

Algebra

1 Vektorové priestory, lineárne zobrazenia (priestor, podpriestor, lineárna závislosť, báza, dimenzia. Steinzova veta, súčty podpriestorov, lineárne zobrazenia, kompozícia lineárnych zobrazení, inverzné lineárne zobrazenia, matica lineárneho zobrazenia, jadro a obraz lineárneho zobrazenia)

Vektorový priestor:

Definícia 4.1.1. Nech F je pole a $V \neq \emptyset$ je množina. Nech $+$ je binárna operácia na V a každej dvojici $c \in F$, $\vec{\alpha} \in V$ je priradený prvok $c \cdot \vec{\alpha} \in V$, pričom platí pre libovoľné $c, d \in F$ a $\vec{\alpha}, \vec{\beta} \in V$:

- (i) $(V, +)$ je komutatívna grupa,
- (ii) $c \cdot (\vec{\alpha} + \vec{\beta}) = c \cdot \vec{\alpha} + c \cdot \vec{\beta}$,
- (iii) $(c + d) \cdot \vec{\alpha} = c \cdot \vec{\alpha} + d \cdot \vec{\alpha}$,
- (iv) $(c \cdot d) \cdot \vec{\alpha} = c \cdot (d \cdot \vec{\alpha})$,
- (v) $1 \cdot \vec{\alpha} = \vec{\alpha}$.

Potom hovoríme, že V je *vektorový priestor* nad polom F .

Vektorový podpriestor:

Definícia 4.2.1. Ak V je vektorový priestor nad polom F , $S \neq \emptyset$ a $S \subseteq V$, tak S nazveme *podpriestorom* (alebo tiež *vektorovým podpriestorom*) priestoru V , ak

- (i) pre libovoľné $\vec{\alpha}, \vec{\beta} \in S$ platí $\vec{\alpha} + \vec{\beta} \in S$,
- (ii) pre libovoľné $\vec{\alpha} \in S$ a $c \in F$ platí $c\vec{\alpha} \in S$.

Inými slovami, podpriestor vektorového priestoru V je taká podmnožina S , ktorá je uzavretá vzhľadom sčítavanie aj vzhľadom na násobenie skalárom.

Poznámka 4.2.2. Všimnime si, že každý *podpriestor* S priestoru V musí obsahovať nulový vektor $\vec{0}$. Vyplýva to z toho, že $S \neq \emptyset$, teda obsahuje aspoň jeden vektor $\vec{\alpha}$. Z uzavretosti na násobenie skalárom vyplýva, že musí obsahovať aj vektor $\vec{0} = 0 \cdot \vec{\alpha}$.

Lineárna závislosť:

Definícia 4.3.9. Nech V je vektorový priestor nad polom F . Vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sú *lineárne závislé*, ak existujú $c_1, \dots, c_n \in F$, ktoré nie sú všetky nulové a platí

$$c_1 \vec{\alpha}_1 + \dots + c_n \vec{\alpha}_n = \vec{0}.$$

(Stručne: $\vec{0}$ je nenulovou lineárnnou kombináciou vektorov $\vec{\alpha}_1, \dots, \vec{\alpha}_n$.)

V opačnom prípade hovoríme, že vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ *lineárne nezávislé*.

Báza:

Definícia 4.4.2. Nech V je vektorový priestor nad polom F . Množinu vektorov $\{\vec{\alpha}_1, \dots, \vec{\alpha}_n\}$ nazývame *bázou* priestoru V , ak

- (i) vektorov $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sú lineárne nezávislé,
- (ii) $V = [\vec{\alpha}_1, \dots, \vec{\alpha}_n]$.

(Stručne: Báza je taká množina lineárne nezávislých vektorov, ktorá generuje celý priestor.)

Dimenzia:

Definícia 4.4.9. *Dimensiou* konečnorozmerného vektorového priestoru V nazývame počet prvkov ľuboľnej jeho bázy. (Pre nulový priestor dodefinujeme $d(\{0\}) = 0$.) Toto číslo označujeme $d(V)$.

Steinitzova veta:

Veta 4.3.15 (Steinitzova veta o výmene). *Nech V je vektorový priestor nad polom F . Ak $V = [\vec{\alpha}_1, \dots, \vec{\alpha}_n]$ (vektorový priestor V je generovaný vektormi $\vec{\alpha}_1, \dots, \vec{\alpha}_n$) a $\vec{\beta}_1, \dots, \vec{\beta}_s \in V$ sú lineárne nezávislé vektorov, tak*

- (i) $s \leq n$,
- (ii) z vektorov $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ sa dá vybrať $n - s$ vektorov, ktoré spolu s vektormi $\vec{\beta}_1, \dots, \vec{\beta}_s$ generujú V .

Súčty podpriestorov:

Veta 4.5.1. *Nech S, T sú vektorové podpriestory vektorového priestoru V nad polom F . Potom*

$$S + T = \{\vec{\alpha} + \vec{\beta}; \vec{\alpha} \in S, \vec{\beta} \in T\}$$

je podpriestorom vektorového priestoru V .

Táto veta vlastne hovorí, že množina všetkých vektorov, ktoré sa dajú získať ako súčty vektorov z S a z T , tvorí vektorový podpriestor. Všimnite si, že v predchádzajúcom príklade bolo $S + T = [(1, 0, 0), (0, 1, 0)]$.

Dôkaz. Overíme podmienky z definície vektorového podpriestoru. Množina $S + T$ je *neprázdna*, lebo $\vec{0} \in S, \vec{0} \in T$, čiže $\vec{0} = \vec{0} + \vec{0} \in S + T$.

S + T je uzavretá na súčty: Ak $\vec{\gamma}_1, \vec{\gamma}_2 \in S + T$, tak vektorov $\vec{\gamma}_1, \vec{\gamma}_2$ sa dajú napísat v tvare $\vec{\gamma}_1 = \vec{\alpha}_1 + \vec{\beta}_1, \vec{\gamma}_2 = \vec{\alpha}_2 + \vec{\beta}_2$, kde $\vec{\alpha}_1, \vec{\alpha}_2 \in S$ a $\vec{\beta}_1, \vec{\beta}_2 \in T$. Potom $\vec{\gamma}_1 + \vec{\gamma}_2 = (\vec{\alpha}_1 + \vec{\beta}_1) + (\vec{\alpha}_2 + \vec{\beta}_2) = (\vec{\alpha}_1 + \vec{\alpha}_2) + (\vec{\beta}_1 + \vec{\beta}_2)$. (Využili sme komutativnosť a asociatívnosť sčítovania.) Pretože S je

vektorový podpriestor vektorov $\vec{\alpha}_1 + \vec{\alpha}_2$ patrí do S , podobne $\vec{\beta}_1 + \vec{\beta}_2 \in T$. Ukázali sme, že vektor $\vec{\gamma}_1 + \vec{\gamma}_2$ sa dá napísat ako súčet vektorov z S a vektorov z T , teda $\vec{\gamma}_1 + \vec{\gamma}_2 \in S + T$.

S + T je uzavretá na násobenie skalárom: Ak $\vec{\gamma} \in S + T$, tak $\vec{\gamma} = \vec{\alpha} + \vec{\beta}$ pre nejaké $\vec{\alpha} \in S$ a $\vec{\beta} \in T$. Nech $c \in F$ je ľuboľný skalár. Potom $c\vec{\gamma} = c\vec{\alpha} + c\vec{\beta}$. Pritom $c\vec{\alpha} \in S, c\vec{\beta} \in T$, čiže $c\vec{\gamma} \in S + T$. \square

Definícia 4.5.2. Ak S, T sú podpriestory vektorového podpriestoru V , tak vektorový podpriestor $S + T$ sa nazýva *lineárny súčet* podpriestorov S a T .

Vidno, že S aj T sú podmnožiny $S + T$, čiže $S + T$ obsahuje oba podpriestory S aj T . ($\vec{\alpha} \in S \Rightarrow \vec{\alpha} = \vec{\alpha} + \vec{0} \in S + T$, podobne pre T .) Priestor $S + T$ je skutočne najmenší vektorový podpriestor priestoru V , ktorý obsahuje S aj T . Ak totiž $S, T \subseteq U$ a U je vektorový podpriestor V , tak U musí obsahovať všetky súčty tvaru $\vec{\alpha} + \vec{\beta}$, pretože $\vec{\alpha} \in S \subseteq S + T$ a $\vec{\beta} \in T \subseteq S + T$.

Definícia 4.5.5. Nech S, T sú podpriestory vektorového priestoru V nad poľom F a nech $S \cap T = \{\vec{0}\}$. Potom podpriestor $S + T$ nazývame *direktný (priamy) súčet* podpriestorov S a T a označujeme ho $S \oplus T$.

Lineárne zobrazenia:

Definícia 5.3.1. Ak V a W sú vektorové priestory nad poľom F a $f: V \rightarrow W$ je zobrazenie z V do W , tak hovoríme, že f je *lineárne zobrazenie*, ak pre ľubovoľné $\vec{\alpha}, \vec{\beta} \in V$ a ľubovoľné $c \in F$ platí

- (i) $f(\vec{\alpha} + \vec{\beta}) = f(\vec{\alpha}) + f(\vec{\beta})$,
- (ii) $f(c\vec{\alpha}) = cf(\vec{\alpha})$.

Inými slovami, lineárne zobrazenia sú tie zobrazenia, ktoré zachovávajú základné operácie popisujúce vektorový priestor.

Kompozícia lineárnych zobrazení:

Inverzné lineárne zobrazenia:

Pripomeňme, že zobrazenie $g: Y \rightarrow X$ nazývame inverzným zobrazením k zobrazeniu $f: X \rightarrow Y$, ak

$$\begin{aligned} g \circ f &= id_X \\ f \circ g &= id_Y \end{aligned}$$

(definícia 2.2.15) a označujeme ho f^{-1} . Ďalej vieme, že inverzné zobrazenie k zobrazeniu f existuje práve vtedy, keď f je bijektia (tvrdenie 2.2.16).

Matica lineárneho zobrazenia:

Definícia 5.3.8. Nech F je pole. *Matica lineárneho zobrazenia* $f: F^m \rightarrow F^n$ je matica typu $m \times n$ ktorej k -ty riadok je vektor $f(\vec{e}_k)$.

Maticu zobrazenia f budeme označovať A_f .

Každému lineárному zobrazeniu $f: F^m \rightarrow F^n$ sme takto priradili nejakú maticu A_f typu $m \times n$.

Obrátene, ľubovoľnou maticou typu $m \times n$ je jednoznačne určené lineárne zobrazenie $f: F^m \rightarrow F^n$. (Riadky matice určujú obrazy bázových vektorov, jednoznačnosť a existencia takéhoto zobrazenia vyplývajú z vety 5.3.7.) Lineárne zobrazenie prislúchajúce matici A budeme označovať f_A .

Veta 5.3.7. Nech V, W sú vektorové priestory. Nech $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ je báza priestoru V a nech $\vec{\beta}_1, \dots, \vec{\beta}_n \in W$. Potom existuje práve jedno lineárne zobrazenie $f: V \rightarrow W$ také, že

$$f(\vec{\alpha}_i) = \vec{\beta}_i$$

pre $i = 1, 2, \dots, n$.

