# Polia, rozšírenia polí

Martin Sleziak

25. septembra 2024

# Obsah

# Kapitola 1

# Úvod

Verzia: 25. septembra 2024

## 1.1 Predhovor

## 1.2 Témy, ktorým sa tento text venuje

### 1.2.1 Polia a rozšírenia polí

- Základné vlastnosti polí a niektoré príklady polí.
- Rozšírenia polí.
- Konečné rozšírenia, algebraické čísla.
- Skonštruovateľné čísla – nie všetky dĺžky úsečiek vieme skonštruovať, ak máme povolené používať iba pravítko a kružidlo.
- Niektoré základné výsledky o konečných poliach.

### 1.2.2 Grupy

# Kapitola 2

# Opakovanie

{opak:CHAPTEROPAK}

Cieľom tejto kapitoly je pripomenúť nejaké veci, ktoré by ste mali poznať z nižších ročníkov – ide najmä o veci týkajúce sa vektorových priestorov.

## 2.1 Vektorové priestory

Aspoň veľmi stručne na tomto mieste pripomenieme niektoré veci o vektorových priestoroch. (A spomenieme niektoré príklady, ktoré sú pre nás zaujímavé v súvislosti s vecami, ktorým sa venuje tento text.)

Dá sa nájsť veľa rôznej literatúry obsahujúcej základné veci o vektorových priestorov – a aj mnoho ďalšieho z lineárnej algebry. V slovenčine napríklad [KGGS, K, KG, Z].

{vpr:DEFVPR}

**Definícia 2.1.1.** Trojica $(V, +, \cdot)$ sa nazýva *vektorový priestor* nad poľom[1] $F$ ak $V$ je množina, $+$ je binárna operácia na množine $V$ a $\cdot$ priradí prvkom $c \in F$ a $\vec{v} \in V$ nejaký prvok $c \cdot \vec{v} \in V$ a súčasne platí:

{vpr:DEFVPRitemKG}

(i) $(V, +)$ je komutatívna grupa.

(ii) Pre ľubovoľné $c, d \in F$, $\vec{v} \in V$ platí

$$(c + d)\vec{v} = c\vec{v} + d\vec{v}.$$

(iii) Pre ľubovoľné $c \in F$, $\vec{v}, \vec{w} \in V$ platí

$$c(\vec{v} + \vec{w}) = c\vec{v} + c\vec{w}.$$

(iv) Pre ľubovoľné $c, d \in F$, $\vec{v} \in V$ platí

$$c(d\vec{v}) = (cd)\vec{v}.$$

(v) Pre ľubovoľné $\vec{v} \in V$ platí

$$1 \cdot \vec{v} = \vec{v}.$$

[1] Definícia poľa je v tomto texte až neskôr – definícia 4.1 v časti 4.1. Tento pojem by ste ale mali poznať z nižších ročníkov – prinajmenšom ste ho spomenuli, ak ste definovali vektorový priestor nad ľubovoľným poľom.

Prvky množiny $V$ zvyčajne voláme vektory *vektory*, prvky poľa $F$ voláme *skaláry.*

Neutrálny prvok grupy $(V,+)$ sa zvykne nazývať *nulový vektor* a označovať $\vec{0}$. Inverzný prvok k $\vec{x}$ vzhľadom na operáciu $+$ sa zvykne označovať $-\vec{x}$.

Dobre poznáme najmä priestory tvaru $V = F^n$. (A pre mnohé aplikácie sú práve takéto typy vektorových priestorov najdôležitejšie.)

V mnohých oblastiach majú využitie najmä vektorové priestory nad $\mathbb{R}$ a $\mathbb{C}$. Pri veciach, ktorými sa chceme zaoberať tu, ale budú dôležité aj vektorové priestory nad inými poliami.

Spomeňme aj takýto príklad, ktorý môže vyzerať pomerne neobvykle – je to však typ vektorového priestoru, s ktorým sa v tomto texte stretneme viackrát. (Niečo pododbné budeme potrebovať, keď sa budeme rozprávať o rozšíreniach polí – tvrdenie 4.4.3.)

{vpr:PRIKLRnadQ}

**Príklad 2.1.2.** $\mathbb{R}$ je vektorový priestor nad $\mathbb{Q}$.

To isté vysvetlené detailnejšie: Položme $V = \mathbb{R}$ a $F = \mathbb{Q}$. (T.j. naše vektory sú reálne čísla a pracujeme nad poľom racionálnych čísel.) Ako sčitovanie vektorov použijeme obvyklé sčitovanie reálnych čísel. Ako násobenie skalárom, tiež použijeme obvyklé násobenie – s tým rozdielom, že teraz je zúžené z $\mathbb{R} \times \mathbb{R}$ na $\mathbb{Q} \times \mathbb{R}$.

Overiť podmienky z definície vektorového priestoru by malo byť v tomto prípade pomerne jednoduché.

Pre ilustráciu sa pozrime na jednu z nich. Mali by sme overiť, či platí

$$(\forall c \in \mathbb{Q})(\forall v, w \in \mathbb{R}) c(v+w) = cv + cw.$$

Táto vlastnosť ale platí pre ľubovoľné reálne číslo $c$, je to iba distributívny zákon. Tým skôr takáto vlastnosť zostane v platnosti, ak sme sa obmedzili na nejakú menšiu množinu.

Aj pre ostatné vlastnosti z definície pomerne rýchlo prídeme na to, že to je podmienka, ktorej platnosť pre reálne čísla poznáme.

**Definícia 2.1.3.** Nech $V$ je vektorový priestor nad poľom $F$. Vektory $\vec{v}_1, \ldots, \vec{v}_n \in V$ sú *lineárne nezávislé,* ak z rovnosti

$$c_1\vec{v}_1 + \cdots + c_n\vec{v}_n = \vec{0}$$

vyplýva $c_1 = \cdots = c_n = 0$.

Lineárna nezávislosť teda znamená, že nulový vektor sa dá dostať ako lineárna kombinácia daných vektorov iba triviálnym spôsobom, t.j. iba ak všetky koeficienty sú nulové.

**Definícia 2.1.4.** Nech $V$ je vektorový priestor nad poľom $F$. Pre vektory $\vec{v}_1, \ldots, \vec{v}_n \in V$ označujeme

$$[\vec{v}_1, \ldots, \vec{v}_n] = \{c_1\vec{v}_1 + \cdots + c_n\vec{v}_n; c_1, \ldots, c_n \in F\}.$$

Táto množina tvorí vektorový podpriestor priestoru $V$ a nazýva sa *lineárny obal* vektorov $v_1, \ldots, v_n$.

Ak $[\vec{v}_1, \ldots, \vec{v}_n] = V$, tak hovoríme, že vektory $\vec{v}_1, \ldots, \vec{v}_n$ *generujú* priestor $V$.

$[\vec{v}_1, \ldots, \vec{v}_n]$ teda označuje množinu všetkých lineárnych kombinácií vektorov $\vec{v}_1, \ldots, \vec{v}_n$. Je to najmenší vektorový podpriestor obsahujúci tieto vektory.

**Definícia 2.1.5.** Vektory $\vec{v}_1, \ldots, \vec{v}_n$ tvoria *bázu* vektorového priestoru $V$ ak sú lineárne nezávislé a generujú $V$.

Ekvivalentne definíciu bázy môžeme povedať tak, že každý vektor $\vec{x} \in V$ sa dá *jednoznačne* zapísať v tvare lineárnej kombinácie

$$\vec{x} = c_1\vec{v}_1 + \cdots + c_n\vec{v}_n.$$

Teda na zadanie bázy sa do istej miery dá pozerať tak, že sme zaviedli „súradnicovú sústavu“ – pre každý vektory $x$ máme jednoznačne priradené jeho „súradnice“ $c_1, \ldots, c_n$. (Samozrejme, ak si zvolíme inú bázu, tak súradnice toho istého vektora budú iné.)

Dá sa ukázať, že ľubovoľné dve bázy vektorového priestoru $V$ majú rovnaký počet prvkov – pomerne často sa učí napríklad dôkaz založený na Steinitzovej leme. Počet prvkov bázy nazývame *dimenzia* priestoru $V$ a označujeme $\dim(V)$.

Ak existuje (konečná) báza priestoru $V$, tak $V$ sa nazýva *konečnorozmerný*.

Konečnorozmerný priestor je jeho dimenziou určený jednoznačne až na izomorfizmus – ak $\dim(V) = n$ tak $V \cong F^n$.

Existujú aj vektorové priestory, ktoré nie sú konečnorozmerné. Dajú sa nájsť aj pomerne jednoduché príklady – pozri úlohy 2.1.1 a 2.1.2. Keďže sme už spomenuli reálne čísla ako vektorový priestor nad $\mathbb{Q}$, azda by sa patrilo spomenúť, že toto je tiež príklad nekonečnorozmerného priestoru.

{vpr:PRIKLRnadQDIM}

**Príklad 2.1.6.** Priestor $\mathbb{R}$ nad poľom $\mathbb{Q}$ z príkladu 2.1.2 nie je konečnorozmerný.

Jeden pomerne jednoduchý argument sa dá urobiť, ak človek ovláda základné veci týkajúce sa kardinality. Dá sa ukázať to, že $\mathbb{Q}^n$, a teda aj ľubovoľný konečnorozmerný priestor nad $\mathbb{Q}$, je spočítateľná množina. Súčasne vieme, že množina reálnych čísel nie je spočítateľná.[2]

Dá sa to však zdôvodniť aj bez toho, aby sa človek musel odvolávať na nejaké veci týkajúce sa spočítateľných a nespočítateľných množín. Jeden možný prístup je skúsiť vymyslieť nejakú nekonečnú množinu prvkov, ktoré sú lineárne nezávislé. Jedna pomerne elegantná možnosť je použiť logaritmy prvočísel – pozri úlohu 2.1.3 alebo linku uvedenú v poznámke pod čiarou.[3]

Ešte o čosi iný argument uvidíme v úlohe 4.6.2, keď budeme vedieť nejaké základné fakty o minimálnom polynóme.

### Cvičenia

{vprcvic:ULOPOST}

**Úloha 2.1.1.** Nech $V$ je množina všetkých postupností reálnych čísel. Dokážte, že $V$ je vektorový priestor nad $\mathbb{R}$. (Súčet dvoch postupností a aj skalárny násobok definujeme prirodzeným spôsobom.)

Ukážte, že tento priestor nie je konečnorozmerný.

{vprcvic:ULOFUN}

**Úloha 2.1.2.** Nech $V$ je množina všetkých zobrazení $\mathbb{R} \to \mathbb{R}$. Dokážte, že $V$ je vektorový priestor nad $\mathbb{R}$. (Aj tu by malo byť jasné, ako definujeme súčet reálnych funkcií a skalárny násobok nejakej funkcie.)

Ukážte, že tento priestor nie je konečnorozmerný.

{vprcvic:ULOLOGPNLN}

**Úloha 2.1.3*.** Nech $p_1, \ldots, p_n$ sú rôzne prvočísla. Dokážte, že potom ich logaritmy $\ln p_1, \ldots, \ln p_n$ sú lineárne nezávislé nad $\mathbb{Q}$. (Hint: Rovnosť $c_1 \ln p_1 + \cdots + c_n \ln p_n$ je ekvivalentná s $p_1^{c_1} \cdots p_n^{c_n} = 1$. Viete dostať takúto rovnosť s celočíselnými exponentami?)

[2] Nejaké základné veci týkajúce sa spočítateľných množín a inch súvisiacich vecí sa dajú nájsť napríklad v [Sl2].

[3] `https://math.stackexchange.com/q/6244` Is there a quick proof as to why the vector space of $\mathbb{R}$ over $\mathbb{Q}$ is infinite-dimensional?

## 2.2 Relácie ekvivalencie

### 2.2.1 Definícia relácie ekvivalencie

Pripomeňme, že formálne reláciu na množine $A$ definujeme tak, že to je nejaká podmnožina karteziánskeho súčinu $A \times A$. Neformálny pohľad je, že máme nejaký vzťah medzi jednotlivými prvkami z $A$, pričom je jasne určené, ktoré prvky z $A$ sú (nie sú) v tomto vzťahu.

Ak dva prvky sú v relácii $R \subseteq A \times A$, tak používame označenie $(a, b) \in R$ alebo $aRb$.

**Definícia 2.2.1.** Relácia $\sim$ na množine $A$ sa nazýva *relácia ekvivalencie,* ak je reflexívna, symetrická a tranzitívna, t.j. ak pre ľubovoľné $a, b, c \in A$ platí:

(i) $a \sim a$

(ii) Ak platí $a \sim b$, tak platí aj $b \sim a$.

(iii) Ak platí $a \sim b$ a súčasne $b \sim c$, tak aj $a \sim c$.

$$a \sim a$$
$$a \sim b \Rightarrow b \sim a$$
$$a \sim b \wedge b \sim c \Rightarrow a \sim c$$

Ako príklad, na ktorom si môžeme ilustrovať pojmy spomenuté v tejto časti, si môžeme zobrať reláciu na množine $\mathbb{Z}$ určenú podmienkou

{relekv:EQKONG4}
$$a \sim b \qquad \Leftrightarrow \qquad 4 \mid a - b. \tag{2.1}$$

T.j. pre celé čísla $a$, $b$ platí $a \sim b$ práve vtedy, keď tieto dve čísla nám dajú rovnaký zvyšok po delení číslom 4.

Samozrejme, nie je veľmi ťažké uvedomiť si, že podobne by to fungovalo ak by sme namiesto štvorky zobrali iné prirodzené číslo. K takýmto reláciám sa ešte vrátime v časti 3.3.6 a poznáte ich už z nižších ročníkov pod názvom kongruencie a ste zvyknutí na označenie

$$a \equiv b \pmod 4.$$

### 2.2.2 Relácie ekvivalencie a rozklady

Ak máme nejakú reláciu ekvivalencie, tak tá nám rozdelí celú množinu na disjunktné časti. Z každej relácie ekvivalencie dostávame rozklad. (A platí aj obrátene, že z rozkladu dostaneme reláciu ekvivalencie.)

**Definícia 2.2.2.** Ak $\sim$ je relácia ekvivalencie na množine $A$ a $a \in A$, tak označíme

$$[a] = \{x \in A; x \sim a\}.$$

Množinu $[a]$ nazývame *trieda ekvivalencie prvku $a$.*

Teda $[a]$ sme definovali tak, že pozostáva zo všetkých prvkov, ktoré sú v relácii s prvkom $a$.

Niekedy sa nám môže hodiť zdôrazniť aj reláciu, z ktorej sme uvažovanú triedu dostali. V takom prípade by sme použili označenie $[a]_\sim$ ak reláciu označujeme $\sim$ alebo $[a]_R$ ak reláciu označujeme $R$.

Ale vo väčšine prípadov, ktoré nás budú zaujímať, budeme pracovať iba s jednou reláciou ekvivalencie. A vtedy je jednoduchšie použiť stručnejšie označenie $[a]$.

**Veta 2.2.3.** *Ak $\sim$ je relácia ekvivalencie na množine $A$, tak množina všetkých tried ekvivalencie tvorí* rozklad *množiny $A$, t.j. platia nasledujúce podmienky:*

- *Zjednotením všetkých tried ekvivalencie dostaneme celú množinu $A$.*

$$A = \bigcup_{a \in A} [a]$$

- *Jednotlivé triedy ekvivalencie sú po dvoch disjunktné, t.j. pre ľubovoľné $a, b \in A$ platí*

$$[a] = [b] \qquad \vee \qquad [a] \cap [b] = \emptyset.$$

Pre rozklad zodpovedajúci relácii $\sim$ používame označenie

$$A/\!\sim = \{[a]; a \in A\}.$$

*Dôkaz. Zjednotenie tried dá celú množinu.* Pre ľubovoľný prvok $a \in A$ máme $a \in [a]$, a teda aj

$$a \in \bigcup_{a \in A} [a].$$

*Triedy sú disjunktné.* Predpokladajme, že $[a] \cap [b] \neq \emptyset$. T.j. existuje nejaký prvok $x \in A$ taký, že $x \in [a]$ aj $x \in [b]$. To znamená, že $a \sim x$ aj $x \sim b$ – a z tranzitívnosti potom máme $a \sim b$. Potom už máme aj $[a] = b$ (úloha 2.2.1). □

Z relácie ekvivalencie teda dostaneme rozklad. Obrátene ak máme rozklad množiny $A$ – čiže ak množinu $A$ vieme dostať ako zjednotenie nejakých podmnožín, ktoré sú navzájom disjunktné – tak vieme z neho dostať zodpovedajúcu reláciu ekvivalencie. (Základná idea prečo naozaj vieme nejako dostať pôvodnú reláciu je to, že $a \sim b$ platí práve vtedy, keď prvky $a$, $b$ ležia v tej istej triede rozkladu, t.j.

$$a \sim b \qquad \Leftrightarrow \qquad [a] = [b].$$

Toto je vlastne podmienka (2.4) v úlohe 2.2.1.)

{relekv:PRIKLROZKADKONG4

**Príklad 2.2.4.** Môžeme sa pozrieť na to, aký rozklad dostaneme z relácie ekvivalencie určenej podmienkou (2.1), t.j. naša relácia je kongruencia modulo 4.

$$a \sim b \qquad \Leftrightarrow \qquad 4 \mid a - b.$$

Jednotlivé triedy rozkladu budú presne zvyškové triedy modulo 4, t.j. trieda $[a]$ pozostáva z tých čísel, ktoré majú rovnaký zvyšok po delení štvorkou ako $a$.

Dostávame štyri triedy ekvivalencie:

$$\begin{aligned}
[0] &= \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\
[1] &= \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\
[2] &= \{\ldots, -6, -2, 2, 6, 10, \ldots\} \\
[3] &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}
\end{aligned}$$

Vidíme, že triedy sú skutočne disjunktné (žiadne celé číslo nie je vo viacerých triedach).

Takisto každé celé číslo patrí do niektorej z týchto štyroch tried – teda zjednotenie tried ekvivalencie je celá množina $\mathbb{Z}$.

Je to teda naozaj rozklad množiny $\mathbb{Z}$.

### 2.2.3 Čo znamená, že funkcia je dobre definovaná?

{relekv:SSECTI

Pri práci s reláciami ekvivalencie a so zodpovedajúcimi rozkladmi sa často vyskytne situácia, že nás bude zaujímať, či nejaká funkcia (prípadne binárna operácia) je *dobre definovaná.* Nám sa konkrétne bude niečo takéto bude hodiť, keď budeme definovať operácie na okruhoch $\mathbb{Z}/(n)$ a $F[x]/(h(x))$ (tvrdenia 3.3.19 a 4.5.1.)

Skúsme si aspoň na nejakom jednoduchom príklade osvetliť, čo sa takýmto niečím rozumie. Uvidíme tiež, že s takýmto niečím sme sa už viackrát stretli – aj keď možno v tých situáciách nebolo explicitne použité takéto pomenovanie.

Situácia, ktorou sa budeme zaoberať je takáto. Máme nejakú množinu $A$ a reláciu ekvivalencie $\sim$ na tejto množine. Už vieme, že potom dostaneme rozklad

$$A/\sim = \{[a]; a \in A\}$$

pozostávajúci z jednotlivých tried ekvivalencie.

A súčasne máme nejaké zobrazenie $f\colon A \to B$, t.j. každému prvku z $a$ sme priradili nejaký prvok $f(a) \in B$. Chceli by sme sa pozrieť na to, či ak triede $[a]$ priradíme hodnotu $f(a)$, tak dostaneme zobrazenie. Práve toto myslím pod tým, že funkcia

$$f\colon A/\sim \to B$$
$$\overline{f}\colon [a] \mapsto f(a)$$

je dobre definovaná.

Vyskúšajme to na najprv nejakom veľmi jednoduchom konkrétnom príklade, neskôr si môžeme ukázať aj nejaké všeobecné tvrdenie, ktoré túto situáciu popisuje.

{relekv:PRIKLDOBREMOD4}

**Príklad 2.2.5.** Pozrime sa opäť na reláciu „kongruencia modulo 4“, čiže reláciu zadanú vzťahom (2.1).

$$a \sim b \qquad \Leftrightarrow \qquad 4 \mid a - b$$

Pre túto reláciu dostávame rozklad $\mathbb{Z}$ na štyri triedy ekvivalencie [0], [1], [2], [3].

$$[a] \mapsto a \bmod 2$$

TODO *je dobre definované zobrazenie.*

$$[a] \mapsto a \bmod 3$$

TODO *nie je dobre definované zobrazenie.*

{relekv:TVRDOBREDEF}

**Tvrdenie 2.2.6.** *Nech $\sim$ je relácia ekvivalencie na množine $A$ a $f\colon A \to B$ je zobrazenie. Predpokladajme navyše, že pre ľubovoľné $a_{1,2} \in A$ platí*

{relekv:EQFREL}

$$a_1 \sim a_2 \Rightarrow f(a_1) = f(a_2). \tag{2.2}$$

*Potom predpis*

{relekv:EQF[A]}

$$\overline{f}([a]) = f(a) \tag{2.3}$$

*určuje dobre definované zobrazenie $\overline{f}\colon A/\sim \to B$.*

Ak máme k dispozícii podmienku (2.2), tak skutočne vieme dostať zobrazenie spôsobom, ktorý sme spomenuli vyššie.

$$\overline{f}\colon A/\sim \to B$$
$$\overline{f}([a]) = f(a)$$

Ak sú v tejto abstraktnej verzii uvedené tvrdenia nie celkom jasné, môže byť užitočné porovnať toto tvrdenie so zobrazeniami, ktoré sa vyskytli v príklade 2.2.5.

*Dôkaz.* Chceme zdôvodniť, že každej triede $[a]$ sme predpisom (2.3) skutočne priradili *jediný* prvok množiny $B$.

T.j. pýtame sa, či hodnota $f(a)$ je jednoznačne určená zvolenou triedou.

Samozrejme, trieda $[a]$ môže byť reprezentovaná rôznymi prvkami z $A$. Teda sa vlastne pýtame, či pre $[a] = [a']$ dostaneme rovnaké hodnoty $f(a)$ a $f(a')$.

$$[a] = [a'] \qquad \Rightarrow \qquad f(a) = f(a')$$

Pretože $[a] = [a']$ platí práve vtedy, keď $a \sim a'$ (úloha 2.2.1), môžeme túto podmienku ekvivaletne prepísať ako

$$a \sim a' \qquad \Rightarrow \qquad f(a) = f(a').$$

Toto je presne podmienka (2.2), ktorá je medzi predpokladmi nášho tvrdenia.

Vidíme teda, že každej triede sme priradili jediný prvok. Súčasne je jasné, že tento prvok patrí do množiny $B$. □

**Poznámka 2.2.7.** Spomeňme stručne aspoň niektoré situácie, v ktorých ste sa inde mohli stretnúť s tým, že pre nejakú funkciu (alebo binárnu operáciu) bolo podstatné aj to, či je dobre definovaná.[4]

**Racionálne čísla ako zlomky.** Toto by mohol byť príklad, ktorý dobre poznáme. Racionálne čísla sme zvyknutí zapisovať ako zlomky:

$$\mathbb{Q} = \{\frac{a}{b}; a, b \in \mathbb{Z}, b \neq 0\}.$$

Samozrejme, každé racionálne číslo môže mať veľa takýchto zápisov – ak čitateľ a menovateľ vynásobíme (vydelíme) tým istým číslom, zlomok predstavuje to isté racionálne číslo:

$$\frac{1}{3} = \frac{2}{6} = \frac{-2}{-6} = \frac{3}{9} = \frac{4}{12} = \frac{5}{15} = \dots$$

Vieme aj povedať, kedy dva zlomky predstavujú to isté číslo:

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b.$$

Sčitovanie a násobenie racionálnych čísel môžeme definovať tak, že povieme, že

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$$
$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$

Pri týchto definíciach si treba dať pozor na to, či výsledok nezávisí od toho, ako sme racionálne čísla reprezentovali.

Ak by sme napríklad zaviedli novú operáciu predpisom

$$\frac{a}{b} * \frac{a'}{b'} = \frac{a + a'}{b + b'},$$

tak nedostaneme binárnu operáciu na racionálnych číslach. Mali by sme totiž napríklad:

$$\frac{1}{2} + \frac{1}{3} = \frac{2}{5},$$
$$\frac{2}{4} + \frac{1}{3} = \frac{3}{7}$$

[4] Pozri aj: `https://msleziak.com/forum/viewtopic.php?t=1293`.

Tento predpis by teda nedefinoval binárnu operáciu na množine $\mathbb{Q}$.

Bolo by to v poriadku, ak by sme navyše pridali požiadavku, že vždy používame zlomky v redukovanom tvare. Alebo tiež, ak by sme pracovali so zlomkami (ako s usporiadanými dvojicami čitateľ a menovateľ) a nie priamo s racionálnymi číslami.

Robiť takéto niečo stále môže byť v niektorých kontextoch užitočné. Napríklad takéto niečo sa používa pri definícii *Fareyových zlomkov*. (Čiže je to konštrukcia, ktorá sa v praxi občas vyskytne. Tu sme ju spomenuli ale najmä ako ukážku toho, že na $\mathbb{Q}$ by sme takto nedostali dobre definovanú binárnu operáciu.)

TODO kardinalita

### Cvičenia

relekv:ULOROVNAKETRIEDY}

**Úloha 2.2.1.** Nech $\sim$ je relácia ekvivalencie na množine $A$.
a) Ukážte, že ak $a \sim b$, tak $[a] = [b]$.
b) Ukážte, že ak $[a] = [b]$, tak $a \sim b$.
Celkovo teda pre relácie ekvivalencie dostávame

{relekv:EQTRIEDY}

$$a \sim b \qquad \Leftrightarrow \qquad [a] = [b]. \tag{2.4}$$

{relekv:ULOZOBR}

**Úloha 2.2.2.** Nech $f\colon A \to B$ je surjektívne zobrazenie. Ukážte potom, že:
a) Predpis

$$a_1 \sim a_2 \Leftrightarrow f(a_1) = f(a_2)$$

definuje reláciu ekvivalencie na množine $A$. (Niekedy, ak by sme potrebovali zdôrazniť aké zobrazenie sme použili, by sme pre túto reláciu mohli použiť označenie $\sim_f$.)
b) Trieda prvku $a$ sa rovná

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

c) Ukážte, že predpis

$$\overline{f}\colon [a] \mapsto f(a)$$
$$\overline{f}\colon A/\!\sim \to B$$

určuje dobre definované zobrazenie a že zobrazenie $\overline{f}$ je bijekcia medzi $A/\!\sim$ a $B$.

{relekv:ULOPRIENIKDVE}

**Úloha 2.2.3.** a) Nech $R_1$, $R_2$ sú relácie ekvivalencie na množine $A$. Ukážte, že aj $R = R_1 \cap R_2$ je relácia ekvivalencie na množine $A$.
b) Ukážte, že pre ľubovoľné $a \in A$ platí

$$[a]_R = [a]_{R_1} \cap [a]_{R_2}.$$

{relekv:ULOPRIENIK}

**Úloha 2.2.4.** Nech $I \neq \emptyset$ a pre každé $i \in I$ je $R_i$ relácia ekvivalencie na množine $A$. Ukážte, že aj prienik týchto relácií $R = \bigcap_{i \in I} R_i$ je relácia ekvivalencie na tej istej množine.[5]

{relekv:ULOSUCINDVE}

**Úloha 2.2.5.** Nech $R_1$ je relácia ekvivalencie na množine $A$ a $R_2$ je relácia ekvivalencie na množine $B$. Definujme reláciu $R$ na $A \times B$ tak, že

$$((a,b),(a',b')) \in R \qquad \Leftrightarrow \qquad (a,a') \in R_1 \wedge (b,b') \in R_2.$$

Ukážte, že $R$ je relácia ekvivalencie na množine $A \times B$.

[5] Ak máme dokázanú takúto vec, tak vidíme aj to, že pre ľubovoľnú podmnožinu $M \subseteq A \times A$ existuje najmenšia relácia ekvivalencie na $A$ obsahujúca $M$.

Ak preferujete takéto označenie, to isté môžeme povedať tak, že pomocou dvoch relácií ekvivalencie $\sim_1$ a $\sim_2$ (pričom prvá z nich je relácia na množine $A$ a druhá na množine $B$) sme definovali novú reláciu na množine $A \times B$ podmienkou

$$(a, a') \sim (b, b') \qquad \Leftrightarrow \qquad a \sim_1 a' \wedge b \sim_2 b'.$$

**Úloha 2.2.6.** Pre danú množinu $A$ a reláciu $\sim$ overte, či ide o reláciu ekvivalencie:
a) $A = \mathbb{N}$, $x \sim y \Leftrightarrow 3 \mid x + 2y$
b) $A = \mathbb{R}$, $x \sim y \Leftrightarrow |x - y| \leq 1$
c) $A = \mathbb{R}$, $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$
d) $A = \mathbb{R}$, $x \sim y \Leftrightarrow x - y \in \mathbb{Q}$

# Kapitola 3

# Okruhy a ideály

## 3.1 Okruhy – definícia a základné vlastnosti

Veci, ktoré v tejto časti chceme spomenúť, ste už mohli stretnúť na bakalárskom štúdiu. Prinajmenšom ste sa určite stretli s definíciou poľa – okruhy sa na polia do istej miery podobajú, ale v definícii poľa sú nejaké vlastnosti navyše.

{okruh:DEFOKRUH}

### 3.1.1 Definícia okruhu

**Definícia 3.1.1.** Nech $R$ je množina, $+$ a $\cdot$ sú binárne operácie na tejto množine. Potom $(R, +, \cdot)$ voláme *okruh,* ak platí:

(i) Operácia $+$ je komutatívna a asociatívna, t.j.,

$$(\forall x, y \in R)x + y = y + x$$
$$(\forall x, y, z \in R)(x + y) + z = x + (y + z)$$

(ii) Operácia $+$ má neutrálny prvok, budeme ho označovať 0.

$$(\exists 0 \in R)(\forall x \in R)x + 0 = 0 + x = x$$

(iii) Pre každé $x \in R$ existuje inverzný prvok vzhľadom na operáciu $+$.

$$(\forall x \in R)(\exists y \in R)x + y = y + x = 0$$

Inverzný prvok k $x$ vzhľadom na sčitovanie budeme označovať $-x$.

