# 1. Izometrie a ortogonální transformace

Veškeré úvahy týkající se abstraktních kořenových prostorů se budou odehrávat v reálných lineárních prostorech se skalárním součinem. Tyto prostory se mnohde nazývají eukleidovskými, takové označení ovšem spíše přísluší prostoru, který nemá žádný význačný bod. Toto ovšem v případě lineárních prostorů není splněno, a proto je zde nebudeme používat.

Jako první se tedy budeme zabývat reálnými lineárními prostory se skalárním součinem a, jak je v matematice zvykem, zobrazeními, které zachovávají linearitu a skalární součin. Těmto zobrazením se říká ortogonální zobrazení.

**1.1. Reálné lineární prostory se skalárním součinem.** Předpokládáme, že pojmy spojené s lineárními prostory se skalárním součinem jsou známy. Omezíme se zde pouze na poznámky rozšiřující platnost výsledků z této kapitoly. Nechť $V$ je reálný vektorový prostor. ***Bilineární formou*** nazveme zobrazení $\langle\cdot,\cdot\rangle : V \times V \to V$, které je lineární v každém svém argumentu, tj.

$$\langle \alpha u + v, w\rangle = \alpha\langle u, w\rangle + \langle v, w\rangle, \quad \langle u, \alpha v + w\rangle = \alpha\langle u, v\rangle + \langle u, w\rangle,$$

pro všechna $u, v, w \in V$ a $\alpha \in \mathbf{R}$. Bilineární formu nazveme ***symetrickou***, jestliže platí $\langle u, v\rangle = \langle v, u\rangle$ pro všechna $u, v \in V$. O symetrické bilineární formě řekneme, že je ***nedegenerovaná***, jestliže z $\langle u, v\rangle = 0$ pro všechna $v \in V$ plyne, že $u = 0$[1]. Pokud platí, že $\langle u, u\rangle \geq 0$ a $\langle u, u\rangle = 0$ právě, když $u = 0$, říkáme, že symetrická bilineární forma je ***pozitivně definitní*** a takovou formu nazýváme ***skalárním součinem***. Pozitivně definitní symetrická bilineární forma je nedegenerovaná. Skutečně, dosaďme v definici nedegenerovanosti $v = u$. Již z toho plyne, že $u = 0$. Výsledky v této kapitole jsou vesměs platné i pro nedegenerované symetrické bilineární formy. Na lineárním prostoru se skalárním součinem je definována ***norma*** vektoru $\|u\| = \sqrt{\langle u, u\rangle}$. Je nasnadě, že takto definované zobrazení splňuje axiomy normy.

**1.2. Komplexifikace a realifikace.** Jelikož těleso reálných čísel není uzavřené vzhledem k algebraickým operacím, vyvstává nutnost komplexifikace reálného lineárního prostoru. Základní věta algebry (důkaz se provádí v komplexní analýze) zaručuje, že těleso komplexních čísel algebraicky uzavřené je — tzn. každý nekonstantní polynom má v $\mathbf{C}$ kořen[2]. ***Komplexifikací*** reálného lineárního prostoru $V$ rozumíme komplexní lineární prostor $V^{\mathbf{C}}$, množinově tvořený uspořádanými dvojicemi $u + \mathrm{i}\, v$, kde $u, v \in V$,

[1] Nerozlišujeme zde nulu v $\mathbf{R}$ a nulový vektor z $V$. Doufejme, že rozdíl bude vždy jasný z kontextu.

[2] Slovo kořen se v matematice používá (nejméně) ve dvou smyslech. Kořenové systémy, kterými se zabývá tato práce, nemají nic společného s kořeny algebraických rovnic.

v němž základní operace definujeme pomocí operací ve $V$:[3]

$$(u + \mathrm{i}\, v) + (w + \mathrm{i}\, z) = (u + w) + \mathrm{i}(v + z)$$
$$(\alpha + \mathrm{i}\, \beta)(u + \mathrm{i}\, v) = (\alpha u - \beta v) + \mathrm{i}(\alpha v + \beta u)$$

Lineární transformace $T: V \to V$ nemusí nutně mít vlastní hodnotu a jí odpovídající vlastní vektor. Ovšem po komplexifikaci $T^{\mathbf{C}}: V^{\mathbf{C}} \to V^{\mathbf{C}}$, kde

$$T^{\mathbf{C}}(u + \mathrm{i}\, v) = T(u) + \mathrm{i}\, T(v),$$

dostáváme lineární transformaci $T^{\mathbf{C}}$, která již nutně má vlastní hodnotu a jí odpovídající vlastní vektor, což plyne právě ze základní věty algebry. Báze $[e_1, e_2, \ldots]$ ve $V$ určuje bázi $[e_1 + \mathrm{i}\, 0, e_2 + \mathrm{i}\, 0, \ldots]$ ve $V^{\mathbf{C}}$ a $T^{\mathbf{C}}$ má vzhledem k této bázi zřejmě stejnou matici jako $T$ vzhledem k $[e_1, e_2, \ldots]$.

Dále je v komplexifikovaném lineárním prostoru $V^{\mathbf{C}}$ definována transformace ***komplexního sdružení*** $\Sigma$ předpisem

$$\Sigma(u + \mathrm{i}\, v) = u - \mathrm{i}\, v.$$

Pozor, nejedná se o lineární transformaci, ale o ***antilineární*** transformaci, tj. $\Sigma(\gamma z) = \gamma^* \Sigma(z)$, pro $z \in V^{\mathbf{C}}$ a $\gamma \in \mathbf{C}$. Skutečně,

$$\Sigma((\alpha + \mathrm{i}\, \beta)(u + \mathrm{i}\, v)) = \Sigma((\alpha u - \beta v) + \mathrm{i}(\alpha v + \beta u)) =$$
$$= (\alpha u - \beta v) - \mathrm{i}(\alpha v + \beta u) = (\alpha - \mathrm{i}\, \beta)(u - \mathrm{i}\, v).$$

Transformace $\Sigma$ je ***involutivní***, tj. platí $\Sigma^2 = \mathrm{id}$.

Obecně řekneme, že ***reálnou strukturu*** na komplexním vektorovém prostoru $Z$ je antilineární involutivní zobrazení $\Sigma: Z \to Z$. $\Sigma$ určuje reálný vektorový prostor v $Z$ daný pomocí pevných bodů $\Sigma$: $\{v \in Z | \Sigma(v) = v\}$.

*Příklad* 1. Uvažme lineární transformaci $T: \mathbf{R}^2 \to \mathbf{R}^2$ danou ve standardní bázi maticí

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

Charakteristický polynom $T$ je $\lambda^2 + 1$, nemá tedy reálné kořeny. Nyní přejděme k transformaci $T^{\mathbf{C}}: \mathbf{C}^2 \to \mathbf{C}^2$, která je vzhledem k bázi

$$[(1, 0) + \mathrm{i}(0, 0), (0, 1) + \mathrm{i}(0, 0)]$$

rovněž dána maticí

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

jejíž prvky ovšem považujeme za komplexní čísla. Tato má vlastní hodnoty $\pm\,\mathrm{i}$ a jim příslušné vlastní vektory např. $(\pm\,\mathrm{i}, 1)$.

Reálná struktura je dána zobrazením $\Sigma: u + \mathrm{i}\, v \to u - \mathrm{i}\, v$, tj. $(\alpha, \beta) \to (\alpha^*, \beta^*)$.

