# Matematika I – 3. přednáška
# Geometrie v rovině

Michal Bulant

Masarykova univerzita
Fakulta informatiky

4. 3. 2009

# Obsah přednášky

## Doporučené zdroje

- Martin Panák, Jan Slovák – **Drsná matematika**, *e*-text.
- Roman Hilscher – `MB101`, *e*-text.
- Slidy z přednášek a democvičení

# Doporučené zdroje

- Martin Panák, Jan Slovák – **Drsná matematika**, *e*-text.
- Roman Hilscher – `MB101`, *e*-text.
- Slidy z přednášek a democvičení
- Pavel Horák, Úvod do lineární algebry, MU Brno, skripta (`http://www.math.muni.cz/~horak`)
- Luboš Motl, Miloš Zahradník, Pěstujeme lineární algebru, 3. vydání, Univerzita Karlova v Praze, Karolinum, 348 stran (elektronické vydání také na http://www.kolej.mff.cuni.cz/˜lmotm275/skripta/).

# Plán přednášky

# Afinní rovina a vektorový prostor $\mathbb{R}^2$

Na konci minulé přednášky jsme intuitivně používali elementární pojmy z geometrie reálné roviny. Budeme teď podrobněji zkoumat jak se vypořádávat s potřebou popisovat polohu v rovině, resp. dávat do souvislostí polohy různých bodů roviny.

# Afinní rovina a vektorový prostor $\mathbb{R}^2$

Na konci minulé přednášky jsme intuitivně používali elementární pojmy z geometrie reálné roviny. Budeme teď podrobněji zkoumat jak se vypořádávat s potřebou popisovat polohu v rovině, resp. dávat do souvislostí polohy různých bodů roviny.
Zkusme si množinu $A = \mathbb{R}^2$ představit z pohledu pozorovatele, který sedí v některém pevně zvoleném místě (můžeme mu říkat třeba bod $O = (x_0, y_0) \in \mathbb{R}^2$). Předpokládejme, že ji vnímá jako nekonečnou desku bez jakýchkoliv zvolených měřítek a popisů a ví, co to znamená posunout se v libovolném násobku nějakého směru. Takové rovině budeme říkat afinní rovina.

Aby pozorovatel mohl vidět kolem sebe dvojice reálných čísel, musí si vybrat nějaký bod $E_1$, kterému řekne bod $[1, 0]$ a jiný bod $E_2$, kterému začne říkat bod $[0, 1]$.

Aby pozorovatel mohl vidět kolem sebe dvojice reálných čísel, musí si vybrat nějaký bod $E_1$, kterému řekne bod $[1, 0]$ a jiný bod $E_2$, kterému začne říkat bod $[0, 1]$.

Do všech ostatních se pak dostane tak, že poskočí $a$–krát ve směru $[1, 0]$, pak $b$–krát ve směru $[0, 1]$ a takovému bodu bude říkat bod $[a, b]$. Pokud to bude dělat obvyklým způsobem, nebude výsledek záviset na pořadí, tzn. může také napřed jít $b$–krát ve směru $[0, 1]$ a pak teprve v tom druhém.

Aby pozorovatel mohl vidět kolem sebe dvojice reálných čísel, musí si vybrat nějaký bod $E_1$, kterému řekne bod $[1, 0]$ a jiný bod $E_2$, kterému začne říkat bod $[0, 1]$.

Do všech ostatních se pak dostane tak, že poskočí $a$–krát ve směru $[1, 0]$, pak $b$–krát ve směru $[0, 1]$ a takovému bodu bude říkat bod $[a, b]$. Pokud to bude dělat obvyklým způsobem, nebude výsledek záviset na pořadí, tzn. může také napřed jít $b$–krát ve směru $[0, 1]$ a pak teprve v tom druhém.

To, co jsme popsali, se nazývá volba **(afinního) souřadného systému v rovině**, bod $O$ je jeho **počátkem**, posunutí $E_1 - O$ ztotožňujeme s dvojicí $[1, 0]$, podobně u $E_2$ a obecně každý bod $P$ roviny je ztotožněn s dvojicí čísel $[a, b] = P - O$.

