spôsob, akým sme v dôkaze vety 3.2.10 dokázali existenciu neurčitej by sme mohli zobrať i za definíciu okruhu polynómov. Zápis cez nekonečné by sa odlišoval od zápisu, na ktorý sme zvyknutí, ale prechod medzi týmito dvoma označeniami je len formálna záležitosť. V tomto prípade nemáme problém s existenciou, keďže sme okruh $R[x]$ explicitne skonštruovali. Pomerne pracné je však overenie, že ide skutočne o okruh (toto overenie sme vynechali) a že v ňom už máme neurčitú.

Každopádne, najjednoduchšie je pozerať sa na okruhy polynómov ako na zápisy tvaru $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ s takým násobením a sčitovaním, na aké ste zvyknutí. Azda však nie je úplne na škodu, že sme si ukázali aj to, ako sa okruh polynómov dá zaviesť formálne.

3.2.3 Polynomické funkcie

V súvislosti s polynómami je prirodzené pozrieť sa aj na *polynomické funkcie,* t.j. funkcie tvaru

$$s \mapsto f(s),$$

kde $f(x) \in R[x]$. Inak povedané do $f(x)$ dosadzujeme jednotlivé prvky okruhu R pomocou dosadzovacieho homomorfizmu (definícia 3.2.7).

My sa polynomickými funkciami nebudeme zaoberať, ak by ste sa o nich chceli dozvedieť viac, môžete si o nich niečo prečítať napríklad v [KGGS, Podkapitola 5.1]. Aspoň stručne by sme si povedali niečo o tom, prečo je dôležité rozlišovať medzi polynómami a polynomickými funkciami a ukázali, že tieto dva pojmy nie sú totožné.

Polynóm NIE JE funkcia!

Ako prvú vec si môžeme uvedomiť, že dvom rôznym polynómom môže zodpovedať tá istá polynomická funkcia.

Príklad 3.2.12. Budeme pracovať v okruhu $\mathbb{Z}_2[x]$. Zoberme si polynómy $f(x) = x^2 + x$ a $g(x) = 0$. Ide o rôzne polynómy.

V oboch prípadoch však zodpovedajúca polynomická funkcia je nulová funkcia, máme totiž

$$0 \mapsto 0^2 + 0 = 0;$$
$$1 \mapsto 1^2 + 1 = 0.$$

Vedeli by ste ukázať, že niečo podobné nemôže nastať v prípade okruhu $\mathbb{R}[x]$? Dokonca ani v prípade, že pracujeme s okruhom $F[x]$, kde F je ľubovoľné nekonečné pole. DU

Ďalší aspekt, kvôli ktorému je často užitočné pracovať s polynómami a s polynomickými funkciami je ten, že do polynómov chceme dosť často dosadzovať nielen hodnoty z okruhu R ale aj hodnoty z jeho rôznych nadokruhov – pozri poznámku 3.2.9. Napríklad budeme chcieť mať možnosť do polynómu $x^2 + 1$, ktorý je z $\mathbb{R}[x]$, dosadiť aj komplexné číslo i.

Keby sme pracovali s polynomickou funkciou museli by sme pevne zvoliť definičný obor. (Napríklad si pevne zvoliť jeden nadokruh R.) My však nechceme vopred obmedziť, aké prvky je povolené dosadzovať do polynómu.

3.2.4 Veta o delení so zvyškom

Pre nás bude dôležitý hlavne prípad keď okruh R je pole. Naším plánom je ukázať, že i v tomto prípade platia mnohé tvrdenia, ktoré sme predtým spomenuli v časti 3.1 pre okruh celých čísel $(\mathbb{Z}, +, \cdot)$.

Ako sme už ukázali, pre polynómy nad poľom platí

$$\operatorname{st}(p(x)q(x)) = \operatorname{st} p(x) + \operatorname{st} q(x).$$

Pri dokazovaní rôznych vlastností okruhu polynómov nad poľom bude pre nás často užitočná nasledujúca veta:

{polyndef:VTDEL}

Veta 3.2.13 (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 $\operatorname{st} r(x) < \operatorname{st} g(x)$.

Navyše, $q(x)$ a $r(x)$ sú týmito podmienkami jednoznačne určené.

Definícia 3.2.14. Polynómy $q(x)$ a $r(x)$ jednoznačne určené podmienkami z vety 3.2.13 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 $n = \operatorname{st}(f)$.

1° Ak $\operatorname{st} f(x) < \operatorname{st} g(x)$, stačí položiť $q(x) = 0$ a $r(x) = f(x)$.

2° Nech $n = \operatorname{st} f(x) \geq \operatorname{st} g(x)$ 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 $\operatorname{st}(h) < \operatorname{st}(f)$, 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 3.2.15. 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 3.4.1.

{polyndef:POZDELMONIC}

Poznámka 3.2.16. Tiež si môžeme všimnúť, že monickým polynómom by sme vedeli deliť v ľubovoľnom obore integrity, dôkaz by bol rovnaký ako pre vetu 3.2.13.

Cvičenia

Úloha 3.2.1. Ak charakteristika okruhu R je n, aká je charakteristika okruhu polynómov $R[x]$?

Úloha 3.2.2. Vydeľte dané polynómy so zvyškom v $\mathbb{C}[x]$.
a) $f(x) = x^4 + 3x^3 - 4x + 2$, $g(x) = x^2 + x - 2$
b) $f(x) = x^5 + 2x^3 + 3x + 4$, $g(x) = x^3 + x + 1$
c) $f(x) = x^3 + (2 + 2i)x^2 + 3ix + 1$, $g(x) = x^2 + (2 + i)x + i$

3.3 Deliteľnosť v oboroch integrity

Už sme spomenuli, že by sme sa teraz chceli zaoberať tým, či okruh $(F[x], +, \cdot)$ má podobné vlastnosti ako $(\mathbb{Z}, +, \cdot)$. Pokúsime sa to robiť vo väčšej všeobecnosti – tak aby naše dôkazy fungovali pre tieto dva okruhy a možno aj nejaké ďalšie – vždy sa však oplatí rozmyslieť si, čo sa deje v týchto dvoch konkrétnych prípadoch.

V definícii 3.1.1 sme si povedali, že ak máme obor integrity R a prvky $a, b \in R$, tak

$$a \mid b \qquad \Leftrightarrow \qquad (\exists c \in R) b = ca.$$

V dôkaze niektorých tvrdení o deliteľnosti pre obory integrity sa môže niekedy hodiť nasledujúce pomocné tvrdenie, ktoré je špeciálnym prípadom tvrdenia 2.1.16.

{euklid:LMAB1}

Lema 3.3.1. *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 $b = 1$. □

{euklid:LMDELI}

Lema 3.3.2. *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. DU Dôkaz je prakticky rovnaký ako pre celé čísla – lema 3.1.2. □

Príklad 3.3.3. 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 3.3.4. 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)

{euklid:DEFASOC}

Definícia 3.3.5. 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 $b \mid a$

$$a \mid b \ \wedge \ b \mid a \Leftrightarrow a \sim b$$

{euklid:LMKONJ}

Lema 3.3.6. *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. DU □

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 3.1.2.) Posledná podmienka hovorí, že relácia $\sim$ sa správa rozumne vzhľadom na násobenie.

Definícia 3.3.7. Ak okruh R má jednotku a $ab = 1$, hovoríme, že a je deliteľ jednotky. Množinu všetkých deliteľov jednotky budeme označovať $U(R)$.

{euklid:TVRURSIM}

Tvrdenie 3.3.8. *Nech R je obor integrity. Potom*

{euklid:URSIMit1}

(i) *Delitele jednotky s operáciou násobenia tvoria grupu, t.j. $(U(R), \cdot)$ je grupa.*

{euklid:URSIMit2}

(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 3.3.2 vieme, že $0 \mid a$ iba pre $a = 0$). Samozrejme, $u0 = 0$ pre ľubovoľné $u \in U(R)$.

Zostáva nám teda dokázať tvrdenie pre prípad $a \neq 0$.

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 3.3.1 dostaneme $cd = 1$, čiže c aj d sú delitele jednotky. □

{euklid:PRDELJED}

Príklad 3.3.9. Ľahko sa dá overiť, že ± 1 sú delitele jednotky v $\mathbb{Z}$ a všetky nenulové konštantné polynómy sú delitele jednotky v $F[x]$. (Tento fakt vyplýva aj z lemy 3.3.14, 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 $\operatorname{st} g(x) \geq 0$. Potom (tvrdenie 3.2.5) $\operatorname{st}(fg) = \operatorname{st} f(x) + \operatorname{st} g(x) \geq \operatorname{st} f(x)$. Súčasne vieme $\operatorname{st}(f(x)g(x)) = \operatorname{st} 1 = 0$, preto aj $\operatorname{st} f(x) = 0$ a $f(x)$ je konštantný polynóm. (Nemôže platiť $f(x) = 0$; zdôvodniť to môžeme rovnako ako sme to spravili pre polynóm $g(x)$.)

3.3.1 Euklidovské okruhy

Veta 3.2.13 o delení so zvyškom je dôležitou vlastnosťou okruhu $F[x]$ polynómov nad poľom F. Veta 3.1.3 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.

{euklid:DEFOI

Definícia 3.3.10. 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 3.3.11. 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 3.3.10, tak existuje aj taká norma, ktorá navyše spĺňa $N(a) \leq N(ab)$ (pozri napríklad [R]).

Príklad 3.3.12. Triviálnym príkladom euklidovského okruhu je ľubovoľné pole. Tu dokonca môžeme normu zvoliť úplne ľubovoľne.

Okruh $\mathbb{Z}$ je euklidovský okruh. Ako normu môžeme zvoliť absolútnu hodnotu čísla z, čiže $N(z) = |z|$. Takisto norma daná predpisom $N(z) = |z| + 1$ vyhovuje podmienkam z definície euklidovského okruhu. Alebo tiež $N(z) = |z| - 1$ pre $z \neq 0$ (a $N(0)$ zvolené ľubovoľne).

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).

Príklad 3.3.13. Ďalším príkladom euklidovského okruhu je okruh $\mathbb{Z}[i]$. Dá sa ukázať, že ak použijeme normu $N(z) = |z|^2 = z\overline{z}$, t.j.,

$$N(a + bi) = a^2 + b^2,$$

tak táto norma skutočne vyhovuje definícii euklidovského okruhu. Pozri [KGGS, Príklad 7.2.1].

Ľahko si môžeme všimnúť, že

{euklid:LMNORM0}

Lema 3.3.14. *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 $d = 0$. □

3.3.2 Okruhy hlavných ideálov

Ďalším typom okruhov, ktorý bude pre nás užitočný sú okruhy hlavných ideálov.

Definícia 3.3.15. 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 $a \in R$.

d:TVREOJEOHI}

Tvrdenie 3.3.16. *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 3.3.14). 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 $\{N(b); b \in I \setminus \{0\}; N(b) \neq 0\}$ 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 $a = bc + d$. Pritom $d = a - bc \in I$, 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 3.3.17. 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 $f(x)$.

{euklid:PRID2X}

Príklad 3.3.18. Okruh $\mathbb{Z}[x]$ je príklad oboru integrity, ktorý nie je okruhom hlavných ideálov. Ak uvažujeme ideál

$$(2, x) = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]; a_0 \in 2\mathbb{Z}, a_i \in \mathbb{Z} \text{ pre } i \geq 1\}$$

v okruhu $\mathbb{Z}[x]$ (t.j. ideál generovaný polynómom x a konštantným polynómom 2; pozri poznámku 3.3.20), 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 3.2.5.) 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 3.3.16, že to nie ani euklidovský okruh.

V dôsledku 2.2.19 sme ukázali, že každý maximálny ideál je prvoideál. V okruhu hlavných ideálov platí aj obrátená implikácia:

{euklid:TVROHIPRVOMAX}

Tvrdenie 3.3.19. *Ak $I = (m)$, $I \neq \{0\}$, je vlastný 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:

$$a \mid b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a). \tag{3.3}$$

{euklid:EQIDEDELI}

(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 2.2.9.)

{euklid:POZNIDEGENER}

Poznámka 3.3.20. 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 3.3.21. *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.

{euklid:TVRBEZOUT}

Tvrdenie 3.3.22. *Ak R je okruh hlavných ideálov, tak pre ľubovoľné $a, b \in R$ 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.

{euklid:DOSEUKLEMA}

Dôsledok 3.3.23. *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 3.3.22 máme existenciu $x, y \in R$ takých, že

$$ax + by = 1.$$

Potom

$$a \mid acx + bcy = (ax + by)c = c.$$

□

Tvrdenie 3.3.22 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.* Pre prípad okruhu celých čísel sme si tento algoritmus už ukázali v časti 3.1.2.

Základom Euklidovho algoritmu je nasledujúca lema:

{euklid:LMEUKLIDGCD}

Lema 3.3.24. *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 zvyšku 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 $r_k = x_ka + y_kb$, kde $x_k, y_k \in R$, čiže týmto algoritmom vieme získať takéto vyjadrenie pre $\gcd(a, b)$.

Ukážeme si tento postup na konkrétnych príkladoch. Príklady v okruhu $\mathbb{Z}$ ste už videli – príklady 3.1.14, 3.1.15. (Najväčší spoločný deliteľ v $\mathbb{Z}$ viete zo strednej školy rátať pomocou rozkladu na prvočísla – niečo podobné platí všeobecne, ako uvidíme v tvrdení 3.3.37. 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.)

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 (t.j. normovaný resp. monický polynóm) – potom už je najväčší spoločný deliteľ určený jednoznačne.

Príklad 3.3.25. 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 $g(x)$.

$$3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6 = (x+3)(3x^4 - 4x^3 - x^2 - x - 2) - 3x^3 - 2x^2$$
$$3x^4 - 4x^3 - x^2 - x - 2 = (-3x^3 - 2x^2)(-x+2) + 3x^2 - x - 2$$
$$-3x^3 - 2x^2 = (3x^2 - x - 2)(-x-1) + (-3x - 2)$$

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

$$\gcd(f(x), g(x)) = x + \frac{2}{3} = -f(x)\frac{x^2 - x - 1}{3} + g(x)\frac{x^3 + 2x^2 - 5x - 4}{3}$$

Opäť, pokiaľ by Vám to lepšie vyhovovalo, celý postup si môžete zapísať do tabuľky.

$f(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$	1	0
$g(x) = 3x^4 - 4x^3 - x^2 - x - 2$	0	1
$h_1(x) = f(x) - (x+3)g(x) = -3x^3 - 2x^2$	1	$-(x+3)$
$h_2(x) = g(x) + (x-2)h_1(x) = 3x^2 - x - 2$	$x - 2$	$-(x^2 + x - 7)$
$h_3(x) = h_1(x) + (x+1)h_2(x) = -3x - 2$	$x^2 - x - 1$	$-(x^3 + 2x^2 - 5x - 4)$
$h_2(x) + (x-1)h_3(x) = 0$		

V predposlednom riadku sa naposledy vyskytol nenulový zvyšok, čiže ide o $\gcd(f(x), g(x))$. Z tohoto riadku vieme aj jeho vyčítať vyjadrenie – také isté, ako sme dostali v predchádzajúcom postupe. (Presnejšie povedané, dostali sme rovnaké vyjadrenie až na prenásobenie konštantou – vynormovanie.)