(iv) Operácia $\cdot$ je asociatívna, t.j. platí:

$$(\forall x, y, z \in R)(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

(v) Platia distributívne zákony:

$$(\forall x, y, z \in R)x \cdot (y + z) = x \cdot y + x \cdot z$$
$$(\forall x, y, z \in R)(y + z) \cdot x = y \cdot x + z \cdot x$$

Môžeme si všimnúť, že prvé tri vlastnosti – týkajúce sa iba sčitovania – sa dajú stručne povedať tak, že $(R, +)$ je komutatívna grupa. (Takto sformulovaná definícia má výhodu, že jej rozumie aj človek, ktorý sa s pojmom grupy nestretol.)

**Poznámka 3.1.2.** Operácie v okruhu síce označujeme + a · (a často ich voláme sčitovanie a násobenie) – ale nemusí vždy ísť o sčitovanie a násobenie reálnych čísel.

Takisto neutrálny prvok pre sčitovanie síce označujeme 0; nemusí to však byť číslo nula.

Priamo v definícii okruhu požadujeme od operácie + komutatívnosť aj existenciu neutrálneho prvku. Často nás budú zaujímať aj okruhy, kde podobné vlastnosti má aj násobenie

{okruh:DEF00}

**Definícia 3.1.3.** Okruh $(R, +, \cdot)$ sa nazýva *komutatívny okruh,* ak operácia $\cdot$ je komutatívna.

$$(\forall x, y \in R) x \cdot y = y \cdot x$$

Okruh $(R, +, \cdot)$ nazývame *okruh s jednotkou,* ak existuje neutrálny prvok na násobenie, ktorý je navyše rôzny od nuly. Ak takýto prvok existuje, budeme ho označovať 1.

$$(\exists 1 \in R \setminus \{0\})(\forall x \in R) 1 \cdot x = x \cdot 1 = 1$$

Priamo v definícii požadujeme $1 \neq 0$. V skutočnosti sme tým vlastne ale iba zakázali veľmi triviálny okruh $(\{0\}, +, \cdot)$. V tomto okruhu síce existuje neutrálny prvok pre násobenie – nepovažujeme ho však za okruh s jednotkou.

{okruh:DEFPOZNRNG}

**Poznámka 3.1.4.** Často v literatúre nájdete priamo v definícii okruhu aj požiadavku na existenciu jednotky. V tomto texte používame inú konvenciu – azda to je tak, že ak explicitne použijeme termín *okruh s jednotkou,* tak je jasné, že požadujeme jednotku (a čitateľ nemusí špekulovať o tom, ktorá z týchto dvoch definícií sa tu používa).

V konečnom dôsledku aj tak okruhy, s ktorými budeme pracovať, budú zvyčajne komutatívne okruhy s jednotkou. (Dokonca to zvyčajne budú obory integrity – tento pojem zavedieme o chvíľu.)

{okruh:DEFOI}

**Definícia 3.1.5.** Nech $(R, +, \cdot)$ je okruh. Hovorím, že $R$ je *okruh bez deliteľov nuly,* ak z $a \cdot b = 0$ vyplýva $a = 0$ alebo $b = 0$.

$$(\forall a, b \in R)(a \cdot b = 0 \Rightarrow a = 0 \vee b = 0)$$

Okruh $(R, +, \cdot)$ nazývame *obor integrity,* ak je to komutatívny okruh s jednotkou bez deliteľov nuly.

Môže byť pre nás užitočné si uvedomiť, že niekedy môžeme v okruhu krátiť – nie však úplne vo všeobecnosti. Platí to však, ak pracujeme v okruhu bez deliteľov nuly. (A teda aj pre ľubovoľný obor integrity.)

{okruh:TVROIKRATENIE}

**Tvrdenie 3.1.6.** *Nech $(R, +, \cdot)$ je okruh bez deliteľov nuly a nech $a \neq 0$ je nejaký* nenulový *prvok okruhu $R$.*

*Potom pre ľubovoľné $x, y \in R$ z $ax = ay$ vyplýva $x = y$.*

$$\forall (a, x, y \in R)(a \neq 0 \wedge a \cdot x = a \cdot y \Rightarrow x = y)$$

*Dôkaz.* Ak platí $ax = ay$ tak máme

$$a(x - y) = ax - ay = 0.$$

Pretože $a \neq 0$, z $a(x - y) = 0$ dostaneme

$$x - y = 0,$$

a teda aj

$$x = y.$$

□

### 3.1.2 Príklady okruhov

Príkladmi okruhov sú všetky polia, ako napríklad $\mathbb{Q}$, $\mathbb{R}$ či $\mathbb{C}$ (s obvyklým sčitovaním a násobením). Poďme sa pozrieť aj na nejaké príklady okruhov, ktoré nie sú poľami.

**Príklad 3.1.7.** TODO matice $2 \times 2$

$$R = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix}; a, b, c, d \in \mathbb{R}\}.$$

Ako operácie použijeme obvyklé sčitovanie a násobenie matíc.

Toto je príklad okruhu, kde existujú delitele nuly – úloha 3.1.2.

Aby sme ukázali príklad okruhu, kde operácie nie sú značené $+$ a $\cdot$, ale inak než sme zvyknutí, môžeme skúsiť niečo takéto.

**Príklad 3.1.8.** Nech $X$ je ľubovoľná množina a

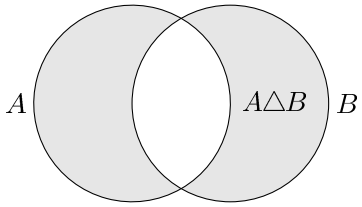
$$\mathcal{P}(X) = \{A; A \subseteq X\}$$

je jej potenčná množina (t.j. množina všetkých podmnožín množiny $X$.)

Potom $(\mathcal{P}(X), \triangle, \cap)$ je komutatívny okruh s jednotkou. Symboly $\triangle$ a $\cap$ označujú symetrickú diferenciu a prienik, t.j.

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$
$$A \cap B = \{x; (x \in A) \wedge (x \in B)\}$$

Vennov diagram pre symetrickú diferenciu je znázornený na obrázku 3.1. Ak by sme aj symetrickú diferenciu chceli zadefinovať pomocou logickej spojky, použili by sme spojku XOR. (T.j. logickú spojku určenú tým, že $p \,\mathrm{XOR}\, q$ je pravdivé práve vtedy, keď $p$ a $q$ majú opačné pravdivostné hodnoty.)




{okr:FIGROZD} Obr. 3.1: Vennov diagram pre symetrickú diferenciu $A \triangle B$

### 3.1.3 Homomorfizmy okruhov

**Definícia 3.1.9.** Nech $R_{1,2}$ sú okruhy a $f\colon R_1 \to R_2$ je zobrazenie. Hovoríme, že $f\colon R_1 \to R_2$ je *homomorfizmus* ak pre ľubovoľné $x_{1,2} \in R_1$ platí:

$$f(x_1 + x_2) = f(x_1) + f(x_2)$$
$$f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2)$$

**Definícia 3.1.10.** Ak $f\colon R_1 \to R_2$ je homomorfizmus a súčasne to je bijekcia, tak hovoríme, že $f$ je *izomorfizmus.*

Okruhy $R_{1,2}$ nazývame *izomorfné,* ak existuje izomorfizmus $R_1 \to R_2$. Označujeme $R_1 \cong R_2$.

Z rôznych situácií, s ktorými sme sa stretli, už vieme, že ak $R_1$ a $R_2$ sú izomorfné okruhy, tak sú „v podstate“ rovnaké. (Podobne ako to bolo napríklad pre izomorfné vektorové priestory.)

### 3.1.4 Podokruh

Podobne ako pri iných typoch štruktúr, aj tu sa môžeme pýtať, kedy daná podmnožina s rovnakými operáciami bude opäť tvoriť okruh. (Tak ako sme pri vektorových priestoroch študovali podpriestory, pri grupách podgrupy.)

{okr:DEFPODOKR}

**Definícia 3.1.11.** Nech $(R, +, \cdot)$ je okruh a $S \subseteq R$. Hovoríme, že $S$ je *podokruh* okruhu $R$, ak:

(i) $S \neq \emptyset$

(ii) Pre ľubovoľné $x, y \in S$ platí aj $x - y \in S$.

(iii) Pre ľubovoľné $x, y \in S$ platí aj $x \cdot y \in S$.

Môžeme si všimnúť, že druhá podmienka vlastne hovorí, že $S$ je podgrupa komutatívnej grupy $(R, +)$. A tiež, že druhá aj tretia podmienka súvisia s tým, že množina $S$ je uzavretá vzhľadom na sčitovanie aj násobenie.

#### Cvičenia

{okruhcvic:ULOAKRATO}

**Úloha 3.1.1.** Nech $R$ je ľubovoľný okruh. Ukážte priamo z definície okruhu, že $a \cdot 0 = 0$.

{okruhcvic:ULOMATSUCINO}

**Úloha 3.1.2.** Nájdite príklad nenulových matíc $A$, $B$ rozmerov $2 \times 2$ nad poľom $\mathbb{R}$ takých, že $A \cdot B = 0$.

{okruhcvic:ULOOBRAZNULY}

**Úloha 3.1.3.** Ukážte, že ak $f\colon R \to R'$ je homomorfizmus okruhov, tak $f(0) = 0$.

{okruhcvic:ULOFCIE}

**Úloha 3.1.4.** Nech $R$ je okruh. Pre ľubovoľné $f, g\colon R \to R$ môžeme definovať súčet a súčin funkcií predpisom:

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

Dokážte, že množina všetkých zobrazení $R \to R$ s takto definovaným sčitovaním a násobením tvorí okruh.

Ak navyše $R$ je komutatívny okruh, aj okruh funkcí je komutatívny. Ak $R$ je okruh s jednotkou, tak aj okruh funkcií je okruh s jednotkou.

**Úloha 3.1.5.** Nech $R = \{f\colon \mathbb{R} \to \mathbb{R}\}$ je množina všetkých funkcií z $\mathbb{R}$ do $\mathbb{R}$. Na tejto množine vieme definovať operácie sčitovania a násobenia ako

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

Dostaneme takto okruh (úloha 3.1.4).

Nech $a \in \mathbb{R}$. Ukážte, že potom množina

$$I = \{f \in R; f(a) = 0\}$$

tvorí ideál v okruhu $\mathbb{R}$.

Vedeli by ste nájsť homomorfizmus $\varphi\colon R \to \mathbb{R}$, ktorého jadrom je tento ideál?

{okruhcvic:ULOPODOKROI}

**Úloha 3.1.6.** Ukážte, že ľubovoľný podokruh poľa obsahujúci jednotku je obor integrity.

## 3.2 Ideály v okruhoch

{ideal:DEF}

**Definícia 3.2.1.** Nech $R$ je okruh a $I \subseteq R$. Hovoríme, že $I$ je *ideál* v $R$ ak $I \neq \emptyset$ a súčasne platí:

(i) Pre ľubovoľné $a, b \in I$ aj $a - b \in I$.

(ii) Pre ľubovoľné $a \in I$ a $r \in R$ platí aj $ar, ra \in I$.

$$(\forall a, b \in I) a - b \in I$$
$$(\forall a \in I)(r \in R) a \cdot r, r \cdot a \in I$$

My sa najčastejšie budeme zaoberať komutatívnymi okruhmi – v takom prípade stačí samozrejme v druhej časti definície použiť iba jedno poradie.

**Poznámka 3.2.2.** Opäť aj tu by sa prvá časť definície dala ekvivalentne povedať tak, že $I$ je podgrupa grupy $(R, +)$. My sme však uprednostnili definíciu, ktorá je sformulovaná bez použitia pojmu grupy.

{ideal:PRIKLTTRIV}

**Príklad 3.2.3.** Ako dva veľmi triviálne prípady dostaneme, že $\{0\}$ a $R$ sú ideály v okruhu $R$ (úlohy 3.2.2 a 3.2.3).

{ideal:PRIKLPOLE}

V niektorých situáciách nedostaneme iné ideály, ako tieto dva:

**Príklad 3.2.4.** Ak $F$ je pole, tak jediné ideály v $F$ sú $\{0\}$ a celé $F$.

Skutočne, ak $I$ je ideál v nejakom poli a existuje $a \neq 0$ patriace do $I$, tak potom aj

$$1 = a \cdot a^{-1} \in I.$$

Z toho, že $I$ obsahuje jednotku, už pre všetky $x \in F$ dostaneme

$$x = 1 \cdot x \in I.$$

Pomerne jednoduchú triedu ideálov dostaneme tak, že si vezmeme jeden konkrétny prvok a všetky jeho násobky.

**Príklad 3.2.5.** Ak $R$ je komutatívny okruh s jednotkou a $a \in R$, tak označme

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

Pomerne ľahko sa overí, že táto množina je ideál v $R$, ktorý obsahuje $a$. (Je to najmenší ideál s týmito vlastnosťami.) Ideál takéhoto tvaru sa nazýva *hlavný ideál.*

Poďme sa presvedčiť, že za uvedených predpokladov množina

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

skutočne spĺňa podmienky z definície ideálu.

Máme $a = a \cdot 1 \in I$, čiže $I \neq \emptyset$.

Pre ľubovoľné dva prvky z $I$ je aj ich rozdiel uvedeného tvaru:

$$ax_1 - ax_2 = a(x_1 - x_2)$$

A ak nejaký násobok prvku $a$ vynásobíme ľubovoľným prvkom z okruhu, tak znovu dostaneme násobok $a$.

$$(ax)r = a(xr)$$

Nás budú zaujímať najmä okruhy $(\mathbb{Z}, +, \cdot)$ a $(F[x], +, \cdot)$, t.j. celé čísla a polynómy nad nejakým poľom. V týchto okruhoch sú všetky ideály hlavné - tvrdenia 3.3.4 a 3.4.28.

eal:TVRJADRO}

**Tvrdenie 3.2.6.** *Nech $R, R'$ sú okruhy a $f\colon R \to R'$ je homomorfizmus okruhov. Potom množina*

$$\operatorname{Ker} f = \{x \in R; f(x) = 0\}$$

*je ideál v $R$. Túto množinu nazývame* jadro homomorfizmu $f$.

*Dôkaz.* $0 \in \operatorname{Ker} f$. Stačí si uvedomiť, že $f(a) = 0$ (úloha 3.1.3). Dostávame teda, že $0 \in I$, čiže $I \neq \emptyset$.

*Ak $a, b \in \operatorname{Ker} f$, tak aj $a - b \in \operatorname{Ker} f$.* Prepokladajme, že $f(a) = f(b) = 0$. Pretože $f$ je homomorfizmus, dostávame potom

$$f(a - b) = f(a) - f(b) = 0 - 0 = 0.$$

*Ak $a \in \operatorname{Ker} f$ a $x \in R$, tak aj $ax, xa \in \operatorname{Ker} f$.* Ak platí $f(a) = 0$, tak máme aj

$$f(ax) = f(a) \cdot f(x) = 0 \cdot f(x) = 0,$$
$$f(xa) = f(x) \cdot f(a) = f(x) \cdot 0 = 0.$$

To znamená, že aj $ax, xa \in \operatorname{Ker} f$.

Využili sme fakt, že v okruhu po vynásobení ľubovoľného prvku nulou dostaneme opäť nulu – úloha 3.1.1. □

**Cvičenia**

{idealcvic:ULOIDENULA}

**Úloha 3.2.1.** Nech $R$ je ľubovoľný okruh a $I \subseteq R$ je ideál v $R$. Ukážte, že $0 \in I$.

Stručne: Každý ideál obsahuje nulu.

{idealcvic:ULOIDENULOVY}

**Úloha 3.2.2.** Nech $R$ je ľubovoľný okruh. Dokážte, že:
a) Množina $I = \{0\}$ je ideál v $R$.
b) Ak navyše $R$ je komutatívny okruh s jednotkou, tak $\{0\} = (0)$, t.j. tento ideál je hlavný ideál generovaný nulou.

{idealcvic:ULOIDECELY}

**Úloha 3.2.3.** Nech $R$ je ľubovoľný okruh. Dokážte:
a) Množina $I = R$ je ideál v $R$.
b) Ak navyše $R$ je komutatívny okruh s jednotkou, tak platí $R = (1)$.

{idealcvic:ULOPRIENIKDVO

**Úloha 3.2.4.** Dokážte, alebo nájdite kontrapríklad:
a) Ak $R$ je komutatívny okruh s jednotkou a $I_1$, $I_2$ sú ideály v okruhu $R$, tak aj $I_1 \cap I_2$ je ideál v $R$.
b) Ak $R$ je komutatívny okruh s jednotkou a $I_1$, $I_2$ sú ideály v okruhu $R$, tak aj $I_1 \cup I_2$ je ideál v $R$.

{idealcvic:ULOPRIENIK}

**Úloha 3.2.5.** Nech $R$ je komutatívny okruh s jednotkou. Nech

## 3.3 Okruh celých čísel

{okruhZ:SECT}

Chceme na tomto mieste pripomenúť aj nejaké veci súvisiace s deliteľnosťou celých čísel. Mnohé z nich už poznáte z nižších ročníkov – možno niektoré z nich ste sformulovali pre prirodzené čísla a nie pre celé čísla, ale to je veľmi malý rozdiel. Spomíname ich hlavne preto,

že veľmi podobné veci budeme robiť s polynómami – azda niektoré veci budú zrozumiteľnejšie ak si najprv pripomenieme analogické vlastnosti celých čísel.

Azda jediné, čo by mohlo byť nové, je to, že si ukážeme nejaké veci o ideáloch v okruhu $\mathbb{Z}$. A tiež, že niektoré vlastnosti pre n.s.d. dvoch čísel potom ukážeme pomocou ideálov.

Okruh $(\mathbb{Z}, +, \cdot)$ je oborom integrity. V tejto časti si ukážeme, že okrem toho má aj tú vlastnosť, že každý ideál v $\mathbb{Z}$ je hlavný. Neskôr uvidíme, že obe tieto vlastnosti má aj okruh polynómov.

Mohli by sme budovať všeobecnejšie teóriu takým spôsobom, aby sme tieto vlastnosti dokázali naraz pre širšiu triedu okruhov a všetky vlastnosti, ktoré spomíname pre $\mathbb{Z}$ a $F[x]$, by sme dostali ako špeciálne prípady. Pri práci s rozšíreniami polí budeme pracovať najmä s okruhom $F[x]$. Nesnažíme sa tu teda budovať všeobecnú teórie – keďže nás zaujímajú iba dva konkrétne prípady, pričom jeden z nich už dôverne poznáme. Ale aj tak sú tu viaceré veci sformulované tak, aby bolo vidno nejakú podobnosť medzi okruhmi $\mathbb{Z}$ a $F[x]$. (Z toho sa potom dá vidieť aj to, že pravdepodobne existuje nejaká možnosť, ako tieto veci zmysluplne zovšeobecniť.)

### 3.3.1 Veta o delení so zvyškom

{okruhZ:SSECTLONGDIV}

Nasledujúci výsledok dobre poznáte – spomíname ho tu najmä preto, že ho chceme viackrát použiť. A že výsledok delenia so zvyškom je základom modulárnej aritmetiky – čo je vec, o ktorej sa nám hodí aspoň niečo spomenúť.

Súčasne ho chceme pripomenúť aj preto, že sa nám bude hodiť analogický výsledok pre polynómy – tvrdenie 3.4.11.

{okruhZ:TVRLONGDIV}

**Tvrdenie 3.3.1** (Veta o delení so zvyškom)**.** *Nech $a, b \in \mathbb{Z}$ a $b \neq 0$. Potom existujú celé čísla $q, r$ také, že platí*

$$a = q \cdot b + r, \qquad 0 \leq r < |b|.$$

*Navyše čísla $q$ a $r$ sú týmito podmienkami jednoznačne určené.*

*Číslo $q$ nazývame* podiel *a číslo $r$* zvyšok *čísla $a$ po delení číslom $b$. Pre zvyšok budeme používať označenie $r = a \bmod b$.*

Dôkaz ste videli v nižších ročníkoch – tu ho nebudeme opakovať. Stručne sa dôkaz dá povedať tak, že sa pozrieme na najväčší celočíselný násobok čísla $b$ taký, že $qb \leq a$. A skontrolujeme, že ak za $q$ vezmeme takéto číslo, tak platia vlastnosti, ktoré požadujeme od $q$ a $r$.

**Poznámka 3.3.2.** Možno ste tento výsledok videli sformulovaný pre $b > 0$ (t.j. pre prirodzené čísla $b$). Medzi zdôvodnením takejto formulácie a formulácie pre kladné $b$ nie je veľký rozdiel. (Samozrejme, ak pracujeme iba s kladnými číslami, tak podmienku $0 \leq r < |b|$ môžeme nahradiť podmienkou $0 \leq r < b$.)

Keď už spomíname nejaké rôzne variácie tejto vety, ktoré sa odlišujú viac-menej iba v drobných detailoch, tak ak by sme vynechali podmienku o jednoznačnosti, tak môžeme použiť aj formuláciu s podmienkou $|r| < |b|$.

Teda tri podoby tejto vety, ktoré sme spomenuli, sa stručne dajú zapísať takto:

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z} \setminus \{0\})(\exists! q, r \in \mathbb{Z})(a = q \cdot b \wedge 0 \leq r < |b|)$$
$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{N} \setminus \{0\})(\exists! q, r \in \mathbb{Z})(a = q \cdot b \wedge 0 \leq r < b)$$
$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z} \setminus \{0\})(\exists q, r \in \mathbb{Z})(a = q \cdot b \wedge |r| < |b|)$$

### 3.3.2 Deliteľnosť

{okruhZ:SSECTDELIT}

**Definícia 3.3.3.** Ak $a, b \in \mathbb{Z}$ tak hovoríme, že $a$ *delí* $b$, ak existuje celé číslo $q$ také, že $b = qa$. Označujeme $a \mid b$.

Teda $a \mid b$ je vlastne definované tak, že $b$ je celočíselným násobkom čísla $a$. Pre $a \neq 0$ to ekvivalentne môžeme povedať aj tak, že zlomok $\frac{b}{a}$ je celé číslo.

Ak $a$ nie je deliteľom čísla $b$, tak používame označenie $a \nmid b$.

Základné vlastnosti deliteľnosti poznáte z nižších ročníkov – a budeme ich bežne používať. Napríklad medzi vlastnosti, ktoré sa nám niekedy môžu hodiť, patrí to, že pre ľubovoľné $a, b, c \in \mathbb{Z}$ platí:

- $1 \mid a$, $a \mid 0$;
- Ak $0 \mid a$, tak $a = 0$.
- $a \mid a$;
- Ak $a \mid b$ aj $b \mid a$, tak $a = \pm b$ (úloha 3.3.1).
- Ak $a \mid b$ a $b \mid c$, tak aj $a \mid c$.
- Ak $a \mid b$ aj $a \mid c$, tak $a \mid b \pm c$.
- Ak $a \mid b$ aj $a \mid c$, tak platí $a \mid bx + cy$ pre ľubovoľné $x, y \in \mathbb{Z}$.
- Ak $a, b \in \mathbb{N}$, tak z $a \mid b$ vyplýva $a \leq b$.
- Ak $a \mid b$ a $b \neq 0$, tak $|a| \leq |b|$.

### 3.3.3 Ideály v okruhu $\mathbb{Z}$

{okruhZ:SSECTIDE}

Ukážeme si, že každý ideál v $(\mathbb{Z}, +, \cdot)$ je hlavný.

{okruhZ:TVROHI}

**Tvrdenie 3.3.4.** *Nech $I \subseteq \mathbb{Z}$ je ideál v okruhu $(\mathbb{Z}, +, \cdot)$. Potom existuje $a \in \mathbb{Z}$ také, že*

$$I = (a) = \{ax; x \in \mathbb{Z}\}.$$

*Ak navyše pridáme podmienku $a \geq 0$, tak číslo $a$ je jednoznačne určené.*

Celý dôkaz sa stručne dá zhrnúť tak, že:

- Zoberieme si najmenšie kladné $a$ patriace do ideálu $I$.
- Ukážeme, že všetky ostatné prvky v $I$ sú násobky čísla $a$.

Samozrejme, treba tam doplniť ďalšie detaily. A ak chceme postupovať podľa naznačenej stratégie, tak možno ako prvé sa oplatí pozrieť na to, či v $I$ musí existovať nejaký kladný prvok. (A čo urobíme, ak by neexistoval.)

*Dôkaz.* Pripomeňme, že priamo z definície ideálu vieme, že $I \neq \emptyset$ (definícia 3.2.1).

*Prípad $I = \{0\}$.* Ak ideál $I$ obsahuje iba nulu, tak môžeme zobrať $a = 0$, pozri úlohu 3.2.1.

Budeme sa teda odteraz teda už zaoberať iba *prípadom, že $I \neq \{0\}$*. Teda $I$ obsahuje aj nejaké nenulové prvky.

*Existencia.* Predpokladáme teda, že $I \setminus \{0\} \neq \emptyset$. Pretože pre každé $x \in I$ máme aj $-x = (-1) \cdot x \in I$, určite existuje aspoň jeden kladný prvok v $I$. Potom môžeme zobrať

$$a = \min\{x \in I; x > 0\}.$$

(Využívame, že každá neprázdna podmnožina prirodzených čísel má najmenší prvok.)

Chceme ukázať, že $I = (a)$. T.j. že $I$ obsahuje presne celočíselné násobky prvky $a$.

$\boxed{(a) \subseteq I}$ Pretože $a \in I$, priamo z definície ideálu máme aj $ax \in I$ pre

$\boxed{I \subseteq (a)}$ Zoberme si ľubovoľný prvok $x \in I$. Na základe vety o delení so zvyškom (veta 3.3.1) máme

$$x = q \cdot a + r$$

pre nejaké $q, r \in \mathbb{Z}$ a $0 \leq r < a$.

Ak by platilo $r \neq 0$, dostali by sme

$$r = x - q \cdot a \in I,$$

keďže $x$ aj $qa$ patria do ideálu $I$. To je ale *spor s minimalitou* – zobrali sme za $a$ najmenší kladný prvok v $I$ a zistili sme, že $r$ je od neho menší. Takáto možnosť teda *nemôže nastať.*

Zostáva teda iba možnosť, že $r = 0$. To znamená, že

$$x = q \cdot a \in (a).$$

*Jednoznačnosť.* Ak pre $a, b \in \mathbb{Z}$ platí $(a) = (b)$, znamená to, že $a \mid b$ aj $b \mid a$. Potom ale $a = \pm b$ (úloha 3.3.1). Teda z týchto dvoch čísel bude nezáporné iba jedno. □

Môžeme si tiež všimnúť vzťah medzi hlavnými ideálmi a deliteľnosťou. Pomerne ľahko sa dá skontrolovať, že pre $a, b \in \mathbb{Z}$ platí $a \mid b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$. (Overenie týchto ekvivalencií sme nechali ako cvičenie – úloha 3.3.2).

### 3.3.4 Najväčší spoločný deliteľ

{okruhZ:DEFNSD}

**Definícia 3.3.5.** Nech $a, b \in \mathbb{Z}$. Celé číslo $d \geq 0$ nazveme *najväčší spoločný deliteľ* čísel $a$, $b$ ak $d \geq 0$ a platí:

(i) $d \mid a$, $d \mid b$ (T.j. $d$ je súčasne deliteľ $a$ aj deliteľ $b$.)

(ii) Pre každé $c \in \mathbb{Z}$ také, že $c \mid a$, $c \mid b$ platí aj $c \mid d$.

Označujeme: $d = \gcd(a, b)$.

Pri prirodzených číslach ste mohlo boli zvyknutí na definíciu, kde sa v druhej časti namiesto $c \mid d$ vyskytuje $c \leq d$. My sme zvolili takúto definíciu – neskôr budeme deliteľnosť definovať pre polynómy, takto je jasnejšie vidno, že definície vyzerajú analogicky.

Pre prirodzené čísla by sme dostali ekvivalentnú definíciu aj ak by sme ju sformulovali s podmienkou $c \leq d$. Pre celé čísla by sme mohli použiť $d \leq |c|$ a opäť by táto definícia bola takmer rovnocenná – jediná výnimka je prípad $a = b = 0$. (Môžeme si na tomto mieste tiež uvedomiť, že pri našej definícii máme $\gcd(0, 0) = 0$.)

{okruhZkPOZNSDEXISTUJE}

**Poznámka 3.3.6.** Oplatí sa uvedomiť si to, že pre ľubovoľné celé čísla $a$, $b$ najväčší spoločný deliteľ skutočne existuje a je aj jednoznačne určený.

Na dôkaz jednoznačnosti si stačí uvedomiť, že ak dve čísla $d$, $d'$ spĺňajú podmienky z definície 3.3.5, tak pre ne platí

$$d \mid d' \text{ aj } d' \mid d.$$

Súčasne máme $d, d' \geq 0$, takže už dostávame $d = d'$.

Existenciu dostaneme z tvrdenia 3.3.7, ktoré ideme teraz dokázať..

{okruhZ:TVRIDEALNSD}

**Tvrdenie 3.3.7.** *Nech $a, b \in \mathbb{Z}$. Potom množina*

$$(a, b) = \{ax + by; x, y \in \mathbb{Z}\}$$

*je ideál v $\mathbb{Z}$.*

*Navyše ak $d \geq 0$ je celé číslo také, že $d = (a, b)$, tak $d$ je najväčší spoločný deliteľ $(a, b)$.*

Pripomeňme, že už vieme, že každý ideál v $\mathbb{Z}$ je hlavný (tvrdenie 3.3.4). Akonáhle sa nám teda podarí dokázať, že uvedaná množina je skutočne ideál, tak máme existenciu čísla $d$ s uvedenými vlastnosťami

*Dôkaz.* Označme $I = \{ax + by; x, y \in \mathbb{Z}\}$. Overenie, že táto množina tvorí ideál je pomerne priamočiare – ponecháme ho ako cvičenie (úloha 3.3.3).

Z tvrdenia 3.3.4 potom vieme, že existuje nezáporné celé číslo $d$ také, že $I = (d)$.

Ešte chceme overiť, či toto číslo $d$ spĺňa podmienky z definície 3.3.5, t.j. či $d = \gcd(a, b)$.

Je jasné, že ak $c \mid a$ aj $c \mid b$, tak $c \mid ax + by$ pre ľubovoľné celé čísla $x$ a $y$. Teda platí aj $c \mid d$, pretože číslo $d$ je tiež takéhoto tvaru.

Potrebujeme ešte ale overiť, že číslo $d$ je spoločným deliteľom $a$ aj $b$. Máme $a \in I$, a teda aj

$$a \in (d),$$

čo vlastne znamená, že $d \mid a$. Rovnakým spôsobom môžeme zdôvodniť aj $d \mid b$. □

Vidíme, že sme dostávame trochu iný dôkaz *Bézoutovej identity* – tentokrát pomocou ideálov. (Aj keď v dôkaze, ktorý ste videli na iných predmetoch, sa pravdepodobne používali podobné argumenty ako tu – ale nevyskytlo sa tam slovo ideál.)