Aby pozorovatel mohl vidět kolem sebe dvojice reálných čísel, musí si vybrat nějaký bod $E_1$, kterému řekne bod $[1, 0]$ a jiný bod $E_2$, kterému začne říkat bod $[0, 1]$.
Do všech ostatních se pak dostane tak, že poskočí $a$–krát ve směru $[1, 0]$, pak $b$–krát ve směru $[0, 1]$ a takovému bodu bude říkat bod $[a, b]$. Pokud to bude dělat obvyklým způsobem, nebude výsledek záviset na pořadí, tzn. může také napřed jít $b$–krát ve směru $[0, 1]$ a pak teprve v tom druhém.
To, co jsme popsali, se nazývá volba **(afinního) souřadného systému v rovině**, bod $O$ je jeho **počátkem**, posunutí $E_1 - O$ ztotožňujeme s dvojicí $[1, 0]$, podobně u $E_2$ a obecně každý bod $P$ roviny je ztotožněn s dvojicí čísel $[a, b] = P - O$.
Všimněme si, že volbou pevného počátku $O$ jsou zároveň ztotožněny jednotlivé body $P$ roviny se směry posuvu $v = P - O$ a že všechny takové posuvy umíme skládat (budeme říkat sčítat) a také jednotlivé směry násobit v poměru každého reálného čísla (budeme říkat násobit skalárem).

# Přímky v rovině

Naše operace sčítání bodů v rovině a jejich násobení skaláry splňují hodně vlastností skalárů. Budeme místo o směrech posuvu mluvit o **vektorech** a od bodů je budeme rozlišovat tím, že budou dány dvojicemi souřadnic v kulatých závorkách místo hranatých.

# Přímky v rovině

Naše operace sčítání bodů v rovině a jejich násobení skaláry splňují hodně vlastností skalárů. Budeme místo o směrech posuvu mluvit o **vektorech** a od bodů je budeme rozlišovat tím, že budou dány dvojicemi souřadnic v kulatých závorkách místo hranatých.
Když se náš pozorovatel umí posouvat o libovolný násobek pevného vektoru, pak také ví, co je to **přímka**. Je to podmnožina $p \subset A$ v rovině taková, že existují bod $O$ a vektor $v$ takové, že

$$p = \{P \in A;\ P - O = t \cdot v,\ t \in \mathbb{R}\}.$$

# Přímky v rovině

Naše operace sčítání bodů v rovině a jejich násobení skaláry splňují hodně vlastností skalárů. Budeme místo o směrech posuvu mluvit o **vektorech** a od bodů je budeme rozlišovat tím, že budou dány dvojicemi souřadnic v kulatých závorkách místo hranatých.
Když se náš pozorovatel umí posouvat o libovolný násobek pevného vektoru, pak také ví, co je to **přímka**. Je to podmnožina $p \subset A$ v rovině taková, že existují bod $O$ a vektor $v$ takové, že

$$p = \{P \in A;\ P - O = t \cdot v,\ t \in \mathbb{R}\}.$$

Popišme si $P = P(t) \in p$ ve zvolených souřadnicích s volbou $v = (\alpha, \beta)$:

$$x(t) = x_0 + \alpha \cdot t, \quad y(t) = y_0 + \beta \cdot t.$$

Jednoduchým výpočtem dostaneme (vyloučíme $t$ z parametrického vyjádření pro $x$ a $y$, když pro určitost předpokládáme, že třeba $\alpha \neq 0$)

$$-\beta x + \alpha y + (\beta x_0 - \alpha y_0) = 0.$$

To je obecná rovnice přímky

$$ax + by = c,$$

se známým vztahem dvojice čísel $(a, b)$ a vektoru $v = (\alpha, \beta)$

$$a\alpha + b\beta = 0.$$

Jednoduchým výpočtem dostaneme (vyloučíme $t$ z parametrického vyjádření pro $x$ a $y$, když pro určitost předpokládáme, že třeba $\alpha \neq 0$)

$$-\beta x + \alpha y + (\beta x_0 - \alpha y_0) = 0.$$

To je obecná rovnice přímky

$$ax + by = c,$$

se známým vztahem dvojice čísel $(a, b)$ a vektoru $v = (\alpha, \beta)$

$$a\alpha + b\beta = 0.$$

Výraz nalevo v rovnici přímky můžeme vidět jako skalární funkci $F$ závislou na bodech v rovině a s hodnotami v $\mathbb{R}$, samu rovnici pak jako požadavek na její hodnotu.

Mějme dvě přímky $p$ a $q$ a ptejme se na jejich průnik $p \cap q$. Ten bude popsán jako bod, splňující rovnice obou přímek:

$$ax + by = r$$
$$cx + dy = s.$$

Mějme dvě přímky $p$ a $q$ a ptejme se na jejich průnik $p \cap q$. Ten bude popsán jako bod, splňující rovnice obou přímek:

$$ax + by = r$$
$$cx + dy = s.$$

Opět můžeme levou stranu vnímat jako přiřazení, které každé dvojici souřadnic $[x(P), y(P)]$ bodů v rovině přiřadí vektor hodnot dvou skalárních funkcí $F_1$ a $F_2$.