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 (príklad 3.4.11), 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.

3.3.3 Gaussove okruhy

Pojem analogický k pojmu prvočísla je v okruhu pojem ireducibilného prvku.

Definícia 3.3.26. 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 3.3.27. Vieme, že prvočísla boli definované tak, že ich rozklad na súčin $p = ab$ dvoch prirodzených čísel 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 3.3.28. *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 3.3.29. *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 3.3.1), čiže b je deliteľ jednotky.

Keďže ideál p je vlastný, p nie je deliteľ jednotky. □

V OHI platí aj obrátená implikácia.

{euklid:TVROH

Tvrdenie 3.3.30. *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 (3.3)) nasledujúci veľmi dôležitý vzťah.

{gcc:DOSPRVOC}

Dôsledok 3.3.31. *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.

{gcc:TVROHIJEUFD}

Tvrdenie 3.3.32. *Každý okruh hlavných ideálov je okruhom s jednoznačným rozkladom.*

Dôkaz. Chceme dokázať existenciu a jednoznačnosť rozkladu na súčin ireducibilných prvkov. Jednoznačnosť vyplýva z dôsledku 3.3.31.

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 3.3.33. 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 3.3.34. 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 3.3.31 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 rovný ± 1.

Poznamenajme, že podobný spôsobom sa dá ukázať, že aj 3 a $1 \pm \sqrt{5}i$ sú ireducibilné.

Príklad 3.3.35. 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 7.4.1], [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 3.3.18.)

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 3.3.36. *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 $q_{f(k)} \sim p_k$ pre $k = 1, \dots, m$.*

(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. □

{euklid:TVRGCDIRED}

Tvrdenie 3.3.37. *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 3.3.1. Vypočítajte $d(x) = \gcd(f(x), g(x))$ a vyjadrite ho v tvare $d(x) = u(x)f(x) + v(x)g(x)$.
a) $f(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$, $g(x) = 3x^4 - 4x^3 - x^2 - x - 2$;
b) $f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$, $g(x) = 2x^3 - x^2 - 5x + 4$;
c) $f(x) = x^4 + 6x^3 + 9x^2 - 2x - 9$, $g(x) = x^3 + 4x^2 + 2x - 7$;
d) $f(x) = x^8 - 1$, $g(x) = x^5 - 1$
(Výsledky: a) $u(x) = -\frac{1}{3}x^2 + \frac{1}{3}x + \frac{1}{3}$, $v(x) = \frac{1}{3}x^3 + \frac{2}{3}x^2 - \frac{5}{3}x - \frac{4}{3}$, $d(x) = x + \frac{2}{3}$
b) $u(x) = -\frac{x-1}{3}$, $v(x) = \frac{2x^2-2x-3}{3}$, $d(x) = x - 1$
c) $d(x) = 1$, $u(x) = 1/30(2x^2 + 5x - 1)$, $v(x) = -1/30(2x^3 + 9x^2 + 7x + 3)$)

3.4 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 spomenuli, že ak R je Gaussov okruh, tak aj $R[x]$ je Gaussov okruh.)

3.4.1 Korene polynómov

{polyn2:SSECTKORENE}

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 3.2.7.)

Definícia 3.4.1. 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 predchádzajúcej definícii dosadzujeme do polynómu z $F[x]$ prvok z nadpoľa F'. To však nie je problém – keďže koeficienty polynómu $f(x)$ sú z $F \subseteq F'$, tento polynóm súčasne patrí do $F'[x]$.

Príklad 3.4.2. 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.

{polyn2:LMZVYSOKJEFC}

Lema 3.4.3. *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*

{polyn2:EQZVYSOKJEFC}

$$f(x) = (x - c)g(x) + f(c). \tag{3.4}$$

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

{polyn2:LMLINDELI}

Lema 3.4.4. *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 (3.4.3) 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 3.4.3) $f(c) = 0$ a c je koreň polynómu f. □

n2:DEFNASKOR}

Definícia 3.4.5. 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 3.4.6. 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 3.4.7. 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}	$\ldots$
c		$a_n c$	$(a_n c + a_{n-1})c$	$\ldots$
	a_n	$a_n c + a_{n-1}$	$a_n c^2 + a_{n-1}c + a_{n-2}$	$\ldots$

$\ldots$	a_1	a_0
$\ldots$	$\ldots$	$(a_n c^{n-1} + a_{n-1}c^{n-2} + \cdots + a_1)c$
$\ldots$	$a_n c^{n-1} + a_{n-1}c^{n-2} + \cdots + a_1$	$a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0 = f(c)$

Príklad 3.4.8. 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 napríklad [KGGS, kapitola 6.1] alebo [Sl1, Dodatok B]).

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 $\mathbb{Q}$).

3.4.2 Racionálne korene polynómu s celočíselnými koeficientami

{polyn2:RACKOR}

Tvrdenie 3.4.9. *Ak $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ 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), 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 3.3.23).

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 3.4.9).

lyn2:RACKOR2}

Tvrdenie 3.4.10. *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 aj b_0 byť celé číslo a navyše $q \mid pb_0$. Pritom $\gcd(p,q) = 1$, teda $q \mid b_0$ (dôsledok 3.3.23).

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.

{polyn2:PRRACKOR}

Príklad 3.4.11. Nájdite racionálne korene polynómu $f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6$ (aj s násobnosťami).

Podľa tvrdenia 3.4.9 má platiť $p \mid 6$, $q \mid 24$. Dostávame teda možnosti:
$p \in \{\pm1, \pm2, \pm3, \pm6\}$
$q \in \{1, 2, 3, 4, 6, 8, 12, 24\}$
$\frac{p}{q} \in \{\pm1, \pm\frac{1}{2}, \pm\frac{1}{3}, \ldots\}$
(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	$\boxed{0}$
$\frac{1}{2}$		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 poslednom výpočte sme nerátali do konca – zastavili sme sa pri zlomku $-\frac{1}{2}$. Mohli sme to urobiť vďaka tvrdeniu 3.4.10.)

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	$\boxed{-105}$

	4	1	1	-3
$\frac{3}{2}$		6	$\frac{21}{2}$	
	4	7		$\neq 0$

	4	1	1	-3
$-\frac{3}{2}$		-6	$-\frac{15}{2}$	
	4	-5		$\neq 0$

	4	1	1	-3
$\frac{3}{4}$		3	3	3
	4	4	4	$\boxed{0}$
$\frac{3}{4}$		3	$\frac{21}{4}$	
	4	7	$\neq 0$	

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

$$f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6 = 24\left(x - \frac{1}{2}\right)\left(x + \frac{2}{3}\right)\left(x - \frac{3}{4}\right)(x^2 + x + 1).$$

(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

$$f(x) = (2x - 1)(3x + 2)(4x - 3)(x^2 + x + 1).$$

3.4.3 Algebraicky uzavreté polia

{polyn2:DEFALGUZE}

Definícia 3.4.12. 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:

{polyn2:TVRALGUZE}

Tvrdenie 3.4.13. *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 3.4.14 (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:

{polyn2:VTSTEINITZ}

Veta 3.4.15 (Steinitz)**.** *Pre každé pole F existuje algebraicky uzavreté nadpole F'.*

Všimnime si ešte jednu užitočnú vlastnosť komplexných koreňov polynómov s reálnymi koeficientami.

{polyn2:TVRKOMPZDR}

Tvrdenie 3.4.16. *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 3.4.1.

DOSREALNEPAR}

Dôsledok 3.4.17. *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). □

3.4.4 Ireducibilné polynómy

Definícia 3.4.18. 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 3.4.19. 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 3.4.20 (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.

{polyn2:TVRIRI

Tvrdenie 3.4.21. *Ak F je pole a $f(x) \in F[x]$ je polynóm stupňa 2 alebo 3, tak polynóm $f(x)$ je ireducibilný 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 3.4.4 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 3.4.22. 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 $\mathbb{Q}[x]$.

3.4.5 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 3.4.23. V príklade 3.4.11 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 koreňové 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 [Gu1, Gu2].

3.4.6 Ireducibilita polynómov s celočíselnými koeficientami

V tejto časti by sme sa chceli zaoberať niektorými kritériami, ktoré nám pomôžu overiť o polynóme s celočíselnými koeficientami zistiť, či je ireducibilný v $\mathbb{Q}[x]$. (Jedno kritérium takého typu už poznáme – vieme zistiť, či polynóm s celočíselnými koeficientami má racionálne korene.) Niektoré veci sa však budeme snažiť formulovať všeobecnejšie, napríklad dosť často budeme pracovať namiesto $\mathbb{Z}$ a $\mathbb{Q}$ s okruhmi R a $Q(R)$, kde R je ľubovoľný Gaussov okruh. Mnohé dôkazy sú totiž prakticky totožné pre tieto dve situácie, preto sa zdá byť vhodné dokázať všeobecnejšie tvrdenia. (Ak vám to však vyhovuje lepšie, môžete si jednotlivé dôkazy rozmyslieť najprv pre $\mathbb{Z}$. To je aj prípad, ktorý budeme najčastejšie používať.)

Najdôležitejšie veci z tejto podkapitoly sú dve kritériá na zisťovanie ireducibility – Eisensteinovo kritérium a kritérium využívajúce ireducibilitu v $\mathbb{Z}_p$. Čiže na prednáške spomenieme len tieto dve kritéria (a veci potrebné na ich odvodenie), ostatné časti v tejto podkapitoly si môžete samostatne pozrieť tu alebo v [KGGS, Kapitola 7.4] ak vás zaujmú, ku skúške ich však nevyžadujem. Jedna z týchto vecí navyše je napríklad dôkaz zaujímavého faktu, že ak R je okruh s jednoznačným rozkladom, má túto vlastnosť aj okruh polynómov $R[x]$.

Primitívne polynómy a Gaussova lema

V mnohých úvahách v tejto časti bude pre nás užitočný pojem primitívneho polynómu.

Definícia 3.4.24. Polynóm $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$ budeme nazývať *primitívny,* ak najväčší spoločný deliteľ jeho koeficientov v R je 1; t.j. $\gcd(a_n, a_{n-1}, \ldots, a_0) \sim 1$.

Špeciálne si môžeme všimnúť, že každý monický polynóm je primitívny.

Ľahko sa dá všimnúť, že každý polynóm v $\mathbb{Z}[x]$ sa dá napísať ako konštantný násobok primitívneho polynóm, pričom takýto zápis je jednoznačný až na asociovanosť.

{eisen:LMRXCPRIM}

Lema 3.4.25. *Nech R je okruh s jednoznačným rozkladom. Potom ľubovoľný polynóm $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$ sa dá zapísať ako*

$$f(x) = dg(x),$$

kde $d \in R$ a $g(x) \in R[x]$ je primitívny polynóm.

Navyše pre ľubovoľný takýto rozklad platí $d \sim \gcd(a_n, a_{n-1}, \ldots, a_0)$.

Dôkaz. DU (Pozri aj [KGGS, Lema 7.4.2].) □

Skúsme sa teraz pozrieť, či by nám primitívne polynómy vedeli dať nejakú užitočnú informáciu pre polynómy z $\mathbb{Q}[x]$ resp. $Q(R)[x]$.

Prvky z podielového poľa $Q(R)$ budeme už teraz označovať $\frac{a}{b}$, podobne ako sme zvyknutí pre racionálne čísla.

{eisen:LMQRXC

Lema 3.4.26. *Nech R je okruh s jednoznačným rozkladom, $F = Q(R)$ a $f(x) \in F[x]$ je nenulový polynóm. Potom $F[x]$ sa dá napísať ako*

$$f(x) = \frac{a}{b} g(x),$$

kde $a, b \in R$, $b \neq 0$ a polynóm $g(x)$ je primitívny v $R[x]$.

Navyše, ak máme dva takéto rozklady

$$f(x) = \frac{a}{b} g(x) = \frac{c}{d} h(x),$$

tak tieto rozklady sa líšia iba deliteľom jednotky v R, t.j. existuje také $u \in U(R)$, že $\frac{a}{b} = u\frac{c}{d}$ a $h(x) = ug(x)$.

Dôkaz. Nech

$$f(x) = \frac{a_n}{b_n} x^n + \cdots + \frac{a_1}{b_1} x + \frac{a_0}{b_0}.$$

Nech b je najmenší spoločný násobok čísel $a_0, a_1, \ldots, a_n$. Potom máme

$$f(x) = \frac{z(x)}{b},$$

kde $z(x) \in R[x]$. (Vlastne sme len polynóm $f(x)$ upravili na spoločného menovateľa všetkých koeficientov.)

Podľa lemy 3.4.25 máme $z(x) = ag(x)$ pre nejaké $a \in R$ a polynóm $g(x)$, ktorý je primitívny v $R[x]$. Dostávame tým hľadaný rozklad

$$f(x) = \frac{a}{b} g(x).$$

Ak máme

$$\frac{a}{b} g(x) = \frac{c}{d} h(x),$$

pričom oba rozklady spĺňajú predpoklady vety, tak dostávame po úprave

$$adg(x) = bch(x).$$

Podľa lemy 3.4.25 je tento rozklad určený jednoznačne až na asociovanosť v R. Teda existuje $u \in U(R)$ tak, že $ad = ubc$, čo je ekvivalentné s $\frac{a}{b} = u\frac{c}{d}$.

Súčasne z tejto rovnosti vyplýva

$$u\frac{c}{d} g(x) = \frac{c}{d} h(x)$$

a po vykrátení nenulovým prvkom $\frac{c}{d}$ dostávame $h(x) = ug(x)$. □

Ukážeme teraz, že súčin primitívnych polynómov je opäť primitívny. Začneme najprv jedným pomocným tvrdením

{eisen:LMIREDDELI}

Lema 3.4.27. *Nech R je okruh s jednoznačným rozkladom, $p \in R$ je ireducibilný a $f(x), g(x) \in R[x]$. Ak v $R[x]$ platí $p \mid f(x)g(x)$, tak pre niektorý z polynómov $f(x)$, $g(x)$ platí, že všetky jeho koeficienty sú deliteľné p.*

Dôkaz. Označme $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ a $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$, pričom $a_n, b_m \neq 0$. T.j. polynóm $h(x) := f(x)g(x)$ má stupeň $m+n$, označme jeho koeficienty $c_{m+n}, \ldots, c_0$.

Najprv si uvedomme, že $p \mid h(x)$ znamená, že všetky koeficienty polynómu $h(x)$ sú násobky p.

Postupujme sporom, teda prepokladajme, že pre žiaden z polynómov $f(x)$, $g(x)$ nie sú všetky koeficienty deliteľné p. Zvoľme najmenšie k, l také, že $p \nmid a_k$, $p \nmid b_l$. Pozrime sa na koeficient

$$c_{k+l} = \sum_{i+j=k+l} a_i b_j.$$

Všimnime si, že s výnimkou členu $a_k b_l$ pre všetky členy vystupujúce v súčte na pravej strane rovnosť okrem členu $a_k b_l$ platí buď $i < k$ alebo $j < l$. V prvom prípade platí $p \mid a_i$ a v druhom $p \mid b_j$, každopádne v oboch prípadoch máme $p \mid a_i b_j$.