[3]Všimněme si, že znaménko + se v definicích vyskytuje v několika významech — formálním: pro zápis uspořádané dvojice reálných vektorů, které tvoří komplexní vektor, a zápis uspořádané dvojice reálných čísel, které tvoří komplexní číslo, — faktickém v definovaném součtu dvou komplexních vektorů pomocí součtu reálných vektorů. Obdobně lze třídit i násobení skalárem, to ovšem neznačíme nijak.

Je-li $Z$ lineární prostor nad $\mathbf{C}$, definujeme jeho ***realifikaci*** $Z_{\mathbf{R}}$ tak, že povolíme násobení pouze reálnými skaláry a každý komplexní vektor $u = (\alpha^j + \mathrm{i}\,\beta^j)e_j$ v bázi $[e_1, e_2, \dots]$ v $Z$ zapíšeme jako $u = (\alpha^j e_j + \beta^j\,\mathrm{i}\,e_j)$, kde $[e_1, e_2, \dots\ \mathrm{i}\,e_1, \mathrm{i}\,e_2, \dots]$ je báze v $Z_{\mathbf{R}}$. Upozorňujeme, že komplexifikací reálného lineárního prostoru dimenze $n$ dostáváme komplexní lineární prostor dimenze $n$, zatímco realifikací komplexního lineárního prostoru dimenze $n$ dostáváme reálný lineární prostor dimenze $2n$.

***Komplexní strukturou*** na reálném lineárním prostoru rozumíme lineární transformaci $J$ takovou, že $J^2 = -\,\mathrm{id}$.

*Příklad* 2. Lineární transformace $U : \mathbf{C}^2 \to \mathbf{C}^2$ je v kanonické bázi $[(1,0),(0,1)]$ zadána maticí

$$\begin{pmatrix} 1 & \mathrm{i} \\ -\mathrm{i} & 0 \end{pmatrix}.$$

Její realifikace je v bázi $[(1,0),(0,1),\mathrm{i}(1,0),\mathrm{i}(0,1)]$ zadána maticí

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

Komplexní struktura je ve stejné bázi dána maticí

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

*Poznámka* 1. Zřejmě jak při komplexifikaci reálného lineárního prostoru, tak při realifikaci komplexního lineárního prostoru, dochází ke ztrátě informace. V prvním případě je úplná informace dána reálnou strukturou, v druhém pak komplexní strukturou.

**1.3. Izometrie a jejich vlastnosti.** ***Izometrií*** nazýváme takové zobrazení $f : V \to V$, které zachovává metrické vzdálenosti, tj. $d(f(u), f(v)) = d(u, v)$, pro všechna $u, v \in V$, kde $d(u, v) = \|u - v\|$ je metrika definovaná normou, a navíc je surjektivní. Lineární transformaci $T : V \to V$ nazýváme ***ortogonální***, platí-li $\langle Tu, Tv\rangle = \langle u, v\rangle$.

**Věta 1.** *Buď $f : V \to V$ izometrie. Potom $f(u) = Tu + v$, kde $v \in V$ a $T$ je ortogonální transformace.*

*Důkaz.* Je-li $f(u) = Tu + v$, potom $f(0) = v$ a $Tu = f(u) - f(0)$. Musíme tedy dokázat, že $Tu := f(u) - f(0)$ je ortogonální transformace. Z definice izometrie platí, že $\|Tu - Tv\| = \|u - v\|$ pro všechna $u, v \in V$, tedy zejména pro $v = 0$ $\|Tu\| = \|u\|$. S kvadratickou formou $\|u\|^2$ můžeme vždy asociovat skalární součin pomocí tzv. ***polarizace*** $2\langle u, v\rangle = \|u - v\|^2 - \|u\|^2 - \|v\|^2$. Musí tedy platit $\langle Tu, Tv\rangle = \langle u, v\rangle$.

Zbývá dokázat linearitu $T$. Každá izometrie je nutně injektivní, protože pokud $u \neq v$, je $\|u - v\| > 0$ a tedy i $\|f(u) - f(v)\| > 0$ a tedy $f(u) \neq f(v)$. Je tedy i $T :=$

$f(u) - f(0)$ injektivní a z definice surjektivní, tedy celkem bijektivní. Obrazem libovolné ortonormální báze $[e_1, \dots, e_n]$ ve $V$ je tedy rovněž $[Te_1, \dots, Te_n]$ ortonormální systém a tedy báze. Rozvojem $u$ a $Tu$ do těchto bází dostáváme

$$u = \sum_{i=1}^{n} \langle u, e_i \rangle e_i$$
$$Tu = \sum_{i=1}^{n} \langle Tu, Te_i \rangle Te_i = \sum_{i=1}^{n} \langle u, e_i \rangle Te_i,$$

což ukazuje linearitu. ■

Zde leží zdroj důležitosti ortogonálních transformací v geometrii a fyzice. Abychom ukázali některé důležité charakteristiky ortogonálních transformací, musíme napřed ukázat, jak se lineární zobrazení chovají vzhledem ke komplexifikaci.

**Lemma 2.** *Každá reálná lineární transformace $T : V \to V$ má jedno- nebo dvourozměrný invariantní podprostor $W$, tj. $T(W) \subset W$.*

*Důkaz.* Uvažujme komplexifikaci $V^{\mathbf{C}}$, komplexifikaci $T^{\mathbf{C}}$, to vše společně s reálnou strukturou $\Sigma$. Ze základní věty algebry vyplývá, že $T^{\mathbf{C}}$ má alespoň jednu (obecně komplexní) vlastní hodnotu $\lambda = \alpha + \mathrm{i}\,\beta$ příslušnou vlastnímu vektoru $z = u + \mathrm{i}\,v$ ($\Sigma u = u$, $\Sigma v = v$). Platí tedy

$$Tu + \mathrm{i}\,Tv = T^{\mathbf{C}}(u + \mathrm{i}\,v) = \lambda(u + \mathrm{i}\,v) = (\alpha + \mathrm{i}\,\beta)(u + \mathrm{i}\,v) = \alpha u - \beta v + \mathrm{i}(\alpha v + \beta u),$$

z čehož porovnáním reálné a imaginární části dostáváme

$$Tu = \alpha u - \beta v$$
$$Tv = \alpha v + \beta u.$$

Je tedy $W = \mathrm{span}\{u, v\}$ invariantní podprostor, jeho dimenze je dva, pokud $u$ a $v$ jsou lineárně nezávislé, v případě jejich lineární závislosti je $\dim W = 1$. Situace $u = v = 0$ nemůže nastat, jelikož nulový vektor $0 + \mathrm{i}\,0$ nemůže být vektorem vlastním. ■

**Lemma 3.** *Ortogonální transformace $T$ v dvojrozměrném lineárním prostoru $V$ je buď otočení, nebo zrcadlení.*

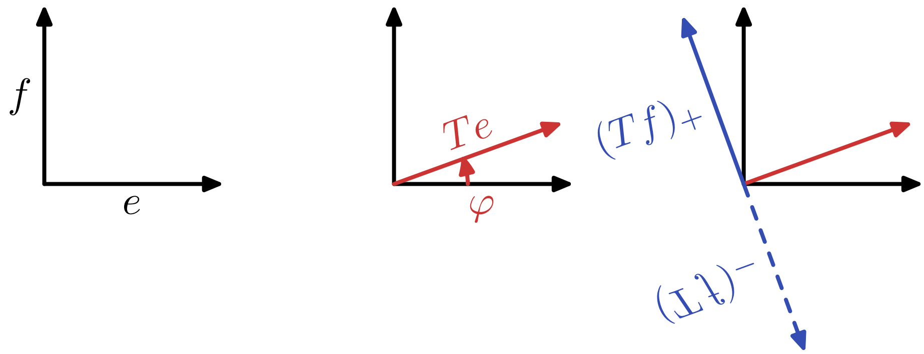
*Důkaz.* Nechť $[e, f]$ je libovolná ortonormální báze ve $V$ a pišme $Te = \alpha e + \beta f$ a $Tf = \gamma e + \delta f$. Pak i $[Te, Tf]$ je ortonormální báze, tj. platí

$$\|Te\| = \alpha^2 + \beta^2 = \|e\| = 1$$
$$\|Tf\| = \gamma^2 + \delta^2 = \|f\| = 1$$
$$\langle Te, Tf \rangle = \alpha\gamma + \beta\delta = \langle e, f \rangle = 0.$$

