Vektorové prostory

Definice 1. *Těleso* $(T, +, .)$ splňuje:

S1: $(\exists 0)(\forall a), a + 0 = 0 + a = a$
S2: $(\forall a)(\exists(-a)), a + (-a) = 0$
S3: $(\forall a, b, c), (a + b) + c = a + (b + c)$
SK: $(\forall a, b), a + b = b + a$
N1: $(\exists 1)(\forall a), a.1 = 1.a = a$
N2: $(\forall a \neq 0)(\exists a^{-1}), a.a^{-1} = a^{-1}.a = 1$
N3: $(\forall a, b, c), (a.b).c = a.(b.c)$
NK: $(\forall a, b), a.b = b.a$
D1: $(\forall a, b, c), a.(b + c) = a.b + a.c$
D2: $(\forall a, b, c), (b + c).a = b.a + c.a$

Axiomy S1, S2 a S3 říkají, že jde o grupu vůči sčítání, axiom SK, že je to grupa komutativní. Totéž N1,N2,N3 a NK vůči násobení. D1 a D2 jsou distributivní zákony, které obě operace svazují. Charakteristika tělesa je počet jedniček v součtu $1 + 1 + \ldots + 1 = 0$. Pokud žádný součet jedniček v tělese nedá nulu, definuje se $\operatorname{char} T = 0$.

Příklad 1.

(1) $(\mathbb{Q}, +, .)$: racionální čísla s obvyklým sčítáním a násobením.
(2) $(\mathbb{R}, +, .)$: reálná čísla s obvyklými operacemi
(3) $(\mathbb{C}, +, .)$: komplexní čísla. Objevuje se unární operace $*$, komplexní sdružení
(4) $\mathbb{H}$: kvaterniony. Těleso se 3 imaginárními jednotkami $i^2 = j^2 = k^2 = -1$, které se násobí podle pravidla $ij = -ji = k$ (+ cyklická záměna). V $\mathbb{H}$ ale neplatí axiom NK, je to tedy nekomutativní těleso. Kvaterniony se hodí k popisu rotací ve 3-rozměrném prostoru.
(5) $\mathbb{O}$: oktoniony. Těleso se 7 imaginárními jednotkami. Narušena asociativita násobení. Lze pokračovat dál po mocninách dvojky, ale už sedeniony obsahují dělitele nuly, tedy nenulová a, b mohou dát $a.b = 0$. Seriózní role v matematice se zatím připisuje pouze prvním čtyřem $\mathbb{R}, \mathbb{C}, \mathbb{H}$ a $\mathbb{O}$.
(6) $\mathbb{N}$ není těleso. Např. neexistují inverzní prvky ke sčítání.
(7) $\mathbb{Z}$ není těleso. Neexistují inverzní prvky k násobení.
(8) $\mathbb{Z}_p$, množina zbytkových tříd po dělení p. Je tělesem, pouze když p je prvočíslo. Charakteristika je p.
(9) $GF(p^n)$, tzv. Galoisova tělesa, p prvočíslo. Pro $n = 1$ je to $\mathbb{Z}_p$, pro $n > 1$ je to množina polynomů stupně menšího než n s koeficienty v $\mathbb{Z}_p$, které se sčítají a násobí modulo nějaký polynom f stupně n, tedy je třeba $a + b$, resp ab vydělit f a součtem či součinem je zbytek po dělení. Polynom f musí být ireducibilní, tj. nesmí jít zapsat jako součin polynomů nižšího stupně. Jiná konečná tělesa neexistují. Vidíme, že charakteristika tělesa je buď 0, nebo prvočíslo.

Definice 2. *Vektorový prostor* $(V, +, .)$ nad tělesem T splňuje:

KG: $(V, +)$ je komutativní grupa.
NJ: $0_T.v = 0_V$, $(-1)_T.v = -v$
D1: $\lambda.(\mu.v) = (\lambda.\mu).v$
D2: $\lambda.(u + v) = \lambda.u + \lambda.v$
D3: $(\lambda + \mu).v = \lambda.v + \mu.v$

Zde vždy $\lambda, \mu \in T$, $u, v \in V$. Axiom NJ říká, že násobení nulou z tělesa je nulový vektor z vektorového prostoru a že násobení (-1) je totéž jako inverze ke sčítání. D1,D2 a D3 jsou distributivní zákony svazující sčítání a násobení v T se sčítáním ve V a s násobením prvků V prvky z T.