Znamená to potom, že $p \mid a_k b_l$. (Keďže $a_k b_l = c_{k+l} - \sum_{i=0}^{k-1} a_i b_{k+l-i}$ a p delí všetky členy na pravej strane tejto rovnosti.) Potom buď $p \mid a_k$ alebo $p \mid b_l$. Tým dostávame spor. □

Z tejto lemy už ľahko dostaneme:

{eisen:VTGAUSLMPRIM}

Veta 3.4.28 (Gaussova lema)**.** *Nech R je okruh s jednoznačným rozkladom, nech $f(x), g(x) \in R[x]$ sú primitívne polynómy. Potom aj polynóm $h(x)$ je primitívny.*

Dôkaz. Ak by $h(x)$ nebol primitívny, znamená to, že máme ireducibilný prvok $p \mid f(x)g(x)$. Podľa lemy 3.4.27 ale potom p delí niektorý z týchto dvoch polynómov, bez ujmy na všeobecnosti nech $p \mid f(x)$. To znamená, že p delí všetky koeficienty polynómu $f(x)$, čiže $f(x)$ nie je primitívny. □

Ďalší dôsledok je nasledujúca veta, ktorá je takisto známa pod názvom Gaussova lema.

{eisen:VTGAUSLMIRED}

Veta 3.4.29 (Gaussova lema)**.** *Nech R je okruh s jednoznačným rozkladom a $F = Q(R)$. Nech $f(x) \in R[x]$.*

Ak je polynóm $f(x)$ ireducibilný v $R[x]$, tak je ireducibilný aj v $F[x]$.

Dôkaz. Ukážeme, že ak $f(x)$ je reducibilný v $F[x]$, tak sa dá rozložiť aj v $R[x]$.

Nech $f(x)$ má nejaký netriviálny rozklad v $F[x]$, t.j. $f(x) = g(x)h(x)$, kde oba polynómy majú stupeň aspoň 1. Podľa lemy 3.4.26 potom máme

$$f(x) = g(x)h(x) = \frac{a}{b}\frac{c}{d}\overline{g}(x)\overline{h}(x),$$

ak $g(x) = \frac{a}{b}\overline{g}(x)$ a $h(x) = \frac{c}{d}\overline{h}(x)$ sú vyjadrenia polynómov $g(x)$, $h(x)$ pomocou im zodpovedajúcich primitívnych polynómov $\overline{g}(x), \overline{h}(x) \in R[x]$.

Označme $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$. Podľa vety 3.4.28 je polynóm $\overline{f}(x)$ primitívny. Dostali sme teda vyjadrenie v tvare

$$f(x) = \frac{e}{r}\overline{f}(x).$$

Môžeme pritom bez ujmy na všeobecnosti predpokladať, že $\gcd(e, r) \sim 1$.

Aby sme dostali takýmto spôsobom polynóm s koeficientami z R, musí nutne r deliť všetky koeficienty polynómu $\overline{f}(x)$. To znamená, že $r \sim 1$, bez ujmy na všeobecnosti predpokladajme priamo $r = 1$. Máme teda

$$f(x) = e\overline{f}(x) = e\overline{g}(x)\overline{h}(x).$$

Dostali sme rozklad $f(x)$ v $R[x]$ na súčin nekonštantných polynómov v $R[x]$. □

Príklad 3.4.30. Môžeme si všimnúť, že polynóm môže byť ireducibilný v $Q(R)[x]$ a reducibilný v $R[x]$. Stačí zobrať $f(x) = 5x$ a pozrieť sa naň v $\mathbb{Z}[x]$ a $\mathbb{Q}[x]$. V $\mathbb{Q}$ je každé celé číslo deliteľ jednotky, takže máme $f(x) \sim x$ a ide o ireducibilný polynóm. V $\mathbb{Z}[x]$ máme netriviálny rozklad $f(x) = 5 \cdot x$.

Môžeme si všimnúť, že v predošlom dôkaze sme vlastne ukázali súčasne nasledujúce tvrdenie:

{eisen:DOSROZKLADZX}

Dôsledok 3.4.31. *Nech R je okruh s jednoznačným rozkladom a $F = Q(R)$. Nech $f(x) \in R[x]$.*

Ak $f(x)$ je reducibilný v $F[x]$, tak sa dá rozložiť na súčin dvoch polynómov nižšieho stupňa v $R[x]$.

Môžeme si všimnúť, že rozklad v $R[x]$ bude vo všeobecnosti vyzerať podobne ako v predošlom príklade.

Tvrdenie 3.4.32. *Nech R je komutatívny okruh s jednotkou a $R[x]$ je okruh s jednoznačným rozkladom. Potom aj R je okruh s jednoznačným rozkladom.*

Navyše, ak $f(x)$ je ireducibilný prvok v $R[x]$ práve vtedy, keď keď nastane niektorá z týchto dvoch situácií:
a) $f(x)$ je konštatný polynóm, ktorý je ireducibilný v R;
b) $f(x)$ je primitívny polynóm, ktorý je ireducibilný v $Q(R)[x]$.

Dôkaz. Pozri [KGGS, Lema 7.4.1] a [KGGS, Veta 7.4.1]. □

Z toho vyplýva, že rozklad v $R[x]$ dostaneme v tvare $p_1 \dots p_k f_1(x) \dots f_l(x)$, kde $p_1 \dots p_k$ je rozklad v R a $f_1(x) \dots f_l(x)$ je rozklad primitívneho polynómu v $Q(R)[x]$.

Dokonca platí i obrátená implikácia k prvej časti predošlej vety:

Veta 3.4.33. *Ak R je okruh s jednoznačným rozkladom, tak aj $R[x]$ je okruh s jednoznačným rozkladom.*

Dôkaz. Pozri [KGGS, Veta 7.4.2]. □

Ireducibilita v $\mathbb{Z}_p[x]$

Ak p je prvočíslo, tak $\mathbb{Z}_p[x]$ je pole a – ako sme už videli – okruh $\mathbb{Z}_p[x]$ má v takomto prípade veľa peknych vlastností.

Ak máme polynóm s koeficientami zo $\mathbb{Z}$, môžeme ho uvažovať ako polynóm zo $\mathbb{Z}_p[x]$. Stačí nahradiť všetky koeficienty ich zvyškami modulo p.

Vlastne ide o použitie homomorfizmu $\varphi_p \colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, ktorý je podľa vety 3.2.6 jednoznačne určený homomorfizmom $a \mapsto a \mod p$ zo $\mathbb{Z}$ do $\mathbb{Z}_p$.

Všimnime si jednu vlastnosť homomorfizmu φ_p, ktorá bude pre nás v tomto kontexte užitočná. Ak $f(x) \in \mathbb{Z}[x]$ je polynóm, ktorého vedúci koeficient nie je násobok p, tak jeho obraz $f\varphi_p \in \mathbb{Z}_p[x]$ je polynóm rovnakého stupňa.

{eisen:TVRIREDZP}

Tvrdenie 3.4.34. *Nech p je prvočíslo a $f(x) \in \mathbb{Z}[x]$ je polynóm, ktorého vedúci koeficient nie je deliteľný číslom p. Nech $f_p(x) \in \mathbb{Z}_p[x]$ je polynóm, ktorý dostaneme, ak nahradíme všetky koeficienty polynómu f ich zvyškami po delení číslom p. Ak $f_p(x)$ je ireducibilný v $\mathbb{Z}_p[x]$, tak $f(x)$ je ireducibilný v $\mathbb{Q}[x]$.*

Dôkaz. Ak by bol polynóm $f(x)$ reducibilný v $\mathbb{Q}[x]$, tak sa dá v $\mathbb{Z}[x]$ rozložiť na súčin dvoch polynómov nižšieho stupňa – dôsledok 3.4.31. T.j. máme $f(x) = g(x)h(x)$, kde $g(x), h(x) \in \mathbb{Z}[x]$.

Súčasne vedúce koeficienty týchto polynómov nemôžu byť deliteľné číslom p. (Potom by aj ich súčin – vedúci koeficient polynómu $f(x)$ – bol násobok p.)

Ak teda $f(x) = g(x)h(x)$ zobrazíme homomorfizmom φ_p, dostaneme netriviálny rozklad v $\mathbb{Z}_p[x]$. □

Keby seme chceli predošlú vetu nejako zovšeobecniť, tak by sme mohli dostať napríklad takéto tvrdenie (pozri napríklad [DF, p.309, Proposition 9.4.12]):

Tvrdenie 3.4.35. *Nech I je vlastný ideál v obore integrity R a nech $f(x)$ je monický polynóm stupňa aspoň 1. Ak sa obraz polynómu $f(x)$ v $(R/I)[x]$ nedá rozložiť na súčin dvoch polynómov nižšieho stupňa, tak $f(x)$ je ireducibilný v $R[x]$.*

Ekvivalentne: Nech $\varphi\colon R \to R'$ homomorfizmus okruhov taký, že $1\varphi = 1$, pričom R je obor integrity. Tento homomorfizmus indukuje homomorfizmus $\overline{\varphi}\colon R[x] \to R'[x]$. Nech $f(x)$ je monický polynóm stupňa aspoň 1. Ak $\overline{\varphi}f(x)$ nemá rozklad v $R'[x]$ na súčin dvoch polynómov nižšieho stupňa, tak $f(x)$ je ireducibilný v $R[x]$.

Ako súvisia uvedené dve formy tohoto tvrdenia? DU

V tvrdení 3.4.34 sme sa vedeli zbaviť predpokladu o tom, že $f(x)$ je monický vďaka tomu, že sme pracovali v $Q(R)$ namiesto v R. Tu by sme mohli analogické tvrdenie sformulovať i tak, že by sme predpokladali o vedúcom koeficiente $a_n \notin I$, resp. $a_n\varphi \neq 0$, a vyslovili by sme tvrdenie o tom, či sa $f(x)$ dá rozložiť v $R[x]$ na súčin polynómov nižšieho stupňa (nie priamo o tom, či je reducibilný).

Na dôkaz uvedeného tvrdenia si stačí uvedomiť, že monický polynóm je reducibilný práve vtedy, keď sa dá rozložiť na súčin polynómov nižšieho stupňa a tiež to, že $\overline{\varphi}$ zachováva stupeň polynómu. DU

Pozrime sa na aplikáciu tohoto kritéria na niekoľkých príkladoch.

Príklad 3.4.36. Pre polynómy x^2+x+1, x^3+x+1 ľahko overíme, že v $\mathbb{Z}_2[x]$ sú ireducibilné, keďže nemajú korene. (Stačí si všimnúť, že 0 ani 1 nie je koreň v $\mathbb{Z}_2[x]$.) Podľa tvrdenia 3.4.34 sú teda ireducibilné v $\mathbb{Q}[x]$. Keďže sú to monické polynómy, sú ireducibilné aj v $\mathbb{Z}[x]$.

Polynóm $x^2 + 1$ je ireducibilný v $\mathbb{Z}_3[x]$ (nemá korene). Teda je ireducibilný aj v $\mathbb{Q}[x]$ a $\mathbb{Z}[x]$ (je to monický polynóm). Môžeme si všimnúť, že v $\mathbb{Z}_2[x]$ platí $x^2 + 1 = (x + 1)^2$, teda nad $\mathbb{Z}_2$ sa tento polynóm dá rozložiť. Teda tvrdenie 3.4.34 sa nedá obrátiť.

Príklad 3.4.37. Uvažujme polynóm $f(x) = x^4 + x + 1$. Chceme o ňom ukázať, že je ireducibilný nad $\mathbb{Q}[x]$, podľa tvrdenia 3.4.34 nám stačí ukázať, že je ireducibilný v $\mathbb{Z}_2[x]$.

Dosadením zistíme, že 0 ani 1 nie sú v $\mathbb{Z}_2$ korene.

Ak sa teda tento polynóm dá rozložiť v $\mathbb{Z}_2$, musí to byť súčin dvoch ireducibilných monických polynómov stupňa dva.

Všetky monické polynómy stupňa dva sú x^2, x^2+1, x^2+x, x^2+x+1. Z nich iba x^2+x+1 je ireducibilný.

Delením so zvyškom sa ľahko presvedčíme, že tento polynóm nie je deliteľom zadaného polynómu: $x^4 + x + 1 = (x^2 + x + 1)(x^2 + x) + 1$.

Príklad 3.4.38. Ukážeme, že polynóm tvaru

$$f(x) = x^p - x - a$$

kde p je prvočíslo a $p \nmid a$, je ireducibilný v $\mathbb{Q}[x]$. Keďže je to monický polynóm, je potom ireducibilný aj v $\mathbb{Z}[x]$.

Podľa tvrdenia 3.4.34 nám stačí ukázať, že tento polynóm je ireducibilný v $\mathbb{Z}_p$. Predpokladajme, že by v $\mathbb{Z}_p$ platilo

$$f(x) = x^p - x - a = g(x)h(x),$$

pričom $g(x)$ je ireducibilný v $\mathbb{Z}_p[x]$ a $h(x)$ je nekonštantný polynóm.

Podľa vety 2.5.10 pre každý prvok $b \in \mathbb{Z}_p$ platí $b^p = b$. Spolu s rovnosťou $(x + b)^p = x^p + b^p = x^p + b$ dostaneme

$$f(x + b) = (x + b)^p - (x + b) - a = x^p - x - a = g(x + b)h(x + b),$$

teda

$$f(x) = g(x + b)h(x + b).$$

Polynóm $g(x+b)$ je zrejme opäť ireducibilný polynóm.

Zistili sme teda, že $f(x)$ je deliteľné ireducibilnými polynómami $g(x+b)$ pre $b = 0, 1, \ldots, p-1$. Keďže predpokladáme $\operatorname{st} g(x) < p$, tieto polynómy sú navzájom rôzne, pretože

$$(x+b)^n - (x+b')^n = n \times (b-b')x^{n-1},$$

z čoho vyplýva, že sa budú líšiť už v druhom najvyššom člene. (Pretože $n < p$, máme $n \times a_n \neq 0$ pre nenulové a_n.)

Keďže polynóm stupňa p je deliteľný p rôznymi polynómami stupňa $\operatorname{st} g(x)$, jediná možnosť je $\operatorname{st} g(x) = 1$. To by ale znamenalo, že $f(x) = x^p - x = a$ má koreň v $\mathbb{Z}_p[x]$, čo ale nie je pravda, lebo pre ľubovoľné $c \in \mathbb{Z}_p$ máme $f(c) = c^p - c - a = -a \neq 0$.

Predpoklad, že $f(x)$ sa dá rozložiť v $\mathbb{Z}_p[x]$ teda vedie k sporu.

Tento príklad je prebratý z [P, p.73, Problem 2.2.2].

{eisen:VTEISENSTEIN}

Eisensteinove kritérium

Veta 3.4.39 (Eisensteinove kritérium)**.** *Nech R je okruh s jednoznačným rozkladom a $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$. Nech p je ireducibilný prvok v R a nech platí*

(i) $p \nmid a_n$,
(ii) $p \mid a_i$ *pre* $i = 0, \ldots, n-1$
(iii) $p^2 \nmid a_0$.

Označme $F = Q(R)$.

Potom $f(x)$ je ireducibilný v $F[x]$.

Ak $f(x)$ je primitívny polynóm v $R[x]$, tak $f(x)$ je ireducibilný v $R[x]$.