Mějme dvě přímky $p$ a $q$ a ptejme se na jejich průnik $p \cap q$. Ten bude popsán jako bod, splňující rovnice obou přímek:

$$ax + by = r$$
$$cx + dy = s.$$

Opět můžeme levou stranu vnímat jako přiřazení, které každé dvojici souřadnic $[x(P), y(P)]$ bodů v rovině přiřadí vektor hodnot dvou skalárních funkcí $F_1$ a $F_2$.
Můžeme tedy naše rovnice napsat jako jediný vztah $F(v) = w$, kde $F$ je přiřazení, které vektor $v$ popisující polohu obecného bodu v rovině zobrazí na vektor zadaný levou stranou rovnic, a požadujeme, aby se toto zobrazení strefilo do předem zadaného vektoru $w = (r, s)$.

# Plán přednášky

Přiřazení $F$, se kterým jsme pracovali při popisu průniku přímek, zjevně respektuje operace sčítání a násobení s vektory a skaláry:

$$F(r \cdot v + s \cdot w) = r \cdot F(v) + s \cdot F(w)$$

pro všechny $r, s \in \mathbb{R}$, $v, w \in \mathbb{R}^2$. Říkáme, že $F$ je **lineární zobrazení** z $\mathbb{R}^2$ do $\mathbb{R}^2$, a píšeme $F : \mathbb{R}^2 \to \mathbb{R}^2$. Obdobně, v rovnici pro přímku šlo o lineární zobrazení $F : \mathbb{R}^2 \to \mathbb{R}$ a jeho předepsanou hodnotu $c$.

Přiřazení $F$, se kterým jsme pracovali při popisu průniku přímek, zjevně respektuje operace sčítání a násobení s vektory a skaláry:

$$F(r \cdot v + s \cdot w) = r \cdot F(v) + s \cdot F(w)$$

pro všechny $r, s \in \mathbb{R}$, $v, w \in \mathbb{R}^2$. Říkáme, že $F$ je **lineární zobrazení** z $\mathbb{R}^2$ do $\mathbb{R}^2$, a píšeme $F : \mathbb{R}^2 \to \mathbb{R}^2$. Obdobně, v rovnici pro přímku šlo o lineární zobrazení $F : \mathbb{R}^2 \to \mathbb{R}$ a jeho předepsanou hodnotu $c$.

Stručně budeme zapisovat taková zobrazení pomocí **matic** a jejich násobení, které definujeme takto:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ v = \begin{pmatrix} x \\ y \end{pmatrix}$$

$$A \cdot v = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Podobně, můžeme místo vektoru $v$ zprava násobit jinou maticí $B$ stejného rozměru jako je $A$. Prostě aplikujeme předchozí formule po jednotlivých sloupcích matice $B$ a obrdržíme jako výsledek opět matice.

Podobně, můžeme místo vektoru $v$ zprava násobit jinou maticí $B$ stejného rozměru jako je $A$. Prostě aplikujeme předchozí formule po jednotlivých sloupcích matice $B$ a obrdržíme jako výsledek opět matice.
Snadno ověříme tzv. asociativitu násobení:

$$(A \cdot B) \cdot v = A \cdot (B \cdot v).$$

Podobně, můžeme místo vektoru $v$ zprava násobit jinou maticí $B$ stejného rozměru jako je $A$. Prostě aplikujeme předchozí formule po jednotlivých sloupcích matice $B$ a obrdržíme jako výsledek opět matice.
Snadno ověříme tzv. asociativitu násobení:

$$(A \cdot B) \cdot v = A \cdot (B \cdot v).$$

Stejně snadno je vidět i distributivita $A \cdot (B + C) = A \cdot B + A \cdot C$, neplatí však komutativita a existují dělitelé nuly. Např.

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

Výrazu $ad - bc$ říkáme **determinant** matice $A$ a značíme jej $\det A = |A|$, neboli

$$\det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Výrazu $ad - bc$ říkáme **determinant** matice $A$ a značíme jej $\det A = |A|$, neboli

$$\det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Jestliže k výsledku lineárního zobrazení ještě dovolíme přičíst pevný vektor $T = (x(T), y(T))$, tj. naše zobrazení bude

$$v = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \cdot v + T = \begin{pmatrix} ax + by + x(T) \\ cx + dy + y(T) \end{pmatrix},$$

máme popsána právě všechna tzv. **afinní zobrazení roviny** do sebe. Známými příklady jsou všechny afinní podobnosti. Lineární zobrazení pak odpovídají těm afinním zobrazením, které zachovávají pevný bod $O$.