Dôkaz. Nech $\vec{\alpha} \in V$. Pretože $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ tvorí bázu priestoru V , existujú jednoznačne určené skaláry $c_1, \dots, c_n \in F$ také, že

$$\vec{\alpha} = c_1 \vec{\alpha}_1 + \dots + c_n \vec{\alpha}_n.$$

Potom $f(\vec{\alpha})$ definujeme ako

$$f(\vec{\alpha}) = c_1 \vec{\beta}_1 + \dots + c_n \vec{\beta}_n.$$

Jadro a obraz lineárneho zobrazenia:

Definícia 5.8.1. Nech V a W sú vektorové priestory nad poľom F a $f: V \rightarrow W$ je lineárne zobrazenie. Potom *jadrom lineárneho zobrazenia f* nazývame množinu

$$\text{Ker } f = \{\vec{\alpha} \in V; f(\vec{\alpha}) = \vec{0}\}$$

a *obrazom lineárneho zobrazenia f* nazývame množinu

$$\text{Im } f = \{f(\vec{\alpha}); \vec{\alpha} \in V\}.$$

Inými slovami, $\text{Ker } f$ obsahuje práve tie vektory z V , ktoré sa zobrazia na nulový vektor a $\text{Im } f$ obsahuje obrazy všetkých vektorov z V . Lahko sa overí, že $\text{Ker } f$ aj $\text{Im } f$ sú vektorové podpriestory. (Môžete si všimnúť, že ide os špeciálny prípad úlohy 5.3.6.)

2 Matice a riešenia lineárnych rovníc nad poľom F (matice, operácie s maticami (násobenie, sčítanie), elementárne riadkové operácie, trojuholníkový a redukovaný tvar matice, systémy lineárnych rovníc nad poľom F, množina riešení (ne)homogénnych systémov lineárnych rovníc, existencia a tvary riešení)

Matice:

Definícia 5.1.1. Maticou typu $m \times n$ nad polom F nazývame ľubovoľnú tabuľku pozostávajúcu z prvkov pola F , ktorá má m riadkov a n stĺpcov.

Matice zapisujeme v tvare

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

pričom a_{ij} označuje prvok v i -tom riadku a j -tom stĺpca.

Niekedy bude výhodné použiť stručnejší zápis $\|a_{ij}\|$, čím myslíme, že pre stručnosť niekedy len uvedieme predpis pre prvok i -teho riadku a j -teho stĺpca.

Definícia 5.1.6. Maticu typu $n \times n$ (teda takú, ktorá má rovnaký počet riadkov a stĺpcov) nazývame **štvorcová matica**.

Maticu

$$I = I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

typu $n \times n$, ktorá má na diagonále jednotky a mimo diagonály nuly, nazývame **jednotková matica**.

Štvorcová matica, ktorá má mimo diagonály iba nuly (t.j. $a_{ij} = 0$ pre $i \neq j$) sa nazýva **diagonálna matica**. (Príkladom diagonálnej matice je jednotková matica.)

Definícia 5.1.8. Transponovaná matica k matici A typu $m \times n$ je matica A^T typu $n \times m$ určená ako

$$A^T = \|a_{ji}\|.$$

Štvorcová matica A sa nazýva **symetrická**, ak $A = A^T$ a **antisymetrická**, ak $A = -A^T$.

Teda A^T je vlastne matica A prevrátená symetricky podľa hlavnej diagonály.

Môžeme si všimnúť, že platí $I^T = I$, $(A^T)^T = A$, $(A + B)^T = A^T + B^T$ a $(cA)^T = cA^T$

Operácie s maticami:

Definícia 5.1.3. Nech A, B sú matice typu $m \times n$ nad poľom F a $c \in F$.

- (a) Súčet matíc $A = ||a_{ij}||$ a $B = ||b_{ij}||$ je matica $A + B = ||a_{ij} + b_{ij}||$.
- (b) Matica $c.A = ||ca_{ij}||$ sa nazýva c -násobok matice A .

(Teda sčítovanie matíc a násobenie matice skalárom definujeme po súradničiach.)

Všimnime si, že súčet matíc definujeme len pre matice rovnakého typu.

Elementárne riadkové operácie:

Definícia 5.2.3. Elementárne riadkové operácie na matici A nad poľom F sú:

1. výmena 2 riadkov matice,
2. vynásobenie niektorého riadku matice nenulovým prvkom c poľa F ,
3. pripočítanie násobku niektorého riadku k inému riadku.

Hovoríme, že matice A a B sú *riadkovo ekvivalentné* ak maticu B možno z A dostať pomocou konečnej postupnosti elementárnych riadkových operácií. Ak matice A a B sú riadkovo ekvivalentné, zapisujeme to ako $A \sim B$.

Trojuholníkový a redukovaný tvar matice:

Definícia 5.2.8. Matica A je *redukovaná trojuholníková matica*, ak:

- (i) Vedúci (=prvý nenulový) pravok každého riadku matice je 1.
- (ii) Každý stĺpec obsahujúci vedúci pravok niektorého riadku má pravky v ostatných riadkoch nulové.
- (iii) Nulové riadky ležia pod nenulovými riadkami. (Presnejšie povedané: Akýkoľvek nulový riadok musí byť nižšie ako akýkoľvek nenulový riadok.)
- (iv) Vedúci pravok lubovoľného nenulového riadku je napravo od vedúcich pravkov všetkých nenulových riadkov nad ním a naľavo od vedúcich pravkov riadkov pod ním (t.j. vedúce riadky sú usporiadane zľava doprava).

Napríklad matica $\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & \frac{3}{2} \\ 0 & 0 & 0 \end{pmatrix}$, ktorú sme dostali v príklade 5.2.4 je redukovaná trojuholníková matica.

Lubovoľná redukovaná trojuholníková matica vyzerá zhruba takto:

$$\left(\begin{array}{ccccccccc} 0 & \dots & 0 & \boxed{1} & * & 0 & * & 0 & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & \boxed{1} & * & 0 & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & 0 & \boxed{1} & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \end{array} \right)$$

V predchádzajúcej schéme * označuje miesta, kde môže byť lubovoľný pravok (nulový alebo nenulový). Vidíme, že vedúce jednotky (vyznačené štvorčekom) idú zľava doprava

Pole:

Definícia 3.3.1. Nech F je množina, $+$ a \cdot sú binárne operácie na F . Hovoríme, že trojica $(F, +, \cdot)$ je *pole*, ak

- (i) $(F, +)$ je komutatívna grupa, jej neutrálny prvok budeme označovať 0;
- (ii) $(F \setminus \{0\}, \cdot)$ je komutatívna grupa, jej neutrálny prvok budeme označovať 1;
- (iii) pre ľubovoľné $a, b, c \in F$ platí

$$\begin{aligned} a(b+c) &= ab+ac, \\ (a+b)c &= ac+bc. \end{aligned}$$

(Túto vlastnosť nazývame *distributivnosť*.)

Pre inverzný prvok v grupe $(F, +)$ budeme používať označenie $-a$, t.j. pre túto grupu používame aditívny zápis. Prvok $-a$ nazývame *opačný prvok* k prvku a .

Pre grupu $(F \setminus \{0\}, \cdot)$ budeme používať multiplikatívny zápis, teda inverzný prvok k prvku $a \neq 0$ poľa F vzhľadom na operáciu \cdot budeme značiť a^{-1} . Ak použijeme termín *inverzný prvok* v súvislosti s poľom a nešpecifikujeme binárnu operáciu, myslí sa tým práve prvok a^{-1} .

Namiesto $b + (-c)$ budeme používať stručnejší zápis $b - c$.

O operáciach $+$ a \cdot v poli F budeme niekedy hovoriť ako o sčítovaní a násobení (súčte a súčine), presne tak ako je to v najzákladnejších príkladoch polí.

Aby bolo jasné, ktorá operácia sa vykoná najskôr, mali by sme používať zápis ako napríklad $(a.b) + (c.d)$. Budeme používať rovnakú konvenciu, aká je zaužívaná pre reálne čísla – operácia \cdot má vyššiu prioritu ako operácia $+$, teda predchádzajúci zápis môžeme stručnejšie zapísť ako $ab + cd$.

Definícia 3.3.3. Pole je množina F , na ktorej sú definované 2 binárne operácie $+$ a \cdot splňajúce:

- (i) pre všetky $a, b, c \in F$ platí $a + (b + c) = (a + b) + c$,
- (ii) pre všetky $a, b \in F$ platí $a + b = b + a$,
- (iii) existuje prvok $0 \in F$ taký, že pre každé $a \in F$ sa $a + 0 = a$,
- (iv) ku každému $a \in F$ existuje $b \in F$ tak, že $a + b = 0$,
- (v) pre všetky $a, b, c \in F$ platí $a.(b.c) = (a.b).c$,
- (vi) pre všetky $a, b \in F$ platí $a.b = b.a$,
- (vii) existuje prvok $1 \in F$ taký, že $1 \neq 0$ a pre každé $a \in F$ sa $a.1 = a$,
- (viii) ku každému $a \in F$, $a \neq 0$ existuje $b \in F$ tak, že $a.b = 1$,
- (ix) pre všetky $a, b, c \in F$ sa $a.(b + c) = a.b + a.c$.

Overenie ekvivalentnosti týchto 2 definícií ponechávame ako cvičenie (úloha 3.3.1). Možno vám pri tom pomôžu niektoré zo základných vlastností poľa, ktoré odvodíme v nasledujúcom tvrdení. (My budeme používať definíciu 3.3.1. Samozrejme, akonáhle viete dokázať ekvivalentnosť oboch definícií, môžete používať ktorukolvek z nich.)

Sústavy lineárnych rovníc:

Definícia 5.7.1. Sústavou lineárnych rovníc rozumieme systém rovníc tvaru

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = c_1$$

$$a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = c_2$$

...

$$a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = c_m$$

kde $a_{ij}, c_i \in F$ pre všetky prípustné hodnoty indexov i a j .

Riešenie sústavy lineárnych rovníc je n -tica (x_1, \dots, x_n) ktorá spĺňa všetky uvedené rovnice. Ak existuje aspoň jedno riešenie sústavy lineárnych rovníc, hovoríme, že táto sústava je *riešiteľná*. Skaláry c_1, \dots, c_n nazývame *pravé strany*, a_{ij} sú *koeficienty* a x_i sú neznáme.

Maticu

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

nazývame *matica sústavy* (5.2).

Maticu

$$A' = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & c_1 \\ a_{21} & a_{22} & \dots & a_{2n} & c_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} & c_m \end{pmatrix}$$

nazývame *rozšírená matica sústavy* (5.2).

Pomocou matice sústavy môžeme zadefinovať *maticový zápis* sústavy

$$A\vec{x}^T = \vec{c}^T$$

alebo

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix}$$

Skutočne, (x_1, \dots, x_n) je riešením sústavy (5.2) práve vtedy, keď platí uvedená maticová rovnosť.

Veta 5.7.2. Ak rozšírené matice dvoch sústav lineárnych rovníc sú riadkovo ekvivalentné, tak tieto dve sústavy majú rovnakú množinu riešení.