Dôkaz tohoto výsledku je do istej miery podobný na dôkaz lemy 3.4.27.

Dôkaz. Sporom. Predpokladajme, že primitívny polynóm $f(x)$ spĺňa uvedené predpoklady a súčasne $f(x)$ je reducibilný. Potom $f(x)$ sa dá napísať ako súčin $f(x) = g(x).h(x)$ dvoch polynómov nižšieho stupňa. Nech $\operatorname{st} f = m$, $\operatorname{st} h = k$ a $g(x) = b_m x^m + \cdots + b_0$, $h(x) = c_k x^k + \cdots + c_0$. (Rozklad v $R[x]$ totiž nemôže obsahovať konštatný polynóm – spor s predpokladom, že $f(x)$ je primitívny. Alebo tiež dôsledok dôsledok 3.4.31.)

Máme rovnosť $a_0 = b_0 c_0$, z $p \mid a_0$ dostaneme, že p delí b_0 alebo c_0. Z predpokladu $p^2 \nmid a_0$ dostaneme, že p nemôže deliť oba tieto prvky. Bez ujmy na všeobecnosti predpokladajme, že $p \nmid c_0$. Ukážeme potom indukciou, že $p \mid b_i$ pre všetky $i = 1, 2, \ldots, m$. Z toho ľahko vidno, že p delí všetky koeficienty polynómu $f(x)$, čím dostávame spor.

Prvý krok indukcie už máme za sebou – vieme, že $p \mid b_0$.

Predpokladajme teraz, že $p \mid b_i$ pre $i = 0, 1, \ldots, k-1$. Máme rovnosť

$$a_k = b_k c_0 + \sum_{i=1}^{k} b_{k-i} c_k;$$

$$b_k c_0 = a_k - \sum_{i=1}^{k} b_{k-i} c_k.$$

Pretože všetky členy na pravej strane uvedenej rovnosti sú deliteľné p, dostávame $p \mid b_k c_0$. Z predpokladu $p \nmid c_0$ potom vyplýva, že $p \mid b_k$.

Týmto je dokázaná časť vety hovoriaca o primitívnych polynómoch v $R[x]$.

Ak polynóm $f(x)$ nie je primitívny, tak ho vieme prepísať ako $f(x) = c\overline{f}(x)$, kde $\overline{f}(x)$ už je primitívny polynóm – lema 3.4.25. Ak skúmame ireducibilitu v okruhu polynómov $F[x]$ nad poľom F, tak konštatný násobok neovplyvní, či polynóm je alebo nie je ireducibilný. □

Príklad 3.4.40. Polynóm $x^4 + 10x + 5$ je ireducibilný v $\mathbb{Z}[x]$ na základe Eisensteinovho kritéria pre $p = 5$.

Niekedy sa nedá Eisensteinove kritérium použiť priamo, ale môže nám pomôcť fakt, že $f(x + a)$ je ireducibilný práve vtedy, keď polynóm $f(x)$ je ireducibilný.

Príklad 3.4.41. Uvažujme polynóm $f(x) = x^4 + 1$. Pre tento polynóm sa nedá použiť Eisensteinove kritérium – neexistuje prvočíslo, ktoré by delilo všetky koeficienty.

Vyskúšajme polynóm $g(x) = f(x + 1) = (x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$. Tento polynóm už spĺňa predpoklady Eisensteinovho kritéria pre $p = 2$, teda je ireducibilný v $\mathbb{Z}[x]$ a $\mathbb{Q}[x]$.

Typickou aplikáciou Eisensteinovho kritéria je dôkaz ireducibility *cyklotomických polynómov* stupňa $p - 1$.

Príklad 3.4.42. Nech p je prvočíslo a $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Opäť nemožno použiť Eisensteinove kritérium priamo, vyskúšajme teda polynóm $g(x) = f(x + 1)$.

Na použitie Eisensteinovho kritéria potrebujeme poznať jednotlivé koeficienty polynómu $f(x) = (x + 1)^{p-1} + (x + 1)^{p-2} + \cdots + (x + 1) + 1$. Tie vieme vyrátať pomocou binomickej vety.

$$\begin{aligned}
a_{p-1} &= 1 \\
a_{p-2} &= (p-1) + 1 \\
a_{p-3} &= \binom{p-1}{2} + \binom{p-2}{1} + \binom{p-3}{0} \\
&\vdots \\
a_{p-1-k} &= \sum_{j=0}^{k-1} \binom{p-1-j}{j} \qquad\qquad \vdots
\end{aligned}$$

Dostali sme výraz s binomickými koeficientami, ktorý diagonálny súčet čísel v Pascalovom trojuholníku. Môžete overiť, [2] že platí DU

$$\sum_{j=0}^{k-1} \binom{n-j}{k-j} = \binom{n+1}{k},$$

čo v našom prípade dáva

$$a_{p-1-k} = \binom{p}{k}.$$

Keďže p je prvočíslo, každý z týchto koeficientov pre $k = 1, \ldots, p = 1$ je násobok p. DU

Súčasne koeficient a_0 je rovný $\binom{p}{p-1} = p$, čiže nie je deliteľný p^2.

Zistili sme teda, že tento polynóm spĺňa predpoklady Eisensteinovho kritéria pre prvočíslo p, teda je ireducibilný v $\mathbb{Z}[x]$ a v $\mathbb{Q}[x]$.

[2] V našom výraze vystupuje suma tvaru $\sum_{j=0}^{t} \binom{n-j}{t-j} = \sum_{j=0}^{t} \binom{n-j}{n-t} = \sum_{r=n-t}^{n} \binom{r}{n-t}$. Po substitúcii $n - t = s$ máme $\sum_{r=s}^{n} \binom{r}{s} = \binom{n+1}{s+1}$. Identita, ktorú tu používame sa častejšie zvykne uvádzať v tomto tvare. Niekedy sa nazýva aj „hockey-stick identity“. Keď sa pozriete na to, ako sú rozmiestnené v Pascalovom trojuholníku sčítance a súčet, tento tvar skutočne trochu pripomína hokejku. Pozri napríklad `http://www.artofproblemsolving.com/Wiki/index.php/Combinatorial_identity#Hockey-Stick_Identity`.

Koeficienty v polynóme $f(x+1)$ môžeme jednoduchšie získať oveľa jednoduchšie, ak ho vyjadríme ako $f(x) = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\cdots+1$, čiže $f(x+1) = \frac{(x+1)^p-1}{x} = \sum_{k=1}^{p}\binom{p}{k}x^{k-1}$. Čiže koeficienty sú binomické koeficienty $\binom{p}{k}$.[3]

3.4.7 Derivácia a Taylorov rozvoj polynómov

Definícia 3.4.43. *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 3.4.44. 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.

{polyn2:TVRLEIBNIZ}

Tvrdenie 3.4.45. *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 jednoduché). 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.

[3] Môžete si všimnúť, že takto dostávame alternatívne odvodenie identity pre binomické koeficienty, ktorú sme predtým použili.

n2:TVREXROZV}

Tvrdenie 3.4.46. *Nech F je pole, $c \in F$ a $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$. Potom existujú jednoznačne určené $b_0, b_1, \ldots, b_n \in F$ také, že*

yn2:EQEXROZV}

$$f(x) = b_n(x-c)^n + \cdots + b_1(x-c) + b_0. \tag{3.5}$$

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 3.4.3

$$f(x) = g(x)(x-c) + f(c). \tag{3.6}$$ {polyn2:EQEXROZVOJ}

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 (3.5) $x = c$, tak vidíme, že $b_0 = f(c)$. Ďalej polynóm $g(x)$ z (3.6) 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 3.4.47. *Ak F je pole charakteristiky ∞, tak koeficienty $b_0, \ldots, b_n$ z tvrdenia* 3.4.46 *možno vyjadriť ako*

$$b_k = \frac{D^{(k)}f(c)}{k!},$$

kde znak $D^{(k)}$ znamená, že polynóm $f(x)$ zderivujeme k-krát.

Dôkaz. Toto tvrdenie dostaneme priamo z rovnosti (3.5) viacnásobným zderivovaním (resp. ho môžeme ukázať pomocou indukcie). □

Rozvoj v tvare (3.5) 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.

{polyn2:POZNNSDNEZAV}

Poznámka 3.4.48. 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 $F'[x]$.

{polyn2:TVRNASKORNSD}

Tvrdenie 3.4.49. *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 3.4.5 $f(x) = g(x)(x-c)^k$, 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 3.4.48 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 3.4.50. *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 $k \times c = c.(k \times 1) = c.0 = 0$.

{polyn2:TVRBEZNASKOR}

Tvrdenie 3.4.51. *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 korene 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 charakteristikou 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

$$(x-c)^{k+1} \mid g(x)h_1(x)(x-c)^{k-1} = g(x)h(x) = f(x).$$

To je spor s tým, že násobnosť koreňa c je k. □

Príklad 3.4.52. 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

{polyn2cvic:KORINVHOM}

Úloha 3.4.1. 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 3.4.2. Vedeli by ste dokázať dôsledok 3.4.17 na základe poznatkov, ktoré máte z analýzy?

Úloha 3.4.3. Použitím Hornerovej schémy zistite, či c je koreň polynómu $f(x) \in \mathbb{C}[x]$ a vyjadrite tento polynóm v tvare $f(x) = g(x)(x-c) + f(c)$.
a) $f(x) = x^4 + 3x^3 - 4x + 2$, $c = -2$
b) $f(x) = x^5 + 2x^3 + 3x + 4$, $c = -1$
c) $f(x) = x^3 + (2+2i)x^2 + 3ix + 1$, $c = -i$

Úloha 3.4.4. Pomocou Hornerovej schémy vyjadriť:
a) $f(x+3)$ pre $f(x) = x^4 - x^3 + 1$
b) $(x-2)^4 + 4(x-2)^3 + 6(x-2)^2 + 10(x-2) + 20$

Úloha 3.4.5. Nájdite všetky racionálne korene daných polynómov a ich násobnosť
a) $f(x) = 4x^4 - 7x^2 - 5x - 1$
b) $f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6$
c) $f(x) = 6x^4 + 19x^3 - 7x^2 - 26x + 12$
d) $f(x) = 2x^4 - 7x^3 - 18x^2 - 20x - 1$
[a) $-\frac{1}{2}$ dvojnásobný; b) $\frac{1}{2}$, $-\frac{2}{3}$, $\frac{3}{4}$; c) -3, $\frac{1}{2}$; d) -1, $\frac{11}{2}$]

Úloha 3.4.6. Dokážte: Ak $a+bi$ je koreň polynómu $f(x) \in \mathbb{R}[x]$ a $b \neq 0$, tak $x^2 - 2ax + a^2 + b^2 \mid f(x)$.

Úloha 3.4.7*. Nech $f(x) \in \mathbb{Z}[x]$ je polynóm s celočíselnými koeficientami. Dokážte, že ak $a + b\sqrt{3}$ je koreň $f(x)$, tak aj $a - b\sqrt{3}$ je koreň $f(x)$. Dokážte, že podobné tvrdenie platí, ak c nahradíme ľubovoľným prirodzeným číslom, ktoré nie je druhou mocninou prirodzeného čísla.

Úloha 3.4.8. Dokážte, že $x^2 + x + 1 \mid x^{3m} + x^{3n+1} + x^{3p+2}$ (v $F[x]$ pre ľubovoľné pole F).

Úloha 3.4.9. Dokážte, že $x^2 + x + 1 \mid x^{3m} + x^{3n+1} + x^{3p+2}$ v $\mathbb{C}[x]$. (Využite to, čo viete o koreňoch týchto polynómov.)

Úloha 3.4.10. Rozložiť na koreňové činitele (nad $\mathbb{C}$):
a) $x^3 - 6x^2 + 11x - 6$
b) $x^4 + 4$,
c) $x^4 + 4x^3 + 4x^2 + 1$,
d) $x^4 - 10x^2 + 1$,
e) $x^4 - 4x^3 + 4x - 1$.

{polyn2cvic:IQRCSUCIRED}

Úloha 3.4.11. Rozložiť na súčin ireducibilných polynómov nad $\mathbb{R}$:
a) $x^4 + 4$
b) $x^6 + 27$
c) $x^4 + 4x^3 + 4x^2 + 1$
d*) $x^{2n} - 2x^n + 2$
e*) $x^4 - ax^2 + 1$ pre $a \in (-2, 2)$
f*) $x^{2n} + x^n + 1$.

Úloha 3.4.12. Nájdite všetky ireducibilné polynómy nad $\mathbb{Z}_2$ stupňov 2, 3, 4.

Úloha 3.4.13. Nájdite rozklad $f(x)$ na ireducibilné polynómy v $F[x]$.
a) $f(x) = 4x^4 + 3x^3 + 4x^2 + 4x + 6$, $F = \mathbb{Z}_7$
b) $f(x) = x^4 - 1$, $F = \mathbb{Z}_{11}$
c) $f(x) = x^4 - 1$, $F = \mathbb{Z}_{13}$

Úloha 3.4.14. Nájdite rozklad polynómu $f(x) = x^4 + 1$ na ireducibilné polynómy nad $\mathbb{Z}_2$, $\mathbb{Z}_3$ a $\mathbb{Z}_5$.

Úloha 3.4.15. Zistite, či polynóm $x^5 + x^2 + 1$ je ireducibilný nad $\mathbb{Z}_2$.

Úloha 3.4.16. Dokážte, že polynóm $f(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!}$ nemá viacnásobný koreň.

Úloha 3.4.17. Zistite, či je daný polynóm ireducibilný nad $\mathbb{Q}$:
a) $13x^3 - 8x^2 + 11x - 3$;
b) $2x^4 + 6x^3 - 9x^2 + 15$;
c) $x^3 + 2x^2 + 3$
d) $2x^5 + 15x^3 + 10x + 5$;
e) $x^6 + x^3 + 1$;
f) $10x^3 - 7x^2 + 14$
g) $x^4 - 5x^2 + x + 1$
h) $21x^3 - 3x^2 + 2x + 9$
i) $15x^4 - 10x^2 + 9x + 21$
j) $x^5 + 2x + 4$
k) $3x^5 + 15x^4 - 20x^3 - 10x + 20$;
l) $x^5 + 9x^4 + 12x^2 + 6$;

m) $x^4 + x + 1$;
n) $x^2 + 2x - 5$
o) $x^3 + 3x^2 + 5x + 5$
p) $x^5 + 5x^4 + 10x^3 + 10x^2 + 7x + 5$

Kapitola 4

Rozšírenia polí

Prezentácia výsledkov v tejto kapitole je podobná ako v [KGGS, Kapitola 8] a [DF, Chapter 13].

4.1 Drobnosti

Tieto tvrdenia by sa hodili asi skôr do predošlých kapitol, ale keďže tam som ich zabudol povedať a teraz ich budem potrebovať, dám ich sem.

Pomocou vety o izomorfizme ľahko dostaneme nasledujúci výsledok o homomorfizmoch polí:

{dopln:TVRHOMPOLIIZO}

Tvrdenie 4.1.1. *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. □

Môžeme si všimnúť ešte jeden užitočný fakt súvisiaci s charakteristikou poľa.

{dopln:TVRFROBHOM}

Tvrdenie 4.1.2. *Nech* $\operatorname{char}(F) = p$ *(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 homomorfizmus (endomorfizmus poľa F).