{okruhZ:DOSBEZOUT}

**Dôsledok 3.3.8.** *Ak $d = \gcd(a, b)$ tak existujú $x, y \in \mathbb{Z}$ také, že*

$$d = ax + by.$$

Tento výsledok bude užitočný často v prípade, že $\gcd(a, b) = 1$.

**Definícia 3.3.9.** Celé čísla $a$, $b$ nazývame *nesúdeliteľné,* ak $\gcd(a, b) = 1$.

{okruhZ:DOSBEZOUTCOPRIME

**Dôsledok 3.3.10.** *Ak $a, b \in \mathbb{Z}$ sú nesúdeliteľné celé čísla, tak existujú $x, y \in \mathbb{Z}$ také, že*

$$ax + by = 1.$$

Na tomto mieste pripomeniem aj to, že kedysi ste sa naučili postup, akým sa dá algoritmicky hľadať $d = \gcd(a, b)$ v $\mathbb{Z}$ resp. $\mathbb{N}$ a súčasne ako sa dajú nájsť $x, y \in \mathbb{Z}$ spĺňajúce rovnosť $ax + by = d$ – *rozšírený Euklidov algoritmus.*

### 3.3.5 Prvočísla

{okruhZ:SSECTPRVOC}

Vo veľa veciach týkajúcich sa prirodzených (celých) čísel mali špeciálny význam prvočísla. Sú to čísla, ktoré sa nedajú netrivialne zapísať v tvare súčinu.

**Definícia 3.3.11.** Prirodzené číslo $p > 1$ sa nazýva prvočíslo ak pre jeho ľubovoľný zápis v tvare $p = a \cdot b$ platí $a = 1$ alebo $b = 1$.

Dôležitý výsledok o prvočíslach je fakt, že prirodzené čísla vieme jednoznačne zapísať ako súčiny prvočísel.

**Veta 3.3.12** (Základná veta aritmetiky)**.** *Pre každé prirodzené číslo $n > 1$ existujú prvočísla $p_1, p_2, \ldots, p_k$ také, že*

$$n = p_1 \cdot p_2 \cdots p_k.$$

*Navyše takýto zápis je určený jednoznačne až na poradie.*

Jedna z užitočných vlastností prvočísel je sformulovaná v nasledujúcom tvrdení. Dá sa využiť napríklad aj ako jeden krok v dôkaze zákadnej vety aritmetiky.

{okruhZ:TVRPM

**Tvrdenie 3.3.13.** *Nech $p$ je prvočíslo, $a$, $b$ sú celé čísla. Ak $p \mid ab$, tak $p \mid a$ alebo $p \mid b$.*

$$p \mid ab \qquad \Rightarrow \qquad p \mid a \vee p \mid b \tag{3.1}$$

{okruhZ:EQPMI

*Dôkaz.* Ak $p \mid a$, tak uvedené tvrdenie platí.

Zostáva nám teda možnosť $p \nmid a$. Pretože jediné prirodzené čísla deliace $p$ sú 1 a $p$, dostávame v takomto prípade

$$\gcd(p, a) = 1.$$

Potom z dôsledku 3.3.10 dostávame existenciu celých čísle $x, y \in \mathbb{Z}$ takých, že $px + ay = 1$, a teda máme aj

$$pbx + aby = b.$$

Vidíme, že platí

$$\left.\begin{matrix} p \mid p \\ p \mid ab \end{matrix}\right\} \Rightarrow \left.\begin{matrix} p \mid pbx \\ p \mid aby \end{matrix}\right\} \Rightarrow p \mid pbx + aby = b.$$

□

Môžeme si všimnúť, že argument použitý v jednom kroku predchádzajúceho dôkazu sa dá zapísať aj o čosi všeobecnejšie.

**Tvrdenie 3.3.14.** *Ak pre celé čísla $a$, $b$, $c$ platí $a \mid bc$ a $\gcd(a, b)$, tak $a \mid c$.*

*Dôkaz.* Úloha 3.3.4. □

### 3.3.6 Kongruencie

{okruhZ:KONG}

**Definícia 3.3.15.** Ak $a, b, n \in \mathbb{Z}$, tak hovoríme, že čísla $a$, $b$ sú kongruentné modulo $n$, ak platí

$$n \mid a - b.$$

Označujeme $a \equiv b \pmod{n}$.

$$a \equiv b \pmod{n} \qquad \Leftrightarrow \qquad n \mid a - b$$

S pojmom kongruencie pre celé čísla ste sa už stretli na iných predmetoch. Na tomto mieste zopakujeme základné vlastnosti kongruencií – nebudeme však opakovať dôkazy, ktoré ste už videli. Neskôr sa chceme hlavne pozrieť na to, ako počítanie s kongruenciami súvisí s okruhom zvyškových tried modulo $n$.

{okruhZ:POZNKONGNULA}

**Poznámka 3.3.16.** V definícii sme pripustili aj záporné $n$. Môžeme si všimnúť, že

$$a \equiv b \pmod{n} \qquad \Leftrightarrow \qquad a \equiv b \pmod{-n}.$$

Takže pokojne sa stačí venovať prípadom, keď $n \geq 0$.

Tiež si môžeme všimnúť, že prípady $n = 0$ a $n = 1$ sú veľmi triviálne:

$$\begin{aligned} a \equiv b \pmod{0} \qquad &\Leftrightarrow \qquad a = b \\ a \equiv b \pmod{1} \qquad &\Leftrightarrow \qquad a, b \in \mathbb{Z} \end{aligned}$$

T.j. ľubovoľné dve celé čísla sú kongruentné modulo 1. A kongruencia modulo nula nám dáva rovnosť.

Ako prvé si všimnime, že takto dostaneme reláciu ekvivalencie.

hZ:TVRRELEKV}

**Tvrdenie 3.3.17.** *Nech $a, b, c, n \in \mathbb{Z}$. Potom platí:*

(i) $a \equiv a \pmod{n}$

(ii) *Ak* $a \equiv b \pmod{n}$, *tak aj* $b \equiv a \pmod{n}$.

(iii) *Ak platí* $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, *tak aj* $a \equiv c \pmod{n}$.

Tiež je užitočné vedieť to, že kongruencie sa rozumne správajú vzhľadom na operácie sčitovania a násobenia.

{okruhZ:TVRKONGOPER}

**Tvrdenie 3.3.18.** *Nech $a, b, c, d, n \in \mathbb{Z}$. Ak*

$$\begin{aligned} a &\equiv c \pmod{n} \\ b &\equiv d \pmod{n} \end{aligned}$$

*tak platí aj*

$$\begin{aligned} a + b &\equiv c + d \pmod{n} \\ a \cdot b &\equiv c \cdot d \pmod{n} \end{aligned}$$

Tieto vlastnosti kongruencií poznáte z nižších ročníkov (a podobné výsledky pre polynómy neskôr ukážeme v tvrdeniach 3.4.33 a 3.4.34). Samozrejme, na zopakovanie si môžete vyskúšať, či by ste ich vedeli zdôvodniť (úlohy 3.3.6 a 3.3.7).

### 3.3.7 Zvyškové triedy a okruh $\mathbb{Z}/(n)$

Na chvíľu teraz zafixujme nejaké celé číslo $n$ a pozerajme sa na veci, ktoré dostaneme z relácie „byť kongruentný modulo $n$“.

Vieme, že ide o reláciu ekvivalencie. A teda pre každé celé číslo $a$ dostaneme triedu rozkladu – pozostávajúcu z tých čísel, ktoré sú kongruentné s číslom $a$. Okrem označenia $[a]$, ktoré sme zaviedli pri reláciách ekvivalencie, niekedy použijeme aj $\overline{a}$; najmä ak nám to niekedy pomôže niektoré veci zapísať stručnejšie.

$$\overline{a} = [a] = \{x \in \mathbb{Z}; x \equiv a \pmod{n}\}$$

Tieto množiny nazývame aj *zvyškové triedy* modulo $n$.

Označme si množinu zvyškových tried ako

$$Z/(n) = \{\overline{a}; a \in \mathbb{Z}\}.$$

Je zrejmé, že táto množina má $n$ rôznych prvkov.

Chceli by sme na množine zvyškových tried rozumne zaviesť sčitovanie a násobenie. Práve tvrdenie 3.3.18 nám hovorí, že môžeme operácie zaviesť takýmto spôsobom:

$$\begin{aligned} \overline{x} + \overline{y} &= \overline{x + y} \\ \overline{x} \cdot \overline{y} &= \overline{x \cdot y} \end{aligned} \tag{3.2}$$

{okruhZ:EQOPER}

{okruhz:TVRZNJEOKRUH}

**Tvrdenie 3.3.19.** *Nech $n \in \mathbb{Z}$, $n \neq \pm 1$. Potom vzťahy* (3.2) *určujú dobre definované binárne operácie na množine $\mathbb{Z}/(n)$.*

*Množina $\mathbb{Z}/(n)$ s týmito operáciami tvorí komutatívny okruh s jednotkou.*

Ako uvidíme, jediná netriviálna časť je ukázať, že tieto operácie sú dobre definované – ostatné veci už pôjdu veľmi ľahko. To, že takto definované sčitovanie a násobenie sú dobre definované, znamená, že výsledok nezávisí od toho, akým prvkom sme danú triedu reprezentovali. Niečo o tom, kedy je nejaká funkcia dobre definovaná, sme spomenuli v časti 2.2.3.

Keby sme skúsili operácie definovať iným spôsobom – tak, že by to definícia bola založená na celej množine, bez výberu konkrétneho reprezentanta – mohli by sme sa zaobísť bez toho, aby sme potrebovali overovať takúto vec. Iná možnosť definície súčtu, ktorá vedie k tomu istému výslekdu, je naznačená v úlohe 3.3.8.

*Dôkaz. Operácie sú dobre definované.* Skúsme najprv poriadne zapísať, čo takáto vec znamená. Pýtame sa na to, či z $\overline{x}_1 = \overline{x}_2$ a $\overline{y}_1 = \overline{y}_2$ vyplýva aj $\overline{x_1 + x_2} = \overline{y_1 + y_2}$ a tiež $\overline{x_1 \cdot x_2} = \overline{y_1 \cdot y_2}$. (Ak sme sčítali resp. vynásobili dve triedy na základe predpisu z (3.2), tak chceme vedieť, či výsledok vyjde vždy rovnaký.)

Vieme, že $\overline{x}_1 = \overline{x}_2$ je to isté ako $x_1 \equiv x_2 \pmod{n}$. (Pozri aj úlohu 2.2.1.) To znamená, že sa vlastne pýtame na takúto implikáciu:

$$\left.\begin{aligned} x_1 &\equiv x_2 \pmod{n} \\ y_1 &\equiv y_2 \pmod{n} \end{aligned}\right\} \quad \Rightarrow \quad \begin{aligned} x_1 + y_1 &\equiv x_2 + y_2 \pmod{n} \\ x_1 \cdot y_1 &\equiv x_2 \cdot y_2 \pmod{n} \end{aligned}$$

Toto sú vlastnosti, o ktorých vieme, že pre kongruencie platia – sú to presne vlastnosti z tvrdenia 3.3.18.

$\mathbb{Z}/(n)$ *tvorí komutatívny okruh s jednotkou.* Všetky ďalšie vlastnosti sú už teraz pomerne jasné.

Pretože sčitovanie v $\mathbb{Z}$ je asociatívne a komutatívne, dostávame aj:

$$\begin{aligned} \overline{x} + \overline{y} &= \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x} \\ \overline{x} + (\overline{y} + \overline{z}) &= \overline{x + (y + z)} = \overline{(x + y) + z} = (\overline{x} + \overline{y}) + \overline{z} \end{aligned}$$

Pre násobenie je overenie oboch týchto vlastností takmer totožné:

$$\begin{aligned} \overline{x} \cdot \overline{y} &= \overline{x \cdot y} = \overline{y \cdot x} = \overline{y} \cdot \overline{x} \\ \overline{x} \cdot (\overline{y} \cdot \overline{z}) &= \overline{x \cdot (y \cdot z)} = \overline{(x \cdot y) \cdot z} = (\overline{x} \cdot \overline{y}) \cdot \overline{z} \end{aligned}$$

Pre sčitovanie aj násobenie ľahko nájdeme neutrálny prvok:

$$\begin{aligned} \overline{0} + \overline{x} &= \overline{0 + x} = \overline{x} \\ \overline{1} \cdot \overline{x} &= \overline{1 \cdot x} = \overline{x} \end{aligned}$$

Súčasne ale požadujeme, aby $\overline{0} \neq \overline{1}$. T.j. chceme overiť, či

$$0 \not\equiv 1 \pmod{n}.$$

To je presne dôvod, prečo sme v predpokladoch zakázali možnosti $n = \pm 1$. (Kongruencia $0 \equiv 1 \pmod{n}$ platí práve vtedy, keď $n \mid 1$. Jediné celé čísla $n$, pre ktoré takéto niečo platí, sú $n = \pm 1$.)

Ešte chceme overiť, či pre každé $\overline{x}$ existuje inverzný prvok na sčitovanie. Na to nám ale stačí zobrať triedu $\overline{-x}$.

$$\overline{x} + \overline{(-x)} = \overline{x - x} = \overline{0}.$$

□

uhZ:POZNKONG}

**Poznámka 3.3.20.** Podobnú úvahu ešte použijeme aj na inom mieste – konkrétne vo vete 4.5.1. A už sme spomenuli, že viacero vecí z tejto časti by sa dalo robiť aj všeobecnejšie.

KONGKSKDNE}

**Poznámka 3.3.21.** Pokojne by sme sa mohli obmedziť na $n \geq 0$ a v podstate by sme nič nestratili, pretože čísla $n$ a $-n$ generujú ten istý ideál v $\mathbb{Z}$, $(n) = (-n)$. Pre $n > 1$ máme

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

(Pričom tu všetky uvedené triedy sú navzájom rôzne – t.j. $\mathbb{Z}/(n)$ má $n$ prvkov.)

Sú to v podstate inak zapísané zvyškové triedy – s ktorými sme sa už stretli v nižších ročníkoch.

{okruhZ:POZNNULA}

**Poznámka 3.3.22.** Už v dôkaze sme si vysvetlili, prečo sme vylúčili $n = \pm 1$. (Vtedy by sme takto dostali iba jednoprvkovú množinu.)

Môžeme všimnúť, že aj prípade $n = 0$ je pomerne nezaujímavý – každá trieda je jednoprvková a dostaneme okruh izomorfný so $\mathbb{Z}$.

Môžeme si tiež uvedomiť, že aritmetiku so zvyškovými triedami bežne používame v reálnom živote. Napríklad pri „výpočtoch s kalendárom alebo hodinkami“ – keď sa rozprávame napríklad o mesiacoch, dňoch v týždni, hodinách, minútach a podobne.

- Ak je dnes sobota, o tri dni bude utorok.
- Ak od niečoho, čo sa stalo v novembri, prejdú tri mesiace – vieme, že tá druhá udalosť je vo februári.
- Ak je desať hodín dopoludnia, tak o štyri hodiny bude jedna hodina popoludní. Ak trojhodinový film začal o jedenástej v noci, tak skončí o druhej. (Ak máme to šťastie, že ho môžeme pozerať bez prerušovania reklamami.)
- Ak je trištvrte na jednu (alebo dve, tri, štyri, ...) a máme sa vrátiť o polhodinu, vieme že vtedy bude štvrť.

Pri dňoch v týždni vlastne počítame modulo 7, pri mesiacoch v roku modulo 12, pri hodinách modulo 24 alebo 12, pri minútach modulo 60.

{okruhz:TVRZPJEPOLE}

**Tvrdenie 3.3.23.** *Ak $(p)$ je prvočíslo, tak $(\mathbb{Z}/(p), +, \cdot)$ je pole.*

*Dôkaz.* Vieme už, že $\mathbb{Z}/(p)$ tvorí okruh – tvrdenie 3.3.19. Potrebujeme teda ešte ukázať, že ak $\overline{a} \neq \overline{0}$, tak existuje k $\overline{a}$ inverzný prvok vzhľadom na násobenie.

Predpokladajme teda, že $a \equiv 0 \pmod{p}$, čo znamená, že $p \nmid a$. To znamená, že

$$\gcd(a, p) = 1.$$

(Pretože $p$ je prvočíslo, jediné jeho delitele v prirodzených číslach sú 1 a $p$. Teda najväčší spoločný deliteľ čísla $p$ s nejakým číslom môže byť jedine 1 alebo $p$. Ale v tomto prípade to $p$ nebude – zostáva teda iba druhá možnosť.)

Z dôsledku 3.3.8 potom dostávame, že existujú $x, y \in \mathbb{Z}$ také, že

$$ax + py = 1,$$

čo znamená, že

$$ax \equiv 1 \pmod{p}.$$

V okruhu $\mathbb{Z}/(p)$ teda dostávame rovnosť

$$\overline{a} \cdot \overline{x} = \overline{1}.$$

□

Aj túto vetu sme uvádzali najmä preto, že budeme chcieť ukázať analogický výsledok pre okruhy polynómov – veta 4.5.9. (Dokonca aj dôkaz by mal vyzerať do istej miery podobne.)

**Poznámka 3.3.24.** Všimnime si, že kongruencie by úzko súvisia s ideálmi v $\mathbb{Z}$. Pre dve čísla $a$, $b$ máme $a \equiv b \pmod{n}$ práve vtedy, keď ich rozdiel $a - b$ patrí do ideálu $(n)$.

Podobná vec ako sme urobili tu sa dá urobiť všeobecne pre ľubovoľné okruhy.

- Všeobecne pre okruhy by sme mohli definovať pojem *okruhovej kongruencie.* Je to relácia ekvivalencie, ktorá sa slušne správa vzhľadom na obe operácie.
- Takto definované kongruencie úzko súvisia s ideálmi. (Každej okruhovej kongruencii vieme priradiť ideál a obrátene, ak máme nejaký ideál $I$ na $R$, tak vieme z neho jednoducho dostať kongruenciu.)

A oboma spôsobmi – či už na základe kongruencií alebo pomocou ideálov – sa dá definovať *faktorový okruh.*

V tomto texte budeme potrebovať iba jeden konkrétny prípad tejto konštrukcie – konkrétne budeme robiť faktorový okruh z okruhu polynómov $F[x]$, zavedieme ho v časti 4.5. Z toho dôvodu sa tu nezaoberáme faktorovými okruhmi všeobecne – obmedzili sme sa na konkrétny prípad, ktorý budeme potrebovať. Ale ešte predtým sme si povedali niečo aj pre okruh $\mathbb{Z}$, keďže tento okruh dobre poznáte. V okruhu $F[x]$ funguje veľa vecí analogicky, asi pre lepšie pochopenie je užitočné vidieť túto konšturkciu najprv na jednoduchšom príklade.

### Cvičenia

{okruhZcvic:ULOASOC}

**Úloha 3.3.1.** Dokážte, že pre $a, b \in \mathbb{Z}$ z $a \mid b$, $b \mid a$ vyplýva $a = \pm b$.

$$a \mid b \wedge b \mid a \Rightarrow a = \pm b$$

okruhZcvic:ULOADELISUBS}

**Úloha 3.3.2.** Ukážte, že pre celé čísla $a$, $b$ sú tieto tri podmienky ekvivalentné:

(i) $a \mid b$;
(ii) $b \in (a)$;
(iii) $(b) \subseteq (a)$.

{okruhZcvic:ULOIDEAB}

**Úloha 3.3.3.** Nech $a$, $b$ sú celé čísla. Dokážte, že množina $\{ax + by; x, y \in \mathbb{Z}\}$ tvorí ideál v okruhu $\mathbb{Z}$.

{okruhZcvid:ULOEUKLID}

**Úloha 3.3.4.** Ukážte, že pre $a, b, c \in Z$ z $a \mid bc$ a $\gcd(a, b) = 1$ vyplýva $a \mid c$.

kruhZcvic:ULOPRIENIKNSN}

**Úloha 3.3.5.** Nech $a$, $b$ sú prirodzené čísla. Tvorí množina $(a) \cap (b)$ ideál v $\mathbb{Z}$? Ak áno, vedeli by ste nejako charakterizovať $n \in \mathbb{N}$ také, že $(n) = (a) \cap (b)$?

{okruhZcvic:ULORELEKV}

**Úloha 3.3.6.** Nech $n \in \mathbb{Z}$ a reláciu $a \sim b$ na množine $\mathbb{Z}$ je definovaná ako

$$a \sim b \qquad \Leftrightarrow \qquad a \equiv b \pmod{n}.$$

Ukážte, že je to relácia ekvivalencie. (Stručne: Relácia „kongruencia modulo $n$“ je relácia ekvivalencie na množine $\mathbb{Z}$.)

{okruhZcvic:ULOKONGOPER}

**Úloha 3.3.7.** Ukážte, že ak pre $a, b, c, d, n \in \mathbb{Z}$ platí $a \equiv c \pmod{n}$ a $b \equiv d \pmod{n}$, tak platí aj

$$a + b \equiv c + d \pmod{n}$$
$$a \cdot b \equiv c \cdot d \pmod{n}$$

{okruhZcvic:SUCETTRIED}

**Úloha 3.3.8.** Nech $x, y, n \in \mathbb{Z}$. Ukážte, že množina

$$\{a + b; a, b \in \mathbb{Z}, a \equiv x \pmod{n}, b \equiv y \pmod{n}\}$$

sa rovná zvyškovej triede čísla $x + y$ modulo $n$. T.j. že do tejto množiny patria presne také čísla $c$, ktoré spĺňajú $c \equiv x + y \pmod{n}$.

## 3.4 Polynómy a okruh $F[x]$

okruhFx:SECT}

### 3.4.1 Rovnosť, sčitovanie a násobenie polynómov

**Definícia 3.4.1.** Nech $F$ je ľubovoľné pole. Potom ľubovoľný zápis tvaru

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

kde $a_0, \ldots, a_n \in F$ nazývame *polynóm* v premennej $x$ nad poľom $F$. Prvky $a_0, \ldots, a_n$ voláme *koeficienty* polynómu $f(x)$.

Množinu všetkých polynómov nad poľom $F$ označujeme ako $F[x]$.

Ak $a_i = 0$ pre všetky $i = 1, \ldots, n$, tak $f(x) = a_0$ je *konštantný polynóm.* Ak aj $a_0 = 0$, tak je to *nulový polynóm.*

Niekedy použijeme aj stručnejší zápis pomocou sumy, t.j. polynóm zapíšeme ako

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i.$$

{okruhFx:POZNOKRUHY}

**Poznámka 3.4.2.** Polynómy by sme mohli definovať aj všeobecnejšie – namiesto poľa by sme koeficienty mohli brať z nejakého okruhu. Aby sme dostali rozumné vlastnosti, tak by sme chceli aby náš okruh bol oborom integrity, prípadne aspoň komutatívny okruh s jednotkou. Dostali by sme takto množinu $R[x]$ všetkých polynómov nad $R$. A ak $R$ je komutatívny okruh, mohli by sme sčitovanie a násobenie zaviesť podobným spôsobom, ako vysvetlíme nižšie – a dospeli by sme k okruhu $R[x]$.

My sme sformulovali definíciu pre polia – pretože pre naše účely stačí. Nanajvýš sa niekedy vyskytne situácia, že by sme chceli pracovať s polynómami, kde všetky koeficienty sú prvky nejakého podokruhu $R$ poľa $F$. (Napríklad ak pracujeme nad $\mathbb{R}$ a zaujímajú nás polynómy s celočíselnými koeficientami, tak použijeme označenie $\mathbb{Z}[x]$.)

Rovnosť polynómov definujeme tak, že sa musia zhodovať koeficienty – nanajvýš jeden z nich by mohol navyše obsahovať na začiatku nejaké členy s nulovými koeficientami. T.j. napríklad $f(x) = x^2 + x - 2$ a $g(x) = 0x^2 + x^2 + x - 2$ považujeme iba za dva rôzne zápisy toho istého polynómu.

**Definícia 3.4.3.** Dva polynómy $f(x), g(x) \in F[x]$ tvaru

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

kde $m \leq n$ považujeme za rovnaké práve vtedy, keď $a_i = b_i$ pre $i = 0, \ldots, m$ a $a_i = 0$ pre $i = m+1, \ldots, n$.

Vidíme, že každý polynóm môžeme prepísať tak, že ak sú na začiatku nejaké členy s nulovými koeficientami, tak ich vynecháme. (A dostaneme tak tvar, ktorý vyzerá pomerne štandardne.) Jediná výnimka je nulový polynóm – chceme aby náš zápis obsahoval aspoň jeden člen, takže z polynómu $f(x) = 0$ už nebudeme nič vynechávať.

Takáto definícia môže vyzerať veľmi neobvyklá a ťažkopádna. Prirodzene človeku napadne otázka, či miesto takejto formulácie – pri ktorej sme museli ešte zdôrazniť to, kedy považujeme polynómy za rovnaké – by sme nemohli jednoducho zaviesť polynómy ako *funkcie* uvedeného tvaru. Uvidíme, že odpoveď je „áno aj nie“. Vrátime sa k tomu v poznámke 3.4.23. Ale stručne sa dá povedať, že:

- Ak sú pre nás dôležité iba prípady, keď pole $F$ je nekonečné, tak by nám úplne stačilo pozerať sa na polynómy ako na funkcie.
- Ak sa však chceme zaoberať aj konečnými poľami, tak je lepšie rozlišovať polynómy a polynomické funkcie.

Tiež môže byť mätúce to, že pre polynómy a pre funkcie používame rovnaké označenie $f(x)$. Azda však z kontextu bude zvyčajne jasné, o čom hovoríme. (A v situáciách, kedy to bude nutné rozlíšiť, na chvíľu použijeme iné označenie.)

**Definícia 3.4.4.** Nech $F$ je pole a $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ je polynóm nad poľom $F$ zapísaný tak, že $a_n \neq 0$.

Potom číslo $n$ nazývame *stupeň polynómu* a označujeme $\operatorname{st} f(x) = n$. Ak $f(x)$ je nulový polynóm, tak stupeň definujeme ako $\operatorname{st} f(x) = -\infty$.

Výraz $a_n x^n$ voláme *vedúci člen* polynómu $f(x)$ a $a_n$ sa nazýva *vedúci koeficient*.

Posledný výraz $a_0$ voláme *absolútny člen* polynómu $f(x)$.

Polynóm $f(x) = a_n x^n + \cdots + a_1 x + a_0$ nazveme *normovaný* alebo *monický* polynóm, ak $a_n = 1$.

Chceli by sme teraz nejako na množine $F[x]$ zaviesť *sčitovanie* a *násobenie* – a pozrieť sa na to, či takto dostaneme okruh.

Je pomerne jasné, ako budeme sčitovať polynómy – jednoducho sčítame príslušné koeficienty. T.j. pre dva polynómy $f(x)$ a $g(x)$ definujeme ich súčet ako

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ g(x) &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \\ f(x) + g(x) &= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0) \end{aligned}$$

Resp. to isté môžeme zapísať aj stručnejšie ako:

$$\begin{aligned} f(x) &= \sum_{i=0}^{n} a_i x^i \\ g(x) &= \sum_{i=0}^{n} b_i x^i \\ f(x) + g(x) &= \sum_{i=0}^{n} (a_i + b_i) x^i \end{aligned}$$

Samozrejme, súčet chceme mať zadefinovaný aj pre polynómy rôznych stupňov. Môžeme však k jednému z nich pridať na začiatok niekoľko nulových členov tak, aby sme dostali rovnaký počet koeficientov. (Rovnosť polynómov sme definovali tak, že pridanie nulových členov polynóm nezmení.)

Aj pre násobenie polynómov máme vcelku prirodzenú predstavu o tom, čo by sme asi chceli urobiť. Sme zvyknutí bežne pracovať s polynómami s reálnymi koeficientami. Napríklad ak si vezmeme polynóm $f(x) = x^2 + x + 1$ a $g(x) = x^2 - 2x + 3$, tak vieme ich súčin dostať tak, že jednoducho všetko roznásobíme a dáme dokopy členy s rovnakými exponentami.

$$\begin{aligned} f(x)g(x) &= (x^2 + x + 1)(x^2 - 2x + 3) \\ &= x^4 - x^3 + 2x^2 - x + 3 \end{aligned}$$

Napríklad koeficient pri $x^2$ sme získali tak, že sme sa pozreli na všetky členy v prvom a druhom polynóme, kde exponenty dávajú súčet dva. T.j. sú to konkrétne tieto:

$$x^2 \cdot 3 + x \cdot (-2x) + 1 \cdot x^2 = (3 - 2 + 1)x^2.$$

Teda koeficient pri $x^k$ dostaneme tak, že sa pozrieme na členy $a_i x^i$ z prvého polynómu a $b_j x^j$ z druhého polynómu, pre ktoré $i + j = k$. Samozrejme, môže sa stať, že niektoré z týchto členov budú nulové. V uvedenom príklade členy $x^3$ vieme dostať iba ako

$$x^2 \cdot (-2x) + x \cdot x^2,$$

nemáme totiž ani v prvom ani v druhom polynóme člen obsahujúci $x^3$.

{okruhFx:DEFSUCIN}

**Definícia 3.4.5.** Nech $F$ je pole $f(x), g(x) \in F[x]$ sú polynómy určené ako

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$
$$g(x) = b_m x^m + \cdots + b_1 x + b_0.$$

Potom ich *súčin* $h(x) = f(x) \cdot g(x)$ definujeme ako polynóm

$$h(x) = c_{m+n} x^{m+n} + \cdots + c_1 x + c_0,$$

kde koeficienty sú určené predpisom

$$c_k = \sum_{i=0}^{m+n} a_i b_{k-i}, \tag{3.3}$$

{okruhFx:EQKOEFSUCIN1}

pričom položíme $b_j = 0$ ak sa v súčte vyskytnú členy, kde $j > m$ alebo $j < 0$.

Predpis pre koeficient $c_k$ by sme mohli zapísať aj ako

$$c_k = \sum_{i+j=k} a_i b_j, \tag{3.4}$$

{okruhFx:EQKOEFSUCIN2}

kde sčitujeme cez všetky celé čísla dávajúce súčet $k$; ale v prípadoch keď index je záporný alebo je vyšší než stupeň nášho polynómu berieme koeficienty ako nuly.

Takýto zápis vyzerá azda o čosi symetrickejšie.

