Kvaterniony

Definice. Algebra kvaternionů $\mathbb{H}$ je $\mathbb{R}^4 = \mathbb{R}\{1, i, j, k\}$ společně s násobením daným tabulkou

q.r:

q \ r	1	i	j	k
1	1	i	j	k
i	i	−1	k	−j
j	j	−k	−1	i
k	k	j	−i	−1

→ zadává jediné bilineární zobrazení $\mathbb{H} \times \mathbb{H} \to \mathbb{H}$

je potřeba ověřit, že je asociativní ...

$$i^2 = j^2 = k^2 = ijk = -1$$

Kvaternion $q \in \mathbb{H}$ můžeme psát v algebraickém tvaru

$$q = a + bi + cj + dk$$

nebo ve vektorovém tvaru $bi + cj + dk = (b, c, d) = u \in \mathbb{R}^3$

$$q = a + u$$

Pozn.
$\mathbb{H} \subseteq Mat_{2\times 2}\,\mathbb{C}$

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

$i \mapsto \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$

$j \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

Geometrická interpretace násobení kvaternionů

$$(a+u)(b+v) = \underbrace{ab}_{\text{násobení skaláry}} + \underbrace{av + bu}_{\text{násobení skaláry}} + \underbrace{uv}_{-\langle u,v\rangle + u\times v}$$

$-\langle u,v\rangle$: symetrická část; $u \times v$: antisymetrická část

$$u \cdot v = -\langle u, v\rangle + u \times v \implies \frac{1}{2}(u\cdot v + v\cdot u) = -\langle u,v\rangle = \mathrm{Re}(u\cdot v)$$
$$\frac{1}{2}(u\cdot v - v\cdot u) = u\times v = \mathrm{Im}(u\cdot v)$$

$$u\cdot v\cdot w = -\langle u,v\rangle w - \underbrace{\langle u\times v, w\rangle}_{-\mathrm{Vol}(u,v,w)\in\mathbb{R}} + (u\times v)\times w \implies -\mathrm{Vol}(u,v,w) = \mathrm{Re}(u\cdot v\cdot w)$$

Inverze: (jako pro komplexní čísla)

$$q = a + u \implies q^* = a - u$$
$$q\cdot q^* = (a+u)(a-u) = a^2 - au + au \underbrace{- u\cdot u}_{\langle u,u\rangle - \underbrace{u\times u}_{0}} = a^2 + |u|^2 = |q|^2 \in \mathbb{R}$$

$$\implies q^{-1} = \frac{1}{|q|^2}\cdot q^*$$

Goniometrický tvar jednotkového kvaternionu q, tj. t.ž. $|q| = 1 \implies q^{-1} = q^*$

$$a^2 + |u|^2 = |q|^2 = 1$$

$\Rightarrow a = \cos\varphi$, $|u| = \sin\varphi \implies u = v\cdot\sin\varphi$ (v normovaný vektor, např. i, j, k)

$$a = \cos\varphi + v\cdot\sin\varphi = e^{v\cdot\varphi}$$

naopak $(e^{v\cdot\varphi})^{-1} = e^{-v\cdot\varphi}$

↳ nejednoznačnost: $\varphi \in \mathbb{R}/2\pi\mathbb{Z}$) $e^{v\cdot\varphi} = e^{(-v)\cdot(-\varphi)}$

$\cos\varphi + v\cdot\sin\varphi = \cos(-\varphi) + (-v)\cdot\sin(-\varphi)$

$\varphi \to 0 \Rightarrow v$ zcela nejednoznačné

$\varphi = \pi$

Naším cílem bude reprezentovat otočení pomocí násobení kvaterniony

$$\begin{array}{ccc} \mathbb{H} & \longrightarrow & \mathbb{H} \\ u & \longmapsto & e^{v\cdot\varphi}\cdot u\cdot e^{-v\cdot\varphi} \end{array} \qquad \rightsquigarrow \qquad \begin{array}{ccc} \mathrm{Im}\,\mathbb{H} & \longrightarrow & \mathrm{Im}\,\mathbb{H} \\ \| & & \| \\ \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \end{array}$$

Lemma.