Ďalej pre ľubovoľné $n \in \mathbb{N}$ a $q = p^n$ máme

$$(a+b)^q = a^q + b^q$$
$$(ab)^q = a^q b^q$$

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 2.1.11) 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.

Posledná časť tvrdenia, ktorá hovorí o $q = p^n$, sa ľahko odvodí z prvej časti indukciou vzhľadom na n. DU □

4.2 Rozšírenia polí

Definícia 4.2.1. 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 (lema 2.5.8). Pre nás bude zaujímavý hlavne ten prípad, keď je to konečnorozmerný vektorový priestor.

Definícia 4.2.2. 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 4.2.3. 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 4.2.4. Vieme, že $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ je pole (úloha 2.1.3). 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.

{rozs:VTIREDKOREN}

Veta 4.2.5. *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 3.3.19 a 3.3.30). 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 polynómy stupňa aspoň $\operatorname{st} p(x) \geq 1$ (čiže žiadny nenulový konštantný polynóm – žiadny nenulový prvok poľa F). Podľa tvrdenia 4.1.1 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 $x\varphi = \underline{x + (p(x))}$. Kvôli zjednodušeniu zápisu budeme používať označenie $x\varphi = \overline{x}$, resp. $(f(x))\varphi = \overline{f(x)}$ 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, ktorý nemení koeficienty, teda zachováva súčet, súčin a teda aj všetky polynomické výrazy). □

Teraz ukážeme, že rozšírenie K poľa F zostrojené v predchádzajúcej vete je konečným rozšírením.

{rozs:VTSTUPPOL}

Veta 4.2.6. *Nech $p(x) \in F[x]$ je ireducibilný polynóm a $K = F[x]/(p(x))$. Nech $n = \operatorname{st} p$. Označme $u = x + (p(x)) = x\varphi$ (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*

$$K = \{a_{n-1}u^{n-1} + \cdots + a_1u + a_0; a_0, \ldots, a_{n-1} \in F\}.$$

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

$$f(u) = f(x) + (p(x)) = r(x) + (p(x)) = r(u) = a_{n-1}u^{n-1} + \cdots + a_1u + a_0.$$

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 $K = F[x]/(p(x))$

$$b_{n-1}u^{n-1} + \cdots + b_1u + b_0 = 0.$$

Táto rovnosť vo faktorovom okruhu $F[x]/(p(x))$ znamená, že v okruhu $F[x]$ platí

$$b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \in (p(x)).$$

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. □

{rozs:DOSSTUPPOL}

Dôsledok 4.2.7. *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.)

{rozs:PRGF4}

Príklad 4.2.8. 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 3.4.21). 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 4.2.9. 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 $\mathbb{C}$ t.j. $\mathbb{C}\cong\mathbb{R}[x]/(x^2+1)$

Podobne dostaneme $\mathbb{Q}(\sqrt{2})=\mathbb{Q}[x]/(x^2-2)$.

Definícia 4.2.10. 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.*

Podobné označenie sme už používali aj v predošlých kapitolách – pozri vetu 2.1.23.

Vo vete 4.2.5 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.

{rozs:VTFUJEFXPX}

Veta 4.2.11. *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 3.2.7) $\varphi_u\colon F[x] \to F(u)$

$$\varphi_u\colon a(x) \mapsto a(u).$$

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 4.1.1).

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 zovšeobecníme 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.

{rozs:POZNIZOFX}

Poznámka 4.2.12. 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.

$$\hat{\varphi}\colon \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} (a_i\varphi) x^i$$

Pomerne jednoducho sa overí, že ide opäť o izomorfizmus. Keďže ide o izomorfizmus, 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.

{rozs:VTFUIZOM}

Veta 4.2.13. *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 $(p(x))\hat{\varphi}$ (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 4.2.11 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

$$\psi\colon f(x) + (p(x)) \mapsto (f(x))\hat{\varphi} + (p'(x)).$$

Ukážeme, že toto zobrazenie je dobre definované a je to izomorfizmus s požadovanými vlastnosťami.

Ak $f(x) = g(x)p(x) + r(x)$, tak

$$(f(x))\hat{\varphi} = (g(x))\hat{\varphi}p'(x) + (r(x))\hat{\varphi}.$$

(V ďalšom budeme namiesto $(r(x))\hat{\varphi}$ 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 $(f(x))\hat{\varphi}$ 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 $1\varphi = 1$ 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 4.1.1 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. □

Cvičenia

Úloha 4.2.1. Rozložte $p(x)$ na súčin ireducibilných polynómov v $K[x]$ pre $K = F[x]/(p(x))$.
a) $F = \mathbb{Z}_3$, $p(x) = x^2 + 1$
b) $F = \mathbb{Z}_2$, $p(x) = x^3 + x + 1$

4.3 Algebraické rozšírenia

Definícia 4.3.1. 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.*

Prvok, ktorý nie je algebraický nad F, voláme *transcendentný.*

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 4.3.2. 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.

{algroz:VTFUAMINPOLY}

Veta 4.3.3. *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 nekonštantné 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 4.2.11 potom vyplýva $F(u) \cong F[x]/(m_u(x))$ a z dôsledku 4.2.7 máme $[F(u) : F] = \operatorname{st} m_u = [u : F]$. □

{algroz:VTUALGFUKON}

Veta 4.3.4. *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 4.3.3, čo je konečné rozšírenie podľa dôsledku 4.2.7.

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 4.3.5. *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 4.3.6. *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 vektorový priestor 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 4.3.7. *Ak K je konečné rozšírenie poľa L a L je konečné rozšírenie poľa F, tak pre stupne rozšírení platí*

$$[L : F] = [L : K].[K : F].$$

{algroz:DOSSTUPUDELI}

Dôsledok 4.3.8. *Ak $u \in L$, kde L je konečné rozšírenie poľa F, tak*

$$[u : F] \mid [L : F].$$

Už sme ukázali, že konečné rozšírenie konečného rozšírenia je konečné. Podobne to funguje i pre algebraické rozšírenia.

{algroz:DOSALGALG}

Dôsledok 4.3.9. *Ak K je algebraické rozšírenie poľa L a L je algebraické rozšírenie poľa F, tak K je algebraické rozšírenie poľa F.*

Dôkaz. Chceme ukázať, že každý prvok $u \in K$ je algebraický nad K. Vieme, že u je algebraický nad L, teda existuje polynóm $c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$, ktorého koreňom je u a ktorého koeficienty $c_0, \ldots, c_n$ patria do L. To súčasne hovorí, že u je algebraický už nad menším poľom $F(c_0, \ldots, c_n)$. Podľa vety 4.3.4 to znamená, že $F(u)$ je konečné rozšírenie poľa $F(c_0, \ldots, c_n)$.

Súčasne všetky prvky $c_0, \ldots, c_n$ sú algebraické nad F, preto rozšírenia $F(c_i)$ sú konečné rozšírenia poľa F. Z toho sa dá ľahko (indukciou) ukázať, že aj $F(c_0, \ldots, c_n)$ je konečné rozšírenie F.

Celkovo teda dostávame, že $F(u)$ je konečným rozšírením poľa F, čo znamená, že u je algebraický nad F. □

Príklad 4.3.10. 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, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$, konkrétne

$$\begin{aligned}(\sqrt{2}+\sqrt{3})^0 &= 1\\ (\sqrt{2}+\sqrt{3})^1 &= \sqrt{2}+\sqrt{3}\\ (\sqrt{2}+\sqrt{3})^2 &= 5+2\sqrt{6}\\ (\sqrt{2}+\sqrt{3})^3 &= 11\sqrt{2}+9\sqrt{3}\\ (\sqrt{2}+\sqrt{3})^4 &= 49+20\sqrt{6}\end{aligned}$$

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

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) \cong \mathbb{Q}[x]/(x^4-10x^2+1).$$

Môžeme si ukázať ešte jeden spôsob, ako nájsť minimálny polynóm prvku u. Presnejšie povedané, nájdeme nejaký polynóm, ktorého koreňom je u. Keďže už vieme aký je stupeň minimálneho polynóm, ak sa nám podarí nájsť polynóm stupňa 4, tak je to polynóm, ktorý hľadáme.

Z vyjadrenia čísla u postupne dostaneme:

$$\begin{aligned}\sqrt{3} &= u-\sqrt{2}\\ 3 &= u^2-2u\sqrt{2}+2\\ 2u\sqrt{2} &= u^2-1\\ 8u^2 &= u^4-2u^2+1\\ u^4-10u^2+1 &= 0\end{aligned}$$

Vidíme, že u je skutočne koreňom polynómu x^4-10x^2+1.

Poznámka 4.3.11. Pomerne ľahko sa dá ukázať, že kardinalita množiny $\mathbb{A}$ všetkých reálnych (komplexných) čísel, ktoré sú algebraické nad $\mathbb{Q}$ je rovná $\aleph_0$; úloha 4.3.2. Z toho špeciálne vyplýva, množina $\mathbb{R}\setminus\mathbb{A}$ je neprázdna, dokonca má kardinalitu $\mathfrak{c}=2^{\aleph_0}$. Tým sme ukázali, že existujú reálne čísla, ktoré nie sú algebraické (sú transcendentné).

Napriek tomu, že sme veľmi ľahko ukázali existenciu veľkého množstva transcendentných čísel, nájsť nejaký konkrétny príklad takéhoto čísla a dokázať o ňom, že je transcendentné, nie je úplne jednoduché. Prvým známym príkladom čísel, pre ktoré sa to podarilo ukázať, sú Liouvillove čísla, pozri napríklad [O, p.7] alebo [Š, Veta 9.2.3].

Je známe, že napríklad čísla π a e sú transcendentné.

Cvičenia

Úloha 4.3.1. Ukážte, že ak prvok $u\in K$ je transcendentný nad F, tak u je neurčitá nad F. {algrozcvic:ULOKARDALG}

Úloha 4.3.2. Ukážte, že kardinalita množiny $\mathbb{A}$ všetkých všetkých čísel algebraických nad $\mathbb{Q}$ je $\aleph_0$. Z toho špeciálne vyplýva, že existujú čísla z $\mathbb{R}\setminus\mathbb{A}$, t.j. reálne čísla, ktoré nie sú algebraické.

Úloha 4.3.3. Nech L je rozšírenie poľa F a $u \in L$. Dokážte, že ak $[F(u) : F] = 5$, tak $F(u) = F(u^2)$.

Úloha 4.3.4. Ak $[L : F]$ je prvočíslo, tak pre každé $u \in L$ platí $u \in F$ alebo $F(u) = L$.

Úloha 4.3.5. Nech L je rozšírenie poľa F a $u \in L$. Dokážte, že ak stupeň $[F(u) : F]$ je nepárny, tak $F(u) = F(u^2)$.

Úloha 4.3.6. V poli $\mathbb{Q}(\sqrt[3]{2})$ nájdite inverzný prvok k prvku $1 - 2\sqrt[3]{2} + \sqrt[3]{4}$ (treba ho vyjadriť ako $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ pre vhodné $a, b, c \in \mathbb{Q}$.)

Úloha 4.3.7. Nájdite minimálne polynómy týchto čísel nad $\mathbb{Q}$ (a zdôvodnite, že ide skutočne o minimálny polynóm):
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) $\frac{3+\sqrt{7}}{1+2\sqrt{7}}$; i*) $\sqrt[3]{7 - \sqrt{2}}$.
Výsledky: [c) $x^6 - 9x^4 - 6x^3 + 27x^2 - 54x - 18$; e) $x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5$; f) $x^3 - 3x^2 + 9x - 5$;]

Úloha 4.3.8. Nájdite minimálne polynómy týchto čísel nad $\mathbb{Q}$ (a zdôvodnite, že ide skutočne o minimálny polynóm):
a) $1 - 2\sqrt[3]{3} + 3\sqrt[3]{9}$; b) $\sqrt[3]{7 - \sqrt{3}}$; c) $1 + \sqrt[3]{2} + \sqrt[3]{4}$
Výsledky: [b) $(x^3 - 7)^2 - 3 = x^6 - 14x^3 + 46$;]

Úloha 4.3.9. 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) $\mathbb{Q}(1 + \sqrt{2}, 1 - \sqrt{8})$; e) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ (Hint: Môže platiť $\sqrt{5} = a + b\sqrt{3}$ pre nejaké $a, b \in \mathbb{Q}(\sqrt{2})$?); f) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$

Úloha 4.3.10. Ukážte, že uvedené rozšírenia $\mathbb{Q}$ sa rovnajú. Čo z toho viete povedať o stupni daného rozšírenia nad $\mathbb{Q}$?
a) $\mathbb{Q}(\sqrt{2} + \sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$
b) $\mathbb{Q}(\sqrt{3} + \sqrt[3]{3}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) = \mathbb{Q}(\sqrt[6]{3})$

Úloha 4.3.11. Aký je stupeň rozšírenia $\mathbb{Q}(\sqrt{3 + 2\sqrt{2}})$ nad $\mathbb{Q}$?

4.4 Rozkladové polia

{rozklpol:DEF}

Definícia 4.4.1. 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 $K = F(u_1, \ldots, u_n)$ a f sa dá nad K rozložiť ako

$$f = c(x - u_1)(x - u_2)\ldots(x - u_n).$$

V príklade 4.2.8 sme vlastne zostrojili rozkladové pole polynómu $x^2 + x + 1$ nad $\mathbb{Z}_2$.

{rozklpol:VTEXIS}

Veta 4.4.2. *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 4.2.5 existuje rozšírenie poľa F, v ktorom má f aspoň jeden koreň u. (Stačí vo vete 4.2.5 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 $\operatorname{st} g < n$. Nech $F(u)(u_2,\dots,u_n)$ je rozkladové pole $g(x)$ nad $F(u)$. Ľahko vidíme, že $F(u)(u_2,\dots,u_n) = F(u,u_2,\dots,u_n)$ 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 3.4.15, 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.)

{rozklpol:VTJEDN}

Veta 4.4.3. *Nech $\varphi\colon F \to F'$ je izomorfizmus 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 4.2.12 to znamená $f'(x) = (f(x))\hat{\varphi}$.) 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 $c(x-u_2)\dots(x-un)$ 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 podľa vety 4.2.13 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 $\sigma\colon K \to L$. □

{rozklpol:DOSJEDN}

Dôsledok 4.4.4. *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.

{rozkpol:VTPOLEQN}

Veta 4.4.5. *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 $x^{q-1} = 1$ (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 4.1.2), 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. (Pomocou tvrdenia 3.4.49 ľahko ukážeme, že polynóm $x^q - x$ nemá násobné korene, keďže jeho derivácia je -1.) □

4.5 Počítanie ireducibilných polynómov nad $\mathbb{Z}_p$

Pozri napríklad [DF, p.587-588] alebo [IR, p.84]. Výsledky, ktoré tu uvedieme platia aj všeobecnejšie – keby sme pracovali s poľom $\mathbb{F}_q$ namiesto $\mathbb{Z}_p$; pozri napríklad [LN, Section 3.2].