Všetkým problémom s tým, že sme nejako museli dať pozor aj na záporné indexy by sme sa mohli vyhnúť, ak by sme jeden z polynómov doplnili nulovými koeficientami tak, aby sme

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$
$$g(x) = b_n x^n + \cdots + b_1 x + b_0.$$

A potom by sme mohli položiť

$$c_k = \sum_{i=0}^{2n} a_i b_{k-i}. \tag{3.5}$$

{okruhFx:EQKOEFSUCIN3}

Pretože sme pridali iba nulové koeficienty, nemohli sme ovplyvniť výslednú hodnotu – koeficient $c_k$ bude rovnaký ak použijeme ktorékoľvek z uvedených troch vyjadrení (3.3), (3.4) a (3.5).

Všimnime si, že ak vedúce členy polynómov $f(x)$ resp. $g(x)$ sú $a_n x^n$ a $b_m x^m$, tak v súčine ako vedúci koeficient dostaneme $a_n b_m x^{n+m}$. Pričom ak $a_n \neq 0$ a $b_m \neq 0$, tak aj $a_n b_m \neq 0$. To znamená, že pre stupeň súčinu dvoch polynómov dostaneme:

$$\operatorname{st} f(x)g(x) = \operatorname{st} f(x) + \operatorname{st} g(x) \tag{3.6}$$

{okruhFx:EQDEGSUCIN}

(Tento vzťah funguje aj pre nulový polynóm – ak sa držíme dohody, že $-\infty + n = -\infty$ a $(-\infty) + (-\infty) = -\infty$.)

Keď už máme nejako pre polynómy definované sčitovanie a násobenie, môžeme sa zamyslieť nad tým, či sme dostali skutočne okruh.

{okruhFx:TRVF

**Tvrdenie 3.4.6.** *Nech $F$ je pole. Množina $F[x]$ všetkých polynómov nad $F$ s operáciami sčitovania a násobenia zadefinovanými vyššie tvorí komutatívny obor integrity.*

*Navyše množina všetkých konštantných polynómov je podokruh, ktorý je izomorfný s $F$.*

Pretože konštantné polynómy sa pri sčitovaní a násobení správajú rovnako ako prvky poľa $F$, budeme často budeme tieto dve množiny stotožňovať. (Takéto niečo nám niektoré úvahy zjednoduší – ušetríme si pridanie jedného izomorfizmu.)

*Dôkaz.* *$(R[x], +)$ je komutatívna grupa.* Vlastnosti sčitovania sú pomerne jasné, pretože sčitovanie je definované „po súradniciach“. Dostaneme naozaj komutatívnu grupu. Neutrálny prvok je nulový polynóm $f(x) = 0$.

*Komutatívnosť násobenia.* Z viacerých vyjadrení pre koeficienty polynómu $f(x) \cdot g(x)$ sme v (3.4) uviedli

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

Pretože $a_i b_j = b_j a_i$, výsledok sa nezmení, ak vymeníme $f(x)$ a $g(x)$.

*Asociatívnosť násobenia.* Pre polynómy

$$\begin{aligned} f(x) &= a_n x^n + \cdots + a_1 x + a_0, \\ g(x) &= b_n x^n + \cdots + b_1 x + b_0, \\ h(x) &= c_n x^n + \cdots + c_1 x + c_0 \end{aligned}$$

chceme overiť, či $f(x)(g(x)h(x)) = (f(x)g(x))h(x)$.

Tu sa oplatí pozerať sa na koeficienty súčinu pomocou vzťahu (3.4). Pre ľavú aj pravú stranu dostaneme ako koeficient pri $x^l$

$$d_l = \sum_{i+j+k=l} a_i b_j c_k,$$

pričom vo výraze $a_i b_j c_k$ zátvorky môžeme vynechávať – vieme, že v okruhu $F$ je násobenie asociatívne.

*Neutrálny prvok* pre násobenie je konštantný polynóm $f(x) = 1$.

*Distributívnosť.* Máme

$$\begin{aligned} f(x) &= a_n x^n + \cdots + a_1 x + a_0, \\ g(x) &= b_n x^n + \cdots + b_1 x + b_0, \\ h(x) &= c_n x^n + \cdots + c_1 x + c_0 \end{aligned}$$

a chceme overiť, či $f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x)$. Pre polynóm na ľavej reps. pravej strane tejto rovnosti dostaneme ako koeficient pri $x^k$

$$\begin{aligned} c_k &= \sum_{i+j=k} a_i (b_j + c_j), \\ d_k &= \sum_{i+j=k} a_i b_j + a_i c_j. \end{aligned}$$

Tieto dva výrazy sa rovnajú – vďaka distributívnosti v poli $F$.

*Obor integrity.* Z (3.6) vidíme, že v $F[x]$ neexistujú delitele nuly – pri súčin dvoch nenulových polynómov nemôže mať nižší stupeň než polynómy, ktoré násobíme.

*Konštantné polynómy a $F$.* Dôkaz poslednej časti tvrdenia – o konštantných polynómoch – je pomerne priamočiary (úloha 3.4.1). □

Z (3.6) vieme povedať aj to, že súčin dvoch nenulových polynómov nemôže byť nulový. (Násobenie nenulovým polynómom nezníži stupeň.)

{okruhFx:DOSFXJEOI}

**Dôsledok 3.4.7.** *Nech $F$ je pole. Potom $(F[x], +, \cdot)$ je obor integrity.*

### 3.4.2 Dosadzovanie do polynómov

{okruhFx:SSECTDOSAD}

V tejto časti budeme pracovať aj s funkciami aj polynómami. Aby bolo jasné, čo máme na mysli, teraz budeme používať pre polynómy namiesto $f(x)$ iba jednopísmenkové označenie $f$. (A označenie $f(x)$ si necháme pre funkcie resp. funkčné hodnoty.) Neskôr sa opäť vrátime k takému označeniu ako doteraz – a ak by niekedy bolo nejasné, s čím pracujeme, tak sa to budeme snažiť zdôrazniť, či ide o polynóm alebo o funkciu.

Nie je ťažké si uvedomiť, že do polynómov sa dá dosadzovať. Konkrétne, ak máme polynóm

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

a nejaký prvok $c \in F$, tak výraz

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

Tak ako tu, budeme používať označenie $f(c)$ pre hodnotu, ktorú dostaneme, ak do polynómu $f$ dosadíme $c$.

Ak si zvolíme konkrétne $c$, tak sme takto priradili každému polynómu $f \in F[x]$ nejaký prvok $f(c) \in c$. Sčitovanie a násobenie polynómov je definovaná tak, že dosadzovanie do polynómov funguje „rozumne“.

{okruhFx:TVRDOSAD}

**Tvrdenie 3.4.8.** *Nech $F$ je pole a $c \in F$. Potom zobrazenie*

$$\varphi_c \colon F[x] \to F$$
$$\varphi_c \colon f \mapsto f(c)$$

*je okruhový homomorfizmus. T.j. platí*

$$(f+g)(c) = f(c) + g(c)$$
$$(fg)(c) = f(c) \cdot g(c)$$

*Tento homomorfizmus voláme* dosadzovací homomorfizmus.

Stručne sa dá povedať to, že uvedené tvrdenie platí preto, že násobenie a sčitovanie sme definovali presne takým spôsobom, aby takéto niečo fungovalo. (Keď sme definovali súčin polynómov, pozreli sme sa na to, ako by sme roznásobili výrazy predstavujúce polynómy, ak by sme namiesto $x$ mali nejaký prvok z poľa. A aj rovnosť polynómov je definovaná tak, že sa môžu líšiť nanajvýš o nejaké členy s nulovými koeficientmi – takéto členy neovplyvania výsledok, ktorý dostaneme po dosadení.)

Teda dôkaz spočíva vlastne v tom, že si uvedomíme, čo dostaneme po úprave dvoch výrazov tvaru

$$(a_n c^n + a_{n-1} c^{n-1} + \cdots + a_0)(b_m c^m + b_{m-1} c^{m-1} + \cdots + b_0)$$

a tiež to, že pri úpravách sme využívali iba vlastnosti, ktoré platia v každom poli (dokonca v každom komutatívnom okruhu).

V súvislosti s polynómami by sme sa mohli zaoberať aj *polynomickými funkciami,* t.j. funkciami $f\colon F \to F$ tvaru

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

Množinu všetkých polynomických funkcií označíme $F\langle x\rangle$.

Ak pre polynomické funkcie zoberieme obvyklé sčitovanie a násobenie, tak dostaneme komutatívny okruh s jednotkou. (Je to podokruh okruhu všetkých funkcií z $F$ do $F$, ktorý sme videli v úlohe 3.1.4.)

$$\psi\colon F[x] \to F\langle x\rangle$$
$$\psi\colon f \mapsto f(x)$$

t.j. polynómu $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ priradíme funkciu $f\colon F \to F$ určenú predpisom

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

Toto zobrazenie úzko súvisí s dosadzovacím homomorfizmom. Rozdiel je v tom, že pri dosadzovacom morfizme sme mali zafixované jedno konkrétne $c \in F$, tu pracujeme so všetkými prvkami poľa $F$.

{okruhFx:TVRHOMFCIE}

**Tvrdenie 3.4.9.** *Zobrazenie $\psi\colon F[x] \to F\langle x\rangle$ definované vyššie je okruhový homomorfizmus.*

Zdôvodnenie tohto faktu spočíva opäť iba v tom, že si uvedomíme, že $(f+g)(c) = f(c) + g(c)$ a $(fg)(c) = f(c)\cdot g(c)$. (T.j. tie isté dve podmienky ako pri dosadzovacom homomorfizme.)

A ešte si uvedomíme, ako funguje sčitovanie a násobenie funkcií. Takže vďaka tomu, že uvedené rovnosti platia pre všetky $c \in F$ dostávame rovnosti týchto funkcií:

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

{okruhFx:PRIKLZ2FUN}

**Príklad 3.4.10.** Pozrime sa pole $\mathbb{Z}_2$ a zoberme si polynómy

$$f = x^2 + x$$
$$g = 0$$

Zodpovedajúce funkcie $f, g\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ sa rovnajú, pretože pre každý prvok $a \in \mathbb{Z}_2$ platí $a^2 + a = 0$.

Ak počítame v $\mathbb{Z}_2$, tak naozaj máme

$$0^2 + 0 = 0 + 0 = 0$$
$$1^2 + 1 = 1 + 1 = 0$$

Teda vo všeobecnosti polynómy a polynomické funkcie nemusia byť to isté.

Neskôr si ukážeme, že pre nekonečné polia takýto problém nemôže nastať (dôsledok 3.4.22 a poznámka 3.4.23). Ale ak chceme pracovať aj s konečnými poľami, tak musíme tieto dva pojmy rozlišovať.

### 3.4.3 Veta o delení so zvyškom

{SSECTLONGDIV}

**Tvrdenie 3.4.11** (Veta o delení so zvyškom)**.** *Nech $f(x), g(x) \in \mathbb{Z}$ a $g(x) \neq 0$. Potom existujú celé polynómy $q(x), r(x) \in F[x]$ také, že platí*

$$f(x) = q(x) \cdot g(x) + r(x), \qquad \operatorname{st} r(x) < \operatorname{st} g(x).$$

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

*Polynóm $q(x)$ budeme volať* podiel *a polynóm $r(x)$* zvyšok *po delení polynómu $f(x)$ polynómom $g(x)$. Budeme používať označenie $r(x) = f(x) \bmod g(x)$.*

Dôkaz v podstate spočíva v tom, že zapíšeme algoritmus, ktorý bežne používame pri delení polynómov so zvyškom.

*Dôkaz. Jednoznačnosť.* Ak máme

$$f(x) = q(x) \cdot g(x) + r(x)$$
$$f(x) = q'(x) \cdot g(x) + r'(x)$$

tak platí

$$(q(x) - q'(x))g(x) = r'(x) - r(x).$$

Ak $q(x) - q'(x) \neq 0$ tak z (3.6) vidíme, že na ľavej strane je polynóm stupňa aspoň $\operatorname{st} g(x)$. Súčasne na pravej strane máme polynóm stupňa menšieho než $\operatorname{st} g(x)$. Takáto možnosť teda nemôže nastať.

To znamená, že musí platiť $q(x) - q'(x) = 0$. Potom dostaneme aj $r'(x) - r(x) = 0$, a teda

$$q(x) = q'(x),$$
$$r(x) = r'(x).$$

*Existencia.* 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 $b_m \neq 0$. (Polynóm $g(x)$ je nenulový, dá sa teda zapísať tak, že vedúci koeficient nie je nula.)

Ak $f(x) = 0$, tak tvrdenie platí – stačí položiť $q(x) = r(x) = 0$.

Ak $m = 0$, tak $g(x) = b_0$ je konštantný polynóm. V takomto prípade môžeme jednoducho položiť $q(x) = b_0^{-1}$ a $r(x) = 0$.

Vo zvyšku dôkazu už teda môžeme predpokladať $f(x) \neq 0$ a $m \geq 1$.

Budeme postupovať indukciou vzhľadom na $n$.

1° Ak $n < m$, tak môžeme jednoducho položiť $q(x) = 0$ a $r(x) = f(x)$. Dostaneme

$$f(x) = 0 \cdot g(x) + f(x)$$

a súčasne platí $\operatorname{st} f(x) < \operatorname{st} g(x)$, teda táto voľba vyhovuje požadovaným podmienkam.

2° Predpokladajme, že tvrdenie platí pre polynómy stupňa menšieho ako $n$.

Stačí sa zaoberať prípadom $n \geq m$. (Pretože pre $n < m$ sme už tento výsledok zdôvodnili vyššie.)

Označme

$$h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x).$$

Všimnime si, že vedúci člen polynómu, ktorý odčitujeme, je rovný

$$a_n b_m^{-1} x^{n-m} \cdot b_m x^m = a_n x^n.$$

To znamená, že v $h(x)$ dostaneme pri $x^n$ nulový koeficient a

$$\operatorname{st} f(x) = h(x).$$

Teda na polynóm $h(x)$ sa dá použiť indukčný predpoklad a dostaneme takéto vyjadrenie:

$$\begin{aligned} h(x) &= q(x)g(x) + r(x), \\ f(x) &= (a_n b_m^{-1} x^{n-m} + q(x))g(x) + r(x), \end{aligned}$$

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

Dostali sme vyjadrenie pre $f(x)$ požadovaného tvaru. □

Všimnime si, že sme skutočne v dôkaze využívali vlastnosti poľa – potrebovali sme pre $b_m \neq 0$ inverzný prvok.

Môžeme si uvedomiť, že ak by platilo $b_m = 1$, tak by sme v dôkaze nepotrebovali robiť používať inverzné prvky – pozri úlohu 3.4.2.

### 3.4.4 Deliteľnosť v okruhu polynómov

{okruhFx:SSECTDELIT}

Podobne ako pri celých číslach, aj v $F[x]$ sa môžeme pozrieť na to, kedy je jeden polynóm násobkom druhého.

**Definícia 3.4.12.** Nech $F$ je pole a $f(x), g(x) \in F[x]$. Hovoríme, že $f(x)$ *delí* $g(x)$ a označujeme $f(x) \mid g(x)$, ak existuje polynóm $h(x) \in F[x]$ taký, že

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

V opačnom prípade používame označenie $f(x) \nmid g(x)$.

Na to isté sa môžeme pozerať aj cez vetu o delení so zvyškom – ak máme $g(x) = q(x)f(x) + r(x)$ pre $\operatorname{st} r(x) < \operatorname{st} f(x)$, tak

$$f(x) \mid g(x) \qquad \Leftrightarrow \qquad r(x) = 0.$$

Veľa vlastností deliteľnosti pre polynómy má veľmi podobný dôkaz ako v okruhu $\mathbb{Z}$. (Azda jediná vlastnosť, ktorá vyzerá o trochu inak, je popis toho, kedy $f(x) \mid g(x)$ a súčasne aj $g(x) \mid f(x)$.)

Pretože ich budeme často používať, aspoň si ich uveďme a v niektorých prípadoch sa pozrieme aj na dôkaz. (Niektoré dôkazy ponecháme ako cvičenie.)

**Tvrdenie 3.4.13.** *Nech $F$ je pole, $f(x), g(x), h(x) \in F[x]$. Potom platí:*

(i) $1 \mid f(x)$, $f(x) \mid 0$

(ii) *Ak* $0 \mid f(x)$, *tak* $f(x) = 0$.

(iii) $f(x) \mid f(x)$

(iv) *Ak* $f(x) \mid g(x)$ *a* $g(x) \mid h(x)$, *tak* $f(x) \mid h(x)$ .

(v) *Ak* $f(x) \mid g(x)$ *aj* $g(x) \mid f(x)$, *tak existuje* $c \in F$, $c \neq 0$ *také, že* $f(x) = cg(x)$; *a obrátene.*

$$f(x) \mid g(x) \wedge g(x) \mid f(x) \Leftrightarrow f(x) = c \cdot g(x) \text{ pre nejaké } c \in F \setminus \{0\}$$

*Dôkaz.* Posledná časť je jediná, ktorá vyzerá inak ako pre $\mathbb{Z}$, tak pre ňu uveďme aj dôkaz.

Jedna implikácie je ľahká – ak $f(x) = cg(x)$ pre nejaké $c \neq 0$, tak máme aj $g(x) = f^{-1}(x)$. Teda súčasne platí $f(x) \mid g(x)$ aj $g(x) \mid f(x)$.

Obrátene, predpokladajme, že

$$f(x) \mid g(x) \wedge g(x) \mid f(x).$$

To znamená, že existujú polynómy $f_1(x), g_1(x) \in F[x]$ také, že

$$g(x) = g_1(x)f(x)$$
$$f(x) = f_1(x)g(x)$$

Potom máme

$$g(x) = g_1(x)f_1(x)g(x).$$

Pre $g(x) \neq 0$ z tohto už vyplýva $g_1(x)f_1(x) = 1$. (Napríklad na základe tvrdenia 3.1.6.) A teda $g_1(x)$ aj $f_1(x)$ sú nenulové konštantné polynómy.

Zostáva sa už len pozrieť na prípade $g(x) = 0$. Vtedy z $g(x) \mid f(x)$ dostaneme, že aj $f(x) = 0$. □

{okruhFx:TVRDELISUCET}

**Tvrdenie 3.4.14.** *Nech $F$ je pole, $f(x), g(x), h(x) \in F[x]$.*
(i) *Ak $f(x) \mid g(x)$ a $f(x) \mid h(x)$, tak $f(x) \mid g(x) \pm h(x)$.*
(ii) *Ak $f(x) \mid g(x)$, tak aj $f(x) \mid g(x)h(x)$.*

Vlastne obe časti predchádzajúceho tvrdenia môžeme sa dajú spojiť dokopy ako takýto výsledok: Pre ľubovoľné $f(x), g(x), h(x), u(x), v(x) \in F[x]$ platí

$$f(x) \mid g(x) \wedge f(x) \mid h(x) \Rightarrow f(x) \mid u(x)f(x) + v(x)h(x).$$

Dôkaz je opäť podobný ako pre $\mathbb{Z}$ (úloha 3.4.3).

### 3.4.5 Korene polynómov, kedy sa polynomická funkcia rovná nule

Ako sme si už všimli, do polynómov sa dá dosadzovať, t.j. ak máme polynóm $f(x) = a_n x^n + \cdots + a_1 x + a_0$ a nejaké $c \in F$, tak môžeme vyjadriť hodnotu polynómu $f$ v bode $c$ ako

$$f(c) = a_n c^n + \cdots + a_1 c + a_0.$$

Môžeme si všimnúť, že hodnota $f(c)$ prirodzene súvisí s delením polynómom tvaru $x - c$.

{okruhFx:TVRKORENZVYSOK}

**Tvrdenie 3.4.15.** *Nech $F$ je pole, $f(x) \in F[x]$ a $c \in F$. Označme $r$ zvyšok po delení polynómu $f(x)$. Potom platí $f(c) = r$.*

Oplatí sa uvedomiť si, že delíme polynómom stupňa 1, teda zvyšok bude konštantný polynóm.

*Dôkaz.* Máme rovnosť polynómov

$$f(x) = q(x)(x - c) + r.$$

Ak do ľavej a pravej strany dosadíme ten istý prvok z $F$, tak stále platí rovnosť – keďže dosadzujeme do toho istého polynómu.

Ak za $x$ dosadíme $c$, tak prvý člen na pravej strane je $q(c)(c - d) = q(c) \cdot 0 = 0$, a teda dostaneme

$$f(c) = r.$$

□

Často nás budú zaujímať také prvky, pre ktoré je hodnota $f(c)$ nulová.

**Definícia 3.4.16.** Nech $F$ je pole a $f(x) \in F[x]$. Prvok $c \in F$ je *koreň polynómu* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ ak platí $f(c) = a_n c^n + \cdots + a_1 c + a_0 = 0$.

Predtým, než sa pozrieme na konkrétne príklady, nezaškodí si uvedomiť, že pre každý koreň sa z polynómu dá vyňať koreňový činiteľ.

{okruhFx:TVRFACTOR}

**Tvrdenie 3.4.17.** *Nech $F$ je pole, $f(x) \in F[x]$ a $c \in F$. Potom $c$ je koreňom polynómu $f(x)$ práve vtedy, keď $(x-c) \mid f(x)$, t.j. keď existuje polynóm $g(x)$ taký, že*

$$f(x) = (x-c)g(x).$$

*Dôkaz.* Vyplýva z tvrdenia 3.4.15, tu sa vlastne pozeráme na prípad, že zvyšok je nulový. □

V súvislosti s predchádzajúcou vetou je azda pomerne prirodzená definícia násobného koreňa:

**Definícia 3.4.18.** Nech $F$ je pole, $f(x) \in F[x]$ a $c \in F$. Hovoríme, že $c$ je *$k$-násobný koreň* polynómu $f(x)$ ak

$$(x-c)^k \mid f(x).$$

Z tvrdenia 3.4.17 vieme dostať fakt, že stupeň polynómu nám dáva horné ohraničenie na počet koreňov.

{okruhFx:VTPOCETKORENOV}

**Veta 3.4.19.** *Nech $f(x) \in F[x]$ je nenulový polynóm nad poľom $F$. Potom počet koreňov polynómu $f(x)$ v $F$ je nanajvýš* $\operatorname{st} f(x)$.

V podstate by malo byť toto tvrdenie zrejmé – ak by sme mali $n+1$ koreňov, kde $n = \operatorname{st} f(x)$, tak polynóm $f(x)$ je násobok polynómu $(x-c_0)(x-c_1)\cdot(x-c_n)$, ktorý má stupeň $n+1$.

Formálne dôkaz môžeme zapísať indukciou.

*Dôkaz.* 1° Ak $f(x) = a_1 x + a_0$, tak vieme priamo vypočítať jediný koreň

$$c = -a_0 a_1^{-1}.$$

2° Nech $\operatorname{st} f(x) = n$. Predpokladajme, že uvedené tvrdenie platí pre polynómy stupňa menšieho než $n$.

Nech $c$ je nejaký koreň polynómu $f(x)$. Potom máme

$$f(x) = (x-c)g(x)$$

a $\operatorname{st} g(x) = n-1$. Podľa indukčného predpokladu má polynóm $g(x)$ nanajvýš $n-1$ koreňov.

Korene polynómu $f(x)$ sú $c$ a všetky korene polynómu $g(x)$. Teda ich je spolu nanajvýš $n$. □

Veta 3.4.19 nám ako dôsledok hneď dáva:

{okruhFx:TVRNULOVY}

**Tvrdenie 3.4.20.** *Nech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ je polynóm nad poľom $F$ stupňa $n$. Predpokladajme navyše, že $F$ obsahuje aspoň $n+1$ rôznych prvkov.*

*Ak $f(c) = 0$ pre všetky $c \in F$, tak $a_0 = a_1 = \cdots = a_n = 0$ a $f(x)$ je nulový polynóm.*

Špeciálne si môžeme všimnúť, že takýto výsledok platí v každom nekonečnom poli.

Tento výsledok nám vlastne hovorí, že polynomická funkcia je nulová iba ak všetky koeficienty sú nulové. Dostaneme to iba za predpokladu, že máme dostatočne veľa rôznych prvkov – v príklade 3.4.10 sme si ukázali polynóm stupňa dva nad poľom $\mathbb{Z}_2$, pre ktorý to neplatí.

Z tvrdenia 3.4.20 dostávame nasledujúce kritérium o rovnosti polynomických funkcií.

x:DOSROVNOST}

**Dôsledok 3.4.21.** *Nech $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ a $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ sú polynómy nad poľom $F$, pričom $F$ obsahuje aspoň $n+1$ rôznych prvkov.*

*Ak $f(c) = g(c)$ pre všetky $c \in F$ tak platí*

$$a_i = b_i$$

*pre $i = 0, 1, \ldots, n$.*

*Dôkaz.* Máme takéto polynómy:

$$\begin{aligned} f &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \\ g &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0 \\ f - g &= (a_n - b_n)x^n + (a_{n-1} - b_{n-1})x^{n-1} + \cdots + (a_0 - b_0) \end{aligned}$$

Vieme, že pre každé $c \in F$ platí $(f-g)(c) = 0$. Potom z tvrdenia 3.4.20 máme $a_n - b_n = a_{n-1} - b_{n-1} = \cdots = a_0 - b_0 = 0$. □

{okruhFx:DOSIZOMFCIE}

**Dôsledok 3.4.22.** *Ak $F$ je nekonečné pole, tak homomorfizmus $\psi\colon F[x] \to F\langle x\rangle$ z tvrdenia 3.4.9 je injektívny, a teda okruh polynómov a okruh polynomických funkcií sú izomorfné.*

$$F[x] \cong F\langle x\rangle$$

{okruhFx:POZNFCIE}

**Poznámka 3.4.23.** Na tomto mieste by azda už mohla byť jasná vec, ktorú už niekoľkokrát sme spomenuli.

Ak $F$ je nekonečné pole, tak okruh polynómov $F[x]$ aj okruh polynomických funkcií $F\langle x\rangle$ sú dva izomorfné okruhy – a teda pre akékoľvek účely sú úplne rovnocenné. Pritom pracovať s polynomickými funkciami by nám ušetrilo nejaké veci, ktoré sme museli robiť – funkcie vieme sčitovať, násobiť, dosadzovať do nich, vieme kedy rovnajú. Pretože polynómy sme nedefinovali ako funkcie, museli sme definovať rovnosť, súčet, súčin a zdôvodniť nejaké vlastnosti dosadzovania.

Takže ak by nás zaujímal iba prípad, keď $F$ je nekonečné pole, viacero vecí by sme vedeli urobiť o čosi jednoduchšie. V rámci tohto textu by sme chceli ukázať aj nejaké výsledky o konečných poliach – a pri nich sa nám budú hodiť aj nejaké výsledky o polynómoch.

Niekedy sa nám bude hodiť pre polynóm s celočíselnými koeficientami vedieť nájsť jeho racionálne korene. Platí nasledujúci výsledok:

{VTRACKOR}

**Veta 3.4.24.** *Nech $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ pričom $a_n \neq 0$ a všetky koeficienty sú celé čísla. Ak racionálne číslo $\frac{p}{q}$ je koreňom polynómu $f(x)$, pričom $\gcd(p,q) = 1$, tak platí*

$$p \mid a_0, \qquad q \mid a_n.$$

Dôkaz tejto vety sme ponechali ako cvičenie – úloha 3.4.8. (Pravdepodobne ste sa s týmto výsledkom však už stretli na bakalárskom štúdiu.)

Z vety 3.4.24 napríklad hneď vidíme, že ak monický polynóm má racionálne korene, tak to v skutočnosti nemôžu byť zlomky – iba celé čísla.

{DOSRACKORMON

**Dôsledok 3.4.25.** *Ak $f(x)$ je monický polynóm s celočíselnými koeficientami a $\alpha$ je nejaký racionálny koreň polynóm $f(x)$, tak platí $\alpha \in \mathbb{Z}$.*

*Dôkaz.* Ak máme $\alpha = \frac{p}{q}$ pre nejaký monický polynóm, tak z vety 3.4.24 dostávame $q = \pm 1$, čiže $\alpha = \pm p$ je celé číslo. □

{orkuhFx:PRIK

**Príklad 3.4.26.** Napríklad vidíme, že polynómy $f(x) = x^2 - 2$ a $g(x) = x^3 - 2$ nemajú racionálne korene. (Z vety 3.4.24 resp. z dôsledku 3.4.25 dostaneme ako jediné prípustné hodnoty $\pm 1$ a $\pm 2$, žiadne z týchto čísel nie je koreňom.)

Z toho opäť dostávame už známy fakt, že $\sqrt{2}$ aj $\sqrt[3]{2}$ sú iracionálne.

**Príklad 3.4.27.** Uvedený postup sa dá využiť na to, aby sme pre nejaký zadaný polynóm s celočíselnými (prípadne racionálnymi) koeficientami našli všetky jeho racionálne korene.

### 3.4.6 Ideály v okruhu polynómov

{okruhFx:SSECTIDE}

Keďže budeme pracovať s ideálmi, tak nie je zlé si uvedomiť, že aj tu (podobne ako v celých číslach) sú ekvivalentné podmienky:

- $f(x) \mid g(x)$
- $g(x) \in (f(x))$
- $(g(x)) \subseteq (f(x))$

Napríklad 3.4.14 by sme mohli zdôvodniť aj tak, že násobky daného polynómu tvoria ideál, a teda sú uzavreté na súčet, rozdiel a aj na násobenie ľubovoľným polynómov.

Takisto ako v $\mathbb{Z}$, aj tu vieme ukázať, že každý ideál v $F[x]$ je hlavný – a opäť pri tom pomôže veta o delení so zvyškom.

{okruhFx:TVROHI}

**Tvrdenie 3.4.28.** *Nech $F$ je pole a $I \subseteq F[x]$ je ideál v okruhu $(F[x], +, \cdot)$. Potom existuje polynóm $a(x) \in F[x]$ taký, že*

$$I = (a(x)) = \{a(x)f(x); f(x) \in F[x]\}.$$

*Ak navyše pridáme podmienku, že polynóm $a(x)$ je monický alebo nulový, tak je polynóm $a(x)$ ideálom $I$ jednoznačne určený.*

Dôkaz sa bude do istej miery ponášať na dôkaz analogického tvrdenia pre $\mathbb{Z}$ (tvrdenie 3.3.4). Tam sme vybrali z $I$ najmenší kladný prvok. Tu namiesto toho budeme brať polynóm najnižšieho možného stupňa.

*Dôkaz. Jednoznačnosť.* Nech by platilo $(a(x)) = (b(x))$ pre nejaké dva monické polynómy. To znamená, že jeden z nich dostaneme z druhého vynásobením nejakou nenulovou konštantou $c$. Ale pretože oba polynómy sú monické, jediná možnosť je $c = 1$.