V bázi $[e, f]$ dostávám pro matici $T$

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = \begin{pmatrix} \cos\varphi & \mp\sin\varphi \\ \sin\varphi & \pm\cos\varphi \end{pmatrix},$$

kde horní znaménka přísluší otočení o $\varphi$ a dolní totéž otočení následované zrcadlením vzhledem k otočenému vektoru $Tf$. Geometricky je situace zjevná z obrázku 1 Na




Obrázek 1: Otočení a zrcadlení ve dvourozměrném prostoru

prvním obrázku vidíme ortonormální bázi $[e, f]$, na druhém obraz $Te$ bázového vektoru $e$. Tento obraz je omezen podmínkou $\|Te\| = 1$. Označme úhel $\angle(e, Te) = \varphi$, $\varphi \in [0, 2\pi)$. Obraz druhého bázového vektoru $f$ musí rovněž splňovat $\|Tf\| = 1$ a navíc musí platit, že $Te$ a $Tf$ svírají pravý úhel. Jsou tedy možná dvě řešení $(Tf)_+$ a $(Tf)_-$. ■

**Věta 4.** *Nechť $V$ je reálný lineární prostor se skalárním součinem $\langle \cdot, \cdot \rangle$. Potom každou ortogonální transformaci $T$ na $V$ lze rozložit na součin dvourozměrných rotací a jednorozměrných zrcadlení na vzájemně ortogonálních podprostorech prostoru $V$.*

*Důkaz.* Podle předchozího lemmatu 2 existuje ve $V$ invariantní podprostor $TW = W$ (rovnost píšeme vzhledem k tomu, že $T$ je bijekce) dimenze jedna nebo dvě.

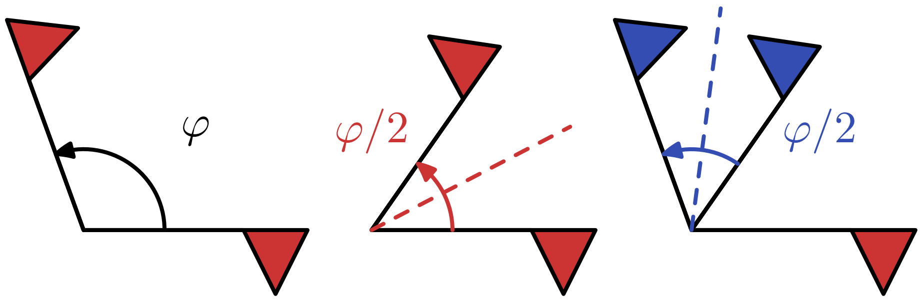
Dokážeme nyní, že jeho ortogonální doplněk $W^\perp := \{v \in V | \langle v, w \rangle = 0$, pro všechna $w \in W\}$ je rovněž invariantním podprostorem. Je $\langle w, v \rangle = 0$ pro všechna $w \in W$ a $v \in W^\perp$ z definice ortogonálního doplňku a rovněž $\langle Tw, v \rangle = 0$ z invariance podprostoru $W$ vůči $T$. Ale $\langle Tw, v \rangle = \langle w, T^{-1}v \rangle = 0$ a platí tedy, že $T^{-1}v \in W^\perp$ pro všechna $v \in W^\perp$, tj. $TW^\perp = W^\perp$.

Dále můžeme postupovat indukcí vzhledem k dimenzi $V$. Definujme transformaci $T_W$ jako $T$ na $W$ a jako identitu na $W^\perp$ a transformaci $T_{W^\perp}$ jako $T$ na $W^\perp$ a identitu na $W$. Evidentně platí, že $T = T_W T_{W^\perp} = T_{W^\perp} T_W$ a celý postup opakujeme pro $V = W^\perp$, přičemž je zaručeno $\dim V > \dim W^\perp$. Pokud je podprostor $W$ jednorozměrný, je na $W$ zúžená ortogonální transformace $T_W = \pm\,\mathrm{id}$, tedy identita nebo zrcadlení. Pokud je $W$ dvourozměrný, řeší situaci lemma 3. ■

Každé otočení v konečněrozměrném prostoru dimenze $n$ je tedy součinem nejvýše $\lfloor n/2 \rfloor$ rovinných otočení. Zbývá už jen poslední krok.

**Lemma 5.** *Každé otočení v rovině lze realizovat jako dvě po sobě následující zrcadlení.*

*Důkaz.* Důkaz pro názornost provedeme konstrukčně pomocí obrázku 2. ∎




Obrázek 2: Konstrukce otočení v rovině pomocí dvou zrcadlení

Shrneme-li získané výsledky, zjistíme, že každou ortogonální transformaci lze vyjádřit jako složení konečného počtu zrcadlení. Proto následující oddíl věnujeme jejich vlastnostem.

**1.4. Zrcadlení a jejich vlastnosti.** Zrcadlení $s_v : V \to V$ vzhledem k vektoru $v \in V$ je určeno v souladu s předchozím oddílem následovně: zrcadlení zobrazí zvolený vektor $v \in V$ na vektor opačný, tedy $-v$, přičemž libovolný vektor $w \in v^{\perp}$ z ortogonálního doplňku $v$ ve $V$ zůstává nezměněn. Definujme ***zrcadlení*** vzhledem k vektoru $v$ jako zobrazení

$$
\begin{aligned}
s_v : V &\to V \\
u &\mapsto s_v(u) = u - 2\frac{\langle u, v\rangle}{\langle v, v\rangle} v
\end{aligned}
$$

Následující lemma ukazuje, že výše definovaná transformace má všechny požadované i další intuitivně zřejmé vlastnosti.

**Lemma 6.** *Platí:*

*(1)* $s_v(v) = -v$ *a* $s_v(w) = w$ *pro* $w \in v^{\perp}$.

*(2)* $s_v$ *je ortogonální transformace.*

*(3)* $s_v^2 = \mathrm{id}$, *tj.* $s_v$ *je involuce.*

*Důkaz.* Vše získáme přímým výpočtem z definičních vztahů.

