1. POLIA A VEKTOROVÉ PRIESTORY

V tejto kapitole zavedieme dva druhy algebraických štruktúr, ktoré budú hrať v celom ďalšom výklade kľúčovú úlohu, a dokážeme o nich niekoľko jednoduchých základných tvrdení. Ide štruktúry, ktoré zahŕňame pod pojem *poľa* a pojem *vektorového priestoru*.

Prvky poľa budeme nazývať *skaláry*, a niekedy len čísla. Fyzikálne ich možno interpretovať ako hodnoty fyzikálnych veličín, ktoré sú určené iba svojou veľkosťou a znamienkom. Prvky vektorového priestoru, t. j. *vektory*, zasa zodpovedajú fyzikálnym veličinám, ktoré sú okrem veľkosti určené tiež smerom a orientáciou.

1.1. Základné číselné obory

Predpokladáme, že čitateľ pozná základné číselné obory, ako sú *prirodzené čísla*, *celé čísla*, *racionálne čísla*, *reálne čísla* a *komplexné čísla*. Každý z týchto číselných oborov tvorí množinu. Dohodneme sa, že ich budeme označovať tzv. tučnými tabuľovými písmenami:

$\mathbb{N}$ – množina všetkých prirodzených čísel,
$\mathbb{Z}$ – množina všetkých celých čísel,
$\mathbb{Q}$ – množina všetkých racionálnych čísel,
$\mathbb{R}$ – množina všetkých reálnych čísel,
$\mathbb{C}$ – množina všetkých komplexných čísel.

Ešte poznamenajme, že i nulu považujeme za prirodzené číslo, t. j. $0 \in \mathbb{N}$. *Imaginárnu jednotku* (ktorá je prvkom $\mathbb{C} \smallsetminus \mathbb{R}$) budeme značiť i.

Konštatovaním, že uvedené číselné obory tvoria množiny, sme však ich štruktúru zďaleka nevyčerpali. Omnoho dôležitejšie je, že na každej z týchto množín sú definované dve binárne operácie, *sčítanie* $+$ a *násobenie* $\cdot$. Pritom na každej z uvedených množín sú obe tieto operácie asociatívne a komutatívne. Navyše, násobenie je (z oboch strán) *distributívne* vzhľadom na sčítanie, t. j. pre všetky prvky x, y, z príslušnej množiny platí

$$x(y+z) = xy + xz, \qquad (x+y)z = xz + yz.$$

Číselný obor $\mathbb{N}$ je v porovnaní s obormi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ akýsi „chudobnejší“ – kým rovnice tvaru $x + a = b$ majú v oboroch $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ riešenie $x = b - a$ pre ľubovoľné a, b, v $\mathbb{N}$ je takáto rovnica riešiteľná len ak $a \leq b$. Obory $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ sú však „bohatšie“ nielen v porovnaní s $\mathbb{N}$ no i so $\mathbb{Z}$ – rovnice tvaru $ax = b$ majú v oboroch $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ riešenie pre ľubovoľné $a \neq 0$ a b, kým v $\mathbb{N}$ či $\mathbb{Z}$ sú riešiteľné len ak a je deliteľom b.

Nás budú zaujímať práve vlastnosti číselných oborov $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ s operáciami sčítania a násobenia. Pritom využijeme, že uvedené operácie na týchto oboroch majú rad spoločných vlastností, čo nám umožňuje skúmať ich do veľkej miery jednotným spôsobom a súčasne. To dosiahneme tým, že sformulujeme abstraktný pojem *poľa*, pod ktorý zahrnieme všetky spomínané prípady, ako i mnohé ďalšie, ktoré sa nám objavia až akosi dodatočne. Ako sme spomínali už v úvode, práve takýto prístup je charakteristický pre algebru, presnejšie, v ňom spočíva jej podstata.

1.2. Polia

Poľom nazývame množinu K s dvoma význačnými prvkami – *nulou* 0 a *jednotkou* 1 – a dvomi binárnymi operáciami na K – *sčítaním* $+$ a *násobením* $\cdot$ – takými, že platí

$$
\begin{array}{ll}
(\forall\, a,b \in K)(a+b=b+a), & (\forall\, a,b \in K)(a\cdot b=b\cdot a),\\
(\forall\, a,b,c \in K)(a+(b+c)=(a+b)+c), & (\forall\, a,b,c \in K)(a\cdot(b\cdot c)=(a\cdot b)\cdot c),\\
(\forall\, a \in K)(a+0=a), & (\forall\, a \in K)(1\cdot a=a),\\
(\forall\, a \in K)(\exists\, b \in K)(a+b=0), & (\forall\, a \in K\smallsetminus\{0\})(\exists\, b \in K)(a\cdot b=1),\\
(\forall\, a,b,c \in K)(a\cdot(b+c)=(a\cdot b)+(a\cdot c)), & 0\neq 1.
\end{array}
$$

Teda sčítanie a násobenie v poli sú komutatívne a asociatívne operácie a násobenie je distributívne vzhľadom na sčítanie. Ďalej 0 je neutrálny prvok sčítania a 1 je neutrálny prvok násobenia, pričom tieto dva prvky sú rôzne. Jednoducho možno nahliadnuť, že prvok $b \in K$ taký, že $a+b=0$, t. j. inverzný prvok vzhľadom na operáciu sčítania, je k danému prvku $a \in K$ určený jednoznačne (pozri paragraf 0.4). Tento jednoznačne určený prvok k danému a označujeme $-a$ a nazývame *opačný prvok* k a. Miesto $a+(-b)$ zvykneme písať len $a-b$. Takisto prvok $b \in K$ taký, že $a\cdot b=1$, je k danému $0\neq a\in K$ určený jednoznačne – označujeme ho a^{-1} alebo $\frac{1}{a}$, prípadne $1/a$ a nazývame *inverzný prvok* k a alebo *prevrátená hodnota* prvku a. Miesto $a\cdot b^{-1}$ píšeme tiež $\frac{a}{b}$ alebo a/b.

Znak násobenia budeme väčšinou vynechávať a násobenie bude mať prednosť pred sčítaním, teda napr. miesto $(a\cdot b)+c$ budeme písať len $ab+c$. Asociatívnosť nám umožňuje vynechávať zátvorky a súčty či súčiny ľubovoľných konečných postupností prvkov poľa jednoznačne zapisovať v tvare $a_1+a_2+\ldots+a_n$ resp. $a_1\cdot a_2\cdot\ldots\cdot a_n$ prípadne len $a_1a_2\ldots a_n$; komutatívnosť nám navyše dovoľuje nestarať sa o poradie sčítancov resp. činiteľov. Kvôli úplnosti sa dohodneme, že pre $n=1$ sa oba uvedené výrazy rovnajú a_1; pre $n=0$ kladieme prázdny súčet rovný 0 a prázdný súčin rovný 1. Ak $a_1=\ldots=a_n=a$, tak miesto $a_1+\ldots+a_n$ píšeme na a miesto $a_1\ldots a_n$ len a^n.