- $u\cdot v = v\cdot u \iff u \parallel v$
- $u\cdot v = -v\cdot u \iff u \perp v$

Nechť nyní $u \parallel v$:

$$u \longmapsto e^{v\cdot\varphi}\cdot u\cdot e^{-v\cdot\varphi} = (\cos\varphi + v\cdot\sin\varphi)\cdot u\cdot(\cos\varphi - v\cdot\sin\varphi)$$

$$= \underbrace{e^{v\cdot\varphi}\cdot e^{-v\cdot\varphi}}\cdot u = u$$

$\Rightarrow$ zobrazení je id na přímce generované v.

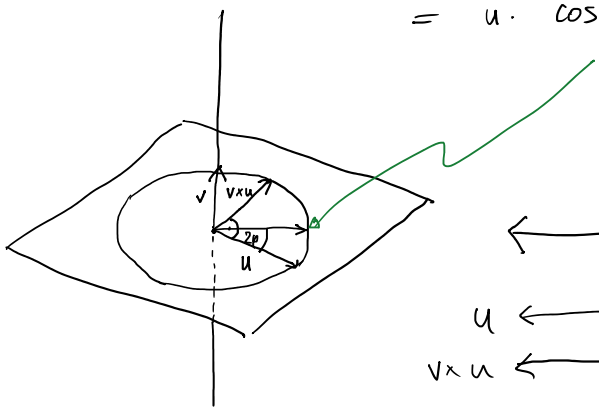
Nechť nyní $u \perp v$:

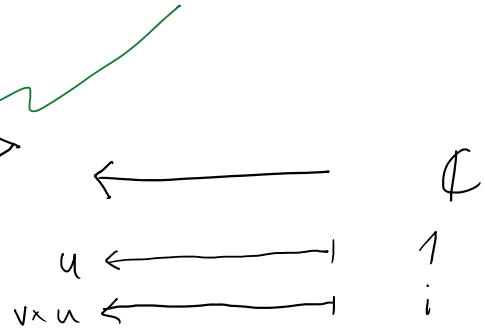
$$u \longmapsto e^{v\cdot\varphi}\cdot u\cdot e^{-v\cdot\varphi} = (\cos\varphi + v\cdot\sin\varphi)\cdot u\cdot(\cos\varphi - v\cdot\sin\varphi)$$

$$= e^{v\cdot\varphi}\cdot e^{v\cdot\varphi}\cdot u = e^{v\cdot(2\varphi)}\cdot u$$

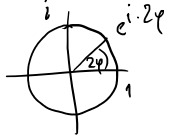
$$= (\cos(2\varphi) + v\cdot\sin(2\varphi))\cdot u$$

$$= u\cdot\cos(2\varphi) + v\times u\cdot\sin(2\varphi)$$





konformní zobrazení
$\Rightarrow$ zachovává poměry velikostí a úhly (obrazy kolmé a stejně veliké)



$\Rightarrow$ zobrazení je rotace o úhel 2φ v rovině $v^\perp$
+ směr „podle pravidla pravé ruky" = ve směru od u k $v \times u$.

Věta. Zobrazení $u \mapsto e^{v\cdot\varphi} \cdot u \cdot e^{-v\cdot\varphi}$ dané konjugací jednotkovým kvaternionem $e^{v\cdot\varphi}$ je na $\mathbb{R}^3 = \mathrm{Im}\,\mathbb{H}$ rotace okolo vektoru v o úhel 2φ.

Poznámka. Prostor rotací $SO(3)$

$$S^3 \longrightarrow SO(3)$$
$$q \longmapsto (u \mapsto qnq^{-1})$$

je surjektivní homomorfismus grup. Jaké je jeho jádro?

$e^{v\cdot\varphi} \in \ker$, $|v|=1$, $\varphi \in [0,\pi] \iff \varphi = 0$ nebo $\varphi = \pi$

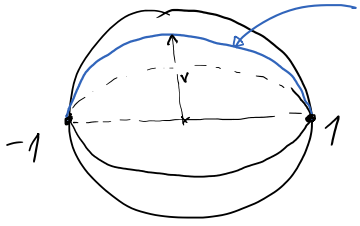
$\Rightarrow \ker = \{\pm 1\}$

$$S^3/\{\pm 1\} \xrightarrow{\cong} SO(3)$$

„dvojnásobné natočení"