*Existencia.* Vieme, že $I \neq \emptyset$.

Ak by platilo $I = \{0\}$, tak môžeme zobrať $a(x) = 0$.

Zaoberajme sa teda už iba prípadom, že $I \neq \{0\}$. To znamená, že v $I$ máme aspoň jeden polynóm, ktorého stupeň je nejaké nezáporné celé číslo. (T.j. jeho stupeň nie je $-\infty$.)

Nech $f(x)$ je polynóm najmenšieho možného stupňa v $I \setminus \{0\}$. (Taký polynóm existuje, lebo množina $\{\operatorname{st} f(x); f(x) \in I \setminus \{0\}\}$ je neprázdna zdola ohraničená podmnožina celých čísel.) Tento polynóm vynásobme $a_n^{-1}$, kde $a_n$ je jeho vedúci koeficient, a dostaneme tak nový polynóm

$$a(x) = a_n^{-1} f(x),$$

ktorý je už monický.

Chceme ukázať, že $I = \{(a(x))\}$. Ľahko vidíme, že $(a(x)) \subseteq I$, chceme ale ukázať opačnú inklúziu.

Zoberme si ľubovoľný polynóm $g(x) \in I$. Podľa vety o delení so zvyškom existujú polynómy $q(x)$ a $r(x)$ také, že

$$g(x) = q(x)a(x) - r(x), \qquad \operatorname{st} r(x) < \operatorname{st} a(x).$$

Z rovnosti

$$r(x) = g(x) - q(x)a(x)$$

vidíme, že aj $r(x)$ patrí do $I$. Pretože jeho stupeň je menší než stupeň polynómu $a(x)$, tak z minimality dostávame $r(x) = 0$. Teda

$$g(x) = q(x)a(x)$$

a $g(x) \in a(x)$.

□

Podobne ako pre celé čísla, aj pre polynómy vieme zadefinovať ich najväčší spoločný deliteľ.

{okruhFx:DEFNSD}

**Definícia 3.4.29.** Nech $F$ je pole a $f(x), g(x) \in F[x]$. Hovoríme, že polynóm $d(x) \in F[x]$ je *najväčší spoločný deliteľ* polynómov $f(x)$ a $g(x)$, ak platí

- $d(x) \mid f(x)$, $d(x) \mid g(x)$
- Pre ľubovoľný polynóm $c(x) \in F[x]$ taký, že $c(x) \mid f(x)$ a $c(x) \mid g(x)$ platí aj $c(x) \mid d(x)$.

$$c(x) \mid f(x) \wedge c(x) \mid g(x) \Rightarrow c(x) \mid d(x)$$

Polynóm $d(x)$ nie je podmienkami z definície 3.4.29 určený jednoznačne. Pre ľubovoľné dva polynómy spĺňajúce uvedené podmienky však máme $d(x) \mid d'(x)$ a súčasne aj $d'(x) \mid d(x)$; to znamená, že sa líšia iba vynásobením nenulovou konštantou.

Ak navyše požadujeme, že polynóm $d(x)$ je monický alebo nulový, tak už je týmito podmienkami určený jednoznačne a v takomto prípade ho budeme označovať

$$d(x) = \gcd(f(x), g(x)).$$

{okruhFx:TVRNSDIDE}

**Tvrdenie 3.4.30.** *Nech $F$ je pole a $f(x), g(x), d(x) \in F[x]$. Potom množina*

$$I = \{u(x)f(x) + v(x)g(x); u(x), v(x) \in F[x]\}$$

*je ideál v okruhu $F[x]$.*

*Polynóm $d(x)$ je najväčší spoločný deliteľ polynómov $f(x)$ a $g(x)$ práve vtedy, keď $(d(x)) = I$.*

$$(d(x)) = \{u(x)f(x) + v(x)g(x); u(x), v(x) \in F[x]\}$$

*Dôkaz.* Fakt, že $I$ je ideál sa overí pomerne jednoducho priamo z definície – takže toto ponecháme ako cvičenie (úloha 3.4.4).

Zaujímavejšia je asi druhá časť tvrdenia. Do istej miery sa dá povedať, že si stačí uvedomiť, aký je vzťah medzi deliteľnosťou, inklúziou hlavných ideálov a n.s.d.

Všimnime si najprv ako podmienku, že nejaký polynóm delí $f(x)$ aj $g(x)$, môžeme preformulovať v reči ideálov.

Podmienka, že $c(x) \mid f(x)$ a súčasne $c(x) \mid g(x)$ sa ekvivalentne dá povedať tak, že

$$f(x), g(x) \in (c(x)).$$

Nie je veľmi ťažké si uvedomiť to, že ďalšia možnosť ako ju môžeme ekvivalentne vyjadriť, je

$$I \subseteq (c(x)).$$

Uvedomili sme si teda, že platí takáto ekvivalencia:

$$I \subseteq (c(x)) \qquad \Leftrightarrow \qquad c(x) \mid f(x) \wedge c(x) \mid g(x). \tag{3.7}$$ {okruhFx:EQSP

Pozrime sa na to, čo nám ešte chýba na dokončenie dôkazu.

$\boxed{\Rightarrow}$ Predpokladajme, že $d(x)$ je najväčší spoločný deliteľ $f(x)$ a $g(x)$. Prvá podmienka z definície 3.4.29 nám vlastne hovorí, že $I \subseteq (d(x))$ – toto je presne vec, ktorá je vyjadrená ekvivalenciou (3.7).

Súčasne vieme, že $I$ je hlavný ideál (tvrdenie 3.4.28), teda existuje polynóm $c(x)$ taký, že $I = (c(x))$. Takýto polynóm je podľa (3.7) spoločným deliteľom $f(x)$ aj $g(x)$, čo znamená, že $c(x) \mid d(x)$ (opäť z definície 3.4.29). To je ale v reči ideálov môžeme zapísať ako $(d(x)) \subseteq (c(x))$, čiže máme

$$(c(x)) = I \subseteq (d(x)) \subseteq (c(x)).$$

Zistili sme, že v skutočnosti všetky uvedené inklúzie musia byť rovnosťami a platí

$$I = (d(x)).$$

$\boxed{\Leftarrow}$ Predpokladajme, že $(d(x)) = I$. Opäť si stačí uvedomiť, že z (3.7) vidíme, že $d(x)$ je deliteľom $f(x)$ aj $g(x)$.

Nech teraz $c(x) \mid f(x)$ aj $c(x) \mid g(x)$. Znovu môžeme použiť (3.7) na to, aby sme dostali

$$(d(x)) \subseteq (c(x)).$$

To je ale presne to isté ako $c(x) \mid d(x)$. Overili sme tým aj druhú podmienku z definície 3.4.29. □

Z uvedeného tvrdenia dostávame existenciu $\gcd(f(x), g(x))$. Súčasne ako dôsledok dostávame Bézoutovu identitu pre polynómy.

{okruhFx:DOSBEZOUT}

**Dôsledok 3.4.31.** *Nech $F$ je pole a $f(x), g(x) \in F[x]$. Ak $d(x) = \gcd(f(x), g(x))$, tak existujú polynómy $u(x), v(x) \in F[x]$ také, že*

$$d(x) = u(x)f(x) + v(x)g(x).$$

Opäť – podobne ako pri celých číslach – aj tu by sme vedeli polynómy $u(x)$ a $v(x)$ s uvedenými vlastnosťami nájsť pomocou rozšíreného Euklidovho algoritmu – jediný rozdiel je, že teraz počítame s polynómami a nie s celými číslami. (Čiže takáto úloha je výpočtovo náročnejšia.)

### 3.4.7 Kongruencie

{okruhFx:SSECTKONG}

Veľmi podobným spôsobom ako v celých číslach, aj tu vieme pomocou deliteľnosti zadefinovať pojem kongruencie.

uhFx:DEFKONG}

**Definícia 3.4.32.** Nech $F$ je pole a $a(x), b(x), f(x) \in F[x]$. Hovoríme, že polynómy $a(x)$ a $b(x)$ sú *kongruentné modulo* $f(x)$ ak platí

$$f(x) \mid a(x) - b(x).$$

Pre takúto situáciu používame označenie $a(x) \equiv b(x) \pmod{f(x)}$.

$$a(x) \equiv b(x) \pmod{f(x)} \qquad \Leftrightarrow \qquad f(x) \mid a(x) - b(x)$$

A aj tu sa dajú dokázať základné vlastnosti kongruentnosti podobne ako v celých číslach. Pre nás bude dôležité vedieť, že ide o reláciu ekvivalencie. A tiež to, že táto relácia rešpektuje obe okruhové operácie – sčitovanie aj násobenie polynómov.

Pri celých číslach sme dôkazy jednotlivých faktov o kongruenciách vynechali – poznáte ich z nižších ročníkov. Tu aspoň niektoré spravíme.

{okruhFx:TVRRELEKV}

**Tvrdenie 3.4.33.** *Nech $f(x), a(x), b(x), c(x) \in F[x]$. Potom platí:*

(i) $a(x) \equiv a(x) \pmod{f(x)}$

(ii) *Ak* $a(x) \equiv b(x) \pmod{f(x)}$, *tak aj* $b(x) \equiv a(x) \pmod{f(x)}$. {okruhFx:itKONGTRANZ}

(iii) *Ak* $a(x) \equiv b(x) \pmod{f(x)}$ *a* $b(x) \equiv c(x) \pmod{f(x)}$, *tak aj* $a(x) \equiv c(x) \pmod{f(x)}$.

*Dôkaz.* Prvé dve časti – úlohy 3.4.6 a 3.4.7.

(iii) Ak platí $a(x) \equiv b(x) \pmod{f(x)}$ a $b(x) \equiv c(x) \pmod{f(x)}$, znamená to, že

$$f(x) \mid a(x) - b(x,)$$
$$f(x) \mid b(x) - c(x).$$

Potom $f(x)$ delí aj súčet týchto dvoch polynómov, t.j.

$$f(x) \mid (a(x) - b(x)) + (b(x) - c(x)) = a(x) - c(x).$$

Dostali sme, že $f(x)$ delí $a(x) - c(x)$, čo podľa definície znamená $a(x) \equiv c(x) \pmod{f(x)}$. □

{okruhFx:TVRKONGOPER}

**Tvrdenie 3.4.34.** *Nech $f(x), a(x), b(x), c(x), d(x) \in F[x]$.* {okruhFx:itKONGPLUS}

(i) *Ak* $a(x) \equiv c(x) \pmod{f(x)}$, $b(x) \equiv d(x) \pmod{f(x)}$, *tak platí aj* $a(x) + c(x) \equiv b(x) + d(x) \pmod{f(x)}$. {okruhFx:itKONGKRAT}

(ii) *Ak* $a(x) \equiv c(x) \pmod{f(x)}$, $b(x) \equiv d(x) \pmod{f(x)}$, *tak platí aj* $a(x) \cdot c(x) \equiv b(x) \cdot d(x) \pmod{f(x)}$.

Teda z podmienok $a(x) \equiv c(x) \pmod{f(x)}$, $b(x) \equiv d(x) \pmod{f(x)}$ vyplýva:

$$\begin{aligned} a(x) + c(x) &\equiv b(x) + d(x) \pmod{f(x)} \\ a(x) \cdot c(x) &\equiv b(x) \cdot d(x) \pmod{f(x)} \end{aligned} \tag{3.8}$$

{okruhFx:EQKONGOPER}

*Dôkaz.* Ak predpokladáme, že $a(x) \equiv c(x) \pmod{f(x)}$ aj $b(x) \equiv d(x) \pmod{f(x)}$, znamená to, že

$$f(x) \mid a(x) - c(x),$$
$$f(x) \mid b(x) - d(x).$$

Potom platí aj

$$\begin{aligned} f(x) \mid (a(x) - c(x)) + (b(x) - d(x)) \\ = (a(x) + b(x)) - (c(x) + d(x)). \end{aligned}$$

Dostali sme teda

$$a(x) + c(x) \equiv b(x) + d(x) \pmod{f(x)},$$

čím sme dokázali (i).

Súčasne máme aj

$$\begin{aligned} f(x) \mid (a(x) - c(x))b(x) + c(x)(b(x) - d(x)) \\ = a(x)c(x) - b(x)d(x). \end{aligned}$$

Toto je presne kongruencia

$$a(x) \cdot c(x) \equiv b(x) \cdot d(x) \pmod{f(x)},$$

dokázali sme teda aj časť (ii). □

kruhFxcvic:ULOKONSTPOLY}

**Cvičenia**

**Úloha 3.4.1.** Nech $F$ je pole. Ukážte, že zobrazenie, ktoré prvku $c \in F$ priradí zodpovedajúci konštatný polynóm, je injektívny homomorfizmus z $F$ do $F[x]$. (A teda $F$ je izomorfné s podokruhom okruhu $(F[x], +, \cdot)$ pozostávajúcim zo všetkých konštantných polynómov.)

okruhFxcvic:ULODELMONIC}

**Úloha 3.4.2.** Nech $f(x), g(x) \in \mathbb{Z}[x]$ sú polynómy s celočíselnými koeficientami a navyše $g(x)$ je monický. Dokážte, že potom aj podiel a zvyšok $f(x)$ po delení polynómom $g(x)$ sú polynómy s celočíselnými koeficientami.

T.j. ak

$$f(x) = q(x) \cdot g(x) + r(x), \qquad 0 \leq \operatorname{st} r(x) < \operatorname{st} g(x),$$

okrohFxcvic:ULODELIKOMB}

tak všetky koeficienty v $q(x)$ aj $r(x)$ sú celé čísla.

**Úloha 3.4.3.** Nech $F$ je pole. Dokážte, že pre ľubovoľné $f(x), g(x), h(x), u(x), v(x) \in F[x]$ platí

$$f(x) \mid g(x) \wedge f(x) \mid h(x) \Rightarrow f(x) \mid u(x)f(x) + v(x)h(x).$$

{okrohFxcvic:ULOIDEDVA}

**Úloha 3.4.4.** Nech $F$ je pole a $f(x), g(x) \in F[x]$. Dokážte, že množina

$$I = \{u(x)f(x) + v(x)g(x); u(x), v(x) \in F[x]\}$$

tvorí ideál v $F[x]$.

Dokážte ďalej, že pre každý ideál $J$ v $F[x]$ vyhovujúci podmienkam $f(x), g(x) \in J$ platí $I \subseteq J$. (T.j. $I$ je spomedzi všetkých ideálov obsahujúcich $f(x)$ aj $g(x)$ najmenší vzhľadom na inklúziu.)

kruhFxcvic:ULOBKOMPLBIN}

**Úloha 3.4.5.** Nájdite všetky komplexné korene polynóm $f(x) = x^4 + 1$.

okruhFxcvic:ULOKONGREFL}

**Úloha 3.4.6.** Dokážte: Ak $a(x), f(x) \in F[x]$, tak platí

$$a(x) \equiv a(x) \pmod{f(x)}.$$

{okruhFxcvic:ULOKONGSYM}

**Úloha 3.4.7.** Dokážte: Ak $a(x), b(x), f(x) \in F[x]$, tak platí

$$a(x) \equiv b(x) \pmod{f(x)} \qquad \Rightarrow \qquad b(x) \equiv a(x) \pmod{f(x)}.$$

{okruhFxcvic:ULORACKOR}

**Úloha 3.4.8.** Nech $\alpha = \frac{p}{q}$, kde $p, q \in \mathbb{Z}$ a $q \neq 0$. Dokážte, že ak $\alpha$ je koreňom polynóm $f(x) = a_n x^n + \cdots + a_1 x + a_0$ takého, že $a_0, \ldots, a_n \in \mathbb{Z}$, $a_n \neq 0$, tak nutne platí $p \mid a_0$ a $q \mid a_n$.

# Kapitola 4

# Polia a rozšírenia polí

## 4.1 Pole – definícia a základné vlastnosti

{defpola:SECT}

S pojmom poľa ste sa už pravdepodobne stretli. Napríklad pri definícii vektorového priestoru – hoci pre mnohé aplikácie nám stačia vektorové priestory nad $\mathbb{R}$ či $\mathbb{C}$, vektorový priestor ste definovali nad ľubovoľným poľom. (A na tomto predmete sa objavia aj situácie, kedy sa nám bude hodiť pracovať aj s vektorovými priestormi nad inými poľami.) Tiež ste sa s nimi mohli stretnúť, keď ste sa učili o polynómoch – aj tu ste pracovali s polynómami nad ľubovoľným poľom.

{defpola:DEFPOLA}

**Definícia 4.1.1.** Nech $F$ je ľubovoľná množina, $+$ a $\cdot$ sú binárne operácie na množine $F$. Trojicu $(F, +, \cdot)$ nazveme *pole*, ak je to komutatívny okruh s jednotkou na navyše pre ľubovoľný $a \in F \setminus \{0\}$ existuje inverzný prvok vzhľadom na násobenie.

$$(\forall a \in F \setminus \{0\})(\exists b \in F) a \cdot b = 1$$

**Poznámka 4.1.2.** S definíciou poľa ste sa pravdepodobne stretli prvýkrát pri štúdiu lineárnej algebry – keď ste chceli definovať vektorový priestor nad ľubovoľným poľom. Vtedy ste nedefinovali pojem okruhu, takže definícia tohto pojmu bola zapísaná trochu inak. Ale malo by byť vcelku zvládnuteľné si premyslieť, že definície s ktorými ste sa stretli na rôznych predmetoch sú ekvivalentné.

Našu definíciu by sme mohli sformulovať tak, že by sme vymenovali všetky vlastnosti z definície komutatívneho okruhu s jednotkou (definície 3.1.1 a 3.1.3) a potom by sme pridali ešte existenciu inverzného prvku pre všetky nenulové prvky.

Ekvivalentnú definíciu by sme dostali tak, ak by sme okrem toho, že $+$ a $\cdot$ sú binárne operácie na $F$, ešte povedali, že $(F, +)$ a $(F \setminus \{0\}, \cdot)$ sú komutatívne grupy a platí distributívnosť.

Príklady polí, ktoré dobre poznáme sú komplexné čísla $(\mathbb{C}, +, \cdot)$. A tiež niektoré podpolia komplexných čísel, ako napríklad reálne čísla $(\mathbb{R}, +, \cdot)$ alebo tiež racionálne čísla $(\mathbb{Q}, +, \cdot)$.

Z konečných polí poznáme polia $\mathbb{Z}/(p)$, dôkaz, že ide skutočne o pole sme pripomenuli v tvrdení 3.3.23.

Môžeme si tiež všimnúť to, že každé pole je oborom integrity (pozri úlohu 3.1.6).

**Cvičenia**

{defpolacvic:U

**Úloha 4.1.1.** Nech $(F,+,\cdot)$ je pole $K \subseteq F$. Ukážte, že $(K,+,\cdot)$ (s tými istými operáciami – ale zúženými na podmnožinu $K$) tvorí pole, ak:
a) $1 \in K$;
b) Pre ľubovoľné $x, y \in K$ aj $x - y \in K$.
c) Pre ľubovoľné $x, y \in K$ také, že $y \neq 0$ aj $xy^{-1} \in K$.

V takejto situácii hovoríme *podpole* poľa $F$. Resp. že $F$ je *nadpole* poľa $K$.

{defpolacvic:ULOMOCNINA}

**Úloha 4.1.2.** Nech $F$ je konečné pole a $|F| = n$. Označme nenulové prvky tohto poľa ako $a_1, \ldots, a_n$, t.j. $F \setminus \{0\} = \{a_1, \ldots, a_n\}$.
a) Dokážte, že pre ľubovoľné $a \in F \setminus \{0\}$ platí $F \setminus \{0\} = \{aa_1, \ldots, aa_n\}$.
b) Ukážte, že pre ľubovoľné $a \in F$ platí $a^{n-1} = 1$.

{defpolacvic:ULOFERMAT}

**Úloha 4.1.3.** Použite úlohu 4.1.2 na zdôvodnenie, že pre ľubovoľné prvočíslo $p$ platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

(Toto je malá Fermatova veta, ktorú poznáte z iných predmetov.)

## 4.2 Komplexné čísla ako matice

{komplexmat:SECT}

S poľom komplexných čísel ste sa už stretli a dobre ho poznáte. Pri definícii komplexných čísel môžeme napríklad postupovať tak, že každé komplexné číslo $a+bi$ je jednoznačne určené dvojicou reálnych čísel $a$, $b$ a zaviesť predpisy pre operácie:

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)i\\ (a+bi)(c+di) &= (ac-bd)+(ad+bc)i\end{aligned}$$

A potom sa dajú skontrolovať rôzne vlastnosti, ktoré takto definované sčitovanie a násobenie má. Napríklad vieme skontrolovať, že $(\mathbb{C},+,\cdot)$ je pole.

Napríklad pri overovaní asociatívnosti násobenia by sme kontrolovali, či platí rovnosť

$$[(a+bi)(c+di)](e+fi) = (a+bi)[(c+di)(e+fi)]$$

pre ľubovoľné $a, b, c, d, e, f \in \mathbb{R}$. Je to síce zdĺhavé prepisovanie – ale na druhej strane je to iba mechanický výpočet; čiže keď sa človek nepomýli, tak takto skontroluje, či veci naozaj fungujú tak ako majú.

Ukážeme si inú možnosť ako sa dajú komplexné čísla zaviesť. Asi takéto niečo by bolo dosť neštandardné ako prvé stretnutie s komplexnými číslami – väčšinou komplexné čísla človek stretne skôr, než prvýkrát vidí matice a to aké vlastnosti má súčin matíc.

Ale azda nie je na škodu vidieť, že s vedomosťami ktoré už o maticiach máme, sa dajú niektoré vlastnosti komplexných čísel overiť ľahko. A azda je to aj vhodná ukážka toho, že prvky poľa môžu vyzerať aj inak – nemusia to nutne byť čísla.

Teraz teda na chvíľu zabudnime, že toto nejako súvisí s komplexnými číslami – k tomu sa vrátime neskôr. Budeme sa pozerať na množinu matíc vhodného tvaru a postupne skontrolujeme, že s obvyklým sčitovaním a násobením matíc táto množina tvorí pole. Označme

$$F = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}; a, b \in \mathbb{R}\}.$$

Ako prvú vec si môžeme všimnúť, že sčitovanie a násobenie matíc sú binárne operácie na množine $F$.

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

Niektoré z vecí, ktoré budeme počítať, sa možno o kúsoček jednoduchšie (a zrozumiteľnejšie) zapíšu, ak si takéto matice rozdelíme na súčet dvoch matíc – zvlášť dáme časť obsahujúcu $a$ a časť obsahujúcu $b$. Vo zvyšku tejto časti budeme ako $A$ označovať maticu

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Oplatí sa všimnúť si súčasne to, že $A^2 = -I$. (A teda $A^3 = -A$, $A^4 = I$.)

Môžeme teraz prepísať

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = aI + bA.$$

Keď sa vrátime k operáciam + a ·, tak vidíme, že platí:

$$(aI + bA) + (cI + dA) = (a+c)I + (b+d)A$$
$$(aI + bA) \cdot (cI + dA) = acI + (ad+bc)A + bdA^2 = (ac-bd)I + (ad+bc)A$$

Teda aj takýmto spôsobom sme sa mohli presvedčiť, že sú to skutočne binárne operácie na $F$.

Či už sa pozeráme na jedno alebo na druhé vyjadrenie, vidíme súčasne to, že operácie + a · sú na množina $F$ komutatívne. (Násobenie matíc $2\times 2$ síce vo všeobecnosti nie je komutatívne – tu sme sa ale obmedzili na pomerne peknú podmnožinu matíc, kde komutatívnosť platí.)

Fakt, že sčitovanie a násobenie sú asociatívne a distributívne máme „zadarmo“ – tieto vlastnosti platia pre sčitovanie a násobenie matíc vo všeobecnosti; zachovajú sa aj ak sa obmedzíme na nejakú podmnožinu množiny $M_{2,2}(\mathbb{R})$.

Pre sčitovanie máme neutrálny prvok – nulovú maticu – aj inverzné prvky:

$$-\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix}.$$

Neutrálny prvok na násobenie je matica $I$, ktorú dostaneme pre $a = 1$, $b = 0$. Zostáva už iba zistiť, či máme aj inverzný prvok vzhľadom na násobenie.

Platí

$$\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2.$$

Vieme, že štvorcová matica je regulárna práve vtedy, keď jej determinant je nenulový. Teda inverzná matica existuje práve vtedy, keď $a^2 + b^2 \neq 0$. Pre $a, b \in \mathbb{R}$ je to ekvivalentné s podmienkou $(a, b) \neq (0, 0)$.

Nie je však na prvý pohľad jasné, že inverzná matica tiež patrí do $F$, t.j. či má predpísaný tvar. Ak si pamätáme, ako sa inverzná matica dá vypočítať pomocou determinantu a adjungovanej matice, tak dostaneme:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Ale aj ak si takéto niečo nepamätáme, vedeli by sme inverznú maticu nájsť aj iným spôsobom. (Prinajmenšom ak nám ju niekto prezradil, tak vieme ľahko skontrolovať, či súčin týchto dvoch matíc skutočne dáva $I$.)

Dostali sme takto pole. Možno by už teraz bol vhodný čas vrátiť sa k otázke, ako to celé súvisí s komplexnými číslami.

**Tvrdenie 4.2.1.** *Množina*

$$F = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}; a, b \in \mathbb{R}\}$$

*s operáciami sčitovania a násobenia matíc tvorí pole. Toto pole je izomorfné s poľom* $(\mathbb{C}, +, \cdot)$.

*Dôkaz.* Definujme zobrazenie $f\colon \mathbb{C} \to F$ predpisom

$$f\colon a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Resp. ak preferujeme tento zápis, môžeme to isté zobrazenie zapísať ako

$$f\colon a + bi \mapsto aI + bA.$$

Je zrejmé, že toto zobrazenie je *bijekcia* – každá komplexné číslo je jednoznačne určené dvojicou reálnych čísel $a$, $b$; to isté platí pre každú maticu v množine $F$.

Treba skontrolovať aj to, či ide o *homomorfizmus* – teda chceme overiť, či pre ľubovoľné komplexné čísla $z_1 = a_1 + b_1 i$ a $z_2 = a_2 + b_2 i$ platí

$$f(z_1) + f(z_1) = f(z_1 + z_2)$$
$$f(z_1) \cdot f(z_1) = f(z_1 \cdot z_2)$$

Pre sčitovanie je to dosť priamočiare – pozrime sa na násobenie. Vypočítajme najprv, čomu sa rovná súčin $z_1$ a $z_2$:

$$z_1 z_2 = (a_1 + b_1 i)(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i.$$

Či už sa pozeráme na jeden alebo druhý zápis, stačí skontrolovať, či súčin $f(z_1) \cdot f(z_2)$ je naozaj rovný $f(z_1 z_2)$, t.j. matici určenej dvojicou $(a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1)$.

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 - b_1 b_2 & a_1 b_2 + b_1 a_2 \\ -b_1 a_2 - a_1 b_2 & -b_1 b_2 + a_1 a_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 - b_1 b_2 & a_1 b_2 + b_1 a_2 \\ -(a_1 b_2 + b_1 a_2) & a_1 a_2 - b_1 b_2 \end{pmatrix}$$
$$(a_1 I + b_1 A)(a_2 I + b_2 A) = a_1 a_2 I + (a_1 b_2 + b_1 a_2)A + b_1 b_2 A^2 = (a_1 a_2 - b_1 b_2)I + (a_1 b_2 + b_1 a_2)$$

V oboch prípadoch je výraz na pravej strane rovný $f((a_1 b_1 - a_2 b_2) + (a_1 b_2 + a_2 b_1)i)$. Teda zobrazenie $f$ je skutočne homomorfizmus. □

## 4.3 Pridávanie $\sqrt{2}$ a $\sqrt{3}$ k poľu $\mathbb{Q}$

{Qsqrt2:SECT}

Chceli by sme sa pozrieť na nejaké ďalšie príklady polí. Do istej miery sme tieto príklady zvolili aj preto, že ilustrujú teóriu, ktorú sa naučíme neskôr. Ale zatiaľ sa na ne chceme pozerať pomerne elementárnymi metódami – okrem definície poľa vlastne nebudeme používať nič, čo by ste nepoznali už zo strednej školy.

Napríklad viackrát využijeme fakt, že $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ a podobné čísla sú iracionálne – pozri úlohy 4.3.1 a 4.3.2.

### 4.3.1 K racionálnym číslam pridáme $\sqrt{2}$

qrt2:SSECTF1}

Chceme sa najprv pozrieť na to, či množina

$$F_1 = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$$

tvorí s obvyklým sčitovaním a násobením pole.

Môže byť užitočné si najprv rozmyslieť, že platí: Ak $a, b \in \mathbb{Q}$, tak

$$a + b\sqrt{2} = 0 \qquad \Leftrightarrow \qquad a = b = 0. \tag{4.1}$$

{QSQRT2:EQABSQRT2NULA}

Pokúste sa samostatne si rozmyslieť, prečo to platí – úloha 4.3.3. Možný pohľad na tento fakt je taký, že $\sqrt{2}$ a $\sqrt{3}$ sú lineárne nezávislé, ak sa na ne pozeráme ako na prvky vektorového priestoru $\mathbb{R}$ nad poľom $\mathbb{Q}$ (príklad 2.1.2).

Z tejto rovnosti pre $a, b, a', b' \in \mathbb{Q}$ máme aj

$$a + b\sqrt{2} = a' + b'\sqrt{2} \qquad \Leftrightarrow \qquad a = a' \wedge b = b'. \tag{4.2}$$

{QSQRT2:EQABSQRT2ROVNE}

Stačí si uvedomiť, že takáto rovnosť nastane práve vtedy, keď $(a - a') + (b - b')\sqrt{2} = 0$, čo je ekvivalentné s $a - a' = b - b' = 0$, čiže $a = a'$ aj $b = b'$.

Vidíme teda, kedy sa dva prvky z $F_1$ rovnajú a tiež to, že každý takýto prvok je *jednoznačne* určený dvojicou racionálnych čísel.

Poďme teraz skontrolovať jednotlivé vlastnosti, ktoré by malo $F_1$ spĺňať, ak je to pole.

V prvom rade by sčitovanie a násobenie mali byť binárne operácie na $F_1$. Pomerne ľahko sa presvedčíme, že to je pravda – pri súčine budeme musieť chvíľu roznásobovať:

$$\begin{aligned}(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) &= (a_1 + a_2) + (b_1 + b_2)\sqrt{2}\\ (a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) &= (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}\end{aligned}$$

Pomerne ľahko skontrolujeme, že pre $a_{1,2}, b_{1,2} \in \mathbb{Q}$ sú aj všetky výrazy v zátvorkách na pravej strane racionálne. Teda súčet aj súčin dvoch prvkov z $F_1$ je opäť z $F_1$.