(1)

$$s_v(v) = v - 2\frac{\langle v, v\rangle}{\langle v, v\rangle} v = -v,$$

a pro $\langle w, v\rangle = 0$ dostáváme

$$s_v(w) = w - \frac{\langle w, v\rangle}{\langle v, v\rangle} v = w.$$

(2)

$$\langle s_v(u), s_v(w)\rangle = \langle u - 2\frac{\langle u, v\rangle}{\langle v, v\rangle} v, w - 2\frac{\langle w, v\rangle}{\langle v, v\rangle} v\rangle =$$
$$= \langle u, w\rangle - 2\frac{\langle u, v\rangle}{\langle v, v\rangle}\langle v, w\rangle - 2\frac{\langle w, v\rangle}{\langle v, v\rangle}\langle u, v\rangle + 4\frac{\langle u, v\rangle}{\langle v, v\rangle}\frac{\langle w, v\rangle}{\langle v, v\rangle}\langle v, v\rangle = \langle u, w\rangle.$$

(3)

$$s_v^2(u) = u - 2\frac{\langle u, v\rangle}{\langle v, v\rangle} v - 2\frac{\langle u - 2\frac{\langle u,v\rangle}{\langle v,v\rangle} v, v\rangle}{\langle v, v\rangle} v = u - 2\frac{\langle u, v\rangle}{\langle v, v\rangle} v + 2\frac{\langle u, v\rangle}{\langle v, v\rangle} v = u.$$

■

Zvolme nyní libovolnou ortonormální bázi $[e_1, \dots, e_n]$ ve $V$ a definujme její permutaci $\sigma \in S_n$ jako $[e_{\sigma(1)}, \dots, e_{\sigma(n)}]$. Zřejmě se jedná o ortogonální transformaci, kterou budeme značit rovněž symbolem $\sigma$. Každou permutaci $\sigma$ lze zapsat jako složení nesouvislých cyklů, každý cyklus jako složení transpozic.

*Příklad* 3. Vezměme například permutaci $\binom{12345}{21534}$, která je složena ze dvou nesouvislých cyklů (12)(354) a je tedy generována třemi transpozicemi např. $t_{34}t_{45}t_{12}$. Tato permutace určuje lineární transformaci s maticí

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Tato matice je zřejmě součinem matic příslušných nesouvislým cyklům, tedy

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

matice příslušné cyklům získáme jako součiny matic příslušných transpozicím

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

**Lemma 7.** *Platí:*

(1) *Transpozice $t_{ij}$ je zrcadlením vzhledem k vektoru $e_i - e_j$.*

(2) *Pro všechna $i, j$ mají transpozice $t_{ij}$ (a tedy i každá permutace $\sigma$) invariantní podprostor generovaný vektorem $e_1 + \cdots + e_n$.*

*Důkaz.* (1) Nechť $v = \sum_{k=1}^{n} \langle v, e_k \rangle e_k$ je libovolný vektor, potom

$$
\begin{aligned}
s_{e_i - e_j}(v) &= v - 2\frac{\langle v, e_i - e_j \rangle}{\langle e_i - e_j, e_i - e_j \rangle}(e_i - e_j) = \\
&= v - \langle v, e_i - e_j \rangle (e_i - e_j) = v - \langle v, e_i \rangle e_i - \langle v, e_j \rangle e_j + \langle v, e_j \rangle e_i + \langle v, e_i \rangle e_j
\end{aligned}
$$

(2)

$$s_{e_i - e_j}(e_1 + \cdots + e_n) = e_1 + \cdots + e_n - \langle e_1 + \cdots + e_n, e_i - e_j \rangle (e_i - e_j) = e_1 + \cdots + e_n$$

■

## 2. Abstraktní kořenové systémy

Abstraktní kořenové systémy jsou na první pohled poměrně uměle vytvořenou matematickou konstrukcí. Mají ovšem jednu důležitou vlastnost — dají se klasifikovat. Na rozdíl od mnoha dalších klasifikovatelných objektů v matematice není tato klasifikace nasnadě. Na druhou stranu je ale tato klasifikace proveditelná a pochopitelná pomocí prostředků, které má k dispozici úspěšný absolvent kurzu lineární algebry, tedy většinou student po ukončení prvního ročníku studia. Dobré pochopení klasifikace abstraktních kořenových systémů je základem pro pochopení teorie polojednoduchých Lieových algeber a jejich reprezentací.

**2.1. Definice a příklady.** Nechť $V$ je reálný lineární prostor se skalárním součinem $\langle \cdot, \cdot \rangle$. Zrcadlení vzhledem k danému vektoru $v \in V$ značíme v souladu s předchozí kapitolou $s_v : V \to V$. ***Abstraktním kořenovým systémem*** rozumíme konečnou množinu $\Delta$ prvků lineárního prostoru $V$ takovou, že

(1) množina $\Delta$ generuje celý lineární prostor $V$, tj. $V = \operatorname{span} \Delta$,

(2) zrcadlením vektoru z $\Delta$ vzhledem k vektoru z $\Delta$ získáme opět vektor z $\Delta$, tj. pro všechna $u, v \in \Delta$ platí $s_v(u) = u - 2\dfrac{\langle u, v \rangle}{\langle v, v \rangle} v \in \Delta$,

(3) pro všechna $u, v \in \Delta$ je číslo $2\dfrac{\langle u, v \rangle}{\langle v, v \rangle}$ celé.

***Kořenem*** nazýváme prvek abstraktního kořenového systému $\Delta$. Poslední bod v definici abstraktního kořenového systému se někdy vynechává, pokud se připustí nazývá se takový abstraktní kořenový systém krystalografickým.

**Tvrzení 8.** *Množina* $\Delta = \{e_i - e_j | i \neq j\}$ *je abstraktním kořenovým systémem na nadrovině* $V = (e_1 + \dots + e_{n+1})^\perp$ *v* $(n+1)$*-rozměrném lineárním prostoru* $W$ *se skalárním součinem* $\langle \cdot, \cdot \rangle$ *a libovolně zvolenou ortonormální bází* $[e_1, \dots, e_{n+1}]$.

*Důkaz.* Ověříme napřed vlastnost (1), tedy že $\Delta$ generuje $W$. Vezměme např. podmnožinu $\Delta \supset \Delta_0 = \{e_1 - e_{n+1}, e_2 - e_{n+1}, \dots, e_n - e_{n+1}\}$. Ukážeme, že $\Delta_0$ generuje $V = \{v \in W | \langle v, e_1 + \dots + e_{n+1} \rangle = 0\}$.

$$\begin{aligned}
0 &= \langle v, e_1 + \dots + e_n + e_{n+1} \rangle \\
\langle v, e_n + 1 \rangle &= -(\langle v, e_1 \rangle + \dots + \langle v, e_n \rangle) \\
v &= \langle v, e_1 \rangle e_1 + \dots + \langle v, e_n \rangle e_n + \langle v, e_{n+1} \rangle e_{n+1} \\
v &= \langle v, e_1 \rangle e_1 + \dots + \langle v, e_n \rangle e_n - (\langle v, e_1 \rangle + \dots + \langle v, e_n \rangle) e_{n+1} \\
v &= \langle v, e_1 \rangle (e_1 - e_{n+1}) + \dots + \langle v, e_n \rangle (e_n - e_{n+1})
\end{aligned}$$

Každý prvek $V$ lze tedy zapsat jako lineární kombinaci prvků z $\Delta_0$. Platí zřejmě rovněž, že $\Delta_0$ je maximální lineárně nezávislý systém ve $V$, tj. $\Delta_0$ je báze $V$.