Z vety 4.4.5 už vieme, že pre každé číslo tvaru $q = p^n$, kde p je prvočíslo, existuje práve jedno q-prvkové pole. V tejto podkapitole ho budeme označovať $\mathbb{F}_q$. Takisto vieme, že $\mathbb{F}_q$ je rozkladové pole polynómu $x^q - x = x^{p^n} - x$ nad $\mathbb{Z}_p$ a pozostáva z koreňov tohoto polynómu.

Všimnime si najprv, že ak $d \mid n$, tak $\mathbb{F}_{p^d}$ je podpole $\mathbb{F}_{p^n}$.

{iredpocet:LMFPDPODPOLE}

Lema 4.5.1. *Nech p je prvočíslo a $n \in \mathbb{N}$, $n \geq 1$. Pole $\mathbb{F}_{p^n}$ obsahuje podpole izomorfné s $\mathbb{F}_{p^d}$ pre každé $d \mid n$.*

Dôkaz. Všimnime si, že ak $d \mid n$, tak $x^{p^d} - x \mid x^{p^n} - x$ DU. Polynóm $x^{p^n} - x$ má v poli $\mathbb{F}_{p^n}$ rozklad na súčin koreňových činiteľov, to isté musí teda platiť i pre jeho deliteľ $x^{p^d} - x$. Z toho vyplýva, že $\mathbb{F}_{p^n}$ obsahuje rozkladové pole polynómu $x^{p^d} - x$, čo je presne $\mathbb{F}_{p^d}$. □

Pre dané číslo d označme $F_d(x)$ súčin všetkých ireducibilných monických polynómov v $\mathbb{Z}_p[x]$ stupňa d.

{iredpocet:VTSUCINIRED}

Veta 4.5.2. *V $\mathbb{Z}_p[x]$ platí rovnosť*

$$x^{p^n} - x = \prod_{d \mid n} F_d(x),$$

teda polynóm $x^{p^n} - x$ je presne súčin všetkých ireducibilných monických polynómov, ktorých stupne sú delitele n.

Dôkaz. Najprv ukážme, že ak $f(x) \mid x^{p^n} - x$ pre nejaký nekonštantný polynóm $f(x)$, tak $f(x)^2 \nmid x^{p^n} - x$, t.j. žiadny netriviálny deliteľ nemôže deliť polynóm $x^{p^n} - x$ v druhej (alebo vyššej) mocnine.

Ak $x^{p^n} - x = f(x)^2 g(x)$, tak derivovaním (s využitím faktu, že sme v poli charakteristiky p) dostaneme

$$-1 = 2f(x)Df(x)g(x) + f(x)Dg(x),$$

z čoho vyplýva $f(x) \mid 1$.

Polynóm $x^{p^n} - x$ sa dá rozložiť na súčin ireducibilných monických polynómov, pričom už sme ukázali, že žiadny z nich sa v rozklade nevyskytne v druhej alebo vyššej mocnine. Aby sme dokázali tvrdenie vety, stačí teda už len ukázať, že ireducibilné monické polynómy deliace $x^{p^n} - x$ sú presne ireducibilné monické polynómy stupňov $d \mid n$.

Najprv nech $p(x)$ je ireducibilný monický polynóm a jeho stupeň d delí n. Potom $K = \mathbb{Z}_p[x]/(p(x))$ je pole, ktoré obsahuje aspoň jeden koreň u polynómu $p(x)$. Súčasne má toto pole p^d prvkov, čiže je izomorfné s $\mathbb{F}_{p^d}$, teda podľa lemy 4.5.1 je to podpole poľa $\mathbb{F}_{p^n}$. Koreň u polynómu $p(x)$ v K je súčasne koreňom $x^{p^n} - x$, pričom $p(x)$ je minimálny polynóm koreňa u nad $\mathbb{Z}_p$. Preto $p(x) \mid x^{p^n} - x$.

Obrátene, nech $p(x)$ je nejaký ireducibilný monický polynóm, ktorý delí $x^{p^n} - x$. Jeho stupeň označme d. Opäť položme $K = \mathbb{Z}_p[x]/(p(x))$. Opäť využijeme, že $p(x)$ má koreň u v poli K a $K = \mathbb{Z}_p(u)$. Prvok u je aj koreňom polynómu $x^{p^n} - x$. Z toho vyplýva, že K je podpole $\mathbb{F}_{p^n}$, lebo $\mathbb{F}_{p^n}$ je rozkladovým poľom pre $x^{p^n} - x$. Toto pole má p^d prvkov.

Z toho, že K je podpole $\mathbb{F}_{p^n}$ špeciálne dostávame, že $(K \setminus \{0\}, \cdot)$ je podgrupa $(\mathbb{F}_{p^n} \setminus \{0\}, \cdot)$ a teda $p^d - 1 \mid p^n - 1$. To môže platiť iba ak $d \mid n$. DU □

Označme teraz N_d počet ireducibilných polynómov stupňa d v $\mathbb{Z}_p[x]$. Z predošlej vety dostaneme:

{iredpocet:DOSPNSUM}

Dôsledok 4.5.3.

$$p^n = \sum_{d|n} dN_d$$

Sumu v predchádzajúcom dôsledku chápeme tak, že sčitujeme cez všetky *prirodzené* čísla d, ktoré delia n.

Skúsme teraz použiť predchádzajúci dôsledok na spočítanie počtu ireducibilných polynómov v nejakom poli $\mathbb{Z}_p$ aspoň pre malé stupne.

Príklad 4.5.4. Pozrime sa najprv na $\mathbb{Z}_2[x]$. Z dôsledku 4.5.3 máme

$$\begin{aligned} 2 &= N_1 \\ 4 &= N_1 + 2N_2 \\ 8 &= N_1 + 3N_3 \\ 16 &= N_1 + 2N_2 + 4N_4 \end{aligned}$$

Očividne, ak poznáme N_d pre $d < k$ vieme z k-tej rovnice vyjadriť aj N_k, v tomto prípade máme $N_1 = 2$, $N_2 = 1$, $N_3 = 2$, $N_4 = 3$.

Môžeme tieto výsledky aj skontrolovať – nájsť všetky ireducibilné monické polynómy daných stupňov.

d	ireducibilné polynómy
1	x, $x+1$
2	x^2+x+1
3	x^3+x^2+1, x^3+x+1
4	x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$

Uvedeným spôsobom teda vieme postupne rátať počet polynómov jednotlivých stupňov. Môžeme sa zamyslieť nad tým, či by sme nevedeli priamo nejakým spôsobom vyjadriť číslo N_n. Dá sa to pomocou Möbiovej funkcie.

Definícia 4.5.5. Pre ľubovoľné prirodzené číslo n definujeme *Möbiovu funkciu* μ predpisom

$$\mu(n) = \begin{cases} 1, & \text{ak } n = 1; \\ (-1)^r, & \text{ak } n = p_1 \dots p_r \text{ je súčin navzájom rôznych prvočísel} \\ 0, & \text{inak.} \end{cases}$$

Vidíme, že $\mu(n) \neq 0$ práve vtedy, keď n je číslo bez kvadratických deliteľov, t.j. n neobsahuje vo svojom rozklade na súčin prvočísel žiadne prvočíslo v druhej alebo vyššej mocnine.

Möbiova funkcia sa dá výhodne použiť práve pre funkcie tvaru $\sum_{m|n} f(m)$. Platia pre ňu nasledujúce dva výsledky:

{iredpocet:VTINV1}

Veta 4.5.6 (Möbiova inverzia)**.** *Ak $g(n) = \sum_{m|n} f(m)$ pre ľubovoľné n, tak*

$$f(n) = \sum_{m|n} \mu(m) g\left(\frac{n}{m}\right) = \sum_{m|n} \mu\left(\frac{n}{m}\right) g(m).$$

{iredpocet:VTI

Veta 4.5.7 (Möbiova inverzia)**.** *Ak* $f(n) = \sum_{m|n} \mu\left(\frac{n}{m}\right) g(m)$*, tak* $g(n) = \sum_{m|n} f(m) = \sum_{m|n} f\left(\frac{n}{m}\right)$.

V dôkaze uvedených viet sa dá použiť nasledujúci, pomerne jednoduchý, výsledok:

{mobi:LMMU}

Lema 4.5.8.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & ak\ n = 1, \\ 0, & inak. \end{cases}$$

Dôkaz. Nech n obsahuje vo svojom rozklade k rôznuych prvočísel. Počet deliteľov n, kde sú všetky prvočísla v prvej mocnine a počet prvočísel je r, je rovný $\binom{k}{r}$. Teda $\sum_{d|n} \mu(d) = \sum_{r=0}^{k} \binom{k}{r}(-1)^r = (1-1)^k$. Pre $k \neq 0$ je uvedená hodnota skutočne 1. Prípad $k = 0$, ktorý zodpovedá $n = 1$, sa ľahko ošetrí samostatne. □

Keď už máme k dispozícii lemu 4.5.8, tak dôkaz viet 4.5.6 a 4.5.7 je v podstate len manipulácia so sumami a výmena poradia sčitovanie – môžete sa pokúsiť dokázať si tieto vzťahy samostatne DU. (Alebo sa môžete pozrieť do [Sl4], resp. takmer do ktorejkoľvek knihy venovanej základom teórie čísel.)

{iredpocet:DOSMOBI}

Dôsledok 4.5.9.

$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}$$

Dôkaz. Použitím vety 4.5.6 pre funkcie $g(n) = p^n$ a $f(n) = nN_n$ dostaneme z dôsledku 4.5.3

$$nN_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = \sum_{d|n} \mu(d) p^{n/d}.$$

□

Príklad 4.5.10. Ak opäť pracujeme nad $\mathbb{Z}_2$ dostaneme

$$\begin{aligned} N_1 &= \mu(1)2 = 2 \\ N_2 &= \frac{\mu(1)4 + \mu(2)2}{2} = \frac{4-2}{2} = 1 \\ N_3 &= \frac{\mu(1)8 + \mu(3)2}{3} = \frac{8-2}{3} = 2 \\ N_4 &= \frac{\mu(1)16 + \mu(2)4 + \mu 42}{4} = \frac{16-4}{4} = 3 \end{aligned}$$

Špeciálne dostávame ešte jeden veľmi užitočný výsledok.

Dôsledok 4.5.11. *Pre každé* $n \in \mathbb{N}$*,* $n > 0$*, existuje aspoň jeden ireducibilný polynóm* $p(x) \in \mathbb{Z}_p[x]$ *stupňa* n*.*

Dôkaz. Suma vystupujúca v dôsledku 4.5.9 obsahuje mocniny čísla p s rôznymi exponentami vynásobené koeficientami ± 1. Takýmto spôsobom nemôžeme dostať nulu. (Stačí si uvedomiť, že $|\sum_{k=0}^{n-1} \alpha_k p^k| \leq \sum_{k=0}^{n-1} p^k < p^n$ pre ľubovoľnú voľbu $\alpha_k \in \{0, \pm 1\}$.) □

Z uvedeného dôsledku vyplýva, že všetky konečné polia sú tvaru $\mathbb{Z}_p[x]/(p(x)) \cong \mathbb{Z}_p(u)$ pre nejaký ireducibilný polynóm $p(x) \in \mathbb{Z}_p[x]$. Vieme tak totiž dostať pole s p^n prvkami pre každé číslo tvaru p^n a už sme ukázali, že existuje jediné takéto pole.

4.6 Existencia algebraicky uzavretého nadpoľa*

Pripomeňme, že pole F sa nazýva algebraicky uzavreté ak každý nekonštantný polynóm z $F[x]$ má v F aspoň jeden koreň alebo, ekvivalentne, ak každý polynóm $f(x) \in F[x]$ sa dá nad F rozložiť na súčin koreňových činiteľov, t.j. polynómov stupňa 1 – pozri definíciu 3.4.12 a tvrdenie 3.4.13.

Definícia 4.6.1. Pole K sa nazýva *algebraickým uzáverom* poľa F, ak K je algebraické rozšírenie poľa F a súčasne K je algebraicky uzavreté.

Najprv uvedieme dôkaz založený na Zornovej leme, pozri vetu 2.4.1. Zhruba rovnaký dôkaz sa dá nájsť napríklad v [W, Theorem 5.3.4].

Začnime pomocným tvrdením, ktoré dáva odhad na kardinalitu algebraického rozšírenia.

Tvrdenie 4.6.2. *Nech F je pole a K je nejaké jeho algebraické rozšírenie. Potom pre kardinality týchto polí platí*

$$\operatorname{card} K \leq \aleph_0 \cdot \operatorname{card} F.$$

V prípade, že F je nekonečná množina, tak $\aleph_0 \operatorname{card} F = \operatorname{card} F$. Čiže zápis uvedený v tvrdení je vlastne stručnejším zápisom toho, že $\operatorname{card} K \leq \aleph_0$ ak F je konečné pole a $\operatorname{card} K \leq \operatorname{card} F$ pre nekonečné polia.

Dôkaz. Každý prvok $a \in K$ je koreňom nejakého polynómu $f(x) \in F[x]$. Polynóm $f(x)$ má len konečne veľa koreňov v K. (Počet jeho koreňov je nanajvýš $\operatorname{st} f$.) Z toho vyplýva, že $\operatorname{card} K \leq \aleph_0 \operatorname{card} F[x]$.

Polynóm stupňa n (alebo menšieho) je jednoznačne určený postupnosťou $(c_0, \ldots, c_n)$ prvkov poľa F, z čoho pre množinu P_n všetkých polynómov z $F[x]$ stupňa nanajvýš n dostaneme $\operatorname{card} P_n \leq (n+1) \operatorname{card} F \leq \aleph_0 \operatorname{card} F$.

Množinu všetkých polynómov môžeme dostať ako spočítateľné zjednotenie $F[x] = \bigcup_{n=0}^{\infty} P_n$, preto

$$\operatorname{card} F[x] \leq \aleph_0 \aleph_0 \operatorname{card} F = \aleph_0 \operatorname{card} F.$$

□

Teraz už môžeme pomocou Zornovej lemy ukázať existenciu algebraicky uzavretého nadpoľa F.

{steinitz:VTSTEINITZ}

Veta 4.6.3. *Každé pole F má algebraický uzáver, t.j. pre každé F existuje algebraické rozšírenie K, ktoré je algebraicky uzavreté.*

Dôkaz. Nech M je ľubovoľná nadmnožina F, ktorá má kardinalitu $2^{\aleph_0 \operatorname{card} F}$.

Pokúsime sa aplikovať Zornovu lemu na množinu

$$\mathcal{P} = \{(L, +, \cdot); L \subseteq M, L \text{ je algebraické rozšírenie poľa } F\}$$

s reláciou

$$(L_1, +, \cdot) \leq (L_2, +, \cdot) \Leftrightarrow L_1 \subseteq L_2 \text{ a } L_2 \text{ je nadpoľom } L_1.$$

Pomerne ľahko sa overí, že ide skutočne o čiastočne usporiadanú množinu. DU

Ak chceme použiť Zornovu lemu, mali by sme ukázať, že pre každý reťazec $\mathcal{C} = \{L_i; i \in I\}$ v $(\mathcal{P}, \leq)$ existuje horné ohraničenie. Položme

$$L = \bigcup_{i \in I} L_i,$$

evidentne platí $L \subseteq M$. Na množine L zadefinujeme $+$ a $\cdot$ tak, že ich prenesieme z L_i, t.j. pre $x, y \in L$ definujeme

$$x + y = x +_i y;$$
$$x \cdot y = x \cdot_i y;$$

ak $x, y \in L_i$. (Pričom $+_i$ a $\cdot_i$ označuje operácie v poli L_i.)