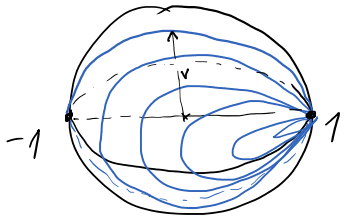
reálný projektivní prostor dimenze 3

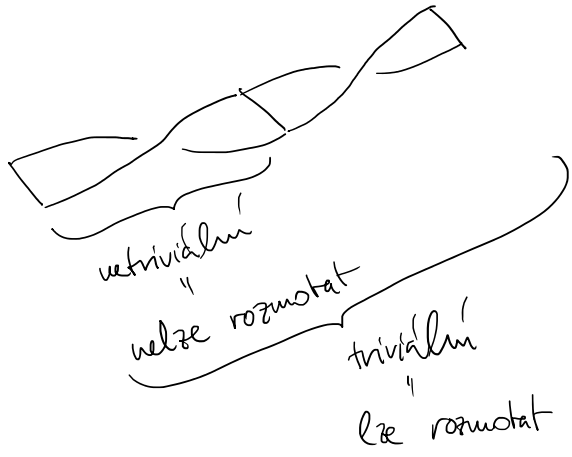
$\Rightarrow SO(3) \cong \mathcal{P}_3 \ (= \mathbb{RP}^3)$



$\cos(\pi\cdot t) + v\cdot\sin(\pi\cdot t) \longmapsto$ rotace okolo v o úhel $2\pi\cdot t$

$t \in [0,1]$





Celočíselné matice, SNF, prezentace abelovských grup

$\mathrm{Mat}_{n\times m}\mathbb{Z}$ ... matice s celočíselnými prvky

Ψ A zadává zobrazení $\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n$, $x \mapsto A\cdot x$ — zjevně homo grup $A(x+y)=Ax+Ay$

Tvrzení. Zobrazení $\mathrm{Mat}_{n\times m}\mathbb{Z} \to \mathrm{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$ je bijekce.

Důkaz. $\varphi : \mathbb{Z}^m \to \mathbb{Z}^n$

$$\varphi(x) = \varphi(x^1 e_1 + \dots + x^m e_m) = x^1\cdot\varphi(e_1) + \dots + x^m \varphi(e_m) = \begin{pmatrix} \varphi(e_1) & \cdots & \varphi(e_m)\end{pmatrix}\begin{pmatrix} x^1 \\ \vdots \\ x^m\end{pmatrix}$$

$$= A\cdot x \qquad \square$$

Implicitně používáme:

M komutativní grupa psaná aditivně $\Rightarrow$ v M umíme „násobit celými čísly"

$k\cdot x = \underbrace{x+\dots+x}_{k\times}$ $\qquad 0\cdot x = 0$ $\qquad (-k)\cdot x = \underbrace{(-x)+\dots+(-x)}_{k\times}$

$\rightsquigarrow$ násobení „skalárem" $\mathbb{Z}\times M \to M$, ale $\mathbb{Z}$ není těleso $\Rightarrow$ spousta LA neplatí

$\rightsquigarrow$ homomorfismy grup zachovávají toto násobení $\Rightarrow$ jsou „lineární"

Cíl: vyjádřit $A : \mathbb{Z}^m \to \mathbb{Z}^n$ „ve vhodných bázích"

$P\cdot A\cdot Q$ (P, Q invertibilní)

jak to vyjde v LA?

$$\begin{matrix}\text{im}\\ \text{im}^\perp\end{matrix}\left(\begin{array}{c|c} E & 0 \\ \hline 0 & 0\end{array}\right) \qquad \begin{matrix}\ker^\perp & \ker\end{matrix}$$

$$\mathbb{k}^m \xrightarrow{A} \mathbb{k}^n$$

$$[\bar e_1, \dots, \bar e_r, \underbrace{\bar e_{r+1}, \dots, \bar e_m}_{\text{báze } \ker A}] \qquad [\underbrace{e_1, \dots, e_r}_{e_i = A\bar e_i}, e_{r+1}, \dots, e_n]$$

Tvrzení. Matice $A \in \mathrm{Mat}_{n\times m}\mathbb{Z}$ je invertibilní $\Leftrightarrow$ $n=m$ a $\det A = \pm 1$.

Důkaz.