Mali by sme skontrolovať, či sčitovanie a násobenie má neutrálny prvok. Na to si stačí uvedomiť, že $0, 1 \in F_1$.

$$\begin{aligned}0 &= 0 + 0 \cdot \sqrt{2}\\ 1 &= 1 + 0 \cdot \sqrt{2}\end{aligned}$$

S inverzným prvkom na sčitovanie nie sú problémy – ak $a, b \in \mathbb{Q}$, tak aj $-a, -b \in \mathbb{Q}$, a teda

$$-(a + b\sqrt{2}) = -a - b\sqrt{2} \in F_1.$$

Pri násobení máme trochu viac počítania, ale tiež vieme dostať

$$\begin{aligned}\frac{1}{a + b\sqrt{2}} &= \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})}\\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2}\\ &= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\end{aligned}$$

a tento výraz tiež patrí do $F_1$. (Tu sa oplatí uvedomiť si aj to, že v menovateli nedostaneme nulu. Z rovnosti (4.1) totiž vidíme, že pre racionálne $a$, $b$ máme $a + b\sqrt{2} = 0 \Leftrightarrow a - b\sqrt{2} = 0$.

Teda tento výraz má zmysel vždy, ak $a+b\sqrt{2} \neq 0$. A je to číslo patriace do $F_1$, dá sa vyjadriť ako súčet racionálneho čísla a racionálneho násobku $\sqrt{2}$.)

Ešte by sme sa mali spýtať na komutatívnosť a asociatívnosť (pre obe operácie) a tiež distributívnosť. Tie však platia – sú to vlastnosti ktoré platia pre sčitovanie a násobenie komplexných (reálnych) čísel, takže tým skôr musia platiť aj ak sa obmedzíme na menšiu množinu.

Zistili sme teda, že $F_1$ **je pole**. Je to najmenšie podpole komplexných čísel, ktoré obsahuje $\mathbb{Q}$ aj $\sqrt{2}$. (Každé takéto pole musí obsahovať všetky výrazy tvaru $a + b\sqrt{2}$.)

### 4.3.2 Skúsime pridať $\sqrt{3}$

{Qsqrt2:SSECTF2}

Chceli by sme teraz hľadať také pole, ktoré obsahuje $F_1$ a súčasne aj $\sqrt{3}$. Možno ako prvú vec sa skúsme opýtať, čo náhodou $\sqrt{3}$ už nie je prvok poľa $F_1$. (A teda v takom prípade by sme nič pridávať nemuseli.)

Pýtame sa, či platí

$$\sqrt{3} = a + b\sqrt{2}$$

pre nejaké racionálne čísla $a$, $b$.

Ak by platila uvedená rovnosť, tak nutne platí aj

$$3 = a^2 + 2ab\sqrt{2} + 2b^2$$

a z (4.2) teda dostaneme

$$\begin{aligned} 3 &= a^2 + 2b^2 \\ 0 &= 2ab \end{aligned}$$

Druhá podmienka nám hovorí, že $a = 0$ alebo $b = 0$. To by ale znamenalo, že $a^2 = 3$ alebo $2b^2 = 3$. Vieme sa však presvedčiť, že takéto racionálne čísla neexistujú. (Potrebujeme si rozmyslieť, že $\sqrt{3}$ a $\sqrt{\frac{3}{2}}$ nie sú racionálne – to je opäť otázka takého typu ako úlohy 4.3.1 a 4.3.2.)

Teda $\sqrt{3}$ nepatrí do $F_1$. Ak by sme chceli pole, ktoré obsahuje $F_1$ aj $\sqrt{3}$, tak určite obsahuje všetky prvky tvaru $a + b\sqrt{2} + q\sqrt{3}$.

Prirodzene sa nám teda núka otázka, či množina

$$F_2 = \{a + b\sqrt{2} + c\sqrt{3}; a, b, c \in \mathbb{Q}\}$$

je pole. Pomerne rýchlo zistíme, že nie – číslo $\sqrt{6}$ totiž nepatrí do $F_2$ (úloha 4.3.4).

Musíme teda pridať prinajmenšom všetky racionálne násobky $\sqrt{6}$. Skúsime si teraz rozmyslieť, že

$$F_3 = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}; a, b, c \in \mathbb{Q}\}$$

už skutočne s obvyklým sčitovaním a násobením reálnych čísel tvorí pole.

Skúsme si najprv rozmyslieť, že túto množinu môžeme prepísať pomocou poľa $F_1$. Platí totiž rovnosť

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = (a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3}.$$

Z nej vidíme, že každý prvok sa dá dostať tak, že urobíme lineárnu kombináciu čísel 1 a $\sqrt{3}$, kde koeficienty sú z $F_1$. Zistili sme, že

$$F_3 = \{x + y\sqrt{3}; x, y \in F_1\}.$$

To je veľmi podobné vyjadrenie ako sme mali pre $F_1$ – ale s tým rozdielom, že vtedy sme používali pole $\mathbb{Q}$ a teraz namiesto neho máme nejaké väčšie pole. Aj tak by ale asi mohla byť šanca, že by sa mohli dať použiť takmer analogické úvahy, ako sme robili vtedy – takže to poďme vyskúšať.

Najprv by sme sa chcel presvedčiť, že pre $a, b \in F_1$ platí

ABSQRT23NULA}
$$a + b\sqrt{3} = 0 \qquad \Leftrightarrow \qquad a = b = 0. \tag{4.3}$$

Ak platí $a + b\sqrt{3} = 0$ a $b \neq 0$, tak by to znamenalo, že $\sqrt{3} = \frac{b}{a}$, t.j. $\sqrt{3} \in F_1$. Už sme ukázali, že $\sqrt{3}$ nie je prvkom $f_1$. Zostáva teda možnosť $b = 0$; potom evidentne aj $a = 0$.

Rovnako ako v predošlom prípade, aj tu z (4.3) vyplýva, že pre $a, b, a', b' \in F_1$ platí ekvivalencia

$$a + b\sqrt{2} = a' + b'\sqrt{2} \qquad \Leftrightarrow \qquad a = a' \wedge b = b'. \tag{4.4}$$
{QSQRT2:EQABSQRT23ROVNE}

Teraz by mohlo byť zrejmé, že aj ostatné veci môžeme urobiť takmer rovnako ako v predošlom prípade.

$F_2$ je uzavreté na sčitovanie – stačí si uvedomiť, že ak $a_1, a_2, b_1, b_2 \in F_1$, tak vo výrazoch

$$\begin{aligned}(a_1 + b_1\sqrt{3}) + (a_2 + b_2\sqrt{3}) &= (a_1 + a_2) + (b_1 + b_2)\sqrt{3}\\ (a_1 + b_1\sqrt{3}) \cdot (a_2 + b_2\sqrt{3}) &= (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{3}\end{aligned}$$

všetky koeficienty na pravej strane rovnosti sú opäť z $F_1$.

Máme v $F_3$ neutrálne prvky pre sčitovanie aj násobenie:

$$\begin{aligned}0 &= 0 + 0 \cdot \sqrt{2}\\ 1 &= 1 + 0 \cdot \sqrt{2}\end{aligned}$$

Pre sčitovanie dostaneme inverzný prvok $-(a + b\sqrt{3}) = -a - b\sqrt{3}$.

A pri násobení dostávame pre $a, b \in F_1$

$$\begin{aligned}\frac{1}{a + b\sqrt{3}} &= \frac{a - b\sqrt{3}}{(a + b\sqrt{3})(a - b\sqrt{3})}\\ &= \frac{a - b\sqrt{3}}{a^2 - 3b^2}\\ &= \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{2}\end{aligned}$$

pričom aj výrazy $a^2 - 3b^2$, $a/(a^2 - 3b^2)$ aj $b/(a^2 - 3b^2)$ patria do $F_1$, teda výraz na pravej strane patrí do $F_3$.

Mali by sme skontrolovať, či pri vyjadrení inverzného prvku sme náhodou nedostali v menovateli nulu. Ale z (4.3) už vieme, že

$$a - b\sqrt{3} = 0 \Leftrightarrow a = b = 0 \Leftrightarrow a + b\sqrt{3}$$

takže pre $a + b\sqrt{3} \neq 0$ je všetko v poriadku.

Komutatívnosť, asociatívnosť i distributívnosť sa zdedia z poľa $\mathbb{R}$ resp. $\mathbb{C}$. Teda aj $F_3$ **je pole**.

Opäť sa oplatí uvedomiť si aj to, že $F_3$ je najmenšia podmnožina množiny $\mathbb{R}$, ktorá je poľom a obsahuje všetky racionálne čísla a aj čísla $\sqrt{2}$, $\sqrt{3}$.

### 4.3.3 Dostali sme $\mathbb{Q}(\sqrt{2})$ a $\mathbb{Q}(\sqrt{2},\sqrt{3})$

Podarilo sa nám teda popísať, ako vyzerajú prvky v najmenšom podpoli poľa komplexných čísel, ktoré obsahuje $\mathbb{Q}\cup\{\sqrt{2},\sqrt{3}\}$.

{Qsqrt2:DEFFU

**Definícia 4.3.1.** Nech $K$ je pole, $F$ je jeho podpole a $u_1,\dots,u_k\in F$.
Symbolom $F(u_1,\dots,u_k)$ označujeme najmenšie podpole poľa $K$ obsahujúce $F\cup\{u_1,\dots,u_k\}$.
V prípade jediného prvku budeme používať označenie $F(u)$.

Samozrejme, ak chceme všeobecne pre nejakú podmnožninu podľa $K$ hovoriť o najmenšom podpoli, ktoré túto množinu obsahuje, treba sa zmysliť aj nad tým, či také podpole naozaj existuje. Dá sa overiť, že to je skutočne tak – úloha 4.3.5

**Cvičenia**

Qsqrt2cvic:ULOSQRT2IRAC}

**Úloha 4.3.1.** Ukážte, že čísla $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ sú iracionálne.

Qsqrt2cvic:ULOSQRTNIRAC}

**Úloha 4.3.2.** Nech $n$ je prirodzené číslo. Ukážte, že $\sqrt{n}$ je iracionálne práve vtedy, keď neexistuje prirodzené číslo $k$ také, že $n=k^2$.

(Okrem dôkazu podobného typu, ako ste videli na strednej škole pre $\sqrt{2}$ a podobné čísla, by sa dalo aj pozrieť na to, čo polynóm $f(x)=x^2-n$ má racionálne korene a použiť vetu 3.4.24 resp. dôsledok 3.4.25.)

{Qsqrt2cvic:ULOSQRT2LK}

**Úloha 4.3.3.** Ukážte, že ak $a,b\in\mathbb{Q}$, tak rovnosť $a+b\sqrt{2}=0$ platí práve vtedy, keď $a=b=0$.

sqrt2cvic:ULOSQRT6NOTIN}

**Úloha 4.3.4.** Ukážte, že $\sqrt{6}$ sa nedá vyjadriť v tvare $a+b\sqrt{2}+c\sqrt{3}$ pre $a,b,c\in\mathbb{Q}$.

{Qsqrt2cvic:ULOPRIENIK}

**Úloha 4.3.5.** Nech $K$ je pole a $\{F_i; i\in I\}$ je nejaký neprázdny systém podpolí poľa $K$. Dokážte, že potom aj prienik

$$F=\bigcap_{i\in I}F_i$$

je podpole poľa $K$.

Ukážte, že pre ľubovoľnú podmnožinu $M\subseteq K$ existuje najmenšie podpole $F$ poľa $K$ také, že $M\subseteq F$. (Vďaka takémuto argumentu vieme, že existuje podpole $F(u_1,\dots,u_k)$, ktoré sme zaviedli v definícii 4.3.1.)

## 4.4 Rozšírenia polí

Zaveďme najprv terminológiu, ktorá je asi pomerne prirodzená:

{rozs:DEF}

**Definícia 4.4.1.** Nech $(K,+,\cdot)$ je pole a $F\subseteq K$ je podmnožina, ktorá s operáciami $+$ a $\cdot$ zúženými na $F$ tiež tvorí pole.
Potom hovoríme, že $F$ je *podpole* poľa $K$. A tiež hovoríme, že $K$ je *rozšírenie* poľa $F$.

**Príklad 4.4.2.** Pole $\mathbb{R}$ je rozšírením poľa $\mathbb{Q}$. Pole $\mathbb{C}$ je rozšírením poľa $\mathbb{R}$.

Bude pre nás užitočné pozerať sa na rozšírenia ako na vektorové priestory. Špeciálny prípad nasledujúcej vety sme videli v príklade 2.1.2 – a dôkaz všeobecného výsledku nie je priveľmi odlišný.

{rozs:TVRVP}

**Tvrdenie 4.4.3.** *Nech $K$ je rozšírenie poľa $F$. Potom $K$ je vektorový priestor nad poľom $F$.*

*Dôkaz.* Chceme vlastne overiť podmienky z definície vektorového priestoru (definícia 2.1.1), pričom množina vektorov je $V = K$ a pracujeme nad poľom $F$.

Ako sčitovanie vektorov aj násobenie skalárom berieme operácie z poľa $K$. (Pri násobení skalárom, sa vlastne namiesto $\cdot : K \times K \to K$ pozeráme na zúženie $F \times K \to K$.)

Rovnako ako v príklade 2.1.2, keď si napíšeme jednotlivé vlastnosti z definície vektorového priestoru, prídeme na to, že všetky z nich vyplývajú z toho, že $K$ je pole.

Konkrétne by sme mali skontrolovať, či $(K, +)$ je komutatívna grupa a či platí

$$(\forall c, d \in F)(\forall v \in K)(c + d) \cdot v = c \cdot v + d \cdot v$$
$$(\forall c \in F)(\forall v, w \in K)c \cdot (v + w) = c \cdot v + c \cdot w$$
$$(\forall c, d \in F)(\forall v \in K)(c \cdot d) \cdot v = (c \cdot d) \cdot v$$
$$(\forall v \in K)1 \cdot v = v$$

Všetky uvedené podmienky naozaj vyplýva z definície poľa. □

{rozs:DEFKONP}

**Definícia 4.4.4.** Nech $K$ je rozšírenie poľa $F$. Hovoríme, že *konečné rozšírenie,* ak $K$ má ako vektorový priestor nad poľom $F$ konečnú dimenziu.

Dimenziu tohto vektorového priestoru potom nazývame *stupeň rozšírenia* a označujeme $[K : F]$.

**Príklad 4.4.5.** Pole $\mathbb{R}$ nie je konečné rozšírenie poľa $\mathbb{Q}$. Tento fakt sme už spomenuli v príklade 2.1.6.

Pre polia $\mathbb{C}$ a $\mathbb{R}$ platí $[\mathbb{C} : \mathbb{R}] = 2$. Príkladom bázy $\mathbb{C}$ nad $\mathbb{R}$ je $\{1, i\}$.

**Príklad 4.4.6.** V časti 4.3 sme skonštruovali pole $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ – najmenšie podpole $\mathbb{R}$, ktoré obsahovalo okrem všetkých racionálnych čísel aj $\sqrt{2}$ a $\sqrt{3}$. Toto pole sme popísali ako

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}; a, b, c, d \in \mathbb{Q}\}.$$

Súčasne vieme, že platí:

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0 \qquad \Leftrightarrow \qquad a = b = c = d = 0. \tag{4.5}$$

{rozs:EQABSQRT23NULA}

Toto je vlastne trochu inak prepísaná podmienka (4.3).

Teda ak sa pozeráme na $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ako na vektorový priestor nad poľom $\mathbb{Q}$, tak vidíme, že všetky jeho prvky sú lineárne kombinácie čísel 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ a súčasne vidíme aj to, že tieto štyri prvky sú lineárne nezávislé. Teda mám bázu pozostávajúcu zo štyroch prvkov

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

Môžeme si súčasne všimnúť, že $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. Máme teda takú situáciu, že máme dve rozšírenia polí

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

a bázu pre dvojnásobné rozšírenie sme dostali z báz jednotlivých rozšírení ich vynásobením jednotlivých prvok dvoch báz:

$$1 \cdot 1 = 1$$
$$\sqrt{2} \cdot 1 = \sqrt{2}$$
$$1 \cdot \sqrt{3} = \sqrt{3}$$
$$\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$$

Toto je presne situácia, ktorú chceme všeobecnejšie popísať v nasledujúcej vete.

Poďme sa ale najprv pozrieť ešte raz ako v tomto prípade zdôvodníme, že uvedené prvky sú lineárne nezávislé. Ideálne takým spôsobom, že najprv využijeme bázu $\mathbb{Q}(\sqrt{2})$ nad poľom $\mathbb{Q}$ a potom sa pozrieme na $\mathbb{Q}(\sqrt{3},\sqrt{2})$ ako nadpole $\mathbb{Q}$.

Vlastne tu opakujeme úplne presne úvahy, ktoré sme už použili v časti 4.3 – ale nie je zlé si ich pripomenúť pred dôkazom všeobecnejšej vety.

Najprv si rozmyslíme to, že 1 a $\sqrt{2}$ sú lineárne nezávislé nad $\mathbb{Q}$. T.j. chceme vidieť, že platí

{rozs:EQABSQRT2NULA}
$$a+b\sqrt{2}=0 \qquad \Leftrightarrow \qquad a=b=0. \tag{4.6}$$

Podobne ako predtým, keď sme uviedli takúto podmienku ako (4.1), túto časť ponecháme ako cvičenie. (Je to v podstate stredoškolská úloha súvisiaca s tým, že $\sqrt{2}\notin\mathbb{Q}$.)

Teraz sa už chceme posunúť na zdôvodnenie podmienky (4.6). Pomôže nám, ak si prvky z tohto poľa zapíšeme ako

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=(a+b\sqrt{2})+(c+d\sqrt{2})\sqrt{3}.$$

Vidíme teda, že

$$\mathbb{Q}(\sqrt{2},\sqrt{3})=\{x+y\sqrt{3}; x,y\in\mathbb{Q}(\sqrt{2})\}.$$

Čiže už stačí skontrolovať, či pre $x,y\in\mathbb{Q}(\sqrt{2})$ platí

{rozs:EQABSQRT23NULA2}
$$x+y\sqrt{3}=0 \qquad \Leftrightarrow \qquad x=y=0. \tag{4.7}$$

A postup je od istej miery podobný ako pre $\sqrt{2}$ a $\mathbb{Q}$.

Ak by sme mali rovnosť $x+y\sqrt{3}=0$ pre nejaké $x,y\in\mathbb{Q}(\sqrt{2})$ a $y\neq 0$, tak po vydelení prvkom $y$ a úprav dostaneme

$$\sqrt{3}=-\frac{x}{y},$$

čo by znamenalo, že $\sqrt{3}\in\mathbb{Q}(\sqrt{2})$. V časti 4.3.2 sme overili, že $\sqrt{3}$ sa nedá zapísať ako kombinácia 1 a $\sqrt{2}$ s racionálnymi koeficientami, t.j. že nepatrí do $\mathbb{Q}(\sqrt{2})$.

Dôkaz nasledujúcej vety by sa naozaj do značnej miery mal podobať na postup uvedený vyššie resp. na úvahy z časti 4.3.2. (Nie všetky z nich sme teraz detailne opakovali.)

{rozs:VTKLF}
**Veta 4.4.7.** *Nech $K$ je konečné rozšírenia poľa $F$, $L$ je konečné rozšírenie poľa $K$. Potom $L$ je aj konečné rozšírenie poľa $F$ a pre ich stupne platí*

{rozs:EQKLF}
$$[K:F]=[K:L]\cdot[L:F] \tag{4.8}$$

*Dôkaz.* Nech prvky $u_1,\dots,u_k\in K$ tvoria bázu $K$ ako vektorového priestoru nad $F$, prvky $v_1,\dots,v_l\in L$ tvoria bázu $L$ ako vektorového priestoru nad $F$. Našim cieľom je ukázať, že

$$\{u_iv_j; i=1,\dots,k, j=1,\dots,l\}$$

je báza $F$ ako vektorového priestoru nad $K$.

Vieme, že každý prvok $x\in K$ sa má tvar

$$x=\sum_{j=1}^{l}d_jv_j$$

pre nejaké $d_1,\dots,d_l\in L$. Súčasne prvky z $L$ vieme zapísať pomocou bázy $u_1,\dots,u_k$, t.j. máme

$$d_j=\sum_{i=1}^{k}c_{ij}u_i$$

pre nejaké $c_{ij} \in F$. Po úprave máme

$$x = \sum_{j=1}^{l} \sum_{i=1}^{k} c_{ij} u_i v_j,$$

zistili sme, že $x$ je lineárna kombinácia prvkov tvaru $u_i v_j$ s koeficientami z $F$.

Zistili sme, že uvedené prvky teda skutočne generujú $K$ ako vektorový priestor nad poľom $F$. Mali by sme ešte overiť aj lineárnu nezávislosť – pri tom budeme robiť do značnej miery podobné úpravy.

Chceme overiť, či z rovnosti

$$\sum_{j=1}^{l} \sum_{i=1}^{k} c_{ij} u_i v_j = 0,$$

pričom všetky $c_{ij}$ patria do $K$, už vyplýva, že koeficienty musia byť nulové.

Ak položíme $d_j = \sum_{i=1}^{k} c_{ij} u_i$, tak pre tieto prvky máme

$$\sum_{j=1}^{l} d_j v_j = 0.$$

Súčasne $d_1, \ldots, d_l \in F$, a pretože $v_1, \ldots, v_l$ tvoria bázu, máme $d_j = 0$ pre všetky $j = 1, \ldots, l$.

To znamená, že pre každé $j$ máme

$$d_j = \sum_{i=1}^{k} c_{ij} u_i = 0.$$

Na základe lineárnej nezávislosti $u_1, \ldots, u_k$ (vo vektorovom priestore $K$ nad poľom $F$) potom dostaneme $c_{ij} = 0$ pre všetky prípustné $i$.

Overili sme, že uvedené prvky generujú $K$ a sú aj lineárne nezávislé. Máme teda bázu, ktorá má $kl$ prvkov a dimenzia $K$ ako vektorového priestoru nad $F$ je

$$[K : F] = k \cdot l = [K : L] \cdot [L : F].$$

□

**Dôsledok 4.4.8.** *Nech $K$ je konečné rozšírenia poľa $F$ a $u \in K$. Potom stupeň prvku $u$ nad $F$ delí stupeň rozšírenia $K$.*

$$[u : F] \mid [K : F]$$

*Dôkaz.* Máme rozšírenie $F \subseteq F(u) \subseteq K$. Pre tieto rozšírenia platí:

$$\begin{aligned} [K : F] &= [K : F(u)] \cdot [F(u) : F] \\ &= [K : F(u)] \cdot [u : F] \end{aligned}$$

□

## 4.5 Faktorový okruh $F[x]/(h(x))$

{faktFx:SECT}

Pre polynómy sme vedeli zadefinovať kongruenciu modulo $h(x)$ (definícia 3.4.32). Videli sme, že to je relácia ekvivalencie (tvrdenie 3.4.33) a že táto relácia rešpektuje sčitovanie aj násobenie polynómov (3.4.34). Vďaka tomu sa dá zmysluplne zaviesť sčitovanie a násobenie aj na množine všetkých tried ekvivalencie – práve to je obsahom nasledujúcej vety. (Sformulujme a dokážme túto vetu najprv všeobecne – neskôr sa pozrieme na konkrétne príklady. Konkrétne v príkladoch 4.5.2 a 4.5.3 budeme vidieť, že takto vieme dostať niektoré polia, ktoré už dobre poznáme.)

{faktFx:VTJEOKRUH}

**Veta 4.5.1.** *Nech $F$ je pole a $h(x) \in F[x]$ je polynóm nad poľom $F$ stupňa $n \geq 1$. Pre reláciu ekvivalencie „byť kongruentné modulo $h(x)$“ na množine polynómov $F[x]$ označme triedy ekvivalencie ako*

$$\overline{f(x)} = \{g(x) \in F[x]; f(x) \equiv g(x) \pmod{h(x)}\}.$$

*Množinu týchto tried ekvivalencie označme ako $F(x)/(h(x))$.*

*Pre každé $f(x) \in F[x]$ existuje práve jeden polynóm $r(x)$ taký, že $f(x) \equiv r(x) \pmod{h(x)}$ a súčasne $\operatorname{st} f(x) < \operatorname{st} h(x)$. (T.j. každá trieda je* jednoznačne *reprezentovaná polynómom stupňa menšieho než $n$.)*

*Predpisy*

{faktFx:EQOPER}

$$\begin{aligned} \overline{f(x)} + \overline{g(x)} &= \overline{f(x) + g(x)} \\ \overline{f(x)} \cdot \overline{g(x)} &= \overline{f(x) \cdot g(x)} \end{aligned} \tag{4.9}$$

*určujú dobre definované binárne operácie na množine $F(x)/(h(x))$ a $(F(x)/(h(x)), +, \cdot)$ s týmito operáciami tvorí komutatívny okruh s jednotkou. Tento okruh voláme* faktorový okruh $F[x]$ podľa $h(x)$.

*Navyše platí, že triedy konštantných polynómov, t.j. množina $\{\overline{c}; c \in F\}$, určujú podokruh, ktorý je izomorfný s poľom $F$.*

Prvú časť sme uviedli hlavne preto, aby sme vedeli jednoduchšie zapisovať operácie v okruhu $F[x]/(h(x))$. Mala by sa podobať na to, že všetky prvky v $\mathbb{Z}/(n)$ sú triedy $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

Aj zvyšok by nám mal výrazne pripomínať to čo sme videli pre $\mathbb{Z}/(n)$ v (3.2) a v tvrdení 3.3.19. (A aj dôkaz je do značnej miery analogický.)

*Dôkaz. Reprezentácia tried pomocou zvyškov.* Pre každé $f(x) \in F[x]$ existuje podľa vety o delení so zvyškom (3.4.11) polynóm $r(x)$ taký, že $f(x) = q(x)h(x) + r(x)$, čo znamená, že

$$f(x) \equiv r(x) \pmod{h(x)}.$$

Pomerne ľahko sa dá skontrolovať aj to, že nemôžu existovať dva rôzne polynómy s takýmito vlastnosťami – úloha 4.5.1.

*Operácie $+$ a $\cdot$ sú dobre definované.*

*Overenie, že ide o komutatívny okruh s jednotkou.*

*Konštantné polynómy určujú podokruh izomorfný s $F$.* □

Nasledujúce dva príklady ilustrujú ako sa počíta vo faktorovom okruhu. Súčasne môžu poslúžiť ako ilustrácie niektorých faktov, ktoré budeme chcieť dokázať vo vete 4.5.9.

{faktFX:PRIKLKOMPLEX}

**Príklad 4.5.2.** Pracujme s polynómom $p(x) = x^2 + 1 \in \mathbb{R}[x]$. Je to polynóm stupňa 2 a nemá korene v $\mathbb{R}$, takže je ireducibilný v $\mathbb{R}[x]$. To znamená, že okruh $\mathbb{R}[x]/(x^2+1)$ tvorí pole.

Súčasne vieme, že jeho prvky sú presne triedy polynómov stupňa menšieho než dva, t.j.

$$\mathbb{R}[x]/(x^2+1) = \{\overline{ax+b}; a, b \in \mathbb{R}\}.$$

Pozrime sa na to ako sa v tomto okruhu počíta. Sčitovanie vyzerá veľmi jednoducho:

$$\overline{ax+b} + \overline{cx+d} = \overline{(a+c)x + (b+d)}.$$

Chceme zistiť, čomu sa rovná $\overline{ax+b} \cdot \overline{cx+d}$; pričom by sme tento prvok opäť chceli vyjadriť pomocou nejakého polynómu prvého stupňa. Môžeme teda jednoducho polynómy vynásobiť a pozrieť sa na to, ako vyzerá zvyšok po delení polynómom $x^2+1$. Priamym výpočtom dostaneme:

$$\begin{aligned}(ax+b)(cx+d) &= acx^2 + (ad+bc)x + bd \\ &= ac(x^2+1) + (ad+bc)x + (bd-ac)\end{aligned}$$

To vlastne znamená, že

$$\overline{ax+b} \cdot \overline{cx+d} = \overline{(ab+cd)x + (bd-ac)}.$$

Iný pohľad na tú istú vec je cez počítanie s kongruenciami. Vieme, že $x^2 \equiv -1 \pmod{x^2+1}$. Ak využijeme tento fakt, tak môžeme písať:

$$\begin{aligned}(ax+b)(cx+d) &\equiv acx^2 + (ad+bc)x + bd \\ &\equiv -ac + (ad+bc)x + bd \\ &\equiv (ad+bc)x + (bd-ac)\end{aligned}$$

V týchto úpravách sme na jednom mieste nahradili výraz $x^2$ číslom $-1$. Ostatné kongruencie sú v skutočnosti rovnosti.

Ešte by sme si na tomto mieste chceli rozmyslieť, že sme vlastne dostali v podstate (t.j. až na izomorfimus) okruh komplexných čísel. T.j. tvrdíme, že

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}.$$

Konkrétne vieme ukázať, že $f\colon \mathbb{R}[x]/(x^2+1) \to \mathbb{C}$ dané predpisom

$$f\colon \overline{ax+b} \mapsto b + ai$$

je izomorfizmus.

Takéto zobrazenie je skutočne bijekcia.

Teda už len stačí porovnať sčitovanie a násobenie v jednotlivých okruhoch. Pre sčitovanie ľahko overíme, že zobrazenie $f$ ho zachováva. Pre násobenie máme v týchto dvoch okruhoch takéto vyjadrenie

$$\begin{aligned}\overline{ax+b} \cdot \overline{cx+d} &= \overline{(ad+bc)x + (bd-ac)} \\ (ai+b) \cdot (ci+d) &= (ad+bc)i + (bd-ac)\end{aligned}$$

Fakt, že nám vyšli komplexné čísla možno nie je až tak prekvapivý: Vlastne sme k poľu $\mathbb{R}$ pridali nejaké nové prvky; pričom medzi nimi bol aj prvok $u = \overline{x}$. Tento prvok spĺňa $u^2 - 1 = 0$. Prvok s takouto vlastnosťou máme aj vtedy, keď k $\mathbb{R}$ pridávame prvok $i$.

Vlastne sme teraz už videli dva ďalšie prístupy ako sa dajú skonštruovať komplexné čísla – jeden v tomto príklade ako špeciálny prípad faktorový okruhu a okrem toho sme v časti 4.2 videli, že komplexné čísla vieme dostať aj ako vhodné matice.