Dále spočtěme výrazy ($i \neq j$ a $k \neq \ell$)

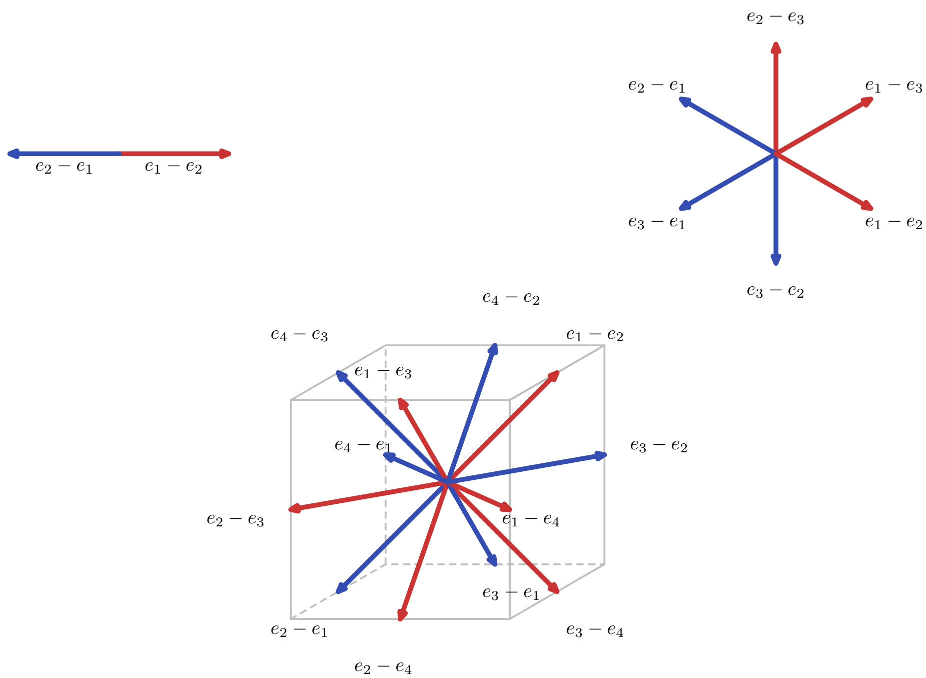
$$\begin{aligned}
s_{e_i - e_j}(e_k - e_\ell) &= e_k - e_\ell - 2\frac{\langle e_k - e_\ell, e_i - e_j \rangle}{\langle e_i - e_j, e_i - e_j \rangle}(e_i - e_j) = \\
&= e_k - e_\ell - \langle e_k - e_\ell, e_i - e_j \rangle (e_i - e_j) = \begin{cases}
e_k - e_\ell & i \neq k \;\; i \neq \ell \;\; j \neq k \;\; j \neq \ell \\
e_k - e_i & i \neq k \;\; i \neq \ell \;\; j \neq k \;\; j = \ell \\
e_i - e_\ell & i \neq k \;\; i \neq \ell \;\; j = k \;\; j \neq \ell \\
e_k - e_j & i \neq k \;\; i = \ell \;\; j \neq k \;\; j \neq \ell \\
e_j - e_\ell & i = k \;\; i \neq \ell \;\; j \neq k \;\; j \neq \ell \\
e_j - e_i & i = k \;\; i \neq \ell \;\; j \neq k \;\; j = \ell \\
e_i - e_j & i \neq k \;\; i = \ell \;\; j = k \;\; j \neq \ell
\end{cases}
\end{aligned}$$

a nakonec si všimneme v předchozím výpočtu výrazu

$$2\frac{\langle e_k - e_\ell, e_i - e_j \rangle}{\langle e_i - e_j, e_i - e_j \rangle} = \langle e_k - e_\ell, e_i - e_j \rangle = \begin{cases}
0 & i \neq k \; i \neq \ell \;\; j \neq k \; j \neq \ell \\
-1 & i \neq k \; i \neq \ell \;\; j \neq k \; j = \ell \\
1 & i \neq k \; i \neq \ell \;\; j = k \; j \neq \ell \\
1 & i \neq k \; i = \ell \;\; j \neq k \; j \neq \ell \\
-1 & i = k \; i \neq \ell \;\; j \neq k \; j \neq \ell \\
2 & i = k \; i \neq \ell \;\; j \neq k \; j = \ell \\
-2 & i \neq k \; i = \ell \;\; j = k \; j \neq \ell,
\end{cases}$$

což jsou skutečně celá čísla. ∎

Kořenové systémy výše uvedeného typu se označují jako $A_n$. Graficky lze znázornit systémy $A_1$, $A_2$ a $A_3$.




Obrázek 3: Kořenové systémy $A_1$, $A_2$ a $A_3$

**Tvrzení 9.** *Množina $\Delta = \{\pm e_i \pm e_j | i \neq j\} \cup \{\pm e_i\}$ v lineárním prostoru $V$ se skalárním součinem $\langle \cdot, \cdot \rangle$, kde $[e_1, \dots, e_n]$ je libovolná ortonormální báze.*

*Důkaz.* Opět přímo ověříme požadované vlastnosti. $\Delta$ zřejmě generuje $V$, jak lze vidět z druhé části sjednocení v definičním vztahu. Ověříme definiční vlastnost (2) a (3).

$$s_{\pm e_i \pm e_j}(\pm e_k \pm e_\ell) = \pm e_k \pm e_\ell - 2\frac{\langle \pm e_k \pm e_\ell, \pm e_i \pm e_j \rangle}{\langle \pm e_i \pm e_j, \pm e_i \pm e_j \rangle}(\pm e_i \pm e_j) =$$

$$= \pm e_k \pm e_\ell - \langle \pm e_k \pm e_\ell, \pm e_i \pm e_j \rangle (\pm e_i \pm e_j) = \begin{cases} \pm e_k \pm e_\ell & i \neq k \;\; i \neq \ell \;\; j \neq k \;\; j \neq \ell \\ \pm e_k \mp e_i & i \neq k \;\; i \neq \ell \;\; j \neq k \;\; j = \ell \\ \mp e_i \pm e_\ell & i \neq k \;\; i \neq \ell \;\; j = k \;\; j \neq \ell \\ \pm e_k \mp e_j & i \neq k \;\; i = \ell \;\; j \neq k \;\; j \neq \ell \\ \mp e_j \pm e_\ell & i = k \;\; i \neq \ell \;\; j \neq k \;\; j \neq \ell \\ \mp e_i \mp e_j & i = k \;\; i \neq \ell \;\; j \neq k \;\; j = \ell \\ \mp e_i \mp e_j & i \neq k \;\; i = \ell \;\; j = k \;\; j \neq \ell, \end{cases}$$

přičemž výrazy z vlastnosti (3) mají opět hodnoty $0, \pm 1, \pm 2$.

$$s_{\pm e_i}(\pm e_k \pm e_\ell) = \pm e_k \pm e_\ell - 2\frac{\langle \pm e_k \pm e_\ell, \pm e_i \rangle}{\langle \pm e_i, \pm e_i \rangle}(\pm e_i) =$$

$$= \pm e_k \pm e_\ell - 2\langle \pm e_k \pm e_\ell, \pm e_i \rangle(\pm e_i) = \begin{cases} \pm e_k \pm e_\ell & i \neq k \;\; i \neq \ell \\ \pm e_k \mp e_i & i \neq k \;\; i = \ell \\ \mp e_i \pm e_\ell & i = k \;\; i \neq \ell, \end{cases}$$

přičemž výrazy z vlastnosti (3) mají hodnoty $0, \pm 2$.

$$s_{\pm e_i \pm e_j}(\pm e_k) = \pm e_k - 2\frac{\langle \pm e_k, \pm e_i \pm e_j \rangle}{\langle \pm e_i \pm e_j, \pm e_i \pm e_j \rangle}(\pm e_i \pm e_j) =$$

$$= \pm e_k - \langle \pm e_k, \pm e_i \pm e_j \rangle(\pm e_i \pm e_j) = \begin{cases} \pm e_k & i \neq k \;\; j \neq k \\ \mp e_i & i \neq k \;\; j = k \\ \mp e_j & i = k \;\; j \neq k, \end{cases}$$