- Nechť $B \in \mathrm{Mat}_{m\times n}\mathbb{Z}$ je inverze k A. Potom jsou inverzní i nad $\mathbb{Q}$

$\Rightarrow n=m$ a $\underbrace{\det A}_{\in\mathbb{Z}}\cdot\underbrace{\det B}_{\in\mathbb{Z}} = \det(A\cdot B) = \det E = 1$.

- Nechť naopak A je čtvercová s $\det A = \pm 1$. Existuje $A^{-1} \in \mathrm{Mat}_{n\times n}\mathbb{Q}$ a je dáno vzorečkem

$$A^{-1} = \frac{1}{\det A}(\text{matice alg. doplňků se znaménky a transponovaná}) \in \mathrm{Mat}_{n\times n}\mathbb{Z}. \qquad \square$$

podmínka na determinant je $\det A \in R^\times$

Poznámka. Stejný důkaz funguje nad libovolným komutativním okruhem R.

Je-li R obor integrity, použijeme namísto R podílové těleso $Q(R)$.

Jinak: $M \subseteq R$ lib. max. ideál $\rightsquigarrow \mathbb{k} = R/M$ a opět dostaneme $n=m$

formulka pro inverzi funguje stejně.

Bez komutativity: existují invertibilní nečtvercové matice!?

v důkazu se používaly determinanty — nedávají smysl

Věta (o Smithově normálním tvaru = SNF).

Nechť $A \in \mathrm{Mat}_{n\times m}\mathbb{Z}$. Pak existují invertibilní matice P, Q t.ž.

- P, Q jsou součiny elementárních matic nad $\mathbb{Z}$
- $P^{-1}AQ = \left(\begin{array}{c|c} q_1 & 0 \\ \ddots & \\ q_r & \\ \hline 0 & 0 \end{array}\right) = S$ } matice ve Smithově normálním tvaru

  přičemž $q_1 \mid \cdots \mid q_r$
- čísla $q_1 \mid \cdots \mid q_r$ jsou jednoznačná až na znaménko (pro nás kladná $\Rightarrow$ jednoznačná); nazývají se invariantní faktory.
- konkrétněji:

  $d_i = \gcd\{\text{minory } i\times i \text{ matice } A\}$; $d_0 = 1$ ← jediný minor $\det() = 1$?

  $q_i = d_i / d_{i-1}$

Důkaz. • Algoritmus vyložíme na cvičení – kombinace Euklidova algoritmu k vyrobení nejv. spol. děl. prvků matice a Gaussovy eliminace k následné eliminaci prvků mimo diagonálu (obojí pomocí elementárních operací).

• Studujme, co se děje s d_i při (ne nutně elem./invert. operacích):

$B = P\cdot A \Rightarrow$ řádky B jsou kombinacemi řádků A

$\Rightarrow$ minory B jsou kombinacemi minorů A ($\Rightarrow$ dělitelné $d_i(A)$)

$\Rightarrow d_i(A) \mid d_i(B)$

Je-li P invertibilní, pak $A = P^{-1}\cdot B \Rightarrow d_i(A) = d_i(B)$

$\Rightarrow d_i(A)/d_{i-1}(A) = d_i(B)/d_{i-1}(B)$

To samé pro sloupcové operace.

$\Rightarrow d_i(A)/d_{i-1}(A) = d_i(S)/d_{i-1}(S) = q_1\cdots q_i / q_1\cdots q_{i-1} = q_i$. □

$S = P^{-1}AQ \Leftrightarrow A = PSQ^{-1}$

$\Rightarrow \mathrm{im}\, A = P(\mathrm{im}\, S) = P[q_1 e_1, \ldots, q_r e_r] = [q_1 Pe_1, \ldots, q_r Pe_r]$ ← sloupce matice P

$\Rightarrow \ker A = Q(\ker S) = Q[e_{r+1}, \ldots, e_m] = [Qe_{r+1}, \ldots, Qe_m]$ ← sloupce matice Q

Prezentace konečně generovaných abelovských grup

Cíl. Strukturní věta pro kon. gen. ab. grupy = popis až na izo

Mějme kon. gen. abelovskou (= komutativní, píšeme aditivně) grupu, generovanou $a_1, \ldots, a_n$