Příklad 2.

(1) $\mathbb{R}$ je VP sám nad sebou.
(2) $\mathbb{R}^n$ je prostor uspořádaných n-tic prvků z $\mathbb{R}$. Dimenze takového prostoru je n, zhruba je to počet nezávislých směrů uvnitř prostoru (výška, šířka, délka). Brzo upřesníme. Prostor uspořádaných n-tic můžeme sformovat nad libovolným tělesem, někdy se nazývá *aritmetický vektorový prostor*.
(3) $\mathbb{C}$ je vektorový prostor jak nad $\mathbb{C}$, tak nad $\mathbb{R}$. V prvním případě dimenze 1, v druhém dimenze 2.
(4) $\mathbb{C}^n, \mathbb{H}^n, \mathbb{O}^n, \ldots$ jsou všechno vektorové prostory nad $\mathbb{R}$ dimenze $2n, 4n, 8n, \ldots$.
(5) Prostor polynomů stupně n není VP, polynomy stupně nejvýše n už VP dimenze $n + 1$ tvoří.
(6) Množina všech funkcí na množině s hodnotami v $\mathbb{R}$ je vektorový prostor nekonečné dimenze. Podobně množina spojitých funkcí na uzavřeném intervalu.
(7) Množina všech nekonečných posloupností i množina všech konvergentních posloupností jsou VP nekonečné dimenze.
(8) Množina všech periodických funkcí není VP, všech periodických funkcí s racionální periodou ano.
(9) Množina všech funkcí na $\langle 0, 1\rangle$, $f(0) = f(1) = 0$.
(10) $\mathbb{R}$ je VP i nad $\mathbb{Q}$.
(11) $\mathbb{R}^+$ je vektorovým prostorem nad $\mathbb{R}$, zavedeme-li "sčítání" $u \oplus v = uv$ a "násobení reálným číslem" $r \odot u = u^r$.
(12) Množina řešení homogenní soustavy lineárních rovnic.
(13) Množina řešení homogenní soustavy lineárních diferenciálních rovnic.
(14) Množina všech magických čtverců.

Podmnožina $W \subset V$ uzavřená na sčítání mezi sebou a násobení prvkem z T se nazývá *podprostor*. Např. množina řešení homogenní soustavy je podprostorem aritmetického vektorového prostoru $\mathbb{R}^n$, kde n je počet neznámých.

Definice 3. *Lineární kombinace* vektorů $u_1, u_2, \ldots u_n \in V$ je konečný součet $u = r_1u_1 + r_2u_2 + \ldots + r_nu_n$, kde $r_i \in T$. Množina všech lineárních kombinací množiny M (i nekonečné) se nazývá *lineární obal* M a značí $\langle M\rangle$.

LK je *triviální*, právě když jsou všechna $r_i = 0$. Vektory jsou *lineárně závislé*, pokud existuje netriviální lineární kombinace, která dává nulový vektor.

PŘÍKLAD 3. Uvažujme vektory z T^n, zapišme si je do matice jako řádky a upravujme Gaussovou eliminací, např.

$$\left(\begin{array}{rrr} 1 & -2 & 0 \\ -3 & 6 & 2 \\ 1 & -2 & -1 \end{array}\right) \sim \left(\begin{array}{rrr} 1 & -2 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & -1 \end{array}\right) \sim \left(\begin{array}{rrr} 1 & -2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{array}\right). \tag{1}$$