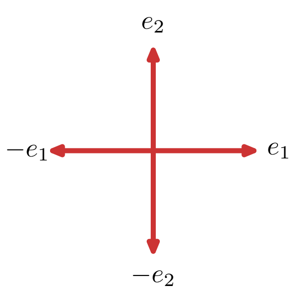
přičemž výrazy z vlastnosti (3) mají hodnoty $0, \pm 1$.

$$s_{\pm e_i}(\pm e_k) = \pm e_k - 2\frac{\langle \pm e_k, \pm e_i \rangle}{\langle \pm e_i, \pm e_i \rangle}(\pm e_i) =$$

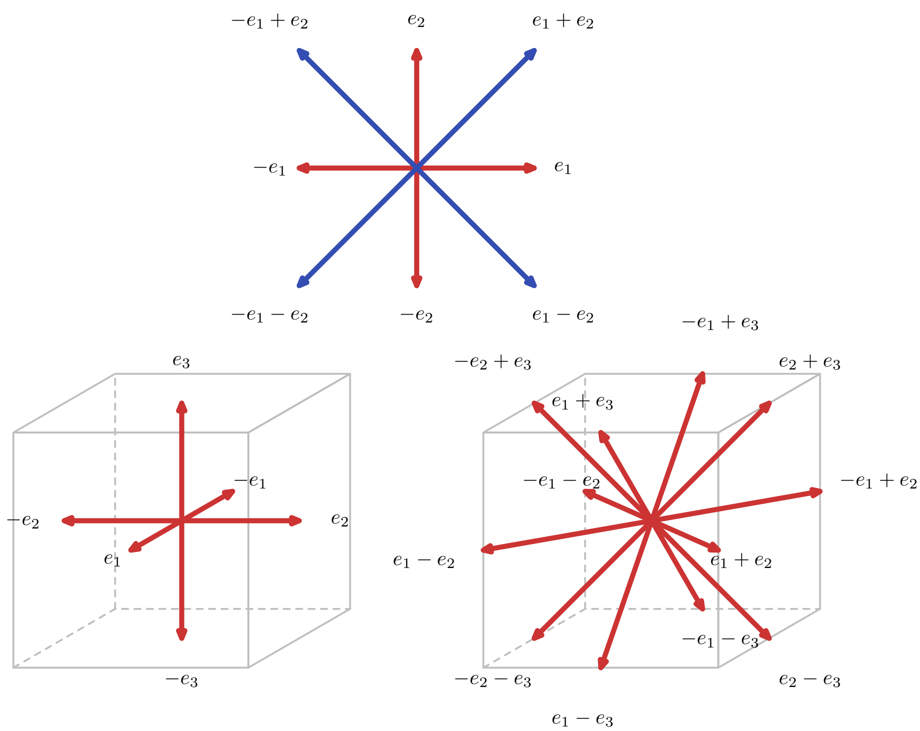
$$= \pm e_k - 2\langle \pm e_k, \pm e_i \rangle(\pm e_i) = \begin{cases} \pm e_k & i \neq k \\ \mp e_k & i = k, \end{cases}$$

přičemž výrazy z vlastnosti (3) mají hodnoty $0, \pm 2$. ■

Kořenové systémy tohoto typu nazýváme $B_n$, $n \geq 2$ (vzhledem k tomu, že $B_1 = A_1$). Graficky lze znázornit systémy $B_2$ a $B_3$.




Abstraktní kořenový systém $\Delta$ nazýváme ***reducibilním***, platí-li $\Delta = \Delta' \cup \Delta''$ a pro všechna $u' \in \Delta'$ a $u'' \in \Delta''$ platí $\langle u', u'' \rangle = 0$, tj. $u' \perp u''$. Zkráceně takovou situaci zapíšeme $\Delta = \Delta' \oplus \Delta''$. V případě, že žádný takový rozklad $\Delta = \Delta' \oplus \Delta''$ neexistuje, nazýváme abstraktní kořenový systém $\Delta$ ***ireducibilním***. Zatím uvedené systémy typu $A_n$ a $B_n$ jsou zřejmě ireducibilní, jelikož vždy obsahují vektory, jež nejsou kolmé. Nejjednodušším příkladem reducibilního kořenového systému je $\bigoplus^n A_1 = \{\pm e_i\}$, kde $[e_1, \dots, e_n]$ je báze ve $V$. Kořenové systémy $A_1 \oplus A_1$ je možno vidět na obrázku na boku a $A_1 \oplus A_1 \oplus A_1$ je (shodou okolností) zobrazen v levé dolní části obrázku 4. K dalšímu popisu je ukázat některé obecné vlastnosti abstraktních kořenových systémů. Budeme používat označení




Obrázek 4: Kořenové systémy $B_2$ a $B_3$ (pro $B_3$ jsou kořeny pro přehlednost ve dvou obrázcích)

$$\Delta_0 = \Delta \cup \{0\}, \qquad n(u,v) = 2\frac{\langle v,u\rangle}{\langle u,u\rangle}.$$

**Lemma 10.** *Nechť $\Delta$ je abstraktní kořenový systém ve $V$ s $\langle\cdot,\cdot\rangle$.*

*(1)* $u \in \Delta \Longrightarrow -u \in \Delta$

*(2)* $u \in \Delta, u/2 \notin \Delta, v = \alpha u, v \in \Delta_0, \alpha \in \mathbf{R} \Longrightarrow \alpha \in \{0, \pm 1, \pm 2\}$

*(3)* $u \in \Delta, v \in \Delta_0 \Longrightarrow n(u,v) \in \{0, \pm 1, \pm 2, \pm 3, \pm 4\}$

*(4)* $n(u,v) = \pm 4 \Longrightarrow v = \pm 2u$

*Důkaz.* (1) Zrcadlení $s_u(u) = -u$ musí být v $\Delta$.

(2) Případ $\alpha = 0$ je zřejmý. Budiž tedy $\alpha \neq 0$; potom

$$2\frac{\langle \alpha u,u\rangle}{\langle u,u\rangle} \in \mathbf{Z}, \qquad 2\frac{\langle u,\alpha u\rangle}{\langle \alpha u,\alpha u\rangle} \in \mathbf{Z}$$

a tedy jak $2\alpha \in \mathbf{Z}$, tak i $2/\alpha \in \mathbf{Z}$. Z druhého plyne zejména $0 < |\alpha| \leq 2$, z prvního potom $\alpha \in \{\pm\frac{1}{2}, \pm 1, \pm 2\}$, $\pm\frac{1}{2}$ ovšem bylo vyloučeno v předpokladech.