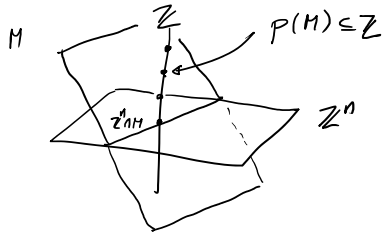
$\varphi: \mathbb{Z}^n \to M$, $e_i \mapsto a_i$, $\varphi(x) = (a_1, \dots, a_m) \cdot \begin{pmatrix} x^1 \\ \vdots \\ x^n \end{pmatrix}$ surjektivní homomorfismus

$\Rightarrow M \cong \mathbb{Z}^n / \ker \varphi$ ... pochopit kon. gen. ab. grupy = pochopit podgrupy $\mathbb{Z}^n$ a příslušné kvocienty

Věta. Každá podgrupa $\mathbb{Z}^n$ je konečně generovaná (ve skutečnosti izomorfní $\mathbb{Z}^m$ pro $m \le n$).

Důkaz. Indukcí: • $n = 0$ triviální

• $M \subseteq \mathbb{Z}^{n+1}$ podgrupa



Označme $p: \mathbb{Z}^{n+1} \to \mathbb{Z}$ projekci na první složku, pak $\ker p \cong \mathbb{Z}^n$ a $\ker p \cap M = [a_1, \dots, a_m]$.

$p(M) \subseteq \mathbb{Z}$ podgrupa $\Rightarrow p(M) = \mathbb{Z} \cdot t$, $t = p(a_0)$

Tvrdíme, že $M = [a_0, a_1, \dots, a_m]$

$x \in M \Rightarrow p(x) \in p(M) = \mathbb{Z} \cdot t \Rightarrow p(x) = y^0 \cdot t = p(y^0 \cdot a_0)$

Tedy $x - y^0 a_0 \in \ker p \cap M \Rightarrow x - y^0 a_0 = y^1 a_1 + \dots + y^m a_m$.

$\Rightarrow x = y^0 a_0 + y^1 a_1 + \dots + y^m a_m$. □

$$\mathbb{Z}^n \xrightarrow{\varphi} M$$

$$\mathbb{Z}^m \xrightarrow{\psi} \ker\varphi \xrightarrow{in} \mathbb{Z}^n \xrightarrow{\varphi} M, \qquad R$$

$\Rightarrow M \cong \mathbb{Z}^n / \ker\varphi = \mathbb{Z}^n / \operatorname{im} R =: \operatorname{coker} R$

$\mathbb{Z}^m \xrightarrow{R} \mathbb{Z}^n \xrightarrow{\varphi} M$ nazveme **prezentací** abelovské grupy M

relace M ↑ | generátory M ↑

- φ surjektivní
- $\operatorname{im} R = \ker\varphi$

$\Big\}$ $M \cong \operatorname{coker} R$ ← matice $R \in \mathrm{Mat}_{n\times m}\mathbb{Z}$ určuje M až na izo

co řekne SNF?

$$\begin{array}{ccccc} \mathbb{Z}^m & \xrightarrow{R} & \mathbb{Z}^n & \longrightarrow & \operatorname{coker} R \cong M \\ Q \uparrow \cong & & \cong \uparrow P & & \uparrow \cong \\ \mathbb{Z}^m & \xrightarrow[S]{} & \mathbb{Z}^n & \longrightarrow & \operatorname{coker} S \cong ? \end{array}$$

určeno P: $Px + \operatorname{im} R$ ↑ $x + \operatorname{im} S$

(inverze určena P^{-1})

$(P(\operatorname{im} S) = \operatorname{im} PS = \operatorname{im} RQ \subseteq \operatorname{im} R)$

Tvrzení. $S = \left(\begin{array}{c|c} q_1 \dots q_r & 0 \\ \hline 0 & 0 \end{array}\right) \Rightarrow \operatorname{coker} S \cong \mathbb{Z}/q_1 \times \dots \times \mathbb{Z}/q_r \times \mathbb{Z}^{n-r}$.

$\operatorname{coker} S = \mathbb{Z}^n / \operatorname{im} S$

$(x^1, \dots, x^n) + \operatorname{im} S \longmapsto (x^1 + \mathbb{Z}q_1, \dots, x^r + \mathbb{Z}q_r, x^{r+1}, \dots, x^n)$

Důkaz. □

Zjevně můžeme vynechat všechny činitele $\mathbb{Z}/1 = 0$.