Množina riešení (ne)homogénnych sústémov lineárnych rovníc:

V prípade, že pravé strany sú nulové ($c_1 = c_2 = \dots = c_n = 0$), nazývame sústavu (5.2) *homogénna* sústava lineárnych rovníc. Lahko si môžeme všimnúť, že v prípade homogénnej sústavy je nulový vektor $(0, 0, \dots, 0)$ riešením sústavy. Toto riešenie nazývame *triviálne riešenie*.

Veta 5.7.3. *Množina všetkých riešení homogénnej sústavy lineárnych rovníc tvorí podpriestor priestoru F^n .*

Dôkaz. Stačí overiť vlastnosti z definície podpriestoru.

Ak $\vec{\alpha}$ a $\vec{\beta}$ sú riešeniami homogénnej sústavy s maticou A , znamená to, že $A.\vec{\alpha}^T = \vec{0}^T$ a $A.\vec{\beta}^T = \vec{0}^T$.

Sčítaním týchto rovností dostaneme $A.(\vec{\alpha} + \vec{\beta})^T = \vec{0}^T$, teda aj $\vec{\alpha} + \vec{\beta}$ je riešením tejto sústavy. Ak prvú rovnosť vynásobíme skalárom F , máme $A.(c\vec{\alpha})^T = \vec{0}^T$, čo znamená, že aj $c\vec{\alpha}$ je riešením sústavy. \square

Rozšírenú maticu sústavy lineárnych rovníc môžeme teda upraviť na redukovanú trojuholníkovú maticu. Predpokladajme, že sme navyše preusporiadali premenné (čo vlastne zodpovedá permutácií niektorých stĺpcov) tak, aby vo výslednej matici boli ako prvé tie stĺpce, kde vystupujú vedúce jednotky. Navyše môžeme vyniechať všetky nulové riadky bez toho, aby sme nejako ovplyvnili množinu riešení. Dostaneme takto maticu, ktorej zodpovedá sústava

$$\begin{aligned} x_1 + c_{1,r+1}x_{r+1} + c_{1,r+2}x_{r+2} + \dots + c_{1,n}x_n &= 0 \\ x_2 + c_{2,r+1}x_{r+1} + c_{2,r+2}x_{r+2} + \dots + c_{2,n}x_n &= 0 \\ &\dots \\ x_r + c_{r,r+1}x_{r+1} + c_{r,r+2}x_{r+2} + \dots + c_{r,n}x_n &= 0 \end{aligned} \tag{5.3}$$

pričom r označuje hodnosť pôvodnej matice (a teda aj matice C).

Vidíme, že ak si zvolíme hodnotu neznámych $x_{r+1}, x_{r+2}, \dots, x_n$, dá sa z týchto rovníc dorátať hodnota neznámych x_1, x_2, \dots, x_r . Ak postupne dosadíme 1 za x_{r+k} a 0 za ostatné neznáme, ktoré si môžeme voliť (pre $k = 1, 2, \dots, n - r$) dostaneme tieto riešenia sústavy

$$\begin{aligned} \vec{\gamma}_{r+1} &= (-c_{1,r+1}, -c_{2,r+1}, \dots, -c_{r,r+1}, 1, 0, \dots, 0), \\ \vec{\gamma}_{r+2} &= (-c_{1,r+2}, -c_{2,r+2}, \dots, -c_{r,r+2}, 0, 1, \dots, 0), \\ &\dots \\ \vec{\gamma}_n &= (-c_{1,n}, -c_{2,n}, \dots, -c_{r,n}, 0, \dots, 0, 1). \end{aligned}$$

Veta 5.7.4. *Vektory $\vec{\gamma}_{r+1}, \vec{\gamma}_{r+2}, \dots, \vec{\gamma}_n$ tvoria bázu priestoru riešení homogénnej sústavy*

Dôsledok 5.7.5. *Nech A je matica typu $m \times n$ a S je priestor riešení homogénnej sústavy lineárnych rovníc s maticou A . Potom*

$$d(S) = n - h(A).$$

Dôsledok 5.7.7. *Homogénna sústava lineárnych rovníc s n neznámymi, ktorej matica má hodnosť n , má len triviálne riešenie.*

Veta 5.7.11. Každý podpriestor priestoru F^n je množinou riešení nejakého homogénneho systému lineárnych rovníc.

Dôkaz. Ak S je podpriestor F^n , tak S je konečnorozmerný (veta 4.4.17). Má teda konečnú bázu $\vec{\alpha}_1, \dots, \vec{\alpha}_r$.

Nech B je matica, ktorej riadky tvoria vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_r$,

$$B = \begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_r \end{pmatrix}.$$

Podľa predchádzajúcej vety má podpriestor riešení homogénnej sústavy

$$B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \vec{0}^T$$

bázu $\vec{\gamma}_{r+1}, \dots, \vec{\gamma}_n$.

Označme ako A maticu, ktorej riadkami sú vektory $\vec{\gamma}_{r+1}, \dots, \vec{\gamma}_n$,

$$A = \begin{pmatrix} \vec{\gamma}_{r+1} \\ \vdots \\ \vec{\gamma}_n \end{pmatrix}.$$

Pretože každý vektor $\vec{\gamma}_i$ je riešením sústavy s maticou B , platí $B \cdot \vec{\gamma}_i^T = \vec{0}^T$. Z toho dostaneme

(treba si uvedomiť, že i -ty stĺpec matice A je $\vec{\gamma}_i^T$, z čoho vyplýva, že stĺpce matice $B \cdot A^T$ môžeme vypočítať ako $B \cdot \vec{\gamma}_i^T$). Transponovaním predchádzajúceho vzťahu dostaneme (na základe (5.1))

$$A \cdot B^T = 0.$$

Ked' porovnáme i -ty stĺpec matice na ľavej a pravej strane predchádzajúcej rovnosti, dostaneme

$$A \vec{\alpha}_i^T = \vec{0}^T,$$

teda vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_r$ sú riešeniami homogénnej sústavy $A \vec{x}^T = \vec{0}^T$.

Označme ako M priestor riešení tejto sústavy. Jeho dimenzia je

$$d(M) = n - h(A) = n - (n - r) = r.$$

Súčasne platí $S \subseteq M$ (pretože všetky vektory $\vec{\alpha}_1, \dots, \vec{\alpha}_r$ patria do M) a $d(S) = d(M)$, teda podľa tvrdenia 4.4.18 platí $S = M$. \square

5.7.2 Gaussova eliminačná metóda

Gaussovou eliminačnou metódou nazývame algoritmus na riešenie sústav lineárnych rovníc, o ktorom sme hovorili v predchádzajúcej kapitole. Ide teda o postup, pri ktorom rozšírenú maticu sústavy najprv upravíme na redukovanú trojuholníkovú matice a z nej už potom vieme zistiť riešenie pôvodnej sústavy.

V prípade, že počas úprav dostaneme riadok tvaru $(0 \dots 0 | c)$, kde $c \neq 0$, sústava nemá riešenie. (Takýto riadok zodpovedá rovnici $0x_1 + \dots + 0x_n = c$.) V takomto prípade samozrejme nemusíme ďalej pokračovať v upravovaní na RTM.

Ak niektoré stĺpce (v upravenej matici) neobsahujú vedúcu jednotku, tak im prislúchajúce premenné zvolíme za parametre.

Ukážeme si tento postup na niekoľkých jednoduchých príkladoch. V prípade homogénnych sústav sme mali dve možnosti – buď existovalo jediné riešenie (pri homogénnej sústave to bolo triviálne riešenie) alebo riešení bolo viac (tvorili pod priestor). Pri nehomogénnej sústave lineárnych rovníc už množina riešení netvorí vektorový pod priestor a navyše pribudne ešte ďalšia možnosť – môže sa stať, že sústava nemá nijaké riešenie.

Príklad 5.7.12. Riešme sústavu

$$\begin{array}{rrrrr} x_1 & -2x_2 & +3x_3 & -4x_4 & = 4 \\ & x_2 & -x_3 & +x_4 & = -3 \\ x_1 & +3x_2 & & -3x_4 & = 1 \\ & -7x_2 & +3x_3 & +x_4 & = -3 \end{array}$$

nad polom \mathbb{R} .

Danú sústavu najprv prepíšeme do matice a potom upravujeme rozšírenú maticu sústavy až kým nedostaneme redukovaný trojuholníkový tvar.

$$\begin{aligned} \left(\begin{array}{cccc|c} 1 & -2 & 3 & -4 & 4 \\ 0 & 1 & -1 & 1 & -3 \\ 1 & 3 & 0 & -3 & 1 \\ 0 & -7 & 3 & 1 & -3 \end{array} \right) &\stackrel{(1)}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 3 & -4 & 4 \\ 0 & 1 & -1 & 1 & -3 \\ 0 & 5 & -3 & 1 & -3 \\ 0 & -7 & 3 & 1 & -3 \end{array} \right) \stackrel{(2)}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 3 & -4 & 4 \\ 0 & 1 & -1 & 1 & -3 \\ 0 & 0 & 2 & -4 & 12 \\ 0 & 0 & -4 & 8 & -24 \end{array} \right) \stackrel{(3)}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 3 & -4 & 4 \\ 0 & 1 & -1 & 1 & -3 \\ 0 & 0 & 1 & -2 & 6 \\ 0 & 0 & 1 & -2 & 6 \end{array} \right) \\ &\stackrel{(4)}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 3 & -4 & 4 \\ 0 & 1 & -1 & 1 & -3 \\ 0 & 0 & 1 & -2 & 6 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) \stackrel{(5)}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 3 & -4 & 4 \\ 0 & 1 & 0 & -1 & -3 \\ 0 & 0 & 1 & -2 & 6 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) \stackrel{(6)}{\sim} \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & -8 \\ 0 & 1 & 0 & -1 & 3 \\ 0 & 0 & 1 & -2 & 6 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) \end{aligned}$$

3 Determinanty (determinant matice, vlastnosti determinantov, Výpočty determinantov a ich použitie pri riešení lineárnych rovníc a hľadaní inverznej matice)

Determinant matice:

Definícia 6.2.3. Nech A je matica typu $n \times n$ nad poľom F , $A = \{a_{ij}\}$. Determinant matice A je

$$|A| = \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} a_{2\varphi(2)} \dots a_{n\varphi(n)}. \quad (6.1)$$

Symbolom $\sum_{\varphi \in S_n}$ rozumieme, že sčítujeme cez celú množinu S_n , teda pre každú permutáciu $\varphi \in S_n$ pripočítame jeden sčítanec uvedeného tvaru. (Množina S_n je konečná, teda takýto súčet je jednoznačne definovaný.)

Definícia 6.2.1. V tejto kapitole budeme označovať ako S_n množinu všetkých permutácií množiny $\{1, 2, \dots, n\}$.

Dvojica $(\varphi(k), \varphi(s))$ sa volá *inverzia* permutácie φ , ak $k < s$ ale $\varphi(k) > \varphi(s)$. Počet inverzií permutácie φ budeme označovať $i(\varphi)$.

Vlastnosti determinantov:

Výpočty determinantov:

6.3.1 Laplaceov rozvoj

Nech A je štvorcová matica typu $n \times n$. Zvoľme si (pevne) nejaké $i \in \{1, 2, \dots, n\}$. Potom determinant matice A sa dá upraviť na tvar

$$|A| = a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in}.$$

Vyplýva to z toho, že v každom sčítanci v sume (6.1) vystupuje práve jeden prvok tvaru a_{ik} (konkrétnie je to $a_{i\varphi(i)}$). Aby sme získali uvedenú rovnosť, stačí vyňať a_{ij} z tých sčítancov v ktorých sa vyskytuje.