# Plán přednášky

Přidejme nyní schopnost našeho pozorovatele vidět vzdálenosti. Pak lze definovat pojmy jako jsou úhel a otočení v rovině.

Přidejme nyní schopnost našeho pozorovatele vidět vzdálenosti. Pak lze definovat pojmy jako jsou úhel a otočení v rovině. Jednoduše si to můžeme představit takto: pozorovatel se rozhodne o nějakých referenčních bodech $E_1$ a $E_2$, že jsou od něj ve vzdálenosti jedna, a zároveň si řekne, že jsou na sebe kolmé. Vzdálenosti ve směrech těchto bodů, tj. ve směrech souřadných os jsou dány příslušným poměrem, obecně používá Pythagorovu větu. Odtud vyjde známý vzorec pro velikost vektoru $v = (a, b)$

$$\|v\| = \sqrt{a^2 + b^2}.$$

Přidejme nyní schopnost našeho pozorovatele vidět vzdálenosti. Pak lze definovat pojmy jako jsou úhel a otočení v rovině. Jednoduše si to můžeme představit takto: pozorovatel se rozhodne o nějakých referenčních bodech $E_1$ a $E_2$, že jsou od něj ve vzdálenosti jedna, a zároveň si řekne, že jsou na sebe kolmé. Vzdálenosti ve směrech těchto bodů, tj. ve směrech souřadných os jsou dány příslušným poměrem, obecně používá Pythagorovu větu. Odtud vyjde známý vzorec pro velikost vektoru $v = (a, b)$

$$\|v\| = \sqrt{a^2 + b^2}.$$

Jiný možný postup by byl, kdyby pozorovatel vyšel z pojmu vzdálenost (a věděl, co znamená být kolmý, třeba díky Pythagorově větě), zvolil první z vektorů velikosti jedna, zvolil si orientaci (třeba proti směru hodinových ručiček) a vybral jednotkový kolmý směr (jednoznačně určí z požadavku platnosti Pythagorovy věty třeba pomocí pravoúhlého trojúhelníku se stranami o velikostech 3, 4 a 5).

Úhel $\varphi$ dvou vektorů $v, w$ vyjadřujeme pomocí goniometrické funkce $\cos\varphi$, která je dána hodnotou první souřadnice jednotkového vektoru, jehož úhel s vektorem $(1, 0)$ je $\varphi$. Zjevně je pak druhá souřadnice takového vektoru dána reálnou hodnotou $0 \leq \sin\varphi \leq 1$ splňující

$$\cos^2\varphi + \sin^2\varphi = 1.$$

Úhel $\varphi$ dvou vektorů $v, w$ vyjadřujeme pomocí goniometrické funkce $\cos\varphi$, která je dána hodnotou první souřadnice jednotkového vektoru, jehož úhel s vektorem $(1, 0)$ je $\varphi$. Zjevně je pak druhá souřadnice takového vektoru dána reálnou hodnotou $0 \leq \sin\varphi \leq 1$ splňující

$$\cos^2\varphi + \sin^2\varphi = 1.$$

Obecně pak pro dva vektory $v$ a $w$ popisujeme jejich úhel pomocí souřadnic $v = (x(v), y(v))$, $w = (x(w), y(w))$ takto:

$$\cos\varphi = \frac{x(v) \cdot x(w) + y(v) \cdot y(w)}{\|v\| \cdot \|w\|}.$$

# Příklady lineárních zobrazení

Příkladem lineárního zobrazení, které zachovává velikosti, je **rotace kolem počátku** $O$ o předem daný úhel $\psi$. Je dána formulí s maticí $R_\psi$:

$$v = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto R_\psi \cdot v = \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

# Příklady lineárních zobrazení

Příkladem lineárního zobrazení, které zachovává velikosti, je **rotace kolem počátku** $O$ o předem daný úhel $\psi$. Je dána formulí s maticí $R_\psi$:

$$v = \begin{pmatrix} x \\ y \end{pmatrix} \mapsto R_\psi \cdot v = \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

Aplikací na jednotkový vektor $(1, 0)$ dostáváme skutečně právě očekávaný výsledek $(\cos\psi, \sin\psi)$.

**Rotaci kolem jiného bodu** $P = O + w$, snadno napíšeme formulí s pomocí posunutí:

$$\begin{aligned}\begin{pmatrix} x \\ y \end{pmatrix} &= v \mapsto v - w \mapsto R_