Věta. Každá konečně generovaná abelovská grupa je izomorfní

$$\mathbb{Z}/q_1 \times \cdots \times \mathbb{Z}/q_r \times \mathbb{Z}^k \qquad \text{kde} \quad 1 \neq q_1 \mid \cdots \mid q_r, \; k \geq 0$$

a tyto parametry jsou jednoznačné. $\Rightarrow$ kanonický tvar

Důkaz. Existenci máme, jednoznačnost uvidíme dílem z další věty. □

$$q = p_1^{t_1} \cdots p_s^{t_s} \quad \Rightarrow \quad \mathbb{Z}/q = \mathbb{Z}/p_1^{t_1} \times \cdots \times \mathbb{Z}/p_s^{t_s}$$

Věta. Každá konečně generovaná abelovská grupa je izomorfní

$$\mathbb{Z}/p_1^{t_1} \times \cdots \times \mathbb{Z}/p_s^{t_s} \times \mathbb{Z}^k \qquad \text{kde } p_1, \dots, p_s \text{ jsou prvočísla}, \; t_1, \dots, t_s \geq 1, \; k \geq 0$$

a tyto parametry jsou jednoznačné. $\Rightarrow$ kanonický tvar

Důkaz. Existenci opět máme. Jednoznačnost:

$$M = \mathbb{Z}/p_1^{t_1} \times \cdots \times \mathbb{Z}/p_s^{t_s} \times \mathbb{Z}^k$$

$$\Rightarrow \quad M/p \cdot M = \prod_{p_i = p} \mathbb{Z}/p \times (\mathbb{Z}/p)^k$$

$$p \cdot M / p^2 \cdot M = \prod_{\substack{p_i = p \\ t_i \geq 2}} \mathbb{Z}/p \times (\mathbb{Z}/p)^k$$

$$\vdots$$

$$p^{t-1} \cdot M / p^t \cdot M = \prod_{\substack{p_i = p \\ t_i \geq t}} \mathbb{Z}/p \times (\mathbb{Z}/p)^k$$

$\mathbb{Z}/q^t / p \cdot \mathbb{Z}/q^t = 0$

↑ p invertibilní modulo q^t $\Rightarrow p \cdot \mathbb{Z}/q^t = \mathbb{Z}/q^t$

rozpozná všechna prvočísla p_i a všechny exponenty t_i a taky $k = \operatorname{rk} M$

└ tzv. řád M.

□

Jednoznačnost v první větě: podobně nebo jako důsledek jednozn. zde.

Příklad. Určete SNF celočíselné matice

$$\begin{pmatrix} 51 & 30 \end{pmatrix} \sim \begin{pmatrix} 21 & 30 \end{pmatrix} \sim \begin{pmatrix} 21 & 9 \end{pmatrix} \sim \begin{pmatrix} 3 & 9 \end{pmatrix} \sim \begin{pmatrix} 3 & 0 \end{pmatrix} \leftarrow \text{SNF}$$

Příklad. Určete SNF celočíselné matice

$$\begin{pmatrix} 2 & 1 & -1 & 1 \\ 4 & 2 & 1 & 6 \\ 6 & 2 & 1 & -2 \\ 4 & 1 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 1 & 2 \\ 2 & 1 & 6 & 4 \\ 2 & 1 & -2 & 6 \\ 1 & 2 & 1 & 4 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & -1 & 1 & 2 \\ 0 & 3 & 4 & 0 \\ 0 & 3 & -4 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 3 & 4 & 0 \\ 0 & 3 & -4 & 2 \\ 0 & 3 & 0 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 4 & 0 \\ 0 & 3 & -4 & 2 \\ 0 & 3 & 0 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 4 & 0 \\ 0 & 7 & -4 & 2 \\ 0 & 3 & 0 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 4 & 0 \\ 0 & 0 & 24 & 2 \\ 0 & 0 & 12 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & +1 & 0 & 0 \\ 0 & 0 & 24 & 2 \\ 0 & 0 & 12 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 24 \\ 0 & 0 & 2 & 12 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 24 \\ 0 & 0 & 0 & -12 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 12 \end{pmatrix} \leftarrow \text{SNF}$$