Lineárna algebra

doc. Michal Zajac

Konštrukcia poľa komplexných čísel a konečných polí.

Popíšeme konštrukciu poľa komplesxných čísel analogickú konštrukcii polí Z_p. Namiesto deliteľnosti celých čísel a zvyškov po delení prvočíslom p použijeme deliteľnosť polynómov a zvyšky po delení irteducibilným polynómom ($f(x)|g(x)$ znamená: „polynóm $f(x)$ je deliteľom polynómu $g(x)$").

Označme $P(R)$ množinu všetkých polynómov s reálnymi koeficientami. Polynóm x^2+1 je ireducibilný v $P(R)$. Analogicky ako v Z definujeme kongruenciu modulo x^2+1:

$$\begin{aligned} f(x) \equiv g(x) \pmod{x^2+1} &\iff (x^2+1)|(g(x)-f(x) \\ f_1(x) \oplus f_2(x) = g(x) \pmod{x^2+1} &\iff f_1(x)+f_2(x) \equiv g(x) \pmod{x^2+1} \\ f_1(x) \odot f_2(x) = g(x) \pmod{x^2+1} &\iff f_1(x)\cdot f_2(x) \equiv g(x) \pmod{x^2+1} \end{aligned}$$

Pole komplexných čísel môžeme teraz stotožniť s množinou tried rozkladu $P(R) \pmod{x^2+1}$, ktorá sa označuje obvykle symbolom $P(R)/(x^2+1)$ alebo ekvivalentne s množinou všetkých zvyškov po delení polynómom x^2+1, t.j. s množinou $P_1(R)$ všetkých mnohočlenov stupňa najviac 1. Pritom sčítanie a násobenie sa počíta modulo x^2+1. Komplexnou jednotkou je $i = x$.

Úloha. Overte, že $C \equiv (P_1(R), \oplus, \odot)$ je pole.

Analogickou konštrukciou dostaneme aj konečné polia

Príklad. Polynóm $f(x) = x^2+x+1$ je ireducibilný polynóm nad Z_2. Popíšte pole $P(Z_2)/(x^2+x+1)$

Prvky tohoto poľa môžeme stotožniť so zvyškami po delení polynómom $f(x)$, t.j. s

$$P_1(Z_2) = \{e_0, e_1, e_2, e_3\}: \quad e_0(x) = 0\,,\ e_1(x) = 1\,,\ e_2(x) = x\,,\ e_3(x) = x+1$$

Pre toto pole napíšte tabuľku násobenia a sčítania.

Lineárne priestory.

Definícia. Trojica $(L, \oplus, \odot)$ sa nazýva lineárny (vektorový) priestor nad poľom $(K, +, \cdot)$, ak
L je neprázdna množina (vektorov) a $\oplus\colon L \times L \to L$; $\odot\colon K \times L \to L$ sú operácie také, že platí:
pre $\forall\, x, y, z \in L$ a pre $\forall\, \alpha, \beta \in K$
(L1) $x \oplus y = y \oplus x$ (komutatívny zákon pre sčítanie)
(L2) $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ (asociatívny zákon pre sčítanie)
(L3) $\exists\, \mathbf{0} \in L$: $x \oplus \mathbf{0} = x$ (existuje neutrálny prvok pre sčítanie)
(L3) $\forall x \in L\ \exists y \in L$ taký, že $x \oplus y = \mathbf{0}$ ($\exists\, y = -x$ opačný prvok k x)
(L5) $\alpha \odot (x \oplus y) = (\alpha \odot x) \oplus (\alpha \odot y)$
(L6) $(\alpha + \beta) \odot x = (\alpha \odot x) \oplus (\beta \odot y)$
(L7) $(\alpha\beta) \odot x = \alpha \odot (\beta \odot x)$
(L8) $1 \odot x = x$

Príkladmi lineárnych priestorov nad R sú priestory funkcií $f\colon A \to R$ s obvyklými operáciami sčítania funkcií a násobenia funkcie reálnym číslom. Rovnako aj množina všetkých funkciíi $f\colon A \to K$ je lineárny priestor nad poľom K. Špeciálne, ak $A = \{1, 2, \ldots, n\}$, tento priestor označujeme K^n a je to lineárny priestor usporiadaných n-tíc prvkov z poľa K.

Úloha. Vypočítajte $(1,0,1,1) \oplus (1,1,0,1)$ v lineárnom priestore K^4, kde
a. $K = R$, b. $K = Z_3$, c. $K = Z_2$.

Definícia. Nech $(L, +, \cdot)$ je lineárny priestor nad poľom K. Podmnožina $M \subset L$ sa nazýva podpriestor lineárneho priestoru $(L, +, \cdot)$, ak je $(M, +, \cdot)$ tiež lineárnym priestorom.