Teraz si ukážeme, ako možno niektoré najzákladnejšie pravidlá počítania, na ktoré sme zvyknutí v číselných oboroch $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$, odvodiť len z axióm poľa. Zhrnieme ich do nasledujúceho tvrdenia. Okrem iného z neho vyplýva, že k 0 nemôže v poli existovať inverzný prvok (podmienka (c)).

1.2.1. Tvrdenie. *Nech K je pole. Potom pre ľubovoľné $n\in\mathbb{N}$ a $a,b,c,b_1,\ldots,b_n\in K$ platí*

(a) $a+b=a+c \Rightarrow b=c$,
(b) $(ab=ac\ \&\ a\neq 0) \Rightarrow b=c$,
(c) $a0=0$,
(d) $ab=0 \Rightarrow (a=0 \vee b=0)$,
(e) $-a=(-1)a$,
(f) $a(b-c)=ab-ac$,
(g) $a(b_1+\ldots+b_n)=ab_1+\ldots+ab_n$.

Dôkaz. (a), (b) Keďže obe podmienky možno dokázať v podstate rovnako, urobíme to len pre druhú z nich. Z $ab = ac$ vyplýva $a^{-1}ab = a^{-1}ac$. Ľavá strana sa rovná b a pravá c.

(c) $a0 + a0 = a(0 + 0) = a0 = a0 + 0$. Podľa (a) z toho vyplýva $a0 = 0$.

(d) Nech $ab = 0$. Potom podľa (c) $ab = 0 = a0$. Ak $a \neq 0$, tak podľa (b) z toho vyplýva $b = 0$.

(e) Vďaka jednoznačnosti opačného prvku k a stačí overiť, že $(-1)a + a = 0$. Jednoduchý výpočet dáva $(-1)a + a = (-1)a + 1a = (-1 + 1)a = 0a = 0$ podľa (c).

(f) Podľa (e) $a(b - c) = a(b + (-1)c) = ab + a(-1)c = ab + (-1)ac = ab - ac$.

(g) Rovnosť zrejme platí pre $n = 0, 1, 2$. Keby neplatila pre všetky prirodzené čísla, označme n najmenšie prirodzené číslo, pre ktoré existujú $a, b_1, \ldots, b_n \in K$ také, že uvedená rovnosť neplatí. Potom $n > 2$ a pre $n - 1$ rovnosť platí. Preto

$$a(b_1 + \ldots + b_{n-1} + b_n) = a(b_1 + \ldots + b_{n-1}) + ab_n = ab_1 + \ldots + ab_{n-1} + ab_n.$$

To je však spor.

Doplňme, že podmienky (a) a (b) sa nazývajú *pravidlá krátenia* pre sčítanie resp. násobenie v poli.

Podmienka (e) nám umožňuje zaviesť ľubovoľné celočíselné násobky prvkov z poľa. Pre $a \in K$, $n \in \mathbb{N}$ kladieme $(-n)a = -(na) = n(-a)$. Podobne možno pre nenulové prvky poľa zaviesť i ľubovoľné celočíselné mocniny. Pre $0 \neq a \in K$, $n \in \mathbb{N}$ kladieme $a^{-n} = (a^n)^{-1} = (a^{-1})^n$.

Čitateľovi prenechávame, aby si sám odvodil nasledujúce rovnosti známe z bežných číselných oborov:

$$\begin{array}{ll}
0a = 0, \quad 1a = a, & a \in K, \\
n(a + b) = na + nb, & a, b \in K,\ n \in \mathbb{Z}, \\
(m + n)a = ma + na, & a \in K,\ m, n \in \mathbb{Z}, \\
(mn)a = m(na), & a \in K,\ m, n \in \mathbb{Z}, \\
(mn)(ab) = (ma)(nb), & a, b \in K,\ m, n \in \mathbb{Z}, \\
a^0 = 1, \quad a^1 = a, & a \in K, \\
(ab)^n = a^n b^n, & a, b \in K,\ n \in \mathbb{Z},\ n < 0 \Rightarrow a \neq 0 \neq b, \\
a^{m+n} = a^m a^n, & a \in K,\ m, n \in \mathbb{Z},\ (m < 0 \vee n < 0) \Rightarrow a \neq 0, \\
a^{mn} = (a^m)^n, & a \in K,\ m, n \in \mathbb{Z},\ (m < 0 \vee n < 0) \Rightarrow a \neq 0,
\end{array}$$

Ešte podotýkame, že v rovnostiach v prvom a šiestom riadku označujú 0 a 1 na ľavých stranách prirodzené čísla, t. j. prvky množiny $\mathbb{N}$, kým 0 a 1 na pravých stranách v prvom riadku označujú prvky poľa K. Vzhľadom na to, že pre všetky tri príklady polí, s ktorými sme doteraz stretli, platí $\mathbb{N} \subseteq K$, môže sa nám toto rozlíšenie zdať nepodstatné. Vo všeobecnosti však uvedená inklúzia platiť nemusí.

Nech K je pole a $L \subseteq K$. Hovoríme, že L je *podpole* poľa K, ak $0, 1 \in L$ a pre všetky $a, b \in L$ platí $a + b \in L$, $ab \in L$, $-a \in L$ a, ak $a \neq 0$, tak aj $a^{-1} \in L$. Inak povedané, podpole poľa K je taká jeho podmnožina L, ktorá obsahuje nulu a jednotku a je uzavretá vzhľadom na sčítanie, násobenie, opačný a inverzný prvok. Zrejme každé podpole poľa K je s týmito operáciami zúženými z K na L i samo poľom. Hovoríme tiež, že pole K je *rozšírením* poľa L.

Zrejme pole $\mathbb{Q}$ je podpoľom poľa $\mathbb{R}$ i poľa $\mathbb{C}$; pole $\mathbb{C}$ je rozšírením poľa $\mathbb{Q}$ aj $\mathbb{R}$.

Charakteristikou poľa K, označenie $\operatorname{char} K$, nazývame najmenšie kladné celé číslo n také, že $n1 = 0$; ak také n neexistuje, t. j. $n1 \neq 0$ pre každé celé $n > 0$, hovoríme že K má charakteristiku ∞ (niektorí autori vtedy kladú $\operatorname{char} K = 0$).

Ak pole K je rozšírením poľa L, tak polia K a L majú tú istú jednotku, preto $\operatorname{char} K = \operatorname{char} L$.

Zrejme $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = \infty$.

1.2.2. Veta. *Nech K je pole. Potom* $\operatorname{char} K$ *je ∞ alebo prvočíslo.*

Dôkaz. Keďže $0 \neq 1$, zrejme $\operatorname{char} K > 1$. Predpokladajme, že $\operatorname{char} K = n$ je zložené číslo. Potom existujú celé čísla $k, l > 1$ také, že $n = kl$. Keďže $k, l < n$, je $k1 \neq 0 \neq l1$. Na druhej strane $(k1)(l1) = (kl)(1 \cdot 1) = n1 = 0$. Podľa 1.2.1(d) z toho vyplýva $k1 = 0$ alebo $l1 = 0$, čo je spor.