{faktFX:PRIKLS

**Príklad 4.5.3.** Poďme sa pozrieť na $\mathbb{Q}[x]/(x^2-2)$. Opäť vieme to, že prvky z tohto okruhu sa dajú reprezentovať polynómami prvého stupňa. Teda máme

$$\mathbb{Q}[x]/(x^2-2) = \{\overline{ax+b}; a, b \in \mathbb{Q}\}.$$

Sčitovanie je jednoduché – počítame „po súradniciach“. Opäť sa môžeme pozrieť na násobenie:

$$\begin{aligned}(ax+b)(cx+d) &\equiv acx^2 + (ab+cd)x + bd \\ &\equiv 2ac + (ab+cd)x + bd \\ &\equiv (ab+cd)x + (bd+2ac)\end{aligned}$$

Máme teda

$$\overline{ax+b} \cdot \overline{cx+d} = \overline{(ab+cd)x + (bd+2ac)}.$$

Pripomeňme ako sa násobíme v okruhu $\mathbb{Q}(\sqrt{2})$, ktorý sme videli v časti 4.3.1. Súčasne priamo zapíšme operácie tak, aby viac vynikla ich podobnosť:

$$\begin{aligned}(b+a\sqrt{2})(d+c\sqrt{2}) &= (bd+2ac) + (ab+cd)\sqrt{2} \\ \overline{b+ax} \cdot \overline{d+cx} &= \overline{(bd+2ac) + (ab+cd)x}\end{aligned}$$

Aj sčitovanie je v oboch okruhoch v podstate rovnaké, teda priradenie

$$b + a\sqrt{2} \mapsto \overline{ax+b}$$

je homomorfizmus. Súčasne to je aj bijekcia, teda dostávame izomorfizmus a platí $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}(\sqrt{2})$.

Vidíme, že aj v tomto prípade sme dostali pole, ktoré vznikne z $\mathbb{Q}$, keď k nemu pridáme koreň polynómu $x^2-2$.

### 4.5.1 Kedy je $F[x]/(h(x))$ pole?

Viackrát sme spomenuli analógiu s okruhom $\mathbb{Z}/(n)$. Takýto okruh nemusí byť pre každé $n$ poľom – stane sa to práve vtedy, keď $n$ je prvočíslo (tvrdenie 3.3.23).

Na tomto mieste sa nám hodí povedať si niečo o ireducibilných polynómoch.

{faktFx:DEFIREC}

**Definícia 4.5.4.** Nekonštantný polynóm $p(x) \in F[x]$ sa nazýva *ireducibilný polynóm* ak pre ľubovoľné $f(x), g(x) \in F[x]$ také, že

$$f(x) \cdot g(x) = p(x)$$

je niektorý z polynómov $f(x)$, $g(x)$ konštantný polynóm.

T.j. ireducibilný polynóm je taký polynóm, ktorý sa nedá zapísať ako súčin dvoch polynómov netriviálnym spôsobom.

Azda nie je na škodu si rozmyslieť:

- Pri otázke, či je daný polynóm ireducibilný, je dôležité brať do úvahy aj to, nad akým poľom pracujeme.
- Ako súvisí otázka, či je polynóm ireducibilný, s existenciou (resp. neexistenciou) koreňov.

Začnime najprv prvou otázkou – pozrieme sa na ten istý polynóm nad rôznymi poľami.

**Príklad 4.5.5.** Polynóm $f(x) = x^4 + 1$ môžeme chápať ako polynóm nad $\mathbb{Q}$, nad $\mathbb{R}$ nad $\mathbb{C}$. V závislosti od toho, aké pole použijeme, zmenia sa rozklady na súčin, ktoré môžeme dostať.

Všimnime si napríklad, že

$$\begin{aligned} x^4 + 1 &= (x^4 + 2x^2 + 1) - 2x^2 \\ &= (x^2 + 1)^2 - (\sqrt{2}x)^2 \\ &= (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1) \end{aligned}$$

Vidíme teda, že nad $\mathbb{R}$ aj nad $\mathbb{C}$ sa dá tento polynóm rozložiť na súčin dvoch polynómov stupňa 2. Teda to nie je ireducibilný polynóm ani v $\mathbb{R}[x]$ ani v $\mathbb{C}[x]$.

Môžeme sa zamyslieť aj nad tým, či by sa tento súčin ešte dal nejako rozložiť na súčin polynómov nižšieho stupňa. Inak povedané, či polynómy $x^2 \pm \sqrt{2}x + 1$ už sú ireducibiliné, alebo nie. Keďže ide o kvadratické polynómy, netriviálny rozklad na súčin by znamenal, že by sme dostali nejaké polynómy stupňa 1 – a teda existenciu dvoch koreňov. Nie je ťažké sa presvedčiť, že neexistujú reálne korene týchto dvoch polynómov. (Napríklad na základe diskriminantu $D = 2 - 4 \cdot 1 \cdot 1 = -2$.) Teda v $\mathbb{R}[x]$ sme $f(x)$ zapísali ako súčin dvoch ireducibilných polynóm.

Súčasne vieme, že nad $\mathbb{C}$ má každý kvadratický polynóm dva korene – v tomto prípadu nemáme reálne korene a dostaneme teda dva komplexne združené korene. Teda v $\mathbb{C}[x]$ máme rozklad tvaru

$$x^4 + 1 = (x - a_1)(x - \overline{a_1})(x - a_2)(x - \overline{a_2}),$$

pričom štyri komplexné korene by sme vedeli vyčísliť rôznymi spôsobmi. Napríklad ak vieme nájsť korene kvadratických rovníc v komplexných číslach. Ale azda jednoduchšie je vyriešiť priamo pôvodnú rovnicu $x^4 + 1 = 0$. Pýtame sa na to, pre aké komplexné čísla máme $x^4 = -1$. Vieme, že mocniny komplexných čísel majú pekný geometrický význam – vďaka tomu vieme vyjadriť riešenia tejto rovnice v goniometrickom tvare. Samotné nájdenie komplexných koreňov sme ponechali ako cvičenie (úloha 3.4.5).

Tento polynóm však bude ireducibilný v $\mathbb{Q}[x]$. Pretože nemá korene v $\mathbb{Q}$, ak by sa nejako dal netriviálnym spôsobom rozložiť na súčin $f(x) = g(x)h(x)$, tak oba polynómy $g(x)$ aj $h(x)$ by boli stupňa 2. Môžeme dokonca priamo zobrať za $g(x)$ a $h(x)$ priamo polynómy s vedúcim koeficientom 1 – vynásobenie racionálnou konštantou neovplyvní to, že všetky koeficienty sú racionálne.

Ak tieto dva polynómy patria do $\mathbb{Q}[x]$, tak súčasne patria aj do $\mathbb{R}[x]$, teda by sme mali nejaký rozklad na súčin aj v $\mathbb{R}[x]$. Pretože v $\mathbb{R}[x]$ už rozklad na ireducibilné polynómy už poznáme, dostali by sme v $\mathbb{R}[x]$ pre niektoré z polynómov $g(x)$, $h(x)$, že je to násobok polynómu $x^2 + \sqrt{2}x + 1$. (Takýto fakt zdôvodníme všeobecne v tvrdení 4.5.8.) A pretože ide o polynómy rovnakého stupňa s rovnakým vedúcim koeficientom, dostali by sme $g(x) = x^2 + \sqrt{2}x + 1$ alebo $h(x) = x^2 + \sqrt{2}x + 1$. To však nie je polynóm s racionálnymi koeficientami.

Alternatívne by sme to isté mohli zdôvodniť aj bez odvolávania sa na tvrdenie 4.5.8. Polynómy $g(x)$ a $h(x)$ by mali v $\mathbb{C}$ nejaký rozklad na koreňové činitele – môžu to však byť iba niektoré z koreňov polynómu $x^4 + 1$, ktoré sme vyššie označili $a_1$, $\overline{a_1}$, $a_2$, $\overline{a_2}$. Ak chceme ako súčin $(x - c_1)(x - c_2)$ pre nejaké $c_{1,2} \in \mathbb{C} \setminus \mathbb{R}$ dostať polynóm, ktorý má reálne koeficienty, tak $c_1$ a $c_2$ musia byť komplexne združené. Teda ako jediné dve možnosti máme $g(x) = (x - a_1)(x - \overline{a_1})$ alebo $g(x) = (x - a_2)(x - \overline{a_2})$, čo sú opäť presne možnosti $g(x) = x^2 \pm \sqrt{2}x + 1$

V predošlom príklade sme videli, že $f(x) = x^4 + 1$ je ireducibilný nad poľom $\mathbb{Q}$, hoci v tomto poli nemá korene. Všimnime si, že takáto situácia nemôže nastať pre polynómy druhého a tretieho stupňa.

{faktFX:TVRIR

**Tvrdenie 4.5.6.** *Nech $F$ je pole a $f(x) \in F[x]$ je polynóm stupňa 2 alebo 3.*
*Polynóm $f(x)$ je ireducibilný práve vtedy, keď nemá korene.*

*Dôkaz.* $\boxed{\Rightarrow}$ Táto implikácia platí pre všetky polynómy stupňa 2 a väčšieho – úloha 4.5.3.
$\boxed{\Leftarrow}$ Ak by sa $f(x)$ dal netriviálnym spôsobom rozložiť ako $f(x) = g(x) \cdot h(x)$, tak máme

$$\operatorname{st} g(x) + \operatorname{st} h(x) = \operatorname{st} f(x) \leq 3.$$

Pretože $\operatorname{st} g(x), \operatorname{st} h(x) \geq 1$, vidíme, že aspoň jeden z polynómov $g(x)$, $h(x)$ má stupeň jedna.
Teda máme $x - u \mid f(x)$ pre nejaké $u \in F$. Takéto $u$ je koreňom polynómu $f(x)$. □

Definícia ireducibilného polynómu snáď aspoň do istej miery pripomína prvočísla. Skutočne, dala by sa dokázať aj veta o existencii a jednoznačnosti rozkladu ľubovoľného polynómu na ireducibilné polynómy. Tento výsledok nebudeme potrebovať – takže ho tu ani nedokazujeme. Bude sa nám však hodiť analógia tvrdenia 3.3.13, ktorá úzko súvisí s jednoznačnosťou rozkladu.

{faktFx:EQPMIDAB}

$$p(x) \mid g(x)h(x) \qquad \Rightarrow \qquad p(x) \mid g(x) \vee p(x)p \mid h(x) \tag{4.10}$$

{faktFx:TVRIREDGCD}

**Tvrdenie 4.5.7.** *Nech $p(x), f(x) \in F[x]$ a $p(x)$ je ireducibilný. Potom $p(x) \mid f(x)$ alebo $\gcd(p(x), f(x)) = 1$.*

*Dôkaz.* □

Teraz už vieme dokázať aj vlastnosť (4.10).

{faktFx:TVRPMIDAB}

**Tvrdenie 4.5.8.** *Nech $p(x)$ je ireducibilný polynóm v $F[x]$. Nech $g(x), h(x) \in F[x]$. Ak $p(x) \mid g(x) \cdot h(x)$, tak platí $p(x) \mid g(x)$ alebo $p(x) \mid h(x)$.*

*Dôkaz.* □

Vlastne teraz máme pripravené veci na to, aby sme vedeli zdôvodniť, kedy nám takáto konštrukcia dá pole – asi nás neprekvapí, že aj tu bude argument veľmi podobný na to, čo sme videli pre $\mathbb{Z}$ a $\mathbb{Z}/(p)$.

{faktFx:VTJEPOLE}

**Veta 4.5.9.** *Nech $F$ je pole a $p(x) \in F[x]$ je ireducibilný polynóm nad $F$. Potom okruh $F[x]/(p(x))$ je pole.*
*Navyše toto pole obsahuje podpole izomorfné s poľom $F$, konkrétne platí, že zobrazenie*

$$\varphi\colon F \to F(x)/(p(x))$$
$$\varphi\colon c \mapsto \overline{c}$$

*je injektívny homomorfizmus.*

*Dôkaz.* *$F(x)/(p(x))$ je pole.* Z vety 4.5.1 už vieme, že $F$ je komutatívny okruh s jednotkou.
Potrebovali by sme ešte overiť, či každý nenulový prvok má multiplikatívny inverz. T.j. ak máme $f(x) \in F[x]$ taký, že $\overline{f(x)} \neq \overline{0}$, t.j.

$$f \not\equiv 0 \pmod{p},$$

tak by sme chceli ukázať existenciu polynómu $u(x) \in F[x]$ takého, že platí $\overline{u(x)f(x)} = \overline{1}$.
Pretože $p(x) \nmid f(x)$, z tvrdenia 4.5.7 máme, že $\gcd(f(x), p(x)) = 1$.

Na základe Bézoutovej identity, t.j. dôsledku 3.4.31, potom existujú $u(x), v(x) \in F[x]$ také, že platí

$$u(x)f(x) + v(x)p(x) = 1.$$

To znamená, že máme

$$u(x)f(x) \equiv 1 \pmod{p(x)},$$

čiže $\overline{u(x)} \cdot \overline{p(x)} = \overline{1}$.

Ukázali sme, že v $F(x)/(p(x))$ má každý nenulový prvok multiplikatívny inverz, teda je to skutočne pole.

*$\varphi$ je injektívny homomorfizmus.* Je jasné, že $\varphi$ je homomorfizmus – ak sčítame alebo vynásobíme dva konštantné polynómy, tak sa iba vynásobia ich absolútne členy.

Súčasne pre ľubovoľné dva konštantné polynómy platí $c \equiv d \pmod{p(x)}$ iba vtedy, ak $c = d$. (Pretože $\operatorname{st} p(x) \geq 1$.) Teda ide o injektívne zobrazenie. □

V poslednej časti – o existencii injektívneho homomorfizmu – sme v skutočnosti nepotrebovali fakt, že $p(x)$ je ireducibilný. (Pozri aj úlohu 4.5.4. Ďalší homomorfizmus súvisiaci s týmto okruhom je spomenutý v úlohe 4.5.5.)

Pretože $F(x)/(p(x))$ obsahuje podpole izomorfné s $F$, ak stotožníme $a_0$ a $\overline{a_0}$ pre ľubovoľný polynóm, tak sa naň môžeme pozerať priamo ako na nadpole poľa $F$. Dostali sme takto nejaké rozšírenie poľa $F$. Môžeme si všimnúť, že sme dostali rozšírenie, v ktorom polynóm $p(x)$ má koreň.

{faktFx:TVRKOREN}

**Tvrdenie 4.5.10.** *Nech $F$ je pole a $p(x) \in F[x]$ je ireducibilný polynóm nad $F$.*

*Ak $L = F[x]/(p(x))$ chápeme ako nadpole poľa $F$, tak $u = \overline{x}$ je koreň polynómu $p(x)$ v tomto poli.*

*Dôkaz.* V tomto tvrdení sme stotočnili $F$ so zodpovedajúcim podpoľom poľa $L$, t.j. $c$ stotožňujeme s triedou konštantného polynómu $\overline{c}$.

Stačí vlastne dosadiť $u$ do polynómu $p(x)$, použiť spomenuté stotožnenie a to, ako počítame v tomto poli.

Ak $p(x) = a_n x^n + \cdots + a_1 x + a_0$, tak dostaneme

$$\begin{aligned} p(\overline{x}) &= a_n \overline{x}^n + \cdots + a_1 \overline{x} + a_0 \\ &= \overline{a_n} \overline{x}^n + \cdots + \overline{a_1} \overline{x} + \overline{a_0} \\ &= \overline{a_n x^n + \cdots + a_1 x + a_0} \\ &= \overline{p(x)} \\ &= \overline{0} = 0 \end{aligned}$$

□

Neskôr si chceme povedať ešte nejaké ďalšie veci o konečných poliach – vrátime sa k nim v časti 4.9. Na tomto mieste si môžeme všimnúť aspoň to, že vieme dostať štvorprvkové pole. (Doteraz sme videli iba také konečné polia, kde počet prvkov bol prvočíslo.)

{faktFx:PRIKLGF4}

**Príklad 4.5.11.** TODO štvorprvkové pole $F = \mathbb{Z}_2[x]/(x^2 + x + 1)$

TODO polynóm $p(x) = x^2 + x + 1$ je ireducibilný v $\mathbb{Z}_2[x]$

Všetky prvky tohto poľa majú tvar $\overline{f(x)}$ pre $f(x) \in \mathbb{Z}_2(x)$, $\operatorname{st}(f(x)) < 2$. V $\mathbb{Z}_2[x]$ máme iba štyri polynómy stupňa nanajvýš dva: 0, 1, $x$, $x + 1$.

Kvôli stručnosti označme $u = \overline{x}$. Potom prvky poľa $F$ sú $\overline{0} = 0$, $\overline{1} = 1$, $\overline{x} = u$ a $\overline{x+1} = u + 1$.

$$F = \{0, 1, u, u + 1\}$$

| $+$ | $0$ | $1$ | $u$ | $u+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $u$ | $u+1$ |
| $1$ | $1$ | $0$ | $u+1$ | $u$ |
| $u$ | $u$ | $u+1$ | $0$ | $1$ |
| $u+1$ | $u+1$ | $u$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $u$ | $u+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $u$ | $u+1$ |
| $u$ | $0$ | $u$ | $u+1$ | $1$ |
| $u+1$ | $0$ | $u+1$ | $1$ | $u$ |

TODO $u$ je koreň $x^2+x+1$

$$(x+u)(x+u+1) = x^2+x+1$$

**Cvičenia**

faktFxcvic:ULOZVYSOKJEN}

**Úloha 4.5.1.** Nech $h(x) \in F[x]$, kde $F$ je pole. Ukážte, že ak $\operatorname{st} h(x) = n$ a $r(x) \equiv r'(x) \pmod{h(x)}$ platí pre dva polynómy $r(x), r'(x) \in F[x]$ stupňa menšieho než $n$, tak platí $r(x) = r'(x)$. (Hint: Môže byť užitočné si najprv rozmyslieť takéto tvrdenie pre prípad $r'(x) = 0$.)

{faktFxcvic:ULOZRUZENE}

**Úloha 4.5.2.** Ukážte, že ak kvadratický polynóm $f(x)$ s reálnymi koeficientami má nejaký koreň $z$ v komplexných číslach, tak aj komplexne združené číslo $\overline{z}$ je koreňom.

Fxcvic:ULOIREDNEMAKOREN}

**Úloha 4.5.3.** Nech $f(x) \in F[x]$, kde $F$ je ľubovoľné pole. Ukážte, že ak polynóm stupňa $\operatorname{st} f(x) \geq 2$ je ireducibilný, tak $f(x)$ nemá koreň v $F$.

{faktFxcvic:ULOKAHOMF}

**Úloha 4.5.4.** Dokážte: Nech $F$ je pole a $h(x) \in F[x]$, pričom $\operatorname{st} h(x) \geq 1$. Potom zobrazenie

$$\varphi\colon F \to F(x)/(p(x))$$
$$\varphi\colon c \mapsto \overline{c}$$

je injektívny homomorfizmus.

{faktFxcvic:ULOKANONHOM}

**Úloha 4.5.5.** Nech $F$ je pole a $h(x) \in F[x]$. Potom zobrazenie

$$\varphi\colon F[x] \to F[x]/(h(x))$$
$$\varphi\colon f(x) \mapsto \overline{f(x)}$$

je surjektívny homomorfizmus.

## 4.6 Algebraické prvky a minimálny polynóm

### 4.6.1 Minimálny polynóm

{minpoly:DEFALG}

**Definícia 4.6.1.** Nech $K$ je rozšírenie poľa $F$ a $u \in K$. Hovoríme, že prvok $u \in F$ je *algebraický* nad $F$, ak existuje polynóm $f(x) \in F[x]$ taký, že $u$ je jeho koreňom.

$$(\exists f(x) \in F[x]) f(u) = 0$$

Ak prvok $u \in K$ nie je algebraický, tak hovoríme, že $u$ je transcendentný prvok.

{minpoly:DEFMINPOLY}

**Definícia 4.6.2.** Nech $K$ je rozšírenie poľa $F$ a $u \in K$ je algebraický prvok nad $F$. Polynóm $m(x)$ sa nazýva *minimálny polynóm* prvku $u$, ak je to nenulový monický polynóm najnižšieho možného stupňa, ktorého koreňom je $u$.

Ak potrebujeme zdôrazniť z akého prvku sme minimálny polynóm dostali, použijeme označenie $m_u(x)$.

Ako prvú vec si skúsme rozmyslieť, že pre každý algebraický prvok minimálny polynóm existuje a je jednoznačne určený.

yTVRDMINASOBNE}

**Tvrdenie 4.6.3.** *Nech $K$ je rozšírenie poľa $F$ a $u \in K$ je algebraický prvok nad $F$.*

*Potom existuje minimálny polynóm $m(x)$ prvku $u$. Tento polynóm je prvkom $u$ určený jednoznačne.*

*Navyše pre ľubovoľný polynóm $f(x) \in F[x]$ platí, že $u$ je koreňom polynómu $f(x)$ práve vtedy, keď $m(x) \mid f(x)$.*

$$f(u) = 0 \Leftrightarrow m(x) \mid f(x) \tag{4.11}$$ {minpoly:EQNULUJEDELI}

*Dôkaz.* Pre prvok $u \in K$ sa pozrime na tie polynómy, ktorých koreňom je $u$.

$$I = \{f(x) \in F[x]; f(u) = 0\}$$

Pomerne ľahko sa dá skontrolovať, že táto množina tvorí ideál v okruhu $F[x]$ (úloha 4.6.1).

Vieme, že existuje polynóm $m(x)$ taký, že $I = (m(x))$ (tvrdenie 3.4.28). Navyše tento polynóm nemôže byť nulový – predpokladáme totiž, že $u$ je algebraický prvok a teda $I \neq \{0\}$. Podmienka, že ide o monický polynóm, nám teda zaručí jednoznačnosť tohto generátora.

Z toho, že $(m(x)) = I$ vidíme, že

$$f(x) \in I \Leftrightarrow m(x) \mid f(x).$$

Podmienka $f(x) \in I$ však hovorí presne to, že $u$ je koreň polynómu $f(x)$. Tým sme dokázali aj druhú časť tvrdenia. □

Z (4.11), teda z toho, že číslo $u$ je koreňom presne tých polynómov, ktoré sú násobkami jeho minimálneho polynómu, ihneď dostávame aj takéto pozorovanie.

{minpoly:DOSKONG}

**Dôsledok 4.6.4.** *Nech $K$ je rozšírenie poľa $F$, $u \in K$ je algebraický prvok nad $F$ a $m(x)$ je jeho minimálny polynóm.*

*Potom pre ľubovoľné polynómy $f(x), g(x) \in F[x]$ platí $f(u) = g(u)$ práve vtedy, keď $f(x) \equiv g(x) \pmod{m(x)}$.*

$$f(u) = g(u) \Leftrightarrow f(x) \equiv g(x) \pmod{m(x)} \tag{4.12}$$ {minpoly:EQKONG}

*Dôkaz.* Stačí použiť (4.11) pre polynóm $h(x) = f(x) - g(x)$.

$$\begin{aligned} f(u) = g(u) &\Leftrightarrow f(u) - g(u) = 0 \\ &\Leftrightarrow m(x) \mid f(x) - g(x) \\ &\Leftrightarrow f(x) \equiv g(x) \pmod{m(x)} \end{aligned}$$

□

**Poznámka 4.6.5.** Videli sme, že minimálny polynóm je generátor vhodného ideálu v $F[x]$. Všimnime si, že na rozdiel od definície 4.6.2 pri definícii tohto ideálu nijako nevystupuje nadpole $K$.

To znamená, že ak sa pozeráme na nejaký prvok $u$, tak pri otázke či ide o algebraický prvok a ako vyzerá jeho minimálny polynóm, si môžeme vybrať ľubovoľné rozšírenie obsahujúce $u$. (Teda nezávisia od voľby $K$; je potrebný iba to, aby $u$ ležalo v $K$.)

Napríklad ak sa pozeráme na minimálny polynóm čísla $u = \sqrt{2}$ nad poľom $\mathbb{Q}$ tak vieme, že vyjde rovnako, bez ohľadu na to, či sa pozeráme na $\sqrt{2}$ ako prvok z $\mathbb{C}$, prvok z $\mathbb{R}$ alebo prvok z $\mathbb{Q}(\sqrt{2})$.

**Príklad 4.6.6.** Minimálny polynóm $m_u(x)$ má stupeň 1 práve vtedy, keď $u \in F$.

Ak totiž $u$ je koreňom nejakého polynómu tvaru $f(x) = x + a_0$, kde $a_0 \in F$, znamená to, že $u = -a_0 \in F$.

Aj obrátene, ak $u \in F$ tak hneď vidíme, že $u$ je koreňom polynómu $x - u$.

**Príklad 4.6.7.** Nech $F = \mathbb{Q}$. Ak $u = \sqrt{2}$, tak máme

$$m_u(x) = x^2 - 2.$$

. (Pretože $\sqrt{2} \notin \mathbb{Q}$, $u$ nie je koreňom polynómu nižšieho stupňa.)

Pre $u = \sqrt[3]{2}$ máme

$$m_u(x) = x^3 - 2.$$

Je jasné, že $u$ je skutočne koreňom polynómu $x^3 - 2$. Aj tu by sme si chceli rozmyslieť, že žiadny nenulový polynóm $f(x) \in \mathbb{Q}[x]$ nižšieho stupňa nemôže mať $\sqrt[3]{2}$ ako koreň.

Z tvrdenia 4.6.3 vieme, že platí

$$m_u(x) \mid x^3 - 2.$$

Stačí si teda rozmyslieť, že $x^3$ je ireducibilný nad $\mathbb{Q}$.

Je to polynóm stupňa tri, stačí sa presvedčiť, že nemá racionálne korene (tvrdenie 4.5.6). Na základe dôsledku 3.4.25 stačí skontrolovať, že čísla $\pm 1$, $\pm 2$ nie sú koreňmi.

Iná možnosť by bola nájsť všetky korene v $\mathbb{C}$ – okrem $\sqrt[3]{2}$ dostaneme ešte dva komplexné korene, žiadny z koreňov nie je racionálny. (Resp. pre naše účely by stačilo, že pri rozklade $x^3 - 2 = (x - u)(x^2 + ux + u^2)$ dostaneme kvadratický polynóm, ktorý nemá reálne korene – a teda určite nemá ani racionálne korene.)

{minpoly:TVRIRED}

**Tvrdenie 4.6.8.** *Nech $m_u(x)$ je minimálny polynóm prvku $u$ nad poľom $F$. Potom $m(x)$ je ireducibilný v $F[x]$.*

*Dôkaz.* Ak by platilo $m(x) = f(x) \cdot g(x)$ pre nejaké polynómy stupňa aspoň 1, tak $u$ by musel byť koreňom polynómu $f(x)$ alebo koreňom polynómu $g(x)$. Dostali by sme tak polynóm, ktorý nuluje $u$ a má nižší stupeň než polynóm $m(x)$. To je evidentne spor. □

{minpoly:VTFU}

**Veta 4.6.9.** *Nech $K$ je nadpole poľa $F$. Nech prvok $u \in K$ je algebraický nad $F$ a jeho minimálny polynóm $m(x)$ má stupeň $n$. Potom*

$$F(u) = \{a_{n-1}u^{n-1} + \cdots + a_1 u + a_0; a_0, \ldots, a_{n-1} \in F\} = \{f(u); f(x) \in F[x], \operatorname{st} f(x) < n\}.$$

*Navyše predpis*

$$\varphi\colon \overline{f(x)} \mapsto f(u)$$

*určuje dobre definované zobrazenie $\varphi\colon F[x]/(m(x)) \to F(u)$ Teda platí*

$$F(u) \cong F[x]/(m(x)).$$

Z tejto vety vidíme, že pole $F(u)$ vyjde „v podstate rovnaké“ (t.j. rovnaké na izomorfizmus), bez ohľadu na to, v akom nadpoli sa pozeráme na prvok

*Dôkaz.* Označme

$$F' = \{a_{n-1}u^{n-1} + \cdots + a_1 u + a_0; a_0, \ldots, a_{n-1} \in F\} = \{f(u); f(x) \in F[x], \operatorname{st} f(x) < n\}.$$

O tejto množine chceme ukázať, že sa v skutočnosti rovná $F(u)$. Pritom je jasné, že $F' \subseteq F(u)$, pretože všetky prvky takéhoto tvaru musia ležať v akomkoľvek poli obsahujúcom $F$

aj $u$. (Pri tejto inklúzii nijako nevyužívame to, že $u$ je algebraický prvok a to, ako vyzerá jeho minimálny polynóm.) Podstatná časť v tomto dôkaze teda bude zdôvodnenie opačnej inklúzie.

*Izomorfizmus s faktorovým okruhom.* Chceme definovať zobrazenie $\varphi\colon F[x]/(m(x)) \to F'$ predpisom

$$\varphi\colon \overline{f(x)} \mapsto f(u).$$

Ako prvé by sme mali skontrolovať, či je toto zobrazenie definované.

Tu sa vlastne pýtame to, či pre dva polynómy patriace do tej istej triedy ekvivalencie dostaneme rovnakú hodnotu v bodu $u$. To je presne podmienka

$$f(x) \equiv g(x) \pmod{m(x)} \Rightarrow f(u) = g(u),$$

ktorú sme si už rozmysleli v (4.12).

Teraz už ľahko vidíme aj to, že $\varphi$ je homomorfizmus.

$$\varphi(\overline{f(x) + g(x)}) = f(u) + g(u) = \varphi(\overline{f(x)}) + \varphi(\overline{g(x)})$$

$$\varphi(\overline{f(x) \cdot g(x)}) = f(u) \cdot g(u) = \varphi(\overline{f(x)}) \cdot \varphi(\overline{g(x)})$$

Toto zobrazenie bude aj bijekcia. Ľubovoľný prvok $f(u) \in F'$ je obrazom triedy $\overline{f(x)}$, a teda $\varphi$ je surjektívne. Súčasne bude aj injektívne, pretože $\varphi(\overline{f(x)}) = \varphi(\overline{g(x)})$ platí práve vtedy, keď $f(u) = g(u)$ a opäť z (4.12) vieme, že to je ekvivalentné s podmienkou $f(x) \equiv g(x) \pmod{m(x)}$. Teda takéto niečo nastane práve vtedy, keď $f(x)$ a $g(x)$ ležia v tej istej triede ekvivalencie.

$$\begin{aligned} \varphi(\overline{f(x)}) = \varphi(\overline{g(x)}) &\Rightarrow f(u) = g(u) \\ &\Rightarrow f \equiv g \pmod{m} \\ &\Rightarrow \overline{f(x)} = \overline{g(x)} \end{aligned}$$

Iná možnosť, ako zdôvodniť že ide o bijekciu, by bolo využiť fakt, že každá trieda z $F[x]/(m(x))$ je reprezentovaná práva jedným polynómom stupňa najviac $n-1$; to sme dokázali vo vete 4.5.1.