Najprv potrebujeme overiť dve veci – či sme takýmto spôsobom zadefinovali výsledok operácie pre ľubovoľnú dvojicu $(x, y) \in L$ a tiež, či sú operácie definované dobre. Inak povedané, či sa pre každú dvojicu $x, y \in L$ dá nájsť $i \in I$ také, že oba prvky x aj y patria do tej istej množiny L_i a tiež to, či výsledok nezávisí od voľby i.

Ak $x, y \in L = \bigcup_{i \in I} L_i$ znamená to, že existujú i, j tak, že $x \in L_i$ a $y \in L_j$. Pretože ide o reťazec, máme buď $L_i \subseteq L_j$ alebo $L_j \subseteq L_i$. V prvom prípade oba prvky patria do L_i, v druhom oba patria do L_j.

Teraz nech $x, y \in L_i \cap L_j$, chceme overiť, či $x +_i y = x +_j y$ a či to isté platí pre násobenie. Opäť, z toho že ide o reťazec máme $L_i \leq L_j$ alebo obrátene $L_j \leq L_i$. Predpokladajme napríklad, že nastane prvá možnosť. To znamená, že L_i je podpole L_j, teda operácie v poli L_i sú zúženia operácií v poli L_j. Čiže dostaneme rovnaký výsledok bez ohľadu na to, či použijeme sčitovanie/násobenie z poľa L_i alebo z L_j.

Zadefinovali sme teda nejaké binárne operácie $+$ a $\cdot$ na množine L. Fakt, že $(L, +, \cdot)$ je pole overíme podobnými úvahami – treba využiť, že pracujeme s reťazcom a že všetky L_i sú polia. DU*

Takisto nie je ťažké overiť, že ide o algebraické rozšírenie poľa F – každý prvok $a \in L$ patrí do niektorého L_i, keďže L_i je algebraické rozšírenie, prvok a je algebraický nad F.

Každé pole L_i je podpoľom poľa L. DU

Dostali sme tak pole $L \in \mathcal{P}$, ktoré je horným ohraničením reťazca $\mathcal{C}$ vzhľadom na čiastočné usporiadanie $\leq$.

Teda čiastočne usporiadaná množina $(\mathcal{P}, \leq)$ spĺňa predpoklady Zornovej lemy, čiže v nej existuje nejaký maximálny prvok K.

Priamo z definície $\mathcal{P}$ je jasné, že K je algebraickým rozšírením poľa F. Stačí nám overiť, že K je aj algebraicky uzavreté.

Predpokladajme, že by to tak nebolo. To znamená, že existuje ireducibilný polynóm $p(x) \in K[x]$, ktorý nemá v K koreň. Vieme, že K možno vnoriť ako podpole do poľa $K' = K[x]/p(x)$, v ktorom už existuje aspoň jeden koreň polynómu $p(x)$.

Súčasne máme $\operatorname{card} K' \leq \aleph_0 \operatorname{card} K \leq \aleph_0 \operatorname{card} F$. DU Z toho vyplýva, že $M \setminus K$ má kardinalitu[1] $2^{\aleph_0 \operatorname{card} F}$, teda je tam dostatok prvkov na to, aby sme mohli vytvoriť bijekciu medzi[2] $K' \setminus K$ a nejakou podmnožinou množiny $M \setminus K$. Cez túto bijekciu môžeme preniesť operácie $+$ a $\cdot$, čiže tak dostaneme nadpole poľa K, označme ho opäť K'. Súčasne K' je algebraické rozšírenie poľa K, teda je to algebraické rozšírenie poľa F (dôsledok 4.3.9).

Pretože v K' existuje aspoň jeden koreň polynómu $p(x)$, platí $K' \supsetneqq K$, čo je spor s maximalitou K. □

Poznámka 4.6.4. Zdá sa byť vcelku prirodzená otázka, či sme nemohli celý dôkaz zjednodušiť – zobrať za $\mathcal{P}$ priamo množinu všetkých algebraických rozšírení poľa F. Takto zmodifikovaný dôkaz by už nebol v poriadku, pretože $\mathcal{P}$ by bola vlastná trieda a nie množina. (Niečo o triedach ste už zrejme počuli v prvom ročníku na diskrétnej matematike, napríklad viete, že neexistuje množina všetkých množín. Môžeme teda hovoriť iba o triede všetkých množín, nie o množine všetkých množín. Podobný problém by bol s množinou všetkých rozšírení poľa F.)

Ďalej ukážeme, že algebraický uzáver je jednoznačný až na izomorfizmus. Opäť použijeme Zornovu lemu.

[1] Z Cantorovej vety vieme $2^{\aleph_0 \operatorname{card} F} > \aleph_0 \operatorname{card} F$. Ak od nekonečnej množiny odčítame množinu menšej kardinality, neovplyvní to kardinalitu.

[2] Píšeme priamo $K' \setminus K$, keďže K sme stotožnili s podmnožinou K'. Presnejšie by bolo písať $K' \setminus \varphi[K]$, kde $\varphi\colon K \to K[x]/(p(x))$ je kanonický homomorfizmus.

Tvrdenie 4.6.5. *Ak F je ľubovoľné pole a $K_{1,2}$ sú jeho algebraické uzávery, tak existuje izomorfizmus $\varphi\colon K_1 \to K_2$ taký, že $\varphi|_F = id_F$.*

Inými slovami: Algebraický uzáver je určený jednoznačne až na izomorfizmus.

Dôkaz. Predpokladáme, že $K_{1,2}$ sú algebraické uzávery poľa F. Chceme ukázať, že existuje izomorfizmus $f\colon K_1 \to K_2$.

Použijeme Zornovu lemu na množinu všetkých vnorení podpoľa K_1, ktoré nemenia prvky F. Čiastočné usporiadanie bude určené tým, či jedno vnorenie je zúžením druhého. Teda máme množinu

$$\mathcal{P} = \{(f, L); F \subseteq L; L \text{ je podpole } K_1; f\colon L \to K_2 \text{ je vnorenie také, že } f|_F = id_F\}$$

a na nej definujeme reláciu $\leq$ ako

$$(f, L) \leq (g, L') \Leftrightarrow L \subseteq L' \wedge g|_L = f$$

Ľahko vidno, že $(\mathcal{P}, \leq)$ je čiastočne usporiadaná množina. DU

Overme, že táto čiastočne usporiadaná množina spĺňa predpoklady Zornovej lemy.

Podľa Zornovej lemy potom existuje maximálny prvok (φ, L) čiastočne usporiadanej množiny $(\mathcal{P}, \leq)$. Na dokončenie dôkazu nám stačí ukázať, že $L = K_1$.

Sporom. Nech by existoval prvok $u \in K_1 \setminus L$. Prvok u je algebraický nad F, čiže je algebraický aj nad L. Označme $p(x) \in L[x]$ minimálny polynóm prvku u nad L. Tento polynóm je ireducibilný nad K_1, čo okrem iného znamená, že nemá v L koreň. Označme $F' = \varphi[F]$. Nech $p'(x) \in F'[x]$ je polynóm, ktorý dostaneme aplikovaním homomorfizmu φ na všetky koeficienty polynómu $p(x)$. Podľa vety 4.2.13 je polynóm $p'(x)$ ireducibilný nad $F'[x]$. Tento polynóm má nejaký koreň v v algebraicky uzavretom poli K_2. Opäť z vety 4.2.13 dostaneme homomorfizmus $\sigma\colon F(u) \to F'(v)$, ktorý rozširuje φ. To znamená, že $(\varphi, F) < (\sigma, F(u))$, čo je spor s maximalitou (φ, F). □

Ukážeme si ešte jeden dôkaz existencie algebraického uzáveru, pozri napríklad [C1], [L, Section V.2].

Chceme ukázať existenciu algebraického rozšírenia daného poľa F, v ktorom bude mať každý polynóm koreň. Ukážme najprv, že stačí nájsť algebraické rozšírenie, kde majú korene všetky polynómy z $F[x]$.

{steinitz:TVRSTACIFX}

Tvrdenie 4.6.6. *Nech $L \supseteq F$ je algebraické rozšírenie poľa F také, že každý polynóm $p(x)$ ireducibilný v $F[x]$ má koreň v L. Potom L je algebraicky uzavreté.*

Dôkaz. Nech $g(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ je nejaký polynóm ireducibilný v $L[x]$.

Nech by $g(x)$ nemal koreň v L.

Vieme, že existuje rozšírenie $L(u) \cong L[x]/(g(x))$, v ktorom už tento polynóm má koreň u.

Prvok u je algebraický nad $F(c_0, \ldots, c_n)$, z čoho vyplýva, že stupeň $[u : F]$ je konečný u je algebraický prvok nad F.

Potom existuje minimálny polynóm $m_u(x)$ prvku u nad F. Tento polynóm je ireducibilný v $F[x]$. Vieme tiež, že $g(x)$ je minimálny polynóm prvku u nad L.

Z toho, že $m_u(u) = 0$, máme

$$g(x) \mid m_u(x).$$

Polynóm $m_u(x) \in F[x]$ sa dá v $L[x]$ rozložiť na súčin koreňových činiteľov, z čoho vyplýva, že to musí platiť aj pre jeho deliteľ $g(x)$. □

Ako ďalší krok ukážeme, že k danému poľu F sa dá nájsť nejaké nadpole, kde už bude mať každý polynóm z $F[x]$ koreň. Neskôr sa vrátime k tomu, že my navyše chceme nájsť nadpole s touto vlastnosťou, ktoré je algebraickým rozšírením poľa F.

Zatiaľ sme nepracovali s polynómami viacerých premenných – môžete sa o nich niečo dozvedieť v [KGGS, Kapitola 5.7] (a hneď v nasledujúcej kapitole [KGGS, Kapitola 5.8] je viacero zaujímavých vecí o symetrických polynómoch). V nasledujúcom dôkaze budeme dokonca potrebovať okruh polynómov v nekonečne veľa premenných x_i, $i \in I$. Snáď veľmi nevadí, ak neuvedieme podrobnú formálnu definíciu tohoto okruhu – intuitívne by mohlo byť jasné aké prvky obsahuje a ako sa s nimi bude počítať. (Možno pár drobností, ktoré sa oplatí spomenúť. Hoci množina neurčitých s ktorými pracujeme môže byť nekonečná, každý polynóm bude pozostávať iba z konečného počtu členov a bude obsahovať iba konečne veľa premenných. Tiež by malo byť jasné ako sa s nimi počíta – polynómy jednoducho roznásobíme a využijeme, že premenné komutujú, t.j. napríklad namiesto $x_1x_2x_3x_1$ môžeme písať $x_1^2x_2x_3$.)

Konštrukcia v tomto dôkaze je do istej miery podobná na postup použitý v dôkaze vety 4.2.5. Tam sme chceli pridať k poľu F koreň polynómu $p(x)$ a na to sme použili pole $F[x]/(p(x))$. Tu chceme urobiť niečo podobné, chceme to však urobiť pre veľa polynómov, nie iba pre jeden.

{teinitz:TVRALGUZNADPOLE}

Tvrdenie 4.6.7. *Nech F je ľubovoľné pole. Potom existuje nadpole K poľa F také, že každý nekonštantný polynóm z $F[x]$ má v K koreň.*

Dôkaz. Nech $\{f_i(x); i \in I\}$ je množina všetkých nekonštantných polynómov z $F[x]$. Budeme pracovať s okruhom polynómov $R := F[x_i; i \in I]$, t.j. pre každý polynóm $f_i(x)$ sme zaviedli jednu novú premennú x_i.

Nech J je najmenší ideál v okruhu R obsahujúci $\{f_i(x_i); i \in I\}$. (Pričom $f_i(x_i)$ znamená, že v polynóme $f(x)$ sme nahradili všetky výskyty premennej x premennou x_i.) Ideál J neobsahuje žiaden nenulový konštantný polynóm, teda je to vlastný ideál. Podľa vety 2.4.2 existuje nejaký maximálny ideál M, ktorý ho obsahuje. Ukážeme, že pole $K := R/M$ má požadované vlastnosti.

Máme prirodzené vnorenie $i\colon F \hookrightarrow R$ poľa F do okruhu polynómov $F[x_i; i \in I]$. Súčasne máme kanonický homomorfizmus $\varphi\colon R \to R/M$. Potom $i \circ \varphi$ je homomorfizmus polí. Máme $1i\varphi \neq 0$, pretože $1 \notin M$. Podľa tvrdenia 4.1.1 je teda $i \circ \varphi$ injektívny homomorfizmus, čiže F je vnorené v K ako podpole.

Pomerne ľahko sa overí, že trieda prvku $x_i + M$ je koreňom polynómu $f_i(x)$ v poli $K = R/M$. DU □

Podarilo sa nám dostať do situácie, kde každý polynóm z F má koreň v nadpoli K. Nevieme však, či je toto nadpole algebraickým rozšírením – čo je jedna z požiadaviek v definícii algebraického uzáveru. Vyriešiť tento problém nám pomôže nasledujúci výsledok, ktorý hovorí, že algebraické prvky tvoria pole.

{steinitz:TVRALGSUPOLE}

Tvrdenie 4.6.8. *Nech K je nadpole poľa F a*

$$A = \{x \in K; x \text{ je algebraický nad } F\}.$$

Potom A je podpole poľa K.

Dôkaz. Vieme, že prvok a je algebraický práve vtedy, keď $F(a)$ je konečné rozšírenie.

Nech a_1, a_2 sú algebraické. Potom $F(a_1 - a_2) \subseteq F(a_1, a_2) = F(a_1)(a_2)$, čo je konečné rozšírenie. (Ide o konečné rozšírenie konečného rozšírenia.) Rovnaký argument funguje pre $a_1 \cdot a_2$.

Na dokončenie dôkazu si už stačí všimnúť iba to, že ľubovoľné $a \neq 0$ máme $F(a^{-1}) = F(a)$. □

Poznámka 4.6.9. Z predchádzajúceho tvrdenia dostávame napríklad, že množina $\mathbb{A}$ všetkých algebraických čísel (=množina algebraických prvkov nad $\mathbb{Q}$ = množina všetkých koreňov s celočíselnými koeficientmi) je pole. Z toho vidíme, že $\mathbb{A}$ je algebraický uzáver poľa $\mathbb{Q}$.

Dôkaz vety 4.6.3. Nech F je ľubovoľné pole. Podľa tvrdenia 4.6.7 existuje nejaké algebraicky uzavreté algebraické rozšírenie L poľa F.

Ak zoberieme množinu A všetkých prvkov poľa L algebraických nad F, tak podľa tvrdenia 4.6.8 dostaneme rozšírenie poľa F, evidentne ide o algebraické rozšírenie.

Keďže každý polynóm z $F[x]$ má koreň v L a každý koreň takéhoto polynómu patrí aj do A, na základe tvrdenia 4.6.6 vieme, že pole A je algebraicky uzavreté. □

Poznámka 4.6.10. Všimnime si, že ani jeden z uvedených dôkazov nie je konštruktívny. V oboch prípadoch sme nejakým spôsobom použili Zornovu lemu (raz priamo a raz na mieste, kde sme využili fakt, že vlastný ideál je obsiahnutý v maximálnom ideále), a teda naše dôkazy využívajú axiómu výberu.