Podobne by sme mohli postupovať aj pre prvky niektorého stĺpca $a_{1j}, a_{2j}, \dots, a_{nj}$. Dostali by sme

$$|A| = a_{1j}A_{1j} + a_{2j}A_{2j} + \dots + a_{nj}A_{nj}.$$

Výraz A_{ij} nazývame *algebraický doplnok* prvku a_{ij} .

Naším najbližším cieľom bude zistiť, čomu sa rovná A_{ij} .

Pokúste sa sami si vyskúšať zistiť všetky možné hodnoty A_{ij} pre maticu 3×3 , výsledky si môžete skontrolovať v nasledujúcim príklade.

6.3.2 Výpočet pomocou riadkových a stĺpcových operácií

V časti 5.2 sme si ukázali, ako možno pomocou elementárnych riadkových úprav upraviť lubovoľnú maticu na redukovanú trojuholníkovú maticu. Ak by sme vedeli, ako elementárne riadkové úpravy ovplyvňujú hodnotu determinantu a ak by sme vedeli vypočítať determinant redukovej trojuholníkovej matice, tak by sme získali ďalšiu metódu na výpočet determinantov. Práve to je naším najbližším cieľom.

Začneme s tým, že overíme, ako menia hodnotu determinantu jednotlivé elementárne riadkové operácie.

Veta 6.3.2. *Pre algebraický doplnok prvku a_{rs} štvorcovej matice A platí*

$$A_{rs} = (-1)^{r+s} |M_{rs}|$$

Veta 6.3.5. *Ak maticu B získame z A vynásobením k -teho riadku skalárom $c \in F$, tak*

$$|B| = c|A|.$$

Výpočet inverznej matice:

Veta 6.5.1. *Ak A je regulárna matica typu $n \times n$, tak*

$$A^{-1} = \frac{1}{|A|} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}$$

kde A_{ij} označuje algebraický doplnok prvku a_{ij} .

4 Grupy (grupy, podgrupy, izomofrizmus a homomorfizmus grúp, cyklické grupy (s klasifikáciou) a ich podgrupy, Lagrangeova veta, normálna podgrupa, faktorizácia grupy podľa podgrupy)

Grupy:

Definícia 3.1.8. Binárna operácia $*$ na množine M je *komutatívna*, ak pre všetky $x, y \in M$ platí

$$x * y = y * x.$$

Definícia 3.1.9. Binárna operácia $*$ na množine M je *asociatívna*, ak pre všetky $x, y, z \in M$ platí

$$(x * y) * z = x * (y * z).$$

Definícia 3.1.10. Nech $*$ je binárna operácia na množine M . Nech $a \in M$ a nech e je neutrálny prvok operácie $*$. Prvok $b \in M$ je *inverzný* k prvku a , ak platí

$$a * b = b * a = e.$$

Definícia 3.2.1. Dvojica $(G, *)$, kde G je množina a $*$ je binárna operácia na G , sa nazýva *grupa*, ak

- (i) operácia $*$ je asociatívna,
- (ii) operácia $*$ má neutrálny prvok, (neutrálny prvok budeme spravidla označovať e)
- (iii) ku každému prvku $g \in G$ existuje inverzný prvok vzhľadom na operáciu $*$. (Tento inverzný prvok budeme označovať g^{-1} .)

Definícia 3.2.4. Grupa $(G, *)$ sa nazýva *komutatívna*, ak operácia $*$ na G je komutatívna. (Tiež sa používa termín *abelovská grupa*.)

Nie každá grupa je komutatívna. Príkladom nekomutatívnej grupy je grupa S_n všetkých permutácií n -prvkovej množiny pre $n \geq 3$ (úloha 3.2.2).

Veta 3.2.5 (Zákony o krátení). *Ak $(G, *)$ je grupa, tak pre ľubovoľné $a, b, c \in G$ platí*

$$\begin{aligned} a * b &= a * c &\Rightarrow b &= c \\ b * a &= c * a &\Rightarrow b &= c \end{aligned}$$

Inak povedané, zákony o krátení hovoria, že v grupe môžeme krátiť ľubovoľným prvkom zľava aj sprava.

Podgrupy:

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

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

Pod zúžením operácie na podmnožinu rozumieme operáciu danú predpisom

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

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

Homomorfizmus grúp:

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

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

platí pre ľubovoľné $g_1, g_2 \in G$.

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

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

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

- (i) $f(e_G) = e_H$ (teda homomorfizmus musí zobraziať neutrálny prvok na neutrálny prvok);
- (ii) $f(a^{-1}) = (f(a))^{-1}$ (teda homomorfizmy zachovávajú aj inverzné prvky).

Izomorfizmus:

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

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

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

- (i) Ak $f: G \rightarrow H$ je izomorfizmus, tak aj $f^{-1}: H \rightarrow G$ je izomorfizmus.
- (ii) Ak $f: G \rightarrow H$ a $g: H \rightarrow K$ sú homomorfizmy, tak aj $g \circ f: G \rightarrow K$ je homomorfizmus.
- (iii) Ak $f: G \rightarrow H$ a $g: H \rightarrow K$ sú izomorfizmy, tak aj $g \circ f: G \rightarrow K$ je izomorfizmus.

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

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

Potom priamo z definície inverzného zobrazenia vyplýva

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

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

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

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

Cyklické grupy:

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

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

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

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

Definícia 2.4.6. Cyklická grupa je grupa G , ktorá je generovaná nejakým jej prvkom $a \in G$.

Prvok a , ktorý generuje grupu G , nazývame **generátor** grupy G .

Príklad 2.4.7. V príklade 2.2.17 sme videli, že $\mathbb{Z} = [1]$, teda $(\mathbb{Z}, +)$ je cyklická grupa. Súčasne platí $\mathbb{Z} = [-1]$, teda generátor cyklickej grupy nemusí byť jednoznačne určený.

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

Dôkaz. Pretože $e = a^0 \in H$, množina H je neprázdna. Overme, či pre H platí kritérium podgrupy.

Ak $a^n, a^m \in H$, tak aj $a^n * a^m = a^{n+m} \in H$.

Ak $a^n \in H$, tak aj $(a^n)^{-1} = a^{-n} \in H$. □

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

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

Veta 2.4.12. Nech G je cyklická grupa a a je jej generátor. Ak rád prvku a je $n \in \mathbb{N}$, tak $G \cong (\mathbb{Z}_n, \oplus)$. Ak rád prvku a je ∞ , tak $G \cong (\mathbb{Z}, +)$. (Teda každá cyklická grupa je izomorfňa so \mathbb{Z} alebo so \mathbb{Z}_n).

Veta 2.4.13. Každá podgrupa cyklickej grupy je cyklická.

Veta 2.4.14. Homomorfný obraz cyklickej grupy je cyklická grupa.

Veta 2.4.17. Grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ je cyklická práve vtedy, ked m a n sú nesúdeliteľné, t.j. ich najväčší spoločný deliteľ $\gcd(m, n) = 1$. V takomto prípade je prvok $(1, 1)$ jej generátorom.

Rozklady grupy podľa podgrupy:

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

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

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

Lema 3.2.2. Nech G je grupa.

- (i) Násobenie podmnožín je asociatívne, t.j. $A(BC) = (AB)C$ pre ľubovoľné podmnožiny $A, B, C \subseteq G$.
- (ii) Pre ľubovoľnú podmnožinu $A \subset G$ platí $eA = Ae = A$.
- (iii) Ak $B \subseteq C$, tak $AB \subseteq AC$ a $BA \subseteq CA$.
- (iv) Ak H je podgrupa grupy G a $h \in H$, tak $hH = H$.
- (v) Ak H je podgrupa grupy G , tak $H^2 = H \cdot H = H$.
- (vi) Pre ľubovoľnú podmnožinu $A \subseteq G$ platí $(A^{-1})^{-1} = A$, kde používame označenie $A^{-1} = \{a^{-1}; a \in A\}$.
- (vii) Ak H je podgrupa grupy G , tak $H^{-1} = \{h^{-1}; h \in H\} = H$.
- (viii) Pre ľubovoľné podmnožiny $A, B \subseteq G$ platí $(AB)^{-1} = B^{-1} \cdot A^{-1}$.
- (ix) Ak K, H sú podgrupy grupy G , tak $(HK)^{-1} = K^{-1} \cdot H^{-1} = KH$.

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

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

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

$$\begin{aligned} aH &= \{ah; h \in H\}, \\ Ha &= \{ha; h \in H\}. \end{aligned}$$

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

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

Lema 3.2.5. Nech H je podgrupa G a $a, b \in G$. Potom $aH = bH$ práve vtedy, ked $b^{-1}a \in H$. (Ďalšou ekvivalentnou podmienkou je $a^{-1}b \in H$).

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

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

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

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

Lagrangeova veta:

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

$$|G| = |H| \cdot [G : H].$$

Teda počet prvkov podgrupy H delí počet prvkov G .

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Normálne podgrupy:

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

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

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

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

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

Dôkaz druhej časti tvrdenia je analogický. \square

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

- (i) $aH = Ha$ pre všetky $a \in G$,
- (ii) $aH \subseteq Ha$ pre všetky $a \in G$,
- (iii) $Ha \subseteq aH$ pre všetky $a \in G$,
- (iv) $aHa^{-1} \subseteq H$ pre všetky $a \in G$,
- (v) $H \subseteq aHa^{-1}$ pre všetky $a \in G$,
- (vi) $aHa^{-1} = H$ pre všetky $a \in G$,
- (vii) $\{aH; a \in G\} = \{Hb; b \in G\}$.

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

$$h \in H \quad \Rightarrow \quad aha^{-1} \in H. \quad (3.1)$$

Faktorizácia grupy podľa podgrupy:

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

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

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

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

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

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

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

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

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

Vety o izomorfizme:

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

$$f: a \mapsto aH$$

je surjektívny homomorfizmus. Tento homomorfizmus voláme kanonický homomorfizmus.

Navyše, jadro kanonického homomorfizmu je práve podgrupa H .

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

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

Teda toto zobrazenie je skutočne homomorfizmus.

Surjektivnosť vyplýva priamo z definície.

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

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

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

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

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

Definujme zobrazenie $\varphi: G/H \rightarrow \text{Im } f$ ako

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

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

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

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

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

teda φ je homomorfizmus.

Surjektivnosť vyplýva z toho, že za obor hodnôt sme zobrali $\text{Im } f$. Aby sme ukázali, že homomorfizmus φ je injektívny, stačí ukázať, že $\text{Ker } \varphi$ obsahuje iba neutrálny prvok (úloha 2.3.7). Skutočne, ak $\varphi(aH) = e'$, znamená to, že $f(a) = e'$ a $a \in \text{Ker } f = H$, teda $aH = H$. \square

Dôsledok 3.5.3. Ak $f: G \rightarrow H$ je surjektívny homomorfizmus grúp, tak grupa H je izomorfná s faktorovou grupou $G/\text{Ker } f$.