(3) Pro $v = 0$ dostaneme $n(u, v) = 0$. Jinak použijeme Cauchy-Buňakovského nerovnost

$$\begin{aligned} |\langle v, u\rangle| &\leq \|u\|\|v\| \\ 4\langle v, u\rangle^2 &\leq 4\langle u, u\rangle\langle v, v\rangle \\ n(u, v)n(v, u) &\leq 4, \end{aligned}$$

ale $n(u, v)$ i $n(v, u)$ jsou celá čísla, takže celkem

$$n(u, v) \in \{0, \pm 1, \pm 2, \pm 3, \pm 4\}.$$

(4) Předpokládejme, že $n(u, v) = \pm 4$ a tedy máme $n(u, v)n(v, u) = 4$. V Cauchy-Buňakovského nerovnosti nastává rovnost a musí platit $v = \alpha u$. Navíc $n(v, u) = \pm 1$.

$$\begin{aligned} n(u, v) &= \pm 4 & n(v, u) &= \pm 1 \\ 2\langle v, u\rangle &= \pm 4\|u\|^2 & 2\langle u, v\rangle &= \pm\|v\|^2 \\ \|v\| &= 2\|u\| \end{aligned}$$

■

**Věta 11.** *Nechť $\Delta$ je abstraktní kořenový systém ve $V$, $\langle\cdot,\cdot\rangle$.*

*(1) Jestliže $u, v \in \Delta$ a $\langle u, v\rangle > 0$, potom $u - v \in \Delta_0$. Jestliže naopak $\langle u, v\rangle < 0$, potom $u + v \in \Delta_0$.*

*(2) Nechť $u \in \Delta$, $v \in \Delta_0$. Jestliže $v + ku \in \Delta_0$, $v + (k+2)u \in \Delta_0$, pak i $v + (k+1)u \in \Delta_0$ pro $k \in \mathbf{Z}$.*

*Důkaz.* (1) Uvažujme zrcadlení

$$\begin{aligned} s_u(v) &= v - n(u, v)u \\ s_v(u) &= u - n(v, u)v \end{aligned}$$

Aby $u - v \in \Delta$, postačuje, aby $n(u, v) = 1$ nebo $n(v, u) = 1$ a aby $u + v \in \Delta$, postačuje $n(u, v) = -1$ nebo $n(v, u) = -1$. Z předchozího lemmatu známe možné hodnoty $n(u, v)$ a $n(v, u)$, které jsou pro přehlednost shrnuty v tabulce 1.

Z tabulky je vidět, že jediný případ, kdy buď $n(u, v)$ nebo $n(v, u)$ není 1 je $n(u, v) = \pm 2$ a $n(v, u) = \pm 2$. V tomto případě opět nastává v Cauchy-Buňakovského nerovnosti rovnost a $u$ je násobkem $v$, navíc z rovnosti $|n(u, v)| = |n(v, u)|$ vyplývá rovnost velikostí $\|u\| = \|v\|$. Je tedy $u = \pm v$ a $u - v = 0$ resp. $u + v = 0$. Evidentně, je-li $\langle u, v\rangle > 0$, pak i $n(u, v) > 0$ a $n(v, u) > 0$ a zrcadlením dostaneme $u - v$ obdobně pro $\langle u, v\rangle < 0$ dostaneme $u + v$.

(2) Důkaz provedeme sporem s použitím části (1) této věty. Víme, že $u + (k+2)v \in \Delta_0$ a $u \in \Delta$, pokud je tedy $\langle u + (k+2)v, u\rangle > 0$ je i $u + (k+1)v \in \Delta_0$. Dále i $u + kv \in \Delta_0$

| $n(u,v) \setminus n(v,u)$ | $\pm1$ | $\pm2$ | $\pm3$ | $\pm4$ |
|---|---|---|---|---|
| $\pm1$ | $\bullet$ | $\bullet$ | $\bullet$ | $\bullet$ |
| $\pm2$ | $\bullet$ | $\bullet$ | | |
| $\pm3$ | $\bullet$ | | | |
| $\pm4$ | $\bullet$ | | | |

Tabulka 1: Možné hodnoty $n(u,v)$ a $n(v,u)$

| $n(u,v) \setminus n(v,u)$ | $\pm1$ | $\pm2$ | $\pm3$ | $\pm4$ |
|---|---|---|---|---|
| $\pm1$ | $\pi/3, 2\pi/3$ | $\pi/4, 3\pi/4$ | $\pi/6, 5\pi/6$ | $0, \pi$ |
| $\pm2$ | $\pi/4, 3\pi/4$ | $0, \pi$ | $\times$ | $\times$ |
| $\pm3$ | $\pi/6, 5\pi/6$ | $\times$ | $\times$ | $\times$ |
| $\pm4$ | $0, \pi$ | $\times$ | $\times$ | $\times$ |

Tabulka 2: Možné hodnoty úhlů $\varphi$ pro daná $n(u,v)$ a $n(v,u)$

a $u \in \Delta$, pokud je tedy $\langle u + kv, u\rangle < 0$ je i $u + (k+1)v \in \Delta_0$. Ale pro každé $k \in \mathbf{Z}$ nastane alespoň jedna z možností

$$\langle u,u\rangle > -(k+2)\langle u,v\rangle \quad \text{nebo} \quad \langle u,u\rangle < -k\langle u,v\rangle$$

a tím dostáváme spor s předpokladem. ∎

Pomocí jednoduchých úvah lze nyní diskutovat možná uspořádání kořenů abstraktních kořenových systémů. Připomeňme, že úhel $\varphi$ svíraný dvěma vektory $u$ a $v$ definujeme pomocí vztahu

$$\varphi = \arccos \frac{\langle u,v\rangle}{\|u\|\|v\|} \in [0,\pi]$$

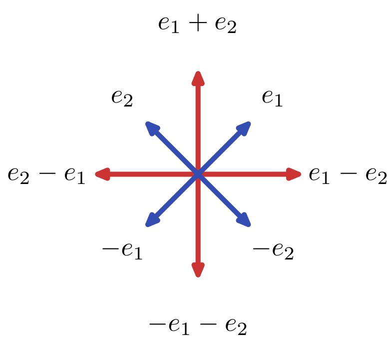
a s jeho pomocí můžeme zapsat

$$n(u,v) = 2\frac{\|v\|}{\|u\|}\cos\varphi, \quad \text{a} \quad n(u,v)n(v,u) = 4\cos^2\varphi.$$

Především je možno přepsat tabulku 1 pomocí na tabulku 2, která vyjádřuje možné úhlů, které svírají kořeny.

| $n(u,v) \setminus n(v,u)$ | $\pm 1$ | $\pm 2$ | $\pm 3$ | $\pm 4$ |
|---|---|---|---|---|
| $\pm 1$ | 1 | $\sqrt{2}$ | $\sqrt{3}$ | 2 |
| $\pm 2$ | $1/\sqrt{2}$ | 1 | $\times$ | $\times$ |
| $\pm 3$ | $1/\sqrt{3}$ | $\times$ | $\times$ | $\times$ |
| $\pm 4$ | $1/2$ | $\times$ | $\times$ | $\times$ |

Tabulka 3: Možné poměry velikostí kořenů $\|u\|/\|v\|$ pro daná $n(u,v)$ a $n(v,u)$




Jako příklad uvedeme některé abstraktní kořenové systémy v rovině. Pro systém $A_2$ máme shodné velikosti kořenů, přilehlé kořeny svírají úhly $\varphi = \pi/3$. Pro systém $B_2$ dostáváme pro poměr velikosti přilehlých kořenů $1/\sqrt{2}$, pro úhel, který svírají, $\varphi = \pi/4$. Kořeny, které svírají pravý úhel, jsou stejně veliké. Ze symetrie poslední tabulky lze naznat, že je další možnost, lišící se od $B_2$ pouze v tom, že poměr přilehlých kořenů je $\sqrt{2}$ a tento systém nazýváme $C_2$ (viz obrázek naboku).

**2.2. Jednoduché a kladné kořeny.** Z výšeuvedených příkladů je zřejmé, že počet kořenů abstraktních kořenových systémů roste rychleji, než dimenze příslušného lineárního prostoru $V$. Proto je vhodné zavést systém ***jednoduchých kořenů*** $\Pi \subset \Delta$, který splňuje

(1) $\Pi$ generuje $V$.