4.7 Nemožnosť niektorých konštrukcií*

Pozri napríklad [KGGS, Podkapitola 4.1 a 8.2], [DF, Section 13.3], [JMP], [St, Chapter 7].

Medzi veľmi známe problémy pochádzajúce už zo staroveku patrí zdvojenie kocky a trisekcia uhla.

Je možné iba použitím pravítka a kružidla

- zostrojiť z úsečky dĺžky a úsečku dĺžky $\sqrt[3]{2}a$, t.j. dĺžku hrany kocky s dvojnásobným objemom?
- zostrojiť z daného uhla α tretinový uhol $\frac{\alpha}{3}$?

Na prvý pohľad by sa mohlo zdať, že riešenie bude pravdepodobne jednoduché – vieme ľahko zostrojiť štvorec s dvojnásobnou plochou, vieme ľahko zostrojiť polovičný uhol.

Ukážeme si, použitím teórie, ktorú sme sa naučili v tejto kapitole, že tieto úlohy sa nedajú (len použitím pravítka a kružidla) vyriešiť. (Samozrejme, pre niektoré konkrétne uhly, ako napríklad $\alpha = \pi$, vieme zostrojiť tretinový uhol. Otázku o trisekcii uhla chápeme tak, že sa pýtame, či vieme zostrojiť uhol $\alpha/3$ pre ľubovoľný daný uhol α.)

Začnime tým, že si ukážeme, čo vieme povedať o takýchto konštrukciach pomocou rozšírení polí.

Najprv si uvedomme, ako môžeme dostať nejaký bod pomocou pravítka a kružidla. Každá konštrukcia, ktorú robíme, má len konečne veľa krokov. Ak už máme zostrojené nejaké nejaké body $P_1, \ldots, P_n$, tak môžeme:

- spojiť niektoré dva body, čím dostaneme priamku;
- zobrať si do kružidla vzdialenosť niektorých dvoch bodov a urobiť kružnicu so stredom v niektorom už zostrojenom bode.

Nové body, ktoré vieme skonštruovať, dostaneme ako priesečníky niektorých dvoch útvarov, ktoré sme dostali takýmto spôsobom (dvoch priamok, priamky a kružnice, dvoch kružníc).

Definícia 4.7.1. Predpokladajme, že máme danú množinu bodov M, ktorá obsahuje body $(0,0)$ a $(0,1)$. Hovoríme, že P bod M je *skonštruovateľný pomocou bodov množiny M,* ak existuje konečná postupnosť krokov uvedeného typu, pomocou ktorej môžeme z bodov množiny M dostať bod P.

Reálne číslo x nazveme *skonštruovateľné z množiny M,* ak existuje skonštruovateľný bod $P = (x, y)$.

V prípade, že $M = \{(0,0),(0,1)\}$, tak hovoríme stručne o *skonštruovateľných* bodoch a množinách. [3]

Tým, že začíname s bodmi $(0,0)$ a $(0,1)$ sme vlastne len zvolili súradnicovú sústavu na základe nejakých daných dvoch bodov.

Z uvedených konštrukcií vieme urobiť mnohé ďalšie, ktoré poznáte zo stredoškolskej geometrie, napríklad:

- Nájsť stred úsečky určenej dvoma (už skonštruovanými) bodmi.
- Pre dané body A, B, C zostrojiť kolmicu z A na priamku BC.
- Zostrojiť rovnobežku s priamkou určenou bodmi A, B cez daný bod C.
- Pre dané body A, B, C zostrojiť os uhla $\angle BAC$.
- Pre dané body A, B, C zostrojiť bod osovo symetrický s bodom C vzhľadom na priamku AB.
- Ak číslo $x > 0$ je skonštruovateľné, vieme skonštruvať aj $\sqrt{x}$.
- Ak x a y sú skonštruovateľné, vieme skonštruovať aj xy. Za predpokladu, že $y \neq 0$, vieme skonštruovať aj $\frac{x}{y}$.

Pomocou uvedených faktov vcelku ľahko vidíme, že reálne číslo $x > 0$ je skonštruovateľné práve vtedy, keď existujú skonštruovateľné body, ktorých vzdialenosť je x. (Ak existujú dva body, ktorých vzdialenosť je x, tak urobím priesečník priamky idúcej cez $(0,0)$ a $(0,1)$ s kružnicou polomeru r. Obrátene, ak mám bod, ktorého prvá súradnica je x, tak viem z spustiť kolmicu z tohoto bodu na priamku cez $(0,0)$ a $(0,1)$.)

Takisto vieme ľahko ukázať, že bod $P = (x,y)$ je skonštruovateľný práve vtedy, keď obe jeho súradnice sú skonštruovateľné. (Z bodu (x,y) vieme zostrojiť bod (y,x).) Z toho vyplýva, že reálne číslo je skonštruovateľné práve vtedy, keď sa vyskytuje v nejakom skonštruovateľnom bode ako druhá súradnica.

Skúsme si ešte uvedomiť, ako závisia súradnice bodov získaných povolenými konštrukciami od súradníc bodov z predošlých krokov konštrukcie.

Najprv predpokladajme, že máme body $A = (a_1,a_2)$, $B = (b_1,b_2)$, $C = (c_1,c_2)$ a $D = (d_1,d_2)$ také, že priamky AB a CD majú jediný priesečník. Chceme vyrátať súradnice priesečníka $P = (x,y)$. Tento bod musí ležať na oboch priamkach, čiže musí spĺňať

$$\frac{y-a_2}{x-a_1} = \frac{b_2-a_2}{b_1-a_1}$$
$$\frac{y-c_2}{x-c_1} = \frac{d_2-c_2}{d_1-c_1}$$

Po úprave dostaneme sústavu dvoch lineárnych rovníc, kde všetky koeficienty sú vyjadriteľné zo súradníc bodov A, B, C, D pomocou operácií súčtu, rozdielu, sčitovania, násobenia. Keď vyjadríme x (napríklad pomocou Cramerovho pravidla), vidíme, že x je koreňom polynómu prvého stupňa, kde koeficienty sú skonštruovateľné čísla (skonštruovateľné pomocou množiny súradníc bodov A, B, C, D).

Skúsme sa teraz pozrieť na prienik priamky a kružnice. Z predošlých úvah už vieme, že priamka zodpovedá rovnici $ax + by = c$ pre nejaké skonštruovateľné čísla a, b, c. Podobne kružnica bude mať rovnicu $(x-d)^2 + (y-e)^2 = r^2$, kde d, e, r sú skonštruovateľné. Ak vyjadríme y z lineárnej rovnice a dosadíme do kvadratickej, dostaneme rovnicu tvaru $Ax^2 + Bx + C = 0$, kde A, B, C sú skonštruovateľné čísla. Čiže v tomto prípade je x koreňom nejakej rovnice druhého stupňa, kde koeficienty sú skonštruovateľné čísla.

[3] Anglicky: constructible number

Zostáva nám pozrieť sa na prípad dvoch kružníc, t.j. riešime sústavu

$$(x-a)^2+(y-b)^2=r^2,$$
$$(x-c)^2+(y-d)^2=s^2.$$

Keď odčítame uvedené dve rovnice, tak členy x^2 a y^2 vypadnú, čiže dostaneme sústavu rovnakého typu o akej sme uvažovali v predošlom odstavci.

Doteraz uvedené úvahy môžeme zosumarizovať takto:

Veta 4.7.2. *Nech M je množina bodov v rovine obsahujúca body $(0,0)$ a $(1,0)$. Potom množina K všetkých reálnych čísel skonštruovateľných z bodov množiny M je pole, ktoré obsahuje $\mathbb{Q}(M)$. Navyše každý prvok $u\in K$ je algebraický nad $\mathbb{Q}(M)$ a platí*

$$[u:\mathbb{Q}(M)]=2^n$$

pre nejaké $n\in\mathbb{N}$, t.j. stupeň prvku u je mocninou dvojky.

Symbolom $\mathbb{Q}(M)$ rozumieme najmenšie nadpole $\mathbb{Q}$, ktoré obsahuje súradnice všetkých bodov z množiny M.

Dôkaz. Ukázali sme, že množina K je uzavretá na súčin, súčet, inverzné prvky.

Ďalej každý prvok $u\in K$ sa získa nejakou konečnou postupnosťou krokov. Videli sme, že čísla, ktoré dostaneme v každom kroku, sú korene polynómu stupňa 2 zostaveného z čísel zostrojených v predošlých krokoch. Z toho vyplýva, že u je algebraický prvok a $[u:\mathbb{Q}(M)]$ delí 2^k, kde k je počet použitých krokov. □

Pozrime sa teraz na to, čo na základe predošlej vety vieme povedať o zdvojení kocky a trisekcii uhla.

Otázka zdvojenia kocky je ekvivalentná s otázkou skonštruovateľnosti čísla $\sqrt[3]{2}$. Pretože $[\sqrt[3]{2}:\mathbb{Q}]=3$, z predošlej vety vidíme, že takáto konštrukcia nie je možná.

Otázka trisekcie uhla je ekvivalentná s otázkou, či vieme zostrojiť čísla $\cos\frac{\alpha}{3}$ a $\sin\frac{\alpha}{3}$ pomocou bodov z množiny $M=\{(0,0),(0,1),(\cos\alpha,\sin\alpha)\}$. Vieme, že platí

$$\cos\alpha=\cos^3\frac{\alpha}{3}-3\cos\frac{\alpha}{3}\sin^2\frac{\alpha}{3}=4\cos^3\frac{\alpha}{3}-3\cos\frac{\alpha}{3}$$
$$\sin\alpha=3\cos^2\frac{\alpha}{3}\sin\frac{\alpha}{3}-\sin^3\frac{\alpha}{3}=3\sin\frac{\alpha}{3}-4\sin^3\frac{\alpha}{3}$$

Vidíme teda, že $\cos\frac{\alpha}{3}$ je koreňom polynómu $f(x)=4x^3-3x-\cos\alpha$, ktorého koeficienty patria do $\mathbb{Q}(M)$.

Pozrime sa na to, čo sa stane ak $\alpha=\frac{\pi}{3}$, čiže $\cos\alpha=\frac{1}{2}$. V tomto prípade máme $\mathbb{Q}(M)=\mathbb{Q}$. Číslo $\cos\frac{\alpha}{3}$ je koreňom polynómu $f(x)=4x^3-3x-\frac{1}{2}$, o ktorom sa vieme presvedčiť, že je ireducibilný nad $\mathbb{Q}$. Môžeme napríklad použiť substitúciu $2x=y$, čím dostaneme nový polynóm $2f(x)=g(y)=y^3-3y-1$. O jeho ireducibilite sa môžeme presvedčiť, keď skontrolujeme, že nemá racionálne korene, alebo pomocou Eisensteinovho kritéria aplikovaného na polynóm $g(s+1)=s^3+3s^2-3$.

Z toho vyplýva, že pre $u=\cos\frac{\alpha}{3}$ máme $[u:\mathbb{Q}]=[u:\mathbb{Q}(M)]=3$. To znamená, že číslo $\cos\frac{\alpha}{3}$, a teda ani uhol $\frac{\alpha}{3}$, sa nedajú skonštruovať pomocou pravítka a kružidla.

Poznámka 4.7.3. Ďalším známym antickým problémom je kvadratúra kruhu – nájdenie štvorca s rovnakou plochou ako má daná kružnica. Možnosť konštrukcie strany takéhoto štvorca pomocou pravítka a kružidla je ekvivalentná otázke, či je skonštruovateľné číslo $\sqrt{\pi}$. Je známe, že číslo π nie je algebraické. (Dôkaz tu však neuvádzame.) Ak uveríme tomuto faktu, tak z predošlej vety vyplýva aj to, že $\sqrt{\pi}$ sa nedá skonštruovať.

Literatúra

[AM] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra.* Adison-Wesley, Reading, 1969.

[BŠ] Bohuslav Balcar and Petr Štěpánek. *Teorie množin.* Academia, Praha, 2001.

[C1] Keith Conrad. Constructing algebraic closures. `http://www.math.uconn.edu/~kconrad/blurbs/`.

[C2] Keith Conrad. Zorn's lemma. `http://www.math.uconn.edu/~kconrad/blurbs/`.

[CH] Grigore Calugareanu and Peter Hamburg. *Exercises in Basic Ring Theory.* Kluwer, Dordrecht, 1998.

[DF] David S. Dummit and Richard M. Foote. *Abstract Algebra.* John Willey and Sons, 3rd edition, 2004.

[Gr] George Grätzer. *Lattice Theory: Foundation.* Birkhäuser, Basel, 2011.

[Gu1] Jaroslav Guričan. Faktorizácia polynómov I. *Obzory matematiky, fyziky a informatiky.* `http://thales.doa.fmph.uniba.sk/katc/pages/member.php?clen=gurican`.

[Gu2] Jaroslav Guričan. Faktorizácia polynómov II. *Obzory matematiky, fyziky a informatiky.* `http://thales.doa.fmph.uniba.sk/katc/pages/member.php?clen=gurican`.

[IR] K. Ireland and M. Rosen. *A Classical Introduction to Modern Set Theory.* Springer, New York, 1990.

[JMP] Arthur Jones, Sidney A. Morris, and Kenneth R. Pearson. *Abstract Algebra and Famous Impossibilities.* Springer-Verlag, New York, 1991. Universitext.

[K] A. I. Kostrikin. *Exercises in Algebra: A collection of Exercises in Algebra, Linear Algebra and Geometry.* OPA, Amsterdam, 1996.

[KGGS] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, and Jaroslav Smítal. *Algebra a teoretická aritmetika 1.* UK, Bratislava, 2002.

[KLŠZ] M. Kolibiar, A. Legéň, T. Šalát, and Š. Znám. *Algebra a príbuzné disciplíny.* Alfa, Bratislava, 1992.

[L] Serge Lang. *Algebra.* Springer-Verlag, New York, rev. 3rd edition, 2002. Graduate Texts in Mathematics, 211.

[LN] Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, 1986.

[O] John C. Oxtoby. *Measure and Category*. Springer-Verlag, New York, 2nd edition, 1980. Graduate Texts in mathematics 2.

[P] Victor V. Prasolov. *Polynomials*. Springer-Verlag, Berlin, 2004.

[R] Kenneth Rogers. The axioms for Euclidean domains. *Amer. Math. Monthly*, 78(10):1127–1128, 1971.

[Š] Tibor Šalát. *Reálne čísla*. Alfa, Bratislava, 1982.

[Sl1] Martin Sleziak. 1-INF-115 Algebra 1. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[Sl2] Martin Sleziak. 1-INF-155 Algebra 2. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[Sl3] Martin Sleziak. Teória množín. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[Sl4] Martin Sleziak. Teória čísel. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[St] Ian Stewart. *Galois theory*. CRC, Boca Raton, 3rd edition, 2004.

[W] Steven H. Weintraub. *Galois Theory*. Springer, New York, 2nd edition.

[Z] Pavol Zlatoš. O dobrom usporiadaní a axióme výberu. `http://thales.doa.fmph.uniba.sk/zlatos/wo/DUAC1w.pdf`.

Register

Zoznam symbolov