Platí, že elementární transformace převádí LN množinu vektorů opět na LN množinu, a LZ na LZ. Poslední množina je evidentně lineárně závislá, protože lineární kombinace $0.(1,-2,0)+0.(0,0,1)+1.(0,0,0)=(0,0,0)$ je netriviální. Tedy i původní množina vektorů je LZ. Gaussova eliminace je tedy efektivní metodou detekce lineární závislosti množiny vektorů. Zpětným rozborem provedených úprav můžeme navíc najít netriviální lin. kombinaci, která nuluje původní množinu vektorů. Označíme-li vektory v průběhu výpočtu systémem (řádek)$_{krok}$, pak

$$0 = (3)_3 = 2.(3)_2 + (2)_2 = 2.((3)_1 - (1)_1) + ((2)_1 + 3.(1)_1) = (1)_1 + (2)_1 + 2.(3)_1$$

je hledaná lineární kombinace. Jinou metodou je vyjít přímo z původní množiny vektorů a pokládat r_i za neznámé homogenní soustavy rovnic

$$(0,0,0) = r_1.(1,-2,0) + r_2.(-3,6,2) + r_3.(1,-2,-1).$$

Ta má matici

$$\left(\begin{array}{rrr} 1 & -3 & 1 \\ -2 & 6 & -2 \\ 0 & 2 & -1 \end{array}\right)$$

Taková matice se označuje jako *transponovaná* matice k matici původní jež má vektory v řádcích.

DEFINICE 4. Podmnožina $M \subset V$ *generuje* V, pokud $\langle M\rangle = V$. Je-li M navíc LN, pak se nazývá *bází* V.

VĚTA 0.1. *Nechť $M = \{u_1, \dots, u_n\}$ je báze V. Pak každý vektor $u \in V$ lze jednoznačně zapsat jako LK $u = \sum_i^n r_i u_i$.*

VĚTA 0.2. *Pokud ve V existuje konečná množina generátorů, pak lze z každé množiny generátorů V vybrat konečnou bázi.*

VĚTA 0.3 (Steinitz). *Buď $\{u_1, \dots, u_n\}$ množina generátorů V a $\{v_1, \dots, v_k\}$ LN množina. Pak $k \le n$ a při vhodném očíslování je $\{v_1, \dots, v_k, u_{k+1}, \dots, u_n\}$ množinou generátorů V.*

Steinitzova věta říká, že každé dvě báze mají stejný počet prvků. "Dělá" to tak, že vkládá do množiny $\{u_i\}$ postupně vektory z $\{v_i\}$, aniž by se změnil lineární obal. Umožňuje definovat *dimenzi* VP jako počet prvků báze. Jejím důsledkem je duální tvrzení k větě 0.2:

VĚTA 0.4. *Je-li $\{v_1, \dots, v_i\}$ LN podmnožina prostoru V dimenze n. Pak lze doplnit tuto množinu $n-k$ vektory $\{v_{k+1}, \dots, v_n\}$ na bázi V.*

Nechť $W, W' \subset V$. Jejich *spojení* $W \vee W'$ je lineární obal sjednocení $\langle W \cup W'\rangle$. Vhodnou volbou bází zůčastněných prostorů lze dokázat vzoreček

$$\dim W \vee W' + \dim W \cap W' = \dim W + \dim W', \tag{2}$$

stačí začít s bází $W \cap W'$ a doplnit ji na bázi W a na bázi W'. Pokud $W \cap W' = 0$, píšeme $\oplus$ místo $\vee$ a mluvíme o *direktním součtu* . Platí, že prvky spojení jsou právě vektory, zapsatelné jako $u + v$, $u \in W$, $v \in W'$. Je-li spojení direktním součtem, jsou u a v určeny jednoznačně. Jsou-li M a M' báze W a W', $W \cap W' = 0$, pak $M \cup M'$ je báze $W \oplus W'$.

Dimenzi lineárního obalu množiny vektorů lze opět zjistit Gaussovou eliminací. Elementární transformace zachovávají lineární obal, takže výpočet 1 ukazuje, že množiny $\{(1,-2,0),(-3,6,2),(1,-2-1)\}$ a $\{(1,-2,0),(0,0,2),(0,0,0)\}$ mají stejný lineární obal. První dva vektory v druhé trojici jsou evidentně jeho bází, takže dimenze je 2.

Podobně vzoreček 2 má nejčastější užití v určení dimenze průniku, kdy Gaussovou eliminací určíme lineární obaly množin M a M', které máme zadány jako generující pro W a W', a množiny $M \cup M'$, která generuje $W \vee W'$.