(2) Každý kořen $v \in \Delta$ lze zapsat jako celočíselnou lineární kombinaci jednoduchých kořenů $u \in \Pi$, všechny koeficienty této lineární kombinace mají pro daný kořen stejné znaménko, tj. pro všechna $v \in \Delta$ existují $u \in \Pi$ a $m_u \in \mathbf{Z}$ tak, že
$$v = \sum_{u \in \Pi} m_u u,$$
kde $m_u \leq 0$ pro všechna $u \in \Pi$ nebo $m_u \geq 0$ pro všechna $u \in \Pi$.

Zkonstruujeme systém $\Pi_t \subset \Delta$, asociovaný s vektorem $t \in V$ a abstraktním kořenovým systémem $\Delta$, který je systémem jednoduchých kořenů.

Nechť $\Delta$ je abstraktní kořenový systém a $t \in V$ takový vektor, že $\langle t, v\rangle \neq 0$ pro všechna $v \in \Delta$. Potom můžeme definovat systém kladných kořenů (vzhledem k $t$)
$$\Delta_t^+ = \{v \in \Delta | \langle t, v\rangle > 0\}$$
a systém záporných kořenů
$$\Delta_t^- = \{v \in \Delta | \langle t, v\rangle < 0\}.$$

**Lemma 12.** *Pro každý abstraktní kořenový systém $\Delta$ ve $V$ existuje $t \in V$ takové, že $\langle t, v\rangle \neq 0$ pro všechna $v \in \Delta$.*

*Důkaz.* Důkaz se zakládá na konečnosti množiny kořenů $\Delta$. Vektor $t$ nesmí ležet v žádné z nadrovin $H_v = \{u \in V | \langle u, v\rangle = 0\}$, pro $v \in \Delta$, tedy $t \notin \bigcup_{v\in\Delta} H_v$. V topologii $V$ indukované normou je předchozí konečné sjednocení topologickou podvarietou ve $V$ dimenze $n-1$, zatímco $V$ je dimenze $n$. Zejména tedy nemůže obsahovat všechny body $V$. ■

**Lemma 13.** $\Delta = \Delta_t^+ \cup \Delta_t^-$.

*Důkaz.* Pro každé $v \in \Delta$ platí buď $\langle v, t\rangle < 0$ nebo $\langle v, t\rangle > 0$. Rovněž víme, že $v \in \Delta$ implikuje $-v \in \Delta$. Je-li tedy $\langle v, t\rangle < 0$ (resp. $> 0$), potom $\langle -v, t\rangle > 0$ (resp. $< 0$). ■

Prvek $u \in \Delta_t^+$ nazýváme ***rozložitelným***, jestliže existují $v, w \in \Delta_t^+$ tak, že $u = v + w$. Pokud taková $v, w$ neexistují nazveme prvek $u$ nerozložitelným. Nechť $\Pi_t \subset \Delta_t^+$ je množina nerozložitelných prvků $\Delta_t^+$. Následující lemmata se týkají vlastností $\Pi_t$ a $\Delta_t^+$ a dokládají, že $\Pi_t$ je vskutku systémem jednoduchých kořenů.

**Lemma 14.** *Každý prvek $v \in \Delta_t^+$ je lineární kombinací prvků z $u \in \Pi_t$ s nezápornými celočíselnými koeficienty $m_u$, tj.*

$$v = \sum_{u\in\Pi_t} m_u u.$$

*Důkaz.* Důkaz provedeme sporem. Nechť tedy $w \in \Delta_t^+$ je prvek, který není vyjádřitelný jako nezáporná celočíselná lineární kombinace prvků z $\Pi_t$. Jelikož $\Delta_t^+$ je konečná množina, můžeme vybrat takové $w$, pro něž je skalární součin $\langle t, w\rangle > 0$ minimální. Protože $w \in \Delta_t^+$ a zároveň $w \notin \Pi_t$. Musí být $w$ z definice rozložitelné. Nechť tedy $w = u + v$, kde $u, v \in \Delta_t^+$. Potom platí $\langle t, w\rangle = \langle t, u\rangle + \langle t, v\rangle$, přičemž $\langle t, u\rangle > 0$ a $\langle t, v\rangle > 0$, což je spor s minimalitou $\langle t, w\rangle$. ■

**Lemma 15.** *Pro všechna $u, v \in \Pi_t$, $u \neq v$ platí $\langle u, v\rangle \leq 0$.*

*Důkaz.* Provedeme opět sporem. Předpokládejme tedy, že $\langle u, v\rangle > 0$. Potom podle tvrzení (1) věty 11 platí, že $u - v \in \Delta$ nebo $u = v$ (toto vylučuje předpoklad lemmatu). Označme $u - v = w$. Musí platit buď $w \in \Delta_t^+$, nebo $w \in \Delta_t^-$. V prvním případě platí $u = v + w$, což je ve sporu s nerozložitelností $u$. V druhém případě platí $-w \in \Delta_t^+$ a $v = -w + u$, což je zase ve sporu s nerozložitelností $v$. ■

Uvažujeme-li tedy o vektorech z množiny $\Pi_t$ jednoduchých kořenů, je zřejmé, že navzájem svírají tupé úhly, tj. $\varphi \in [\pi/2, \pi]$.

**Lemma 16.** *Nechť $t \in V$ je vektor a nechť $\Omega \subset V$ je množina takových $u, v \in V$, že*

*(1)* $\langle t, u\rangle > 0$

*(2)* $\langle u, v\rangle < 0$.

*Potom $\Omega$ tvoří lineárně nezávislou množinu vektorů.*

*Důkaz.* Pro změnu sporem. Předpokládejme tedy, že $\sum_{u\in\Omega} m_u u = 0$ a přitom všechna $m_u$ nejsou nulová. Potom některá $m_u > 0$ a některá naopak $m_u < 0$. Můžeme tedy psát $\sum_{m_u>0} m_u u - \sum_{m_u<0}(-m_u)u = 0$. Označme $w = \sum_{m_u>0} m_u u = \sum_{m_u<0}(-m_u)u \neq 0$. Potom z pozitivní definitnosti skalárního součinu plyne $\langle w, w\rangle \geq 0$. Na druhé straně je

$$\langle w, w\rangle = \langle \sum_{m_u>0} m_u u, \sum_{m_v<0}(-m_v)v\rangle = \sum_{m_u>0}\sum_{m_v<0} m_u(-m_v)\langle u, v\rangle \leq 0.$$

Celkem je tedy $w = 0$. Uvažujme nyní

$$\langle t, w\rangle = \langle t, \sum_{m_u>0} m_u u\rangle = \sum_{m_u>0} m_u \langle t, u\rangle = 0,$$

ale podle předpokladu je $\langle t, u\rangle > 0$ a je tedy pro $m_u > 0$ vskutku $m_u = 0$, což je spor. ■

Nyní je již možno dokázat požadovanou větu.

**Věta 17.** *Pro každé $t \in V$ takové, že $\langle t, u\rangle \neq 0$ pro všechna $u \in \Delta$, je zkonstruovaná množina $\Pi_t$ množinou jednoduchých kořenů a množina $\Delta_t^+$ množinou kladných kořenů.*

*Důkaz.* Z lemmatu 14 víme, že každý prvek $\Delta_t^+$ (resp. $\Delta_t^-$) lze zapsat jako lineární kombinaci prvků z $\Pi_t$ s nezápornými (resp. nekladnými) koeficienty. ■

## 3. Vlastnosti jednoduchých kořenů

## 4. Cartanova matice kořenového systému

## 5. Dynkinovy diagramy a klasifikace kořenových systémů