Veta. *Podmnožina $M \subset L$ je podpriestor lineárneho priestoru $(L, +, \cdot)$ vtedy a len vtedy, ak*
(1) $x, y \in M \implies x + y \in M$
(2) $x \in M,\ \alpha \in K \implies \alpha \cdot x \in M$.

Príklady. Ukážte, že
1. $M = \{(x_1, x_2, x_3) \in K^3\colon x_1 - x_2 + x_3 = 0\}$ je podpriestor lineárneho priestoru K^3.
2. $M = \{(1, 1, , x)\colon x \in Z_2\} = \{(1,1,,0), (1,1,,1)\}$ nie je podpriestor Z_2^3.
3. $M = \{(0, x, y)\colon x, y \in Z_2\}$ je podpriestor Z_2^3.
4. Priestor všetkých polynómov nad R najviac tretieho stupňa je podpriestor LP všetkých funkcií $R \to R$.
5. Priestor všetkých polynómov nad R tretieho stupňa nie je podpriestor LP všetkých funkcií $R \to R$.

Definícia. Nech $(L,+,\cdot)$ je LP nad poľom K.

a. Ak $x_1,x_2,\dots,x_n\in L$; $\alpha_1,\alpha_2,\dots,\alpha_n\in K$, tak sa
$x=\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n\in L$ nazýva *lineárna kombinácia* vektorov $x_1,x_2,\dots,x_n$ s koeficientami $\alpha_1,\alpha_2,\dots,\alpha_n$.

b. Ak $\emptyset\neq M\subset L$, tak sa množina všetkých lineárnych kombinácií prvkov z množiny M nazýva *lineárny obal množiny* M. Označujeme ho $\operatorname{span}M$.

c. Konečná podmnožina vektorov $\{x_1,x_2,\dots,x_n\}\subset L$ sa nazýva *lineárne nezávislá*, ak

$$\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n=0\implies\alpha_1=\alpha_2=\cdots=\alpha_n=0\,.$$

Množina $M\subset L$ sa nazýva lineárne nezávislá, ak je každá konečná podmnožina $M_1\subset M$ lineárne nezávislá. Množina $M\subset L$, ktorá nie je lineárne nezávislá sa nazýva lineárne závislá.

d. $B\subset L$ sa nazýva báza lineárneho priestoru L, ak
1) $\operatorname{span}B=L$, 2) B je lineárne nezávislá.

Ľahko sa dá ukázať, že platí:

Veta. *Podmnožina $M\subset L$ je podpriestor lineárneho priestoru $(L,+,\cdot)$ vtedy a len vtedy, ak $\exists A\subset L$ také, že $M=\operatorname{span}A$.*

Príklad. Ukážte, že
1. V R^3 je $\mathcal{E}=\{\mathbf{e}_1=(1,0,0),\mathbf{e}_2=(0,1,0),\mathbf{e}_3=(0,0,1)\}$ tzv. štandardná báza.
2. V LP funkcií $f\colon R\to R$ je množina $\{\sin t,\sin 2t,\sin 3t,\cos t\}$ lineárne nezávislá.
3. $\{x^0,x^1,x^2,\dots\}$ je lineárne nezávislá množina.
3. $\{\sin^2 t,\cos^2 t,\cos 2t\}$ je lineárne závislá množina.

Veta. *Ak v lineárnom priestore existuje n-prvková báza, tak každá $(n+1)$-prvková množina je lineárne závislá.*

Dôsledok.
Ak v lineárnom priestore existuje jedna n-prvková báza, tak každá jeho báza je n-prvková množina.

Definícia. Nech $(L,+,\cdot)$ je LP nad poľom K. Ak existuje konečná báza priestoru L, tak hovoríme, že L je konečnorozmerný priestor. Počet prvkov bázy sa nazýva dimenzia lineárneho priestoru L a označuje sa $\dim L$.

Príklad. Určte $\dim M$ pre podpriestor $M=\{(x_1,x_2,x_3,x_4)\in C^4\colon x_1-x_2=2_2+x_3-x_4=0\}$.

M je priestor riešení homogénnej sústavy lineárnych rovníc:

$$M=\{(b-a,b-a,a,b)\colon a,b\in C\}=\{a(-1,-1,1,0)+b(1,1,0,1)\colon a,b\in C\}=\operatorname{span}\{(-1,-1,1,0),(1,1,0,1)\}$$
$$a(-1,-1,1,0)+b(1,1,0,1)=(b-a,b-a,a,b)=(0,0,0,0)\implies a=b=0$$

Teda $B=\{(-1,-1,1,0),(1,1,0,1)\}$ je lineárne nezávislá množina a $\operatorname{span}B=M$, t.j. je to báza priestoru M. Počet prvkov množiny B je 2, t.j. $\underline{\dim M=2}$.