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

Môžeme si všimnúť, že veta o izomorfizme nám dáva ďalšiu možnosť ako ukázať, že nejaká podgrupa grupy G je normálna – ak sa nám podarí nájsť homomorfizmus z G do inej grupy, ktorého jadrom je daná podgrupa. Dokonca vieme jednoducho popísat aj triedy rozkladu – do jednej triedy patria tie prvky z G , ktoré majú v tomto homomorfizme ten istý obraz. (Úloha 3.5.12, viac-menej to vidno už aj z dôkazu vety o izomorfizme.)

Z vety o izomorfizme okamžite dostaneme nasledujúce jednoduché dôsledky.

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

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

je dobre definované a je to grupový homomorfizmus.

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

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

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

Overíme teraz, že φ je homomorfizmus.

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

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

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

$$f: aH \mapsto aK$$

je surjektívny homomorfizmus.

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

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

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

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

$$\psi: aH \mapsto aK$$

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

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

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

\square

Veta 3.5.12 (Druhá veta o izomorfizme). Nech G je grupa, N je normálna podgrupa G a S je podgrupa G . Potom množina SN tvorí podgrupu grupy G , N je normálna podgrupa SN , $S \cap N$ je normálna podgrupa S a platí

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

5 Okruhy (základné vlastnosti operácií v okruhoch, podokruh, ideál (hlavný, maximálny, prvoideál), faktorizácia okruhu podľa ideálu, vzťah medzi výsledkom faktorizácie a vlastnosťami ideálu, podľa ktorého sa faktorizuje)

Okruhy:

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

(i) $(R, +)$ je komutatívna grupa,

(ii) operácia \cdot je asociatívna¹,

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

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

$$\begin{aligned} (\forall a, b, c \in R) \quad a \cdot (b + c) &= a \cdot b + a \cdot c \\ (\forall a, b, c \in R) \quad (b + c) \cdot a &= b \cdot a + c \cdot a \end{aligned}$$

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

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

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

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

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

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

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

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

Pomerne jednoducho sa dá overiť, že platí

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

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

$$ab = 0,$$

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

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

Fakt, že R je okruh bez deliteľov nuly môžeme vyjadriť pomocou nasledovnej implikácie⁴

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

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

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

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

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

Komutatívne teleso voláme **pole**.

Tvrdenie 4.1.16. Každé teleso je okruh bez delitelov nuly.

Každé pole je oborom integrity.

Ideál:

Definícia 4.2.8. Ak R je komutatívny okruh a $a \in R$, tak množina

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

je ideálom v R (úloha 4.2.4). Ideály takého tvaru voláme **hlavné ideály**.

Definícia 4.2.14. Ideál I v okruhu R sa nazýva **prvoideál**, ak pre ľubovoľné $a, b \in R$ také, že $a \cdot b \in I$ aspoň jeden z prvkov a, b patrí do I čiže ak platí

$$a \cdot b \in I \quad \Rightarrow \quad a \in I \vee b \in I.$$

Môžeme si všimnúť, že $\{0\}$ je prvoideál v R práve vtedy, keď R nemá delitele nuly.

Definícia 4.2.18. Ideál I v okruhu R nazývame **maximálny**, ak $I \neq R$ a súčasne pre každý ideál J s vlastnosťou $I \subseteq J \subseteq R$ platí $I = J$ alebo $J = R$.

Predchádzajúca definícia vlastne hovorí, že maximálne ideály sú práve maximálne prvky množiny vlastných ideálov okruhu R vzhľadom na usporiadanie \subseteq .

Faktorizácia okruhu podľa ideálu:

Veta 4.2.12. Nech $(R, +, \cdot)$ je ľubovoľný okruh a I je ideál v R . Ak na prvkoch faktorovej⁶ grupy $(R, +)$ podľa podgrupy I

$$R/I = \{a + I; a \in R\}$$

⁶Grupa $(R, +)$ je komutatívna, takže jej podgrupa I je invariantná. Má teda zmysel hovoriť o faktorovej grupe.

definujeme binárnu operáciu \cdot ako

$$(a + I) \cdot (b + I) = (a \cdot b) + I,$$

tak je táto binárna operácia dobre definovaná a $(R/I, +, \cdot)$ je okruh. Tento okruh voláme faktorový okruh R podľa I .

Ak je okruh R komutatívny, tak aj R/I je komutatívny. Ak R je okruh s jednotkou a $I \neq R$, tak $1 + I$ je jednotka faktorového okruhu R/I .

Veta 4.2.13 (Veta o izomorfizme). Ak $f: R \rightarrow R'$ je homomorfizmus okruhov, tak $\text{Ker } f$ je ideál v okruhu R a faktorový okruh $R/\text{Ker } f$ je izomorfný s podokruhom $\text{Im } f$ okruhu R' .

Veta 4.2.20. Nech R je komutatívny okruh s jednotkou a I je ideál v R . Potom faktorový okruh R/I je pole práve vtedy, keď I je maximálny ideál.

Dôsledok 4.2.21. V komutatívnom okruhu s jednotkou je každý maximálny ideál prvoideál.

Vzťah medzi výsledkom faktorizácie a vlastnosťami ideálu, podľa ktorého sa faktorizuje:

???

6 Okruhy hlavných ideálov (existencia jednotky v okruhu, najväčší spoločný deliteľ, vlastnosti deliteľnosti, ireducibilné prvky, veta o jednoznačnom rozklade)

OHI:

Definícia 4.4.15. Ak R je obor integrity, hovoríme, že R je okruh hlavných ideálov, ak každý ideál v R je hlavný, t.j. ak je tvaru

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

pre nejaké $a \in R$.

Tvrdenie 4.4.16. Každý euklidovský okruh je okruh hlavných ideálov.

Dôkaz. Nech R je euklidovský okruh, $I \neq \emptyset$ je ideál v R .

Ak $I = \{0\}$, tak $I = (0)$. Môžeme teda predpokladať, že I obsahuje aspoň jeden nenulový prvok.

⁸ Ak v $I \setminus \{0\}$ existuje prvok s nulovou normou, tak tento prvok je deliteľom jednotky (podľa lemy 4.4.14). To by ale znamenalo, že $I = R = (1)$. V ďalšej časti dôkazu teda môžeme predpokladať, že všetky prvky $I \setminus \{0\}$ majú nenulovú normu.

Nech b je nenulový prvok z I s najmenšou normou. (Taký prvok existuje, lebo $\{N(b); b \in I \setminus \{0\}\}$ je neprázdna podmnožina prirodzených čísel. Každá neprázdna podmnožina prirodzených čísel má najmenší prvok – princíp dobrého usporiadania.)

Tvrdíme, že $I = (b)$. Pre každý prvok $a \in I$ máme $a = bc + d$. Pritom $d = bc - a \in I$, čiže opäť nemôže nastať možnosť $N(d) < N(b)$. Teda $d = 0$ a $a = bc$. Tým sme ukázali, že $I \subseteq (b)$. Inklúzia $(b) \subseteq I$ je zrejmá. \square

Deliteľnosť v OHI:

Všimnime si, že v OHI platí nasledovný vzťah medzi deliteľnosťou v okruhu a hlavnými ideálmi:

$$a | b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a). \quad (4.2)$$

(Vyplýva to priamo z definície deliteľnosti a z definície hlavného ideálu.)

V súvislosti s hlavnými ideálmi si tiež môžeme všimnúť, že $(a) = R$ práve vtedy, keď a je deliteľ jednotky. (Pozri lemu 4.2.9.)

Poznámka 4.4.20. Podobne, ako (a) označuje ideál generovaný prvkom a , znakom (a_1, \dots, a_n) budeme označovať najmenší ideál obsahujúci všetky prvky a_1, \dots, a_n . Lahko sa dá overiť, že v komutatívnom okruhu s jednotkou

$$(a_1, \dots, a_n) = \left\{ \sum_{i=1}^n x_i a_i; x_i \in R \right\}$$

(Je zjavné, že táto množina obsahuje prvky a_1, \dots, a_n . Stačí teda overiť, že to je ideál – to ide ľahko z definície ideálu.)

Špeciálne máme

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

Podobne ako pre celé čísla, aj v oboroch integrity vieme definovať pojem najväčší spoločný deliteľ.

Definícia 4.4.21. Najväčší spoločný deliteľ prvkov $a, b \in R$ je taký prvak $c \in R$, že

- (i) $c | a, c | b$,
- (ii) pre ľubovoľný prvak $d \in R$ taký, že $d | a$ a $d | b$ platí aj $d | c$.

Označujeme ho $\gcd(a, b)$.

Inak povedané, $\gcd(a, b)$ je najväčší (vzhľadom na usporiadanie $|$) prvak z množiny čísel, ktoré súčasne delia a aj b (=spoločné delitele čísel a, b).

Priamo z definície vidno, že najväčší spoločný deliteľ (ak existuje) je určený jednoznačne až na asociovanosť.⁹

Tvrdenie 4.4.22. Ak R je okruh hlavných ideálov, tak pre ľubovoľné $a, b \in R$ existuje v R najväčší spoločný deliteľ $c = \gcd(a, b)$.

Navyše, existujú také $x, y \in R$, že

$$c = xa + yb.$$

Dôkaz. Vieme, že $(a, b) = \{ax + by; x, y \in R\}$ je ideál v R . Pretože R je okruh hlavných ideálov, existuje $c \in R$ také, že $(c) = (a, b)$. Z toho špeciálne máme $a, b \in (c)$, čiže $c | a, c | b$.

Navyše, pretože $c \in (a, b)$, máme zaručenú existenciu $x, y \in R$ s vlastnosťou $ax + by = c$. Z toho potom dostávame, že pre ľubovoľné $d \in R$ také, že $d | a, d | b$, platí

$$d | ax + by = c.$$

□

Dôsledok 4.4.23. Nech R je okruh hlavných ideálov, $a, b, c \in R$, $a, b \neq 0$. Ak $\gcd(a, b) = 1$ a $a | bc$, tak $a | c$.

$$\gcd(a, b) = 1 \quad \wedge \quad a | bc \quad \Rightarrow \quad a | c$$

Dôkaz. Z tvrdenia 4.4.22 máme existenciu $x, y \in R$ takých, že

$$ax + by = 1.$$

Potom

$$a | ac \cdot x + bc \cdot y = (ax + by)c = c.$$

□

Lema 4.4.24. Ak R je obor integrity a $a, b \in R$, tak

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

pre ľubovoľné $x \in R$.

Dôkaz. Kedže najväčší spoločný deliteľ je generátor ideálu (a, b) , stačí dokazovať rovnosť ideálov $(a, b) = (a + bx, b)$.

Priamo z definície ideálu máme $bx \in (a, b)$, teda aj $a + bx \in (a, b)$ a $(a + bx, b) \subseteq (a, b)$.

Podobne sa ukáže $a = (a + bx) - bx \in (a + bx, b)$ a $(a, b) \subseteq (a + bx, b)$. □

Ireducibilné prvky:

4.4.3 Gaussove okruhy

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

Definícia 4.4.28. Prvok $a \neq 0$ okruhu R sa nazýva *ireducibilný*, ak a je nenulový, nie je to deliteľ jednotky a ak z rovnosti $a = bc$ vyplýva, že niektorý z prvkov b, c je deliteľ jednotky v R .

Inými slovami, irreducibilný prvak sa (až na asociovanosť a výmenu poradia) nedá zapísat ako súčin dvoch prvkov z R inak ako $1 \cdot a$.