*$F'$ je pole.* Vieme, že polynóm $m(x)$ je ireducibilný (tvrdenie 4.6.8). Podľa vety 4.5.9 potom $F[x]/(m(x))$ je pole. Pretože $F'$ je izomorfné s týmto okruhom, aj $F'$ je pole.

*Dostali sme popis poľa $F(u)$.* Vidíme teda, že $F'$ je podpole poľa $K$, ktoré obsahuje $F \cup \{u\}$. Súčasne každé podpole poľa $K$ obsahujúce $F$ aj $u$ musí obsahovať aj všetky prvky tvaru $a_{n-1}u^{n-1} + \cdots + a_1 u + a_0$, čiže je to najmenšie takéto pole. Máme teda rovnosť

$$F' = F(u).$$

□

{TVRSTUPENMINPOLY}

**Tvrdenie 4.6.10.** *Nech $K$ je rozšírenie poľa $F$, $u \in K$ je algebraický prvok nad poľom $F$. Potom stupeň rozšírenia $F(u)$ nad poľom $F$ je rovný stupňu jeho minimálneho polynómu.*

$$[F(u) : F] = \deg m_u(x).$$

*Toto číslo budeme tiež nazývať stupeň prvku $u$ nad $F$ a označovať $[u : F]$.*

*Dôkaz.* Označme stupeň minimálneho polynómu $m_u(x)$ ako $n$.

Z vety 4.6.9 vieme, že

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

Teda $1, u, \ldots, u^{n-1}$ generujú $F(u)$ (ako vektorový priestor nad $F$).

Súčasne sú tieto prvky lineárne nezávislé nad $F$, ak by sme totiž mali

$$c_{n-1}u^{n-1} + \cdots + c_1u + c_0 = 0$$

pre nejaké nenulové konštanty, znamenalo by to, že $u$ je koreňom nenulového polynóm stupňa nižšieho ako $n$, čo je spor s definíciou minimálneho polynómu. □

**Príklad 4.6.11.** Pozrime sa na $\mathbb{Q}(\sqrt[3]{2})$, t.j. na najmenšie podpole reálnych čísel obsahujúce všetky racionálne čísla aj $\sqrt[3]{2}$. Vieme, že minimálny polynóm tohto čísla $u = \sqrt[3]{2}$ je

$$m(x) = x^3 - 2.$$

Z vety 4.6.9 potom dostaneme, že všetky prvky v poli $\mathbb{Q}(u)$ sa dajú vyjadriť ako $a_2u^2 + a_1u + a_0$, kde všetky tri koeficienty sú racionálne. (Dokonca vieme aj to, že takéto vyjadrenie je jednoznačné.)

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}; a, b, c \in \mathbb{Q}\}$$

V prípade poľa $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2}; a, b \in \mathbb{Q}\}$ sme boli schopní vcelku ľahko overiť definíciu poľa (pozri časť časť 4.3.1). Konkrétne pre inverzný prvok nám stačilo počítať so súčinom

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}$$

a upraviť ho do tvaru, kde sme už videli, že sa dá zapísať v tvare $x+y\sqrt{2}$ pre nejaké racionálne čísla $x$, $y$. Priamo nájsť inverzný prvok k $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ by bolo náročnejšie – tu však máme existenciu inverzného prvku „zadarmo“ z toho, že $\mathbb{Q}[x]/(m(x))$ je pole – aj keď nemáme k dispozícii priamo explicitný predpis pre inverzný prvok.

### 4.6.2 Algebraické prvky tvoria pole

**Tvrdenie 4.6.12.** *Nech $K$ je rozšírenie poľa $F$ a $u \in K$. Prvok $u$ je algebraický nad $F$ práve vtedy, keď $F(u)$ je konečné rozšírenie poľa $F$.*

*Dôkaz.* $\boxed{\Rightarrow}$ TODO tvrdenie 4.6.10

$\boxed{\Leftarrow}$ Predpokladajme teraz, že $F(u)$ je konečné rozšírenie a označme $[F(u) : F] = n$. Vieme, že

$$1, u, \ldots, u^{n-1}, u^n \in F(u).$$

Máme teda $n+1$ prvkov vo vektorovom priestore dimenzie $n$. Tieto prvky sú teda lineárne závislé. To znamená, že existujú nejaké nenulové konštanty $c_0, \ldots, c_n$ také, že

$$c_nu^n + \cdots + c_1u + c_0 = 0.$$

To znamená, že $u$ je koreňom polynómu

$$p(x) = c_nx^n + \cdots + c_1x + c_0.$$

□

**Tvrdenie 4.6.13.** *Nech $K$ je rozšírenie poľa $F$. Ak $u, v \in K$ sú algebraické nad $F$, tak aj $u \pm v$ a $u \cdot v$ sú algebraické nad $F$. Ak navyše $u \neq 0$, tak aj $u^{-1}$ je algebraický nad $F$-*

*Dôkaz.* □

**Dôsledok 4.6.14.** *Nech $K$ je rozšírenie poľa $F$. Množina*

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

*tvorí pole.*

*Dôkaz.* □

**Cvičenia**

{okruhFxcvic:ULOKORENIDE

**Úloha 4.6.1.** Nech $K$ je rozšírenie poľa $F$ a $u \in K$. Dokážte, že

$$I = \{f(x) \in F[x]; f(u) = 0\}$$

je ideál v okruhu $F[x]$ a ak $u$ je algebraický prvok nad $F$, tak $I \neq \{0\}$.

{minpolycvic:ULOLN}

**Úloha 4.6.2.** Nech $u \in \mathbb{R}$ a minimálny polynóm čísla $u$ nad $\mathbb{Q}$ má stupeň $n$. Ukážte, že potom čísla $1, u, \ldots, n$ sú lineárne nezávislé ak sa na $\mathbb{R}$ pozeráme ako na vektorový priestor nad $\mathbb{Q}$. (Dostávame takto, že $\mathbb{R}$) je nekkonečnorozmerný vektorový priestor nad $\mathbb{Q}$ – o čosi iným spôsobom ako v úlohe 2.1.3.)

## 4.7 Konštrukcie pravítkom a kružidlom

{konstr:SECT}

V tejto časti sa chceme pozrieť na to, že naše vedomosti o poliach nám pomôžu zdôvodniť nemožnosť niektorých geometrických konštrukcií. Napríklad nie je možné zostrojiť iba použitím pravítka a kružidla zo zadanej hrany kocky úsečku, ktorej dĺžka je presne dĺžka hrany kocky dvojnásobného objemu (zdvojenie kocky). Inak povedané, z jednotkovej úsečky sa nám nepodarí zostrojiť úsečku dĺžky $\sqrt[3]{2}$.

V podstate veľmi stručne sa dá celý argument povedať tak, že konštrukciami pravítkom a kružidlom vieme vyrábať prvky takých polí, ktoré obsahujú racionálne čísla a pridávame k nim vždy *druhé* odmocniny – a preto dostaneme iba také prvky, ktorých stupeň nad $\mathbb{Q}$ je mocnina dvojky. Teda nevieme dostať také číslo, ako napríklad $\sqrt[3]{2}$, kde minimálny polynóm má stupeň 3. (Samozrejme, aby sme tento argument vysvetlili poriadne, treba pridať veľa ďalších detailov.)

Veľa o takýchto veciach sa dá nájsť v rôznej literatúre. V slovenčine si o tom môžeme prečítať napríklad v [KGGS, Podkapitola 4.1 a 8.2]. Ďalšie referencie sú napríklad: [DF, Section 13.3], [JMP], [St, Chapter 7]. Niečo nájdete aj v poznámkach k niektorým iným predmetom na našej fakulte, napríklad [Sl1].

### 4.7.1 Skonštruovateľné čísla

Konštrukciou pomocou pravítka a kružidla máme na mysli to, že ak sme už nejaké body zostrojili, tak v ďalšom kroku môžeme:

- Vytvoriť priamku určenú niektorými dvoma bodmi.
- Vytvoriť kružnicu, kde stred je niektorý zo zadaných bodov a polomer je určený tým, že kružnica prechádza niektorým iným bodom.
- Pridať body, ktoré dostaneme, ako prienik niektorých takýchto priamok a kružníc.

Môže byť užitočné pozerať sa na to aj cez súradnice – to budeme pri vlastnostiach skonštruovateľných čísel naozaj používať. Teda iný pohľad je taký, že máme dané dva body $(0,0)$ a $(1,0)$. A pozeráme sa na body, ktoré z nich vieme dostať konečným počtom krokov uvedeného typu. Skonštruovateľné čísla sú presne súradnice bodov, ktoré takto vieme vytvoriť. (Nejaký bod sa dá skonštruovať práve vtedy, keď vieme skonštruovať dĺžky predstavujúce jeho prvú a druhú súradnicu.)

**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 číslach. [1]

Tým, že začíname s bodmi $(0,0)$ a $(0,1)$ sme vlastne len zvolili súradnicovú sústavu na základe nejakých daných dvoch bodov.

Asi by mohlo byť pomerne jasné, že ak $x$, $y$ sú skonštruovateľné, tak aj:

- $\frac{x+y}{2}$, $x+y$, $x-y$ sú skonštruovateľné;
- $xy$ je skonštruovateľné;
- Ak $x \neq 0$, tak aj $\frac{1}{x}$ je skonštruovateľné.

Z vlastností, ktoré sme doteraz vymenovali, by malo byť jasné, že $\mathbb{K}$ je pole a tiež to, že $\mathbb{Q} \subseteq \mathbb{K}$.

**Tvrdenie 4.7.2.** *Množina $\mathbb{K}$ všetkých skonštruovateľných čísel je pole. Platí $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{R}$, je to teda rozšírenie poľa racionálnych čísel.*

Vieme však pridávať aj nejaké ďalšie veci. Napríklad ak číslo $x$ je skonštruovateľné, tak vieme dostať aj jeho odmocninu – úloha 4.7.1.

$$x \in \mathbb{K} \qquad \Rightarrow \qquad \sqrt{x} \in \mathbb{K}$$

Poďme sa pozrieť na to, aké čísla vlastne vieme dostať, ak robíme len priamky, kružnice a ich prieniky – či je nejaká šanca, že by sme dostali aj niečo výrazne odlišné od toho, čo sme zatiaľ spomenuli.

Pretože budeme v rôznych úvahách pozerať na to, čo vieme dostať po nejakom konečnom počte krokov a budeme takto pridávať stále nové body, tak sa nám hodí zaviesť nejaké pomenovanie pre body zostrojiteľné z nejakých vecí, ktoré sme už doteraz skonštruovali.

Pomerne rýchlo by sme si mali byť schopní rozmyslieť, že ak máme zadané nejaké body (alebo čísla – ako ich súradnice), tak keď robíme prieniky priamok, dostaneme lineárne rovnice s koeficientami z tejto množiny. A ak robíme prienik priamky a kružnice alebo prienik dvoch kružníc, tak dostaneme nejaké kvadratické rovnice. Poďme si trochu detailnejšie rozmyslieť prečo je to tak.

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

$$\frac{y - a_2}{x - a_1} = \frac{b_2 - a_2}{b_1 - a_1}$$
$$\frac{y - c_2}{x - c_1} = \frac{d_2 - c_2}{d_1 - c_1}$$

[1] Anglicky: constructible number

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.

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.

Vidíme, že teda ak sa pozeráme na jednotlivé kroky tak, že sme začali s poľom $\mathbb{Q}$ a pridali sme nejaké nové číslo a aj všetko, čo z neho môžeme dostať pomocou súčtu, rozdielu, súčinu, podielu – a teda sme dostali nové pole – tak vždy sme pole zväčšili tak, že sme vlastne pridávali riešenie nejakej kvadratickej rovnice s koeficientami z pôvodného poľa. Ak si túto kvadratickú rovnicu zapíšeme ako $ax^2 + bx + c = 0$, tak sme dostali nové číslo tvaru

$$x_{1,2} = \frac{-b + \sqrt{D}}{2a}$$

pre $D = b^2 - 4ac$. Ak k nejakému podpoľu reálnych čísel obsahujúcemu $\mathbb{Q}$ pridávame takéto číslo, je to to isté ako pridávať $\sqrt{D}$. Na začiatku tejto časti spomenuli niečo v tom zmysle, že pridávať vieme „v podstate iba odmocniny“. Mali sme na mysli to, čo sme teraz sformulovali poriadnejšie.

{konstr:VTSTUPEN2naN}

**Veta 4.7.3.** *Ak číslo $u$ je konštruovateľné, tak $u$ je algebraické číslo a stupeň $[u : \mathbb{Q}]$ je mocnina dvojky.*

$$[u : \mathbb{Q}] = 2^n$$

*Dôkaz.* Indukciou na počet krokov v konštrukcii, ktorou sme dostali hľadaný bod z množiny racionálnych čísel dokážeme, že každé skonštruovateľné číslo leží v nejakom nadpoli $\mathbb{Q}$ takom, že $[F : \mathbb{Q}]$ je mocnina dvojky. Ak sa nám podarí dokázať takúto vec, tak z

$$[u : \mathbb{Q}] \mid [F : \mathbb{Q}] = 2^n$$

vidíme, že aj $[u : \mathbb{Q}]$ musí byť mocninou čísla dva.

1° V nultom kroku máme iba $\mathbb{Q}$. Samozrejme, platí $[\mathbb{Q} : \mathbb{Q}] = 1 = 2^0$

2° Prepokladajme, že všetky body použité v poslednom kroku konštrukcie majú súradnice ležiace v nejakom poli $F$ takom, že $[F : Q] = 2^n$. Z toho, čo sme popísali vyššie vieme, že $u$ je koreňom nejakej lineárnej alebo kvadratickej rovnice s koeficientami z $F$. Teda minimálny polynóm $m_u(x)$ čísla $u$ má stupeň 1 alebo 2 t.j.

$$[F(u) : F] = [u : F] \in \{1, 2\}.$$

Potom ale platí

$$[F(u) : \mathbb{Q}] = [F(u) : F] \cdot [F : \mathbb{Q}] \in \{2^n, 2^{n+1}\}.$$

□

**Poznámka 4.7.4.** Pole $\mathbb{K}$ nie je konečným rozšírením poľa $\mathbb{Q}$ – existujú v ňom prvky s ľubovoľne veľkým stupňom. (Ak si zoberieme $u = \sqrt[2^n]{2}$, tak $[u : \mathbb{Q}] = 2^n$.)

Ukázali sme ale, že pre každý prvok $u \in \mathbb{K}$ je ale $F(u)$ konečné rozšírenie poľa $\mathbb{Q}$. (A tiež to, že stupeň je mocninou dvojky.)

### 4.7.2 Nemožnosť trisekcie uhla a zdvojenia kocky

Vrátime sa teraz k tomu, že o niektorých reálnych číslach vieme ukázať, že nie sú skonštruovateľné pomocou pravítka a kružidla.

Konkrétne sa chceme pozrieť na to, či sa takýmto spôsobom dajú riešiť klasické antické problémy ako trisekcia uhla, zdvojenie kocky a kvadratúra kruhu. (Aj keď v treťom prípade budeme potrebovať využiť fakt, že číslo $\pi$ nie je algebraické – ktorý spomíname iba bez dôkazu.)

Začnime so zdvojením kocky.

{konstr:TVRZDVOJENIE}

**Tvrdenie 4.7.5.** *Číslo $\sqrt[3]{2}$ nie je skonštruovateľné.*

*Dôkaz.* Označme $u = \sqrt[3]{2}$. Chceme sa pozrieť na to, či vieme zistiť, aký je stupeň $[u : \mathbb{Q}]$.

Je zrejmé, že $u$ je koreňom polynómu $x^3 - 2$.

Je pomerne ľahké overiť, že polynóm $x^3 - 2$ je ireducibilný nad $\mathbb{Q}$. (Stačí sa pozrieť na jeho korene – môžeme napríklad použiť dôsledok 3.4.25.) Tým sme zistili, že tento polynóm je minimálny polynóm čísla $\sqrt[3]{2}$ nad poľom $\mathbb{Q}$.

$$m_u(x) = x^3 - 2$$

Z tvrdenia 4.6.10 máme teda $[u : F] = 3$. To ale znamená, že $u$ nie je skonštruovateľné – jeho stupeň by podľa vety 4.7.3 musel byť mocninou dvojky. □

Teraz sa pozrime na trisekciu uhla.

{konstr:TVRCOS20}

**Tvrdenie 4.7.6.** *Číslo $\cos\frac{\pi}{9}$ nie je skonštruovateľné.*

Pretože uhol $\frac{\pi}{3}$ skonštruovať vieme, tak z tohto výsledku je jasné, že neexistuje postup, ktorý by pre *ľubovoľný* uhol umožňoval pomocou pravítka a kružidla dostať tretinový uhol.

*Dôkaz.* Môžu sa nám hodiť vzťahy pre kosínus a sínus trojnásobného uhla.

$$\cos\alpha = \cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3}\sin^2\frac{\alpha}{3} = 4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3}$$
$$\sin\alpha = 3\cos^2\frac{\alpha}{3}\sin\frac{\alpha}{3} - \sin^3\frac{\alpha}{3} = 3\sin\frac{\alpha}{3} - 4\sin^3\frac{\alpha}{3}$$

Vidíme teda, že $\cos\frac{\alpha}{3}$ je koreňom polynómu $f(x) = 4x^3 - 3x - \cos\alpha$ a špeciálne pre $\alpha = \frac{\pi}{3}$ máme

$$f(x) = 4x^3 - 3x - \frac{1}{2}.$$

Tento polynóm je ireducibilný nad $\mathbb{Q}$ (úloha 4.7.2).

Potom to znamená, že pre $u = \cos\frac{\pi}{9}$ máme minimálny polynóm

$$m_u(x) = x^3 - \frac{3}{4}x - \frac{1}{8}$$

stupňa 3. Teda $[u : \mathbb{Q}] = 3$ a z vety 4.7.3 dostaneme, že $u$ nie je skonštruovateľné. □

onstr:POZNPI}

**Poznámka 4.7.7.** Ďalším známym problémom je *kvadratúra kruhu*. Teraz máme zadaný polomer kružnice a pýtame sa, či by sme boli schopní geometricky (len pravítkom a kružidlom) skonštruovať štvorec s rovnakou plochou ako má zadaný kruh.

Inak sformulované, je to vlastne otázka, že $\sqrt{\pi}$ je skonštruovateľné.

Je známe, že číslo $\pi$ je transcendentné. (Aj keď toto tvrdenie uvádzame bez dôkazu.)

To znamená, že $\pi$ nie je skonštruovateľné. (Všetky skonštruovateľné čísla sú algebraické – veta 4.7.3.)

Nie je ťažké si uvedomiť, že potom ani $\sqrt{\pi}$ sa nedá skonštruovať. (Pozri aj úlohu 4.7.3.)

$$\sqrt{\pi} \notin \mathbb{K}$$

**Cvičenia**

{konstrcvic:ULOODM}

**Úloha 4.7.1.** Dokážte, že:
a) Ak $x$, $y$ sú skonštruovateľné čísla, tak aj $\sqrt{xy}$ je skonštruovateľné číslo.
b) Ak $x$ je skonštruovateľné číslo, tak aj $\sqrt{x}$ je skonštruovateľné číslo.

{konstrcvic:ULOIREDTRISE

**Úloha 4.7.2.** Ukážte, že daný polynóm je ireducibilný nad $\mathbb{Q}$:
a) $f(x) = x^3 - 3x - 1$;
b) $g(x) = 8x^3 - 6x - 1$. (Toto je vlastne polynóm $g(x) = f(2x)$.)

{konstrcvic:ULOODMIMPL}

**Úloha 4.7.3.** Ukážte, že ak číslo $\sqrt{x}$ je skonštruovateľné, tak aj $x$ je skonštruovateľné.

## 4.8 Pridávanie koreňa ireducibilného polynómu k poľu

Viackrát sme videli situáciu, kedy nejaký polynóm nemá koreň v nejakom menšom poli $F$, ale vo vhodnom nadpoli $K$ už koreň má.

### 4.8.1 Rozšírenie obsahujúce koreň $p(x)$

### 4.8.2 Algebraický uzáver daného poľa

## 4.9 Konečné polia

{konec:SECT}

V nižších ročníkoch sme sa spomedzi konečných polí stretli iba s poľom $\mathbb{Z}_p$. (A toto pole sme opäť videli aj tu, teraz sme ho označili ako $\mathbb{Z}/(p)$; pozri tvrdenie 3.3.23.)

Existujú však aj iné konečné polia – štvorprvkové pole sme videli v príklade 4.5.11.

Pre konečné polia platí:

- Počet prvkov konečného poľa je mocnina prvočísla, t.j.

$$|F| = p^n$$

  pre nejaké prvočíslo $p$ a kladné celé číslo $n$.
- Obrátene, pre každé číslo tvaru $p^n$ existuje pole $F$ také, že $|F| = p^n$.
- Navyše $p^n$–prvkové pole je jediné až na izomorfizmus.

Fakt, ktorý spomíname v prvom bode nie je príliš ťažké dokázať s vedomosťami, ktoré teraz máme. Dôkaz ďalších dvoch častí je o čosi náročnejší. (Dá sa k nemu dopracovať rôznymi spôsobmi – ale bez ohľadu na to, ktorý z nich si vyberiem, potrebujeme ešte povedať niektoré fakty, ktoré sme doteraz neuviedli.)

### 4.9.1 Charakteristika poľa

**Definícia 4.9.1.** Nech $F$ je pole. Potom číslo $n$ sa volá *charakteristika poľa $F$,* ak $n$ je najmenšie také kladné celé číslo, že

$$n \times 1 = \underbrace{1 + 1 + \cdots + 1}_{n\text{-krát}} = 0.$$

Ak také číslo neexistuje, tak hovoríme, že charakteristika poľa $F$ je nekonečno.

Charakteristiku poľa označíme $\mathrm{char}(F)$.

Podľa definície teda vždy máme $\mathrm{char}(F) = \infty$ alebo $\mathrm{char}(F) = n$ pre nejaké číslo $n$. Definícia sa stručne dá zhrnúť tak, že

$$\mathrm{char}(F) = \min\{n \in \mathbb{Z}; n > 0, n \times 1 = 0\}.$$

Poznamenajme, že výraz $n \times 1$ má zmysel aj pre záporné $n$, stačí položiť $(-n) \times 1 = -(n \times 1)$. Potom má zmysel hovoriť o množine

$$I = \{n \in \mathbb{Z}; n \times 1 = 0\}$$

Môžeme si všimnúť, že táto množina je ideál v $\mathbb{Z}$ (úloha 4.9.1).

Ak je charakteristika nejaké konečné číslo $n$, tak $I = (n)$. T.j. charakteristika je číslo, ktoré generuje tento ideál.

Ak $\mathrm{char}(F) = \infty$, tak $I = (0)$. (Toto je dôvod, prečo sa v literatúre namiesto konvencie $\mathrm{char}(F) = \infty$ pre tento prípade často používa $\mathrm{char}(F) = 0$. My sme použili konvenciu, ktorá je konzistentná s tým, že charakteristiku definujeme ako minimum nejakej množiny.)

Nasledujúce pozorovanie je síce jednoduché, ale využijeme ho na viacerých miestach, takže sme ho sformulovali ako lemu.

{konec:LMNTIMESHOM}

**Lema 4.9.2.** *Pre ľubovoľné $k, l \in \mathbb{Z}$ platí*

$$(k \times 1) + (l \times 1) = (k + l) \times 1$$
$$(k \times 1) \cdot (l \times 1) = (k \cdot l) \times 1$$

*Teda zobrazenie $\mathbb{Z} \mapsto F$ definované ako*

$$n \mapsto n \times 1$$

*je homomorfizmus.*

Zdôvodnenie prečo takéto niečo funguje, je pomerne priamočiare – aj keď treba zvlášť rozoberať niekoľko prípadov v závislosti od toho, či čísla vystupujúce v tejto rovnosti sú kladné alebo záporné.

*Dôkaz.* Úloha 4.9.2. □

**Tvrdenie 4.9.3.** *Ak $F$ je konečné pole, tak $F$ má konečnú charakteristiku a* $\mathrm{char}(F)$ *je prvočíslo.*

*Dôkaz. Charakteristika je konečná.* Ak sa pozrieme na prvky tvaru $n \times 1$ pre kladné celé čísla $n$, tak všetky tieto prvky sa vyskytujú v konečnej množine $F$. Preto sa určite niekedy zopakuje ten istý prvok, t.j. máme dve rôzne kladné celé čísla $k$ a $l$ také, že

$$k \times 1 = l \times 1.$$

BÚNV môžeme predpokladať, že $k > l$. Potom ale platí

$$(k-l)\times = 0.$$

Teda existuje aspoň jedno kladné $n$ také, že $n \times 0$.

*Charakteristika nemôže byť zložené číslo.* Ak máme zložené číslo $n = k \cdot l$ a platí $n \times 1 = 0$, tak potom dostaneme

$$n \times 1 = (k \times 1) \cdot (l \times 1) = 0.$$

To ale znamená, že $k \times 1 = 0$ alebo $l \times 1 = 0$. Teda $n$ nie je najmenšie číslo s takouto vlastnosťou. □

**Tvrdenie 4.9.4.** *Ak $F$ je konečné pole a* $\mathrm{char}(F) = p$*, tak $F$ obsahuje podpole izomorfné so* $\mathbb{Z}_p$*.*

*Dôkaz.* Nech $\mathrm{char}(F) = p$. Vieme, že $p$ je prvočíslo.

Definujme $\varphi\colon \mathbb{Z}_p \to F$ ako

$$\varphi\colon n \mapsto n \times 1.$$

Potom takéto zobrazenie je injektívny homomorfizmus.

Budeme teraz pracovať so sčitovaním a násobením v $\mathbb{Z}_p$ aj v $\mathbb{Z}$. Aby sme ich odlíšili, použijme $\oplus$ a $\odot$ pre operácie v $\mathbb{Z}_p$.

*Kedy* $k \times 1 = l \times 1$. Všimnime si, že pre $k, l \in \mathbb{Z}$ máme

$$k \times 1 = l \times 1 \qquad \Leftrightarrow \qquad k \equiv l \pmod{p}. \tag{4.13}$$ {konec:EQCHARKONG}

(Dôkaz nie je príliš ťažký – úloha 4.9.3.)

*$\varphi$ je homomorfizmus.* Pre ľubovoľné $k, l \in \mathbb{Z}_p$ máme $k \oplus l \equiv k + l \pmod{p}$ a $k \odot l \equiv k \cdot l \pmod{p}$, čiže

$$\begin{aligned}\varphi k \oplus l &= (k \oplus l) \times 1 = (k + l) \times 1 = (k \times 1) + (l \times 1) = \varphi(k) + \varphi(l)\\ \varphi k \odot l &= (k \odot l) \times 1 = (k \cdot l) \times 1 = (k \times 1) \cdot (l \times 1) = \varphi(k) \cdot \varphi(l)\end{aligned}$$

*$\varphi$ je injektívne.* Ak platí $\varphi(k) = \varphi(l)$ pre nejaké $k, l \in \mathbb{Z}_p$, tak podľa (4.13) to znamená, že

$$k \equiv l \pmod{p}.$$

Ak súčasne vieme, že $k, l \in \{0, 1, \ldots, p-1\}$, tak z toho už dostávame $k = l$. □

**Poznámka 4.9.5.** Môžeme si všimnúť, že aj nekonečné pole máme iba dve možnosti – buď $\mathrm{char}(F) = \infty$ alebo $\mathrm{char}(F)$ je prvočíslo. (Druhá časť prechádzajúceho dôkazu funguje pre ľubovoľné pole konečnej charakteristiky.)

**Dôsledok 4.9.6.** *Ak $F$ je konečné pole a* $\mathrm{char}(F) = p$*, tak počet prvkov poľa $F$ je mocnina prvočísla $p$.*

$$|F| = p^n$$

**Tvrdenie 4.9.7.** *Nech $F$ je pole a* $\mathrm{char}(F) = p$*. Potom pre ľubovoľné $x, y \in F$ platí*

$$\begin{aligned}(x+y)^p &= x^p + y^p\\ (x \cdot y)^p &= x^p \cdot y^p\end{aligned}$$

### Cvičenia

{koneccvic:ULO

**Úloha 4.9.1.** Nech $F$ je pole. Ukážte, že potom

$$I = \{n \in \mathbb{Z}; n \times 1 = 0\}$$

je ideál v $\mathbb{Z}$.

{koneccvic:ULO

**Úloha 4.9.2.** Nech $F$ je pole. Ukážte, že zobrazenie $\mathbb{Z} \mapsto F$ definované ako

$$n \mapsto n \times 1$$

je homomorfizmus.

{koneccvic:ULOCHARKONG}

**Úloha 4.9.3.** Nech $F$ je pole a $\mathrm{char}(F) = p$. Dokážte, že platí:

$$k \times 1 = l \times 1 \qquad \Leftrightarrow \qquad k \equiv l \pmod{p}.$$

# Literatúra


[DF] David S. Dummit a Richard M. Foote. *Abstract Algebra.* John Willey and Sons, 3rd edition, 2004.

[JMP] Arthur Jones, Sidney A. Morris, a Kenneth R. Pearson. *Abstract Algebra and Famous Impossibilities.* Springer-Verlag, New York, 1991. Universitext.

[K] Július Korbaš. *Lineárna algebra a geometria I.* UK, Bratislava, 2003.

[KG] Július Korbaš a Štefan Gyürki. *Prednášky z lineárnej algebra a geometrie.* UK, Bratislava, 2013.

[KGGS] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, a Jaroslav Smítal. *Algebra a teoretická aritmetika 1.* UK, Bratislava, 2002.

[Sl1] Martin Sleziak. 1-MAT-260 Algebra 2. Poznámky k prednáške, `https://msleziak.com/vyuka/2011/alg2m/`.

[Sl2] Martin Sleziak. Teória množín pre učiteľov. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

[St] Ian Stewart. *Galois theory.* CRC, Boca Raton, 3rd edition, 2004.

[Z] Pavol Zlatoš. *Lineárna algebra a geometria. Cesta z troch rozmerov s presahmi do príbuzných disciplín.* Marenčin PT, Bratislava, 2011. `http://thales.doa.fmph.uniba.sk/zlatos/`.

# Register

# Zoznam symbolov