1.3. Polia $\mathbb{Z}_p$

V tomto krátkom paragrafe si ukážeme príklady polí, ktorých charakteristika nie je ∞. Z toho dôvodu sa tieto polia výrazne odlišujú od našich dôverne známych číselných polí. Presnejšie, pre každé prvočíslo p zostrojíme isté konečné pole $\mathbb{Z}_p$, ktoré má p prvkov a charakteristiku p. Na druhej strane, spomínané číselné polia (ako vôbec všetky polia nekonečnej charakteristiky) sú nekonečné. Poznamenajme, že pre každé prvočíslo p a kladné celé číslo k existuje p^k-prvkové pole s charakteristikou p ako aj nekonečné polia charakteristiky p. Ich konštrukcia však presahuje rámec nášho úvodného kurzu.

Pre potreby matematickej analýzy, teda aj z hľadiska fyzikálnych aplikácií, sú najdôležitejšími poľami $\mathbb{R}$ a $\mathbb{C}$. Konečné polia však v súčasnosti zohrávajú dôležitú úlohu napr. v kódovaní a kryptografii.

Pre každé kladné celé číslo n označme

$$\mathbb{Z}_n = \{k \in \mathbb{N};\ k < n\} = \{0, 1, \dots, n-1\}.$$

Množinu $\mathbb{Z}_n$ zo zrejmých dôvodov (pozri cvičenia 0.3 a 0.16) nazývame *množinou zvyškových tried modulo n*. Na tejto množine teraz zavedieme dve binárne operácie – sčítanie $\oplus$ a násobenie $\odot$ (toto trochu ťažkopádne označenie budeme používať len v tomto paragrafe, neskôr sa vrátime k obvyklým $+$ a $\cdot$; v definícii však treba odlíšiť sčítanie a násobenie v $\mathbb{Z}_n$ od príslušných operácií v $\mathbb{Z}$). Pre $a, b \in \mathbb{Z}_n$ kladieme

$$a \oplus b = \text{zvyšok po delení } (a+b) : n,$$
$$a \odot b = \text{zvyšok po delení } (ab) : n.$$

Čitateľovi prenechávame na overenie (prípadne na uverenie), že $\oplus$ a $\odot$ sú asociatívne a komutatívne operácie na $\mathbb{Z}_n$ a násobenie je distributívne vzhľadom na sčítanie. Ďalej 0 je neutrálny prvok sčítania a, pre $n > 1$, je 1 neutrálny prvok násobenia. Navyše $\ominus a = n - a$ je opačný prvok k $a \in \mathbb{Z}_n \setminus \{0\}$; pre $a = 0$ je samozrejme $\ominus 0 = 0$.

1.3.1. Veta. *Množina $\mathbb{Z}_n$ s operáciami $\oplus$ a $\odot$ je pole práve vtedy, keď n je prvočíslo.*

Dôkaz. Zrejme n je najmenšie kladné celé číslo také, že

$$n1 = \underbrace{1 \oplus \ldots \oplus 1}_{n\text{-krát}} = 0.$$

Preto, ak $\mathbb{Z}_n$ je pole, tak $\operatorname{char} \mathbb{Z}_n = n$, a podľa 1.2.2 je n prvočíslo.

Dokážeme, že $\mathbb{Z}_p$ je pole pre každé prvočíslo p. Najprv overíme, že v $\mathbb{Z}_p$ platí zákon o krátení

$$(a \odot b = a \odot c \ \& \ a \neq 0) \ \Rightarrow \ b = c.$$

Rovnosť $a \odot b = a \odot c$ znamená, že číslo $ab - ac = a(b-c)$ je deliteľné číslom p. Keďže p je prvočíslo, musí byť aspoň jedno z čísel a, $b - c$ deliteľné číslom p. Nakoľko $0 < a < p$, može to byť len $b - c$. Pre $b, c \in \mathbb{Z}_p$ to však znamená $b = c$.

Zostáva overiť existenciu inverzného prvku ku každému $0 \neq a \in \mathbb{Z}_p$. Uvažujme postupnosť mocnín $a^1 = a$, $a^2 = a \odot a$, $a^3 = a \odot a \odot a, \ldots$, atď. Keďže $a \neq 0$, z dokázaného krátenia vyplýva, že všetky jej členy sú nenulové. Pretože množina $\mathbb{Z}_p$ je konečná, nemôžu byť všetky členy uvedenej postupnosti rôzne. Musia preto existovať kladné celé čísla k, l také, že $a^k = a^{k+l} = a^k \odot a^l$. Potom platí $a^k \odot a^l = a^k \odot 1$, z čoho krátením dostávame $a^l = 1$. Keďže $a^l = a \odot a^{l-1}$, je $a^{-1} = a^{l-1}$ inverzný prvok k a.

Multiplikatívne tabuľky sčítania a násobenia v poli $\mathbb{Z}_5$ sme si ako príklady binárnych operácií uviedli v paragrafe 0.4.

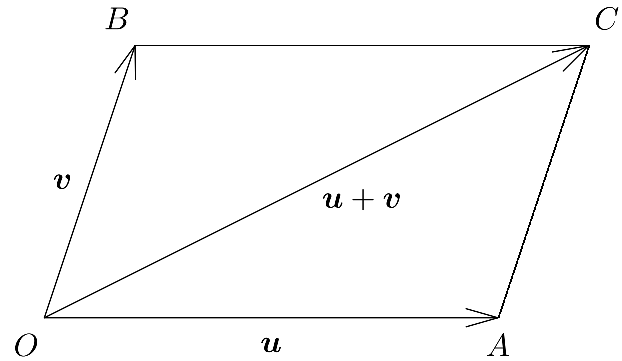
1.4. Vektory v rovine a v trojrozmernom priestore

Vektory v rovine či v priestore si predstavujeme ako orientované úsečky, t. j. úsečky, ktorých jeden krajný bod považujeme za počiatočný a druhý za koncový – ten je označený šípkou. Pritom dve rovnako dlhé, rovnobežné a súhlasne orientované úsečky predstavujú ten istý vektor – hovoríme, že sú umiestneniami toho istého vektora. Ak si teda zvolíme nejaký pevný bod O, tak všetky vektory v rovine či priestore môžeme jednoznačne reprezentovať ako orientované úsečky $\overrightarrow{OA}$ s počiatkom v O, pričom ich koncom môže byť ľubovoľný bod A roviny či priestoru, bod O nevynímajúc – orientovaná úsečka $\overrightarrow{OO}$ totiž predstavuje tzv. nulový vektor.

Vektory v rovine i v priestore možno sčítať pomocou tzv. *vektorového rovnobežníka*. Súčet vektorov $\boldsymbol{u} = \overrightarrow{OA}$, $\boldsymbol{v} = \overrightarrow{OB}$ je potom znázornený orientovanou uhlopriečkou $\boldsymbol{u} + \boldsymbol{v} = \overrightarrow{OC}$ rovnobežníka, ktorého dve priľahlé strany tvoria úsečky OA, OB.