Definícia 4.4.30. Okruh s jednoznačným rozkladom (alebo tiež *Gaussov okruh*) je obor integrity, v ktorom pre každý prvak $x \in R$, ktorý je nenulový a nie je deliteľom jednotky, existuje rozklad

$$x = p_1 \cdots p_k$$

na súčin irreducibilných prvkov a navyše je tento rozklad jednoznačný až na asociovanosť a poradie.

Tvrdenie 4.4.31. Ak ideál (p) v obore integrity R je vlastný prvoideál a $p \neq 0$, tak p je irreducibilný v R .

Dôkaz. Ak (p) je prvoideál a $ab = p$, tak jeden prvak z dvojice a, b musí byť násobkom p (pretože patrí do (p)). Bez ujmy na všeobecnosti, nech $a = kp$. Potom $p = ab = (kb)p$, z čoho $kb = 1$ (lema 4.4.1), čiže b je deliteľ jednotky.

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

V OHI platí aj obrátená implikácia.

Tvrdenie 4.4.32. Ak p je irreducibilný prvak v OHI R , tak (p) je prvoideál.

Dôkaz. Nech p je irreducibilný. Ukážeme, že ideál p je maximálny (a teda je to prvoideál). Nech by $(p) \subseteq (m)$. Z toho vyplýva $p = mc$. Potom buď m je asociovaný s p a $(p) = (m)$, alebo m je invertibilný a $(m) = R$. □

Z toho dostávame (pomocou (4.2)) nasledujúci veľmi dôležitý vzťah.

Dôsledok 4.4.33. V OHI pre ľubovoľný irreducibilný prvak p platí implikácia

$$p \mid ab \quad \Rightarrow \quad p \mid a \vee p \mid b.$$

Teraz už sme schopní vyslovíť a dokázať tvrdenie o rozklade na súčin irreducibilných prvkov.

Tvrdenie 4.4.34. Každý okruh hlavných ideálov je okruhom s jednoznačným rozkladom.

Dôkaz. Chceme dokázať existenciu a jednoznačnosť rozkladu na súčin irreducibilných prvkov. Jednoznačnosť vyplýva z dôsledku 4.4.33.

Existencia. Spôsobom. Nech by x bol taký prvak, ktorý sa nedá v R rozložiť na súčin irreducibilných prvkov (pričom $x \neq 0$, x nie je deliteľ jednotky). Pretože x nie je irreducibilný, vieme ho zapísat ako $x = r_1 \cdot q_1$. Keby obidva prvky r_1 aj q_1 boli irreducibilné, máme rozklad x . Teda jeden z nich nie je irreducibilný, bez ujmy na všeobecnosti nech je to q_1 . Potom $q_1 = r_2 \cdot q_2$ pre nejaké $r_2, q_2 \in R$. Takýmto spôsobom indukciou zostrojíme nekonečnú postupnosť prvkov $r_n \in R$ takú, že nasledujúci vždy delí predchádzajúci, teda $r_{n+1} \mid r_n$. To je ekvivalentné s tým,

že $(r_n) \subseteq (r_{n+1})$ a takto dostávame nekonečnú postupnosť ideálov $I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_n \subsetneq \dots$, kde I_k označuje ideál (r_k) . Ukážeme, že v OHI takáto postupnosť nemôže existovať, čím dostaneme požadovaný spor.

Skutočne, ak by sme mali takýto rastúci reťazec ideálov. Potom aj $I = \bigcup_{n=1}^{\infty} I_n$ je ideál. Pretože R je OHI, existuje $a \in R$ také, že $(a) = I$. Lenže z toho, že $a \in \bigcup_{n=1}^{\infty} I_n$ vyplýva existencia čísla n_0 s vlastnosťou $a \in I_{n_0}$. Potom pre všetky $n > n_0$ máme $(a) \subseteq I_{n_0} \subseteq I_n \subseteq I$, čiže od n_0 počnúc sa už všetky ideály I_n rovnajú. \square

Lema 4.4.38. Nech R je Gaussov okruh a $a, b \in R$. Ak $a = p_1 \dots p_n$ a $b = q_1 \dots q_m$ sú rozklady týchto prvkov na súčin ireducibilných činitelov, tak $a \mid b$ práve vtedy, ked existuje injekcia $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, m\}$ s vlastnosťou $q_{f(m)} \sim p_m$.

(Toto tvrdenie je len formálny zápis faktu, že všetky ireducibilné prvky z rozkladu a sa musia vyskytnúť aj v rozklade b , pričom ak sa tam vyskytuje viackrát prvek z tej istej triedy asociovanosti, tak sa toľkokrát musí vyskytnúť aj v rozklade b .)

Dôkaz. \square

7 Okruhy polynómov (pojem algebraického a transcendentného prvku pre daný okruh, okruh polynómov $R[x]$, okruhy polynómov $F[x]$ nad poľom F ako okruh hlavných ideálov, veta o jednoznačnom rozklade polynómov nad daným poľom, substitučný homomorfizmus (veta o substitúcii), korene, viacnásobné korene, Hornerova schéma)

Polynómy:

Definícia 4.3.1. Nech R je komutatívny okruh s jednotkou. Potom formálne zápisu tvaru

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

kde n je prirodzené číslo a $a_i \in R$ pre $i = 0, \dots, n$ nazývame *polynómy* v premennej x nad okruhom R .

Namiesto zápisu $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ budeme často používať stručnejší zápis

$$p = \sum_{i=0}^n a_i x^i.$$

Prvky $a_n, a_{n-1}, \dots, a_0 \in R$ voláme *koeficienty* polynómu p .

Definícia 4.3.3. Nech R je komutatívny okruh s jednotkou. Nech $p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ a $q = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$ sú ľubovoľné polynómy nad R . (Tým, že u oboch polynómov predpokladáme rovnaký počet koeficientov sme sa nijako neobmedzili – v prípade potreby je možné niektorý polynóm doplniť nulami.)

Potom *súčet polynómov* p a q je

$$p + q = \sum_{i=0}^n (a_i + b_i) x^i.$$

Súčin polynómov p a q je polynóm $r = \sum_{i=0}^{2n} c_i x^i$, kde

$$c_k = \sum_{j=0}^k a_j b_{k-j}.$$

Teda obe operácie sme definovali rovnako ako v predchádzajúcim príklade – pri sčítovaní sa jednoducho sčítajú koeficienty a pri násobení sú koeficienty výsledného polynómu práve tie výrazy, ktoré by sme dostali roznásobením (koeficient c_k je súčet všetkých možných $a_s b_l$ pre $s + l = k$, čo sú presne všetky možnosti, ako môžeme dostať $x^k = x^s \cdot x^l$).

Definíciu súčinu by sme mohli ekvivalentne prepísať ako

$$c_k = \sum_{m+n=k} a_m b_n.$$

Z tejto ekvivalentnej definícii vidno, že pre násobenie polynómov platí asociatívnosť: pre $p = \sum_{i=0}^n a_i x^i$, $q = \sum_{i=0}^n b_i x^i$, $r = \sum_{i=0}^n c_i x^i$ dostaneme $(pq)r = \sum_{i=0}^{3n} d_i x^i$, kde koeficienty d_k majú hodnoty

$$d_k = \sum_{m+n=k} a_m \sum_{s+t=n} b_s c_t = \sum_{m+s+t=k} a_m b_s c_t.$$

Vďaka tomu dostaneme, že

Tvrdenie 4.3.4. Nech R je komutatívny okruh s jednotkou. Množina všetkých polynómov nad R s násobením a sčítovaním definovaným v predchádzajúcej definícii tvorí komutatívny okruh s jednotkou. Tento okruh označujeme $R[x]$ a voláme ho okruh polynómov nad R .

Sčítovanie a násobenie polynómov sme vlastne definovali tak, aby akákoľvek rovnosť, ktorá platí pre polynómy platila aj keď namiesto x napišeme akýkoľvek prvok okruhu R (alebo nejakého nadokruhu, ktorý obsahuje R). To zdôvodňuje použitie názvu premenná – namiesto x môžeme napísat (dosadiť) hocjaký prvok, čiže sa môže meniť. (Aj dosadzovaniu do polynómov sa budeme ešte venovať.)

Tvrdenie 4.3.6. Ak R je obor integrity, tak pre ľubovoľné nenulové polynómy $f, g \in R[x]$ platí

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

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

Delenie so zvyškom:

Pre nás bude dôležitý hlavne prípad keď okruh R je pole. Ako sme už ukázali, v tomto prípade platí

$$\text{st}(pq) = \text{st } p + \text{st } q.$$

Neskôr bude pre nás dôležitá nasledujúca veta:

Veta 4.3.7 (Veta o delení so zvyškom). Nech F je pole, $f(x), g(x) \in F[x]$ a $g(x) \neq 0$. Potom existujú $q(x), r(x) \in F[x]$ také, že

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

a $\text{st } r(x) < \text{st } g(x)$.

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

Definícia 4.3.8. Polynómy $q(x)$ a $r(x)$ jednoznačne určené podmienkami z vety 4.3.7 sa nazývajú *podiel* a *zvyšok po delení* polynómu $f(x)$ polynómom $g(x)$. Zvyšok po delení označujeme $f(x) \bmod g(x)$.

Veta 4.3.10. Nech a, b sú celé čísla, $b > 0$. Potom existujú celé čísla q a r také, že

$$a = q \cdot b + r \quad a \quad 0 \leq r < q.$$

Navýše, q a r sú týmito podmienkami jednoznačne určené.

Definícia 4.3.11. Číslo r z predchádzajúcej vety sa nazýva *zvyšok a po delení b* a označuje sa $a \bmod b$.

7. Okruhy polynómov [pojem algebraického a transcendentného prvku pre daný okruh, okruh polynómov $R[x]$, okruh polynómov $F[x]$ nad poľom F ako okruh hlavných ideálov, veta o jednoznačnom rozklade polynómov nad daným poľom, substitučný homomorfizmus (veta o substitúcií), korene, viacnásobné korene, Hornerova schéma]

$$\begin{aligned}
 & \xrightarrow{\text{f(x) } \in F[x]} \text{f(m)} + \text{r} \\
 & \text{f(x) } \in F[x] \xrightarrow{\text{HOM}} f(m) \\
 & m \in F \\
 & a_n x^n + \dots + a_1 x + a_0 \xrightarrow{\text{HOM}} a_n m^n + \dots + a_1 m + a_0 \\
 & h(x) = f(x) + g(x) \xrightarrow{\text{HOM}} h(m) = f(m) + g(m) \\
 & h(x) = f(x) \cdot g(x) \xrightarrow{\text{HOM}} h(m) = f(m) \cdot g(m)
 \end{aligned}$$

Substitučný (dosadzovací) homomorfizmus:

Definícia 4.3.15. Ak R je komutatívny okruh a $b \in R$, tak homomorfizmus $f_b: R[x] \rightarrow R$ daný predpisom

$$f_b: f \mapsto a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0$$

voláme *dosadzovací homomorfizmus*.

Transcendentný prvok:

Definícia 4.3.16. Nech R je komutatívny okruh s jednotkou. Predpokladajme, že R je podokruh nejakého komutatívneho okruhu R' a existuje prvok $x \in R'$ taký, že rovnosť

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

pre $a_1, \dots, a_n \in R$ platí práve vtedy, keď $a_1 = \cdots = a_n = 0$. Potom prvok x voláme *transcendentný prvok* nad R .