Veta. *Nech $\mathcal{B}=\{\mathbf{b}_1,\mathbf{b}_2,\dots,\mathbf{b}_n\}$ je usporiadaná báza lineárneho priestoru L nad poľom K. Potom sa každé $\mathbf{x}\in L$ dá jediným spôsobom vyjadriť ako lineárna kombinácia*

$$\mathbf{x}=x_1\mathbf{b}_1+x_2\mathbf{b}_2+\cdots+x_n\mathbf{b}_n\,,\quad x_1,x_2,\dots,x_n\in K$$

Dôkaz. Ak by sa dalo $\mathbf{x}$ dvoma spôsobmi:

$$\mathbf{x}=x_1\mathbf{b}_1+x_2\mathbf{b}_2+\cdots+x_n\mathbf{b}_n=\mathbf{x}=y_1\mathbf{b}_1+y_2\mathbf{b}_2+\cdots+y_n\mathbf{b}_n$$

tak by platilo

$$\mathbf{x}-\mathbf{x}=(x_1\mathbf{b}_1+x_2\mathbf{b}_2+\cdots+x_n\mathbf{b}_n)-(y_1\mathbf{b}_1+y_2\mathbf{b}_2+\cdots+y_n\mathbf{b}_n)=(x_1-y_1)\mathbf{b}_1+(x_2-y_2)\mathbf{b}_2+\cdots+(x_n-y_n)\mathbf{b}_n=\mathbf{0}$$

Z lineárnej nezávislosti $\mathcal{B}$ potom vyplýva:

$$(x_1-y_1)=(x_2-y_2)=\cdots=(x_n-y_n)=0\implies x_1=y_1\,,\ x_2=y_2\,,\ \dots\ x_n=y_n\,.$$

Definícia. Nech $\mathcal{B}=\{\mathbf{b}_1,\mathbf{b}_2,\dots,\mathbf{b}_n\}$ je usporiadaná báza lineárneho priestoru L nad poľom K a $\mathbf{x}\in L$. Potom sa usporiadaná n-tica $[\mathbf{x}]_{\mathcal{B}}=(x_1,x_2,\dots,x_n)^\top\in K^{n\times1}$, pre ktorú platí $\mathbf{x}=x_1\mathbf{b}_1+x_2\mathbf{b}_2+\cdots+x_n\mathbf{b}_n$, nazýva n-tica súradníc vektora $\mathbf{x}$ vyhľadom na bázu $\mathcal{B}$.

Príklad. V R^3 je daná báza $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$; $\mathbf{b}_1 = (1,1,0)$, $\mathbf{b}_2 = (1,-1,1)$, $\mathbf{b}_3 = (0,1,1)$ a $\mathbf{x} = (2,1,-1)$. Vypočítajte $[\mathbf{x}]_{\mathcal{B}}$.

Máme teda určiť čísla x_1, x_2, x_3 tak, aby $\mathbf{x} = x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + x_3\mathbf{b}_3$. Prepíšeme to na sústavu rovníc:

$$x_1 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} + x_3 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ x_1 - x_2 + x_3 \\ x_2 + x_3 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix}$$

Túto sústavu riešime úpravou jej rozšírenej matice na redukovanú stupňovitú maticu pomocou ERO.

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & 2 \\ 1 & -1 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{array}\right) \sim \cdots \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{array}\right) \implies [\mathbf{x}]_{\mathcal{B}} = \begin{pmatrix} 2 \\ 0 \\ -1 \end{pmatrix}.$$

Stĺpce matice sústavy tvoria prvky bázy $\mathcal{B}$, rošírená je o stĺpec vektora $\mathbf{x}$, ktorého súradnice počítame. Po úprave dostaneme jednotkovú maticu roz šírenú o stĺpec súradníc $[\mathbf{x}]_{\mathcal{B}}$.

Veta. *Nech $(L, +, \cdot)$ je lineárny priestor nad poľom K a $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ je jeho usporiadaná báza. Zobrazenie φ $L \to K^{n\times 1}$, $\varphi(\mathbf{x}) = [\mathbf{x}]_{\mathcal{B}}$ má vlastnosti.*

(1) $\mathbf{x}, \mathbf{y} \in L \implies [\mathbf{x}+\mathbf{y}]_{\mathcal{B}} = [\mathbf{x}]_{\mathcal{B}} + [\mathbf{y}]_{\mathcal{B}}$.
(2) $\mathbf{x} \in L, \alpha \in K \implies [\alpha\mathbf{x}]_{\mathcal{B}} = \alpha[\mathbf{x}]_{\mathcal{B}}$.
(3) $[\mathbf{x}]_{\mathcal{B}} = [\mathbf{y}]_{\mathcal{B}} \iff \mathbf{x} = \mathbf{y}$.

Prvé dve vlastnosti vyjadrujú, že φ je lineárne zobrazenie. Tretia hovorí, že je to bijektívne zobrazenie.