Vektory možno taktiež násobiť ľubovoľnými skalármi, t. j. reálnymi číslami: ak $c \in \mathbb{R}$ a $\boldsymbol{v}$ je vektor, tak $c\boldsymbol{v}$ je vektor, t. j. orientovaná úsečka s počiatkom v O, ktorej dĺžka je $|c|$-násobkom dlžky úsečky $\boldsymbol{v}$, leží na tej istej priamke ako $\boldsymbol{v}$ a je orientovaná súhlasne s $\boldsymbol{v}$, ak $c > 0$, resp. nesúhlasne s $\boldsymbol{v}$, ak $c < 0$, (ak $c = 0$ alebo $\boldsymbol{v}$ je nulový vektor, tak, samozrejme, aj $c\boldsymbol{v}$ je nulový vektor, takže nezáleží na jeho smere ani orientácii).

Ak si okrem počiatku O zvolíme v rovine či priestore ešte dve resp. tri súradné osi, t. j. navzájom kolmé priamky prechádzajúce počiatkom, a na každej z nich jeden bod v rovnakej jednotkovej vzdialenosti od počiatku, dostaneme pravouhlý súradnicový systém v rovine či v priestore. Každý bod roviny či priestoru je potom jednoznačne



Obr. 1.1. Vektorov rovnobenk

určený usporiadanou dvojicou, resp. trojicou svojich súradníc a tiež naopak, každá dvojica resp. trojica súradníc jednoznačne určuje nejaký bod roviny či priestoru. Taktiež každý vektor v rovine či v priestore je potom jednoznačne určený súradnicami svojho koncového bodu a tiež naopak ľubovoľná usporiadaná dvojica resp. trojica súradníc jednoznačne určuje nejaký vektor v rovine či priestore. Pri pevnom súradnicovom systéme tak možno množinu všetkých vektorov v rovine stotožniť s množinou $\mathbb{R}^2$ a množinu všetkých vektorov v priestore s množinou $\mathbb{R}^3$.

Ak (pri takomto stotožnení) $\boldsymbol{u} = (u_1, u_2) \in \mathbb{R}^2$, $\boldsymbol{v} = (v_1, v_2) \in \mathbb{R}^2$ sú dva vektory v rovine, tak ľahko nahliadneme, že pre ich súčet $\boldsymbol{u} + \boldsymbol{v}$, daný vektorovým rovnobežníkom, platí

$$\boldsymbol{u} + \boldsymbol{v} = (u_1, u_2) + (v_1, v_2) = (u_1 + v_1, u_2 + v_2).$$

Ak $c \in \mathbb{R}$, tak pre skalárny násobok $c\boldsymbol{u}$ dostávame

$$c\boldsymbol{u} = c(u_1, u_2) = (cu_1, cu_2).$$

Podobne možno reprezentovať aj operácie súčtu a skalárneho násobku vektorov v priestore príslušnými operáciami na množine $\mathbb{R}^3$ všetkých usporiadaných trojíc reálnych čísel.

Ešte si všimnime, že predpoklady kolmosti súradných osí a rovnosti jednotkových dĺžok v jednotlivých smeroch nehrali v našich úvahách nijakú úlohu. Stačí, aby systém súradných osí tvorili dve rôznobežné priamky (v rovine) resp. tri nekomplanárne priamky (v priestore) pretínajúce sa v počiatku O. Za jednotkové dĺžky v smeroch jednotlivých súradných osí možno zvoliť dĺžky ľubovoľných (nie nevyhnutne rovnako dlhých) úsečiek.

Operácie súčtu vektorov a násobenia vektora skalárom majú rad vlastností, ktoré nie sú viazané len na ich špecifickú geometrickú reprezentáciu v rovine či priestore. Napríklad, prostredníctvom súradnicovej reprezentácie vektorov by sme ich mohli priamočiaro zovšeobecniť na usporiadané n-tice skalárov z ľubovoľného poľa K pre akékoľvek $n \in \mathbb{N}$. Tým by sme dostali akési „n-rozmerné vektorové priestory nad poľom K“. V duchu algebry teraz zadefinujeme abstraktný pojem vektorového priestoru nad daným poľom, pričom budeme abstrahovať od akýchkoľvek súradníc aj „dimenzie“. Podstatné budú pre nás len algebraické vlastnosti operácií súčtu vektorov a skalárneho násobku vektora. K spomínaným príkladom sa však budeme sústavne vracať.

1.5. Vektorové priestory

Nech K je pole. *Vektorovým* alebo tiež *lineárnym priestorom* nad poľom K nazývame množinu V s význačným prvkom $\mathbf{0}$ a dvomi binárnymi operáciami – *sčítaním* $+ : V \times V \to V$ a *násobením* $\cdot : K \times V \to V$ – takými, že platí

$$\begin{aligned}
&(\forall\, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in V)(\boldsymbol{x} + (\boldsymbol{y} + \boldsymbol{z}) = (\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z}),\\
&(\forall\, \boldsymbol{x}, \boldsymbol{y} \in V)(\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x}),\\
&(\forall\, \boldsymbol{x} \in V)(\boldsymbol{x} + \mathbf{0} = \boldsymbol{x}),\\
&(\forall\, \boldsymbol{x} \in V)(\exists\, \boldsymbol{y} \in V)(\boldsymbol{x} + \boldsymbol{y} = \mathbf{0}),\\
&(\forall\, a, b \in K)(\forall\, \boldsymbol{x} \in V)(a \cdot (b \cdot \boldsymbol{x}) = (ab) \cdot \boldsymbol{x}),\\
&(\forall\, \boldsymbol{x} \in V)(1 \cdot \boldsymbol{x} = \boldsymbol{x}),\\
&(\forall\, a \in K)(\forall\, \boldsymbol{x}, \boldsymbol{y} \in V)(a \cdot (\boldsymbol{x} + \boldsymbol{y}) = (a \cdot \boldsymbol{x}) + (a \cdot \boldsymbol{y})),\\
&(\forall\, a, b \in K)(\forall\, \boldsymbol{x} \in V)((a + b) \cdot \boldsymbol{x} = (a \cdot \boldsymbol{x}) + (b \cdot \boldsymbol{x})).
\end{aligned}$$

Ako si čitateľ asi všimol, skaláry značíme „obyčajnými“ malými latinskými písmenami a vektory tučnými malými latinskými písmenami. Tejto implicitnej dohody sa budeme väčšinou držať, nie však za každú cenu. Kedykoľvek by nás obmedzovala, nebudeme váhať ju porušiť.

I keď sčítanie skalárov v poli a sčítanie vektorov značíme rovnakým znakom $+$, ide o rôzne operácie. Podobne násobenie v poli a násobenie vektora skalárom sú rôzne operácie, hoci obe značíme $\cdot$. Neskôr tento prístup dovedieme ešte ďalej, keď budeme rovnako značiť príslušné operácie a nuly v rôznych vektorových priestoroch. Rozlišovanie znakov pre nulu $0 \in K$ a $\mathbf{0} \in V$, hoci tieto prvky plnia rovnakú funkciu v K resp. vo V, je tak trochu proti duchu tohto prístupu. Ide vlastne o zbytočný luxus, ktorý je však v zhode s prijatou dohodou o značení skalárov a vektorov.

Z formálneho hľadiska pripomínajú axiómy vektorového priestoru axiómy poľa: sčítanie vektorov je opäť asociatívna a komutatívna binárna operácia na V s neutrálnym prvkom $\mathbf{0} \in V$, operácia násobenia vektora skalárom tiež spĺňa akúsi podmienku „asociatívnosti“, $1 \in K$ je jej „neutrálnym prvkom“ a platia dva „distributívne zákony“. Je tu však jeden podstatný rozdiel – kým násobenie v poli K je binárnou operáciou na množine K, t. j. zobrazením $\cdot : K \times K \to K$, násobenie vo vektorovom priestore V nad poľom K nie je binárnou operáciou na V, ale binárnou operáciou $\cdot : K \times V \to V$. To nám však nebráni zaviesť obdobné dohody ako pre operácie v poli: i teraz bude mať násobenie prednosť pre sčítaním a znak násobenia budeme väčšinou vynechávať, t. j. písať napr. $a\boldsymbol{x} + \boldsymbol{y}$ miesto $(a \cdot \boldsymbol{x}) + \boldsymbol{y}$. Takisto budeme vynechávať zátvorky, ktorých umiestnenie neovplyvní výslednú hodnotu výrazov ako napr. v $ab\boldsymbol{x}$ alebo $a_1\boldsymbol{x}_1 + \ldots + a_n\boldsymbol{x}_n$. Posledný výraz budeme tiež značiť

$$\sum_{i=1}^{n} a_i \boldsymbol{x}_i$$

a nazývať *lineárnou kombináciou* vektorov $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ s koeficientmi $a_1, \ldots, a_n$. Špeciálne pre $n = 1$ to znamená $\sum_{i=1}^{1} a_i\boldsymbol{x}_i = a_1\boldsymbol{x}_1$; kvôli úplnosti pre $n = 0$ ešte kladieme prázdnu lineárnu kombináciu $\sum_{i=1}^{0} a_i\boldsymbol{x}_i$ rovnú $\mathbf{0}$.

Podobne ako v prípade polí, možno z axióm vektorových priestorov odvodiť niektoré základne pravidlá pre počítanie so skalármi a vektormi. Predovšetkým prvok $\boldsymbol{y} \in V$ taký, že $\boldsymbol{x}+\boldsymbol{y} = \mathbf{0}$, je k danému $\boldsymbol{x} \in V$ určený jednoznačne – značíme ho $-\boldsymbol{x}$ a nazývame *opačný vektor* k $\boldsymbol{x}$. Namiesto $\boldsymbol{x} + (-\boldsymbol{y})$ opäť píšeme len $\boldsymbol{x} - \boldsymbol{y}$. Tieto pravidlá zhrnieme v nasledujúcej analógii tvrdenia 1.3.1.

1.5.1. Tvrdenie. *Nech V je vektorový priestor nad poľom K. Potom pre ľubovoľné $n \in \mathbb{N}$, $a, b, a_1, \dots, a_n \in K$ a $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n \in V$ platí*

(a) $\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{x} + \boldsymbol{z} \Rightarrow \boldsymbol{y} = \boldsymbol{z}$,

(b) $(a\boldsymbol{x} = a\boldsymbol{y}\ \&\ a \neq 0) \Rightarrow \boldsymbol{x} = \boldsymbol{y}$, $\qquad (a\boldsymbol{x} = b\boldsymbol{x}\ \&\ \boldsymbol{x} \neq \mathbf{0}) \Rightarrow a = b$,

(c) $a\mathbf{0} = \mathbf{0} = 0\boldsymbol{x}$,

(d) $a\boldsymbol{x} = \mathbf{0} \Rightarrow (a = 0 \vee \boldsymbol{x} = \mathbf{0})$,

(e) $-\boldsymbol{x} = (-1)\boldsymbol{x}$,

(f) $a(\boldsymbol{x} - \boldsymbol{y}) = a\boldsymbol{x} - a\boldsymbol{y}$, $\qquad (a - b)\boldsymbol{x} = a\boldsymbol{x} - b\boldsymbol{x}$,

(g) $a(\boldsymbol{x}_1 + \ldots + \boldsymbol{x}_n) = a\boldsymbol{x}_1 + \ldots + a\boldsymbol{x}_n$, $\qquad (a_1 + \ldots + a_n)\boldsymbol{x} = a_1\boldsymbol{x} + \ldots + a_n\boldsymbol{x}$.

Dôkaz. Všetky podmienky, s výnimkou druhej implikácie v (b), možno dokázať celkom analogicky ako príslušné časti tvrdenia 1.2.1. Dokážeme aj túto. Nech $a\boldsymbol{x} = b\boldsymbol{x}$ a $\boldsymbol{x} \neq \mathbf{0}$. Potom $(a - b)\boldsymbol{x} = a\boldsymbol{x} - b\boldsymbol{x} = \mathbf{0}$. Podľa (d) z toho vyplýva $a - b = 0$, teda $a = b$.

Práve definované vektorové priestory by sme presnejšie mohli nazvať „ľavými“ vektorovými priestormi, lebo v operácii skalárneho násobku píšeme skalár vľavo od vektora. Celkom obdobne by sme mohli definovať aj „pravé“ vektorové priestory, v ktorých by sme operáciu skalárneho násobku chápali ako zobrazenie $V \times K \to V$ a zapisovali ju v tvare $\boldsymbol{x} \cdot a$ alebo len $\boldsymbol{x}a$ pre $\boldsymbol{x} \in V$, $a \in K$. Vďaka komutatívnosti násobenia v poli K si však môžeme dovoliť chápať naše „ľavé“ vektorové priestory zároveň ako „pravé“. Pre všetky $a \in K$, $\boldsymbol{x} \in V$ jednoducho položíme $\boldsymbol{x}a = a\boldsymbol{x}$. Jediný problém – zabezpečiť pre všetky $a, b \in K$, $\boldsymbol{x} \in V$ rovnosť $(ab)\boldsymbol{x} = (ba)\boldsymbol{x}$, ktorá z takejto definície vyplýva výpočtom

$$(ab)\boldsymbol{x} = a(b\boldsymbol{x}) = a(\boldsymbol{x}b) = (\boldsymbol{x}b)a = \boldsymbol{x}(ba) = (ba)\boldsymbol{x},$$

– je vyriešený práve v dôsledku komutatívnosti násobenia v K. Teda, ak sa nám v operácii skalárneho násobku vyskytne skalár vpravo od vektora, nemusí nás to vyviesť z miery – kľudne ho môžeme prehodiť vľavo a ani o zátvorky sa nemusíme príliš starať.

1.6. Príklady vektorových priestorov

1.6.1. Rozšírenia polí. Zrejme každé pole K možno považovať za vektorový priestor nad sebou samým. Všeobecnejšie, ak pole L je rozšírením poľa K, tak L možno považovať za vektorový priestor nad poľom K (formálne stačí „zabudnúť“ násobenie niektorých dvojíc prvkov $a, b \in L$ a súčin ab pripustiť len pre $a \in K$, $b \in L$). Podobným spôsobom možno vektorový priestor V nad poľom L zúžením násobenia $L \times V \to V$ na násobenie $K \times V \to V$ prerobiť na vektorový priestor nad poľom K.

1.6.2. $\boldsymbol{n}$-rozmerné riadkové a stĺpcové vektory nad daným poľom. Pre ľubovoľné pole K a $n \in \mathbb{N}$ množina

$$K^n = \{(x_1, \dots, x_n);\ x_1, \dots, x_n \in K\}$$

všetkých usporiadaných n-tíc prvkov z K spolu s operáciami

$$\begin{gathered}\boldsymbol{x}+\boldsymbol{y}=(x_1,\dots,x_n)+(y_1,\dots,y_n)=(x_1+y_1,\dots,x_n+y_n),\\ c\boldsymbol{x}=c(x_1,\dots,x_n)=(cx_1,\dots,cx_n),\end{gathered}$$

kde $\boldsymbol{x}=(x_1,\dots,x_n)\in K^n$, $\boldsymbol{y}=(y_1,\dots,y_n)\in K^n$ a $c\in K$, tvorí vektorový priestor nad poľom K. Zrejme usporiadaná n-tica $\mathbf{0}_n=(0,\dots,0)$ hrá úlohu nuly v K^n. Ak bude potrebné rozlíšiť nulové vektory v priestoroch K^n pre rôzne prirodzené čísla n, budeme pre nulu v K^n používať označenie $\mathbf{0}_n$. Opačný prvok k $\boldsymbol{x}=(x_1,\dots,x_n)\in K^n$ je zrejme

$$-\boldsymbol{x}=-(x_1,\dots,x_n)=(-x_1,\dots,-x_n)$$

Hovoríme, že operácie na K^n sú definované *po zložkách.* Prvky tohto vektorového priestoru nazývame *n-rozmerné riadkové vektory* nad poľom K. Kvôli úplnosti ešte poznamenajme, že vektorový priestor K^0 pozostáva z jediného prvku $\emptyset$, predstavujúceho „usporiadanú nulaticu“, ktorá tak je nevyhnutne nulou v K^0.

Niekedy je (a väčšinou i bude) výhodnejšie pracovať s *n-rozmernými stĺpcovými vektormi* nad poľom K, t. j. s vektormi tvaru

$$\boldsymbol{x}=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix},$$

kde $x_1,\dots,x_n\in K$. Čitateľ si iste sám doplní definície príslušných operácií (opäť po zložkách) a dalšie podrobnosti. Pokiaľ nebude hroziť nedorozumenie, budeme i tento priestor označovať K^n, prípadne len slovne naznačíme, či tým máme na mysli priestor n-rozmerných riadkových alebo stĺpcových vektorov. V súlade s tým $\mathbf{0}_n$ alebo len $\mathbf{0}$ môže označovať aj nulový vektor-stĺpec.

1.6.3. Polynómy nad daným poľom. Pod *polynómom* alebo tiež *mnohočlenom* $f(x)$ *stupňa* n, kde $n\in\mathbb{N}$, v premennej x nad poľom K rozumieme formálny výraz tvaru

$$f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}+a_nx^n=\sum_{i=0}^{n}a_ix^i,$$

kde $a_0,a_1,\dots,a_{n-1},a_n\in$ sú skaláry, nazývané *koeficienty* polynómu f, a $a_n\neq 0$; nulu $0\in K$ považujeme za polynóm stupňa -1 a nenulové skaláry $a\in K$ za polynómy stupňa 0. Zrejme každý polynóm $f(x)$ definuje (rovnako značenú) funkciu $f\colon K\to K$ danú predpisom $c\mapsto f(c)$, t. j. dosadením konkrétnych hodnôt $c\in K$ za premennú x do polynómu $f(x)$. Množinu všetkých polynómov v premennej x nad K *stupňa nanajvýš* n, kde $-1\le n\in\mathbb{Z}$, budeme značiť $K^{(n)}[x]$; množinu *všetkých polynómov* v premennej x nad K značíme $K[x]$. Ľubovoľný polynóm $g(x)=\sum_{i=0}^{m}b_ix^i\in K[x]$ stupňa $m<n$ môžeme tiež písať v tvare

$$g(x)=b_0+b_1x+\ldots+b_mx^m+0x^{m+1}+\ldots+0x^n,$$

t. j. v tvare $g(x) = \sum_{i=0}^{n} b_i x^i$, kde $b_i = 0$ pre $m < i \leq n$. S použitím tejto konvencie možno definovať súčet $f(x) + g(x)$ polynómov $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$ z $K[x]$ predpisom

$$(f+g)(x) = f(x) + g(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i.$$

Ak navyše $c \in K$, kladieme

$$(cf)(x) = cf(x) \sum_{i=0}^{n} c a_i x^i.$$

Ľahko možno nahliadnuť, že s takto po zložkách definovanými operáciami súčtu a skalárneho násobku tvorí každá z množín polynómov $K^{(n)}[x]$, kde $-1 \leq n \in \mathbb{Z}$, ako i množina všetkých polynómov $K[x]$ vektorový priestor nad poľom K. Štruktúrou vektorového priestoru sa však algebra polynómov nevyčerpáva. Popri súčte a skalárnom násobku možno na $K[x]$ definovať aj súčin $f(x)\,g(x)$ uvedených polynómov $f(x)$, $g(x)$ predpisom

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

kde $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

1.6.4. Priame súčiny vektorových priestorov. Nech V_1 a V_2 sú vektorové priestory nad tým istým poľom K. *Priamym súčinom* (niekedy tiež *vonkajším priamym súčtom*) priestorov V_1, V_2 nazývame množinu $V_1 \times V_2$, t. j. karteziánsky súčin množín V_1, V_2, s operáciami súčtu vektorov a skalárneho násobku definovanými po zložkách. Teda pre $(\boldsymbol{u}_1, \boldsymbol{u}_2)$, $(\boldsymbol{v}_1, \boldsymbol{v}_2) \in V_1 \times V_2$, $c \in K$ kladieme

$$(\boldsymbol{u}_1, \boldsymbol{u}_2) + (\boldsymbol{v}_1, \boldsymbol{v}_2) = (\boldsymbol{u}_1 + \boldsymbol{v}_1, \boldsymbol{u}_2 + \boldsymbol{v}_2),$$
$$c(\boldsymbol{u}_1, \boldsymbol{u}_2) = (c\boldsymbol{u}_1, c\boldsymbol{u}_2).$$

Zrejme $(\mathbf{0}, \mathbf{0})$ je nulou tohto vektorového priestoru a $-(\boldsymbol{u}_1, \boldsymbol{u}_2) = (-\boldsymbol{u}_1, -\boldsymbol{u}_2)$ je opačný prvok k $(\boldsymbol{u}_1, \boldsymbol{u}_2)$. Čitateľovi prenechávame, aby si overil, že priamy súčin $V_1 \times V_2$ s takto definovanými operáciami naozaj tvorí vektorový priestor nad poľom K, a taktiež, aby si premyslel, ako možno uvedenú konštrukciu zovšeobecniť na priamy súčin $V_1 \times \ldots \times V_n$ ľubovoľného konečného počtu vektorových priestorov $V_1, \ldots, V_n$ nad K. Ak $V = V_1 = \ldots = V_n$, tak píšeme $V_1 \times \ldots \times V_n = V^n$ a tento vektorový priestor nazývame n-tou *priamou mocninou* priestoru V. Pre $V = K$ uvedená konštrukcia dáva nám už známy vektorový priestor K^n z 1.5.2.

1.6.5. Vektorové priestory funkcií. Nech V je vektorový priestor nad poľom K a X je ľubovoľná množina. Pripomeňme, že V^X označuje množinu všetkých funkcií $f\colon X \to V$. Teraz ukážeme, ako možno z tejto množiny urobiť vektorový priestor nad poľom K. Operácie súčtu a skalárneho násobku budeme definovať opäť po zložkách. To znamená, že pre $f, g \in V^X$ a $c \in K$ budeme definovať funkcie $f+g \in V^X$ a $cf \in V^X$ tak, že pre každé $x \in X$ položíme

$$(f+g)(x) = f(x) + g(x),$$
$$(cf)(x) = cf(x).$$

Znovu možno ľahko nahliadnuť, že V^X s takto definovanými operáciami tvorí vektorový priestor nad poľom K – nazývame ho *vektorovým priestorom všetkých funkcií* z X do V. Nulou vo V^X je funkcia $\mathbf{0}\colon X \to V$ identicky rovná prvku $\mathbf{0} \in V$; opačným prvkom k funkcii $f \in V^X$ je funkcia $-f \in V^X$ daná predpisom $x \mapsto -f(x)$ pre $x \in X$.

V špeciálnom prípade pre $V = K$ takto dostaneme vektorový priestor K^X všetkých funkcií z množiny X do poľa K. Ak K je pole všetkých reálnych prípadne komplexných čísel a X je napr. nejaký uzavretý interval $\langle a, b\rangle$ reálnych čísel, tak dostávame vektorové priestory funkcií $\mathbb{R}^{\langle a,b\rangle}$ resp. $\mathbb{C}^{\langle a,b\rangle}$, ktoré sa hojne vyskytujú v matematickej analýze.

Cvičenia

1. Vypočítajte v obore komplexných čísel:

(a) $(5+3\mathrm{i}) + (7-\mathrm{i})$, (b) $(11-10\mathrm{i}) - (8-5\mathrm{i})$,
(c) $(-2+5\mathrm{i}) \cdot (3+2\mathrm{i})$, (d) $(4-\mathrm{i}) \cdot (2+9\mathrm{i})$,
(e) $(12+5\mathrm{i})^{-1}$, (f) $(7+\mathrm{i})/(3-4\mathrm{i})$.

2. (a) Pre komplexné číslo $x = a + b\mathrm{i}$, kde $a, b \in \mathbb{R}$, nazývame $a = \operatorname{Re} x$, $b = \operatorname{Im} x$ jeho *reálnou* resp. *imaginárnou časťou*. Teda $\operatorname{Re} x$ aj $\operatorname{Im} x$ sú *reálne čísla*. Dokážte vzorce:

$$\operatorname{Re}(x+y) = \operatorname{Re} x + \operatorname{Re} y, \qquad \operatorname{Re}(xy) = \operatorname{Re} x \operatorname{Re} y - \operatorname{Im} x \operatorname{Im} y,$$
$$\operatorname{Im}(x+y) = \operatorname{Im} x + \operatorname{Im} y, \qquad \operatorname{Im}(xy) = \operatorname{Re} x \operatorname{Im} y + \operatorname{Im} x \operatorname{Re} y.$$

(b) Ak si v (reálnej) rovine zvolíme pravouhlý súradnicový systém, môžeme každé komplexné číslo $x = a + b\mathrm{i}$ reprezentovať bodom či vektorom so súradnicami (a, b). Ak prostredníctvom bijekcie $x \mapsto (\operatorname{Re} x, \operatorname{Im} x)$ stotožníme každé komplexné číslo s jeho obrazom a množinu $\mathbb{C}$ s rovinou (množinou $\mathbb{R}^2$), hovoríme o tzv. *Gaussovej rovine*. Znázornite čísla zo zadaní aj výsledkov cvičenia 1 v Gaussovej rovine.

3. *Absolútna hodnota* komplexného čísla $x = a + b\mathrm{i}$, kde $a, b \in \mathbb{R}$, je definovaná ako $|x| = \sqrt{a^2 + b^2}$, t. j. ako vzdialenosť bodu x od počiatku v Gaussovej rovine. *Komplexne združené číslo* k číslu x je $\overline{x} = a - b\mathrm{i}$, t. j. číslo súmerne združené s x podľa reálnej osi.
(a) Nájdite absolútne hodnoty jednotlivých čísel zo zadaní aj výsledkov v cvičení 1.
(b) Dokážte nasledujúce vzťahy:

$$\operatorname{Re} \overline{x} = \operatorname{Re} x, \qquad \operatorname{Im} \overline{x} = -\operatorname{Im} x;$$
$$\overline{\overline{x}} = x, \qquad xy^{-1} = (x\overline{y})/|y|^2, \quad (y \neq 0),$$
$$\overline{x+y} = \overline{x} + \overline{y}, \qquad \overline{xy} = \overline{x}\,\overline{y},$$
$$|x| = |\overline{x}|, \qquad |x|^2 = x\overline{x},$$
$$|xy| = |x|\,|y|, \qquad |x+y| \le |x| + |y|.$$

(c) V poslednom vzťahu nastane rovnosť práve vtedy, keď existuje nezáporné číslo $c \in \mathbb{R}$ také, že $x = cy$ alebo $y = cx$. Dokážte.

4. Každé komplexné číslo x možno vyjadriť v tzv. *goniometrickom tvare* $x = r(\cos\alpha + \mathrm{i}\sin\alpha)$, kde $r = |x|$ a α je uhol, ktorý (pre $x \neq 0$) zviera v Gaussovej rovine „vektor“ $\overrightarrow{01}$ s „vektorom“ $\overrightarrow{0x}$ (pre $x = 0$ vyhovuje ľubovoľné $\alpha \in \mathbb{R}$).
(a) Pre $x \neq 0$ vyjadrite $\cos\alpha$ a $\sin\alpha$ pomocou $\operatorname{Re} x$, $\operatorname{Im} x$ a $|x|$. Dokážte, že α je určené jednoznačne až na sčítanec $2k\pi$, kde $k \in \mathbb{Z}$.

(b) Pre $x = r(\cos\alpha + \mathrm{i}\sin\alpha)$, $y = s(\cos\beta + \mathrm{i}\sin\beta)$ platí $xy = rs(\cos(\alpha+\beta) + \mathrm{i}\sin(\alpha+\beta))$. Dokážte.
(c) Matematickou indukciou dokážte tzv. *Moivreovu vetu*: $(\cos\alpha + \mathrm{i}\sin\alpha)^n = \cos n\alpha + \mathrm{i}\sin n\alpha$, pre každé $n \in \mathbb{N}$. Rozšírte jej platnosť na všetky $n \in \mathbb{Z}$.
(d) Vyjadrite všetky čísla zo zadaní aj výsledkov v cvičení 1 v goniometrickom tvare.
(e) Pomocou Moivreovej vety vypočítajte $(\sqrt{3} + \mathrm{i})^{11}$, $(1 - \mathrm{i})^{-7}$.
(f) Na základe Moivreovej vety napíšte vzorec pre všetkých n riešení *binomickej rovnice* $x^n = c$, kde $c \in \mathbb{C}$. (*Návod*: Riešte najprv prípad $|c| = 1$.)
(g) Nájdite všetky riešenia binomických rovníc $x^3 = (\sqrt{3} - \mathrm{i})/2$, $y^4 = 1 + \mathrm{i}$ a $z^5 = -4 + 3\mathrm{i}$.

5. Podrobne dokážte vzťahy uvedené za dôkazom tvrdenia 1.2.1. Kde treba, použite matematickú indukciu.

6. V každom z nasledujúcich prípadov rozhodnite, či množina A je podpoľom poľa K. Svoje rozhodnutie zdôvodnite.

(a) $K = \mathbb{Q}$, $A = \mathbb{Z}$;
(b) $K = \mathbb{R}$, $A = \mathbb{Q}\big[\sqrt{2}\big] = \{a + b\sqrt{2};\ a, b \in \mathbb{Q}\}$;
(c) $K = \mathbb{R}$, $A = \langle -1, 1\rangle$;
(d) $K = \mathbb{C}$, $A = \mathbb{Z}[\,\mathrm{i}\,] = \{a + b\mathrm{i};\ a, b \in \mathbb{Z}\}$;
(e) $K = \mathbb{Z}_{11}$, $A = \mathbb{Z}_5$;
(f) $K = \mathbb{C}$, $A = \mathbb{Q}[\omega] = \{a + b\omega + c\omega^2;\ a, b, c \in \mathbb{Q}\}$, kde $\omega = (-1 + \mathrm{i}\sqrt{3})/2$.

7. Zostrojte multiplikatívne tabuľky sčítania a násobenia v $\mathbb{Z}_n$ pre $2 \le n \le 6$. Na ich základe zdôvodnite, prečo $\mathbb{Z}_4$ a $\mathbb{Z}_6$ nie sú polia.

8. Vynechajme z definície poľa podmienku $0 \ne 1$ a podmienku požadujúcu existenciu inverzného prvku vzhľadom na násobenie ku každému nenulovému prvku $a \in K$. Množina K s význačnými prvkami $0, 1 \in K$, vybavená binárnymi operáciami súčtu a súčinu, spĺňajúcimi zvyšné podmienky sa nazýva *komutatívny okruh s jednotkou.*[1] Komutatívny okruh s jednotkou sa nazýva *netriviálny*, ak v ňom predsa len platí $0 \ne 1$. Dokážte postupne nasledujúce tvrdenia:
(a) $\mathbb{Z}$ s obvyklými operáciami súčtu a súčinu je netriviálny komutatívny okruh s jednotkou.
(b) Pre každé $n \in \mathbb{N}$, $n \ne 0$, je $\mathbb{Z}_n$ so sčítaním a násobením modulo n komutatívny okruh s jednotkou. Tento okruh je netriviálny práve vtedy, keď $n \ge 2$.
(c) Komutatívny okruh s jednotkou je netriviálny práve vtedy, keď obsahuje aspoň dva rôzne prvky.

9. (a) V ľubovoľnom komutatívnom okruhu s jednotkou K zadefinujte výrazy tvaru na pre ľubovoľné $n \in \mathbb{Z}$, $a \in K$ rovnako ako v poli. Taktiež zadefinujte výrazy tvaru a^n pre $n \in \mathbb{N}$, $a \in K$. Dokážte pre ne analogické tvrdenia, ako platia v poli. Čo je prekážkou definície a^n pre všetky $n \in \mathbb{Z}$?
(b) Zadefinujte *charakteristiku* ľubovoľného *komutatívneho okruhu s jednotkou* rovnakým spôsobom ako v prípade poľa.
(c) Dokážte, že pre komutatívny okruh s jednotkou K platí $\operatorname{char} K = 1$ práve vtedy, keď K je triviálny.
(d) Pre každé $n \in \mathbb{N}$, $n \ne 0$, platí $\operatorname{char} \mathbb{Z}_n = n$.
(e) Pre každé prvočíslo p zostrojte príklad komutatívneho okruhu s jednotkou, ktorý má charakteristiku p, no nie je poľom. (*Návod*: Pozri cvičenie 12.)

10. (a) Matematickou indukciou dokážte platnosť binomickej vety *v ľubovoľnom komutatívnom okruhu s jednotkou* K (teda aj v ľubovoľnom poli). To znamená, že pre všetky $n \in \mathbb{N}$, $a, b \in K$ platí

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \ldots + \binom{n}{n-1}ab^{n-1} + b^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

(b) Predpokladajme, že charakteristikou komutatívneho okruhu s jednotkou K je prvočíslo p. Nech $m \in \mathbb{Z}$ je násobkom p. Dokážte, že pre každé $c \in K$ platí $mc = 0$.
(c) Na základe (a) a (b) dokážte, že v komutatívnom okruhu s jednotkou prvočíselnej charakteristiky p platí pre exponent $n = p$ nasledujúci „populárny“ variant binomickej vety:

$$(a+b)^p = a^p + b^p.$$

11. Doplňte vynechané časti dôkazu tvrdenia 1.5.1.

[1] Občas sa v literatúre takáto štruktúra nazýva len komutatívny okruh.

12. V každom z príkladov 1.6.1–5 podrobne overte, že uvedená množina s príslušnými operáciami tvorí vektorový priestor.

13. Rovnako ako v príklade 1.6.3 zadefinujte pre ľubovoľný komutatívny okruh s jednotkou K množinu $K[x]$ všetkých polynómov v premennej x s koeficientmi z K a na nej operácie súčtu a súčinu. Dokážte, že $K[x]$ s takto definovanými operáciami je opäť komutatívny okruh s jednotkou a platí $\operatorname{char} K[x] = \operatorname{char} K$.

14. Na množine $\mathbb{R}^+$ všetkých kladných reálnych čísel definujme nové „sčítanie“ $\oplus$ ako násobenie, t. j. $x \oplus y = xy$. Ďalej definujme novú operáciu „skalárneho násobku“ $\odot\colon \mathbb{R} \times \mathbb{R}^+ \to \mathbb{R}^+$ ako umocňovanie, t. j. predpisom $a \odot x = x^a$. Dokážte, že množina $\mathbb{R}^+$ s uvedenými operáciami tvorí vektorový priestor nad poľom $\mathbb{R}$. Čo je nulový vektor $\mathbf{0} \in \mathbb{R}^+$? Ako vyzerá opačný vektor $\ominus x$ k vektoru $x \in \mathbb{R}^+$? Vyjadrite pomocou pôvodných operácií násobenia a umocňovania lineárnu kombináciu $(a_1 \odot x_1) \oplus \ldots \oplus (a_n \odot x_n)$, kde $a_1, \ldots, a_n \in \mathbb{R}$, $x_1, \ldots, x_n \in \mathbb{R}^+$.