Podokruh

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0; n \in \mathbb{N}, a_1, \dots, a_n \in R\}$$

okruhu R' potom voláme *okruhom polynómov* v premennej x nad R .

Okruhy polynómov:

Definícia 4.3.17. Nech R je ľubovoľný komutatívny okruh s jednotkou. Ako $R[x]$ označíme množinu všetkých postupností prvkov z R takých, že iba konečne veľa členov tejto postupnosti je nenulových. Ďalej zadefinujeme sčítovanie dvoch postupností ako

$$(a_n)_{n=1}^{\infty} + (b_n)_{n=1}^{\infty} = (a_n + b_n)_{n=1}^{\infty}$$

a súčin postupností $(a_n)_{n=1}^{\infty}$, $(b_n)_{n=1}^{\infty}$ definujeme ako postupnosť $(c_n)_{n=1}^{\infty}$, ktorej členy sú určené predpisom

$$c_k = \sum_{j=0}^k a_j b_{k-j} = \sum_{m+n=k} a_m b_n.$$

Táto množina postupností s uvedeným sčítovaním a násobením tvorí okruh, ktorý voláme *okruh polynómov* nad R .

Korene polynómu:

Definícia 4.5.1. Nech F je pole a F' je jeho nadpole. Prvok $c \in F'$ nazývame *koreňom* polynómu $f(x) \in F[x] \subset F'[x]$, ak $f(c) = 0$ (t.j. po dosadení c do polynómu F dostaneme 0).

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

Lema 4.5.3. Ak $f(x) \in F[x]$, kde F je pole, a $c \in F$, tak zvyšok polynómu $f(x)$ po delení polynómom $x - c$ je rovný $f(c)$, t.j. existuje polynóm $g(x) \in F[x]$ taký, že

$$f(x) = (x - c)g(x) + f(c). \quad (4.3)$$

Definícia 4.5.5. Nech F' je nadpole poľa F , $f(x) \in F[x]$ a c je koreň $f(x)$. Hovoríme, že *násobnosť* koreňa c je k (alebo tiež, že c je k -násobný koreň $f(x)$), ak $(x - c)^k \mid f(x)$ (t.j. ak existuje polynóm $g(x) \in F'[x]$ taký, že $f(x) = g(x)(x - c)^k$) a súčasne $(x - c)^{k+1} \nmid f(x)$.

Pre $k = 1$ voláme k -násobný koreň *jednoduchý koreň* polynómu $f(x)$, ak $k > 1$ tak hovoríme o násobnom korení.

Hornerova schéma:

Jednoduchý spôsob ako ručne spočítať hodnotu polynómu v danom čísle (a tým zistíť, či toto číslo je koreňom polynómu) je použitie Hornerovej schémy.

Základná idea Hornerovej schémy je, že hodnotu polynómu môžeme vyjadriť ako

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

Stačí nám teda postupne počítať čísla $a_n, a_n c + a_{n-1}, (a_n c + a_{n-1}) c + a_{n-2}$ atď., t.j. predchádzajúci výsledok vždy vynásobíme číslom c a pripočítame k nemu nasledujúci koeficient.

Príklad 4.5.7. Vypočítajte hodnotu polynómu $f(x) = x^4 - 3x^3 + 2x - 1$ nad poľom \mathbb{R} v bode $c = 2$.

Do tabuľky si zapíšeme koeficienty polynómu (dôležité je nezabudnúť na nulový koeficient pochádzajúci z člena $0x^2$) a postupujeme postupom, ktorý sme naznačili.

2	1	-3	0	2	-1	
	2	-2	-4	-4		
	1	-1	-2	-2	-5	

Všimnime sme, že súčasne sme vypočítali, že

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

(Stačí si uvedomiť, že pri Hornerovej schéme vlastne robíme to isté, čo pri algoritme na delenie polynómov.)

Aby sme si uvedomili, čo vlastne v Hornerovej schéme počítame, pokúsme sa ju zapísať o čosi všeobecnejšie (kvôli šírke rozdelené na 2 tabuľky)

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

Príklad 4.5.8. Overte, že 1 je koreňom polynómu $f(x) = x^4 - 3x^3 + 3x - 1 \in \mathbb{R}[x]$. Zistite násobnosť tohto koreňa.

Budeme postupovať pomocou Hornerovej schémy – pri vypočítaní hodnoty $f(1)$ súčasne nájdeme polynóm $g(x)$ taký, že $f(x) = g(x)(x - 1) + f(1)$. Ak $f(1) = 0$, na zistenie, či ide násobnosť tohto koreňa je aspoň 2, stačí overiť, či aj $g(1) = 0$. Analogicky postupujeme ďalej, až kým nedostaneme nenulový zvyšok.

	1	-3	0	3	-1	
1		1	-2	-2	1	
	1	-2	-2	1		0
1		1	-1	-3		
	1	-1	-3		-2	

Zistili sme, že 1 je jednoduchým (jednonásobným) koreňom polynómu $f(x)$ a že

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

pričom $x - 1 \nmid x^3 - 2x^2 - 2x + 1$.

Rátať korene polynómov je vo všeobecnosti ťažká úloha. Zo strednej školy poznáte vzorec na hľadanie koreňov polynómov druhého stupňa – kvadratických polynómov. (Podobné vzorce, aj keď zložitejšie, sa dajú nájsť aj pre rovnice tretieho a štvrtého stupňa. Vo všeobecnosti však také vzorce neexistujú.) Okrem nich vieme ešte v komplexných číslach riešiť binomické rovnice, t.j. rovnice tvaru $x^n = a$, kde $a \in \mathbb{C}$ (pozri I-B.3.2 alebo [KGGS, kapitola 6.1]).

Povieme si, ako pre polynóm s celočíselnými koeficientami vieme nájsť všetky korene, ktoré sú racionálnymi číslami (t.j. všetky korene daného polynómu ležiace v poli \mathbb{Q}).

8 Rozšírenia polí (konečné rozšírenie poľa, stupeň rozšírenia, algebraické rozšírenie, minimálny polynóm daného algebraického prvku)

Rozšírenia polí:

Definícia 5.3.2. Ak K je rozšírenie poľa F také, že K je konečnorozmerný vektorový priestor nad F , tak K nazývame *konečné rozšírenie* poľa F .

Dimenziu $d_F(K)$ poľa K ako vektorového priestoru nad F nazývame *stupeň rozšírenia* a označujeme $[K : F]$.

Veta 5.3.5. Nech F je pole a $p(x)$ je irreducibilný polynóm v $F[x]$. Potom existuje rozšírenie poľa F , v ktorom $p(x)$ má koreň.

Stupeň rozšírenia:

Veta 5.3.6. Nech $p(x) \in F[x]$ je irreducibilný polynóm a $K = F[x]/(p(x))$. Nech $n = \text{st } p$. Označme $u = x + (p(x)) = \varphi(x)$ (kde $\varphi: F[x] \rightarrow K$ označuje kanonický homomorfizmus). Potom $1, u, \dots, u^{n-1}$ je báza K ako vektorového priestoru nad F , čiže

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

Dôsledok 5.3.7. Ak $p(x) \in F[x]$ je irreducibilný polynóm stupňa n , tak $K = F[x]/(p(x))$ je konečné rozšírenie F a stupeň rozšírenia $[K : F]$ je tiež rovný n .

$$[K : F] = \text{st } p(x)$$

Definícia 5.3.10. Ak K je rozšírenie F a $u_1, \dots, u_n \in K$, tak symbolom $F(u_1, \dots, u_n)$ označujeme podpolo generované množinou $F \cup \{u_1, \dots, u_n\}$. (T.j. najmenšie podpolo, ktoré obsahuje túto množinu, čiže prienik všetkých podpolí, ktoré ju obsahujú.)²

V prípade, že existuje $u \in K$ také, že $K = F(u)$ hovoríme o *jednoduchom rozšírení*.

Vo vete 5.3.5 sme ukázali, že pre irreducibilný polynóm $p(x)$ existuje rozšírenie, v ktorom tento polynóm má koreň. Teraz ukážeme, že toto pole je jednoznačne určené až na izomorfizmus.

Algebraické rozšírenie:

Definícia 5.4.1. Nech K je rozšírenie poľa F . Nech $u \in K$. Hovoríme, že prvok u je *algebraický* nad F , ak existuje nenulový polynóm $f(x) \in F[x]$, ktorého koreňom je u .

Ak každý prvok rozšírenia K je algebraický, hovoríme, že K je *algebraické rozšírenie*.

Definícia 5.4.3. Ak u je algebraický prvok nad F , tak *minimálny polynóm* prvku u je normovaný polynóm, ktorý generuje ideál $\{f(x) \in F[x]; f(u) = 0\}$. Označujeme ho $m_u(x)$.

Stupeň algebraického prvku definujeme ako stupeň jeho minimálneho polynómu. Označujeme ho $[u : F]$.

$$[u : F] = \text{st } m_u(x)$$

Pretože v definícii máme požiadavku normovanosti, minimálny polynóm je určený jednoznačne. Je to nenulový normovaný polynóm najnižšieho možného stupňa, ktorý patrí do ideálu $\{f(x) \in F[x]; f(u) = 0\}$.

Veta 5.4.5. Ak u je algebraický pravok nad F a $m_u(x) \in F[x]$ je jeho minimálny polynóm. Potom $m_u(x)$ je ireducibilný polynóm nad F ,

$$F(u) \cong F[x]/(m_u(x))$$

$$\text{a } [u : F] = [F(u) : F].$$

Dôkaz. Ak by bol polynóm $m_u(x)$ reducibilný, t.j. $m_u(x) = f(x)g(x)$ pre nejaké nekonštantné polynómy $f(x), g(x) \in F[x]$, tak z rovnosti $m_u(u) = f(u)g(u) = 0$ vyplýva $f(u) = 0$ alebo $g(u) = 0$. To znamená, že jeden z polynómov $f(x), g(x)$ by patril do ideálu $(m_u(x))$ a súčasne by mal nižší stupeň ako $m_u(x)$, čo je spor.

Z vety 5.3.11 potom vyplýva $F(u) \cong F[x]/(m_u(x))$ a z dôsledku 5.3.7 máme $[F(u) : F] = \text{st } m_u = [u : F]$. \square

Veta 5.4.6. Nech K je rozšírenie F a $u \in K$. Pravok u je algebraický nad F práve vtedy, ked $F(u)$ je konečné rozšírenie F .

Dôsledok 5.4.7. Každé konečné rozšírenie je algebraické.

8 Konečné polia (charakteristika poľa, možné počty prvkov v konečných polí, počítanie v poli, $F[x]/p(x)$ pre irreducibilný polynóm $p(x)$, rozkladové pole polynómu, existencia poľa s p na n prvkami)

Charakteristika poľa:

Definícia 5.2.1. Charakteristika pola F je najmenšie prirodzené číslo $k > 0$ s vlastnosťou $k \times 1 = 0$. Označujeme ju $\text{char}(F)$. Ak neexistuje k s uvedenou vlastnosťou, tak definujeme $\text{char}(F) = \infty$.

Predchádzajúcemu definíciu môžeme preformulovať aj nasledovne

$$\text{char } F = \min\{k \in \mathbb{N}, k > 0; k \times 1 = 0\},$$

pričom minimum z práznej množiny chápeme ako nekonečno.

Charakteristiku možno definovať aj všeobecnejšie – pre ľubovoľný okruh, pozri napríklad [KGGs, Kapitola 4.4]. V prípade oboru integrity je táto všeobecnejšia definícia ekvivalentná s definíciou, ktorú sme tu uviedli pre polia. (My budeme charakteristiku potrebovať iba pre polia.)

Lema 5.2.3. Každé konečné pole F má konečnú charakteristiku.

Tvrdenie 5.2.5. Charakteristika ľubovoľného pola F je prvočíslo alebo ∞ .

Možné počty prvkov konečných polí:

Tvrdenie 5.2.6. Nech F, F' sú polia a zobrazenie $\varphi: F \rightarrow F'$ je okruhový homomorfizmus. Potom bud $\varphi[F] = \{0\}$, alebo $\varphi[F]$ je podpole F' , ktoré je izomorfné s F . (Inými slovami: zobrazenie φ je buď nulové alebo injektívne; čiže vnorenie – izomorfizmus na svoj obraz.)

Dôkaz. Vieme, že $\text{Ker } \varphi$ je ideál v F . Jediné ideály v poli sú však $\{0\}$ a F . V prvom prípade je homomorfizmus φ injektívny, v druhom prípade sa každý prvek zobrazí na nulu. \square

Pomocou predchádzajúceho tvrdenia môžeme ukázať, že (v závislosti od charakteristiky) každé pole obsahuje podpole (izomorfné s) \mathbb{Q} alebo \mathbb{Z}_p .

Tvrdenie 5.2.7. Ak $\text{char } F = \infty$, tak existuje injektívny homomorfizmus z \mathbb{Q} do F .

Ak $\text{char } F = p$ pre nejaké prvočíslo p , tak existuje injektívny homomorfizmus zo \mathbb{Z}_p do F .

Dôkaz. Zobrazenie $\varphi: \mathbb{Z} \rightarrow F$

$$\varphi: z \mapsto z \times 1$$

je okruhový homomorfizmus, pričom $\text{Ker } \varphi$ obsahuje práve tie celé čísla, ktoré sú násobky $\text{char}(F)$ (a v prípade, že $\text{char } F = \infty$ je $\text{Ker } \varphi = \{0\}$).

Ak $\text{char } F = p$, tak máme (na základe vety o faktorovom izomorfizme) izomorfizmus z $\mathbb{Z}/\text{Ker } \varphi = \mathbb{Z}/(\text{char}(F)) = \mathbb{Z}/(p) \cong \mathbb{Z}_p$ na $\text{Im } \varphi$. Tým dostávame hľadaný injektívny homomorfizmus zo \mathbb{Z}_p do F .

Ak $\text{char } F = \infty$, tak $\text{Ker } F = (0)$ a φ je injektívny homomorfizmus zo \mathbb{Z} do F . Ten sa podľa vety 5.1.2 dá rozšíriť na injektívny homomorfizmus $\bar{\varphi}: Q(\mathbb{Z}) \rightarrow F$ z podielového pola oboru integrity \mathbb{Z} do F . Podielové pole \mathbb{Z} je však práve pole racionálnych čísel. \square

Tvrdenie 5.2.8. Nech K , F sú polia a K je nadpole poľa F (t.j. $K \supseteq F$ a operácie na F sú zúženia operácií na K). Potom K je vektorový priestor nad poľom F (so sčítovaním a násobením skalárom rovnakým ako je sčítovanie a násobenie v K).

Dôkaz. Jednoduchý – jednotlivé vlastnosti z definície vektorového priestoru po prepísaní na tento konkrétny príklad sú vlastne známe vlastnosti poľa ako distributivnosť, asociatívnosť násobenia atď. (Dôkaz je skoro identický s postupom použitým v úlohách I-4.1.10 a I-4.1.5)

□

Existencia poľa s p na n prvkami:

Dôsledok 5.2.9. Konečné pole charakteristiky p má p^n prukov pre nejaké $n \in \mathbb{N}$.

Dôkaz. Podľa tvrdenia 5.2.7 každé konečné pole F s $\text{char}(F) = p$ obsahuje podpole (izomorfne so) \mathbb{Z}_p . Teda ho môžeme chápať ako vektorový priestor nad \mathbb{Z}_p . Keďže množina F je konečná, ide o konečnorozmerný vektorový priestor, teda F je (ako vektorový priestor) izomorfný s priestorom $(\mathbb{Z}_p)^n$ pre nejaké n (veta I-5.5.14). □

Z toho vyplýva, že počet prvkov konečného poľa musí byť mocnina prvočísla. Napríklad dostávame, že nemôže existovať 6-prvkové pole. (Platí aj obrátené tvrdenie, pre každú mocninu prvočísla $k = p^n$ existuje k -prvkové pole.)

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

Rozkladové pole polynómu:

Definícia 5.5.1. Nech F je pole, $f(x) \in F[x]$ je nekonštantný polynom. Rozšírenie K poľa F nazývame *rozkladovým poľom polynómu $f(x)$ nad F* , ak existujú $c \in F$, $u_1, \dots, u_n \in K$ také, že $L = F(u_1, \dots, u_n)$ a f sa dá nad L rozložiť ako

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

Veta 5.5.2. Nech F je pole, $f(x) \in F[x]$ a st $f = n > 0$. Potom existuje rozšírenie K poľa F , ktoré je rozkladovým poľom polynómu $f(x)$.

Veta 5.5.3. Nech $\varphi: F \rightarrow F'$ je homomorfizmus polí, $f(x) \in F[x]$ a $f'(x) \in F'[x]$ je polynom, ktorý získame z $f(x)$ aplikovaním φ na všetky koeficienty polynómu $f(x)$. (V označení z poznámky 5.3.12 to znamená $f'(x) = \hat{\varphi}(f(x))$.) Ak K je rozkladové pole polynómu $f(x)$ a L je rozkladové pole polynómu $f'(x)$, tak existuje izomorfizmus $\sigma: K \rightarrow L$, ktorý navyše rozširuje φ , t.j. $\sigma|_F = \varphi$.

Dôsledok 5.5.4. Lubovoľné dve rozkladové polia polynómu $f(x)$ nad F sú izomorfné.

Ireducibilné polynómy:

Definícia 4.5.19. Polynom $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ sa nazýva *normovaný* (alebo tiež *monický*) ak $a_n = 1$ (vedúci koeficient sa rovná 1).

Definícia 4.5.20. Ak R je obor integrity, tak ireducibilné prvky okruhu $R[x]$ nazývame *ireducibilné polynómy* v $R[x]$.

V prípade, že ide o pole, tak z predchádzajúcej kapitoly vieme, že $F[x]$ je euklidovský okruh (a teda je to aj okruh hlavných ideálov a okruh s jednoznačným rozkladom). Tento fakt nám umožní používať všetky výsledky z predchádzajúcej kapitoly aj pre polynómy nad nejakým poľom.

Veta 4.5.21 (Rozklad na irreducibilné polynómy). Ak F je pole, tak každý polynóm $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_0$ možno vyjadriť v tvare

$$f(x) = a_n p_1(x) \dots p_n(x),$$

kde p_1, \dots, p_n sú irreducibilné normované polynómy. Navyše, tento rozklad je (az na poradie činitelov) jednoznačne určený.

Dôkaz. Pretože $F[x]$ je okruh s jednoznačným rozkladom, vieme, že každý polynóm sa dá rozložiť na súčin irreducibilných polynómov a ten rozklad je jednoznačný až na asociovanosť. V okruhu $F[x]$ sú dva prvky asociované práve vtedy, keď sa líšia iba konštantným násobkom. Tým, že vo vete požadujeme normované polynómy, sú teda už jednoznačne určené (z lúbovňa polynómu dostaneme normovaný, keď ho vynásobíme b_m^{-1} , kde b_m je jeho vedúci koeficient; súčin vedúcich koeficientov sme dali pred súčin normovaných činitelov – tento súčin sa rovná a_n). \square

Tvrdenie 4.5.22. Ak F je pole a $f(x) \in F[x]$ je polynóm stupňa 2 alebo 3, tak polynóm $f(x)$ je irreducibilný v F práve vtedy, keď $f(x)$ nemá koreň v F .

Dôkaz. Stačí si všimnúť, že ak chceme polynóm stupňa 2 alebo 3 rozložiť ako súčin polynómov nižších stupňov, nevyhnutne sa tam musí vyskytnúť polynóm stupňa 1. Z lemy 4.5.4 vieme, ako súvisia lineárne delitele polynómu a jeho korene. \square

Počítanie???:

Príklad 5.3.8. Uvažujme polynóm $p(x) = x^2 + x + 1$ nad polom \mathbb{Z}_2 . Tento polynóm je irreducibilný, lebo ide o polynóm druhého stupňa, ktorý nemá v danom poli koreň (tvrdenie 4.5.22). Ak označíme ako u triedu polynómu x vo faktorovom okruhu $GF_4 = \mathbb{Z}_2[x]/(p(x))$, tak prvky pola GF_4 sú $\{0, 1, u, u + 1\}$. Na základe predchádzajúcich úvah vieme vyplniť tabuľku násobenia a sčítovania v tomto poli:

$$(au + b) + (cu + d) = (a + b)u + (b + d)$$

$$(au + b)(cu + d) = acu^2 + (bc + ad)u + bd = ac(u + 1) + (bc + ad)u + bd = (ac + bc + ad)u + (ac + bd)$$

+	0	1	u	$u + 1$.	0	1	u	$u + 1$
0	0	1	u	$u + 1$	0	0	0	0	0
1	1	0	$u + 1$	u	1	0	1	u	$u + 1$
u	u	$u + 1$	0	1	u	0	u	$u + 1$	1
$u + 1$	$u + 1$	u	1	0	$u + 1$	0	$u + 1$	1	u

Samozrejme, keďže polynóm $x^2 + x + 1$ je polynóm druhého stupňa a má v poli GF_4 koreň, musí sa dať rozložiť na lineárne činitele. Skutočne v GF_4 platí $x^2 + x + 1 = (x + u)(x + u + 1)$.

Príklad 5.3.9. Polynóm $p(x) = x^2 + 1$ je ireducibilný nad \mathbb{R} . Uvažujme pole $\mathbb{R}[x]/(x^2 + 1)$. Pokúsmo sa zistiť, čomu sa v tomu poli rovná súčin $(au + b)(cu + d)$. V $\mathbb{R}[x]$ máme rovnosť

$$(ax + b)(cx + d) = acx^2 + (cb + ad)x + bc = ac(x^2 + 1) + (cb + ad)x + (bd - ac).$$

Z toho dostávame rovnosť v poli $\mathbb{R}[x]/(x^2 + 1)$

$$(ax + b)(cx + d) + (p(x)) = (cb + ad)x + (bd - ac) + (p(x)),$$

$$(au + b)(cu + d) = (cb + ad)u + (bd - ac).$$

Vidíme, že predpis pre sčítovanie násobenie je rovnaký ako pre komplexné čísla, čiže sme takto (až na izomorfizmus) získali pole \mathbb{C} t.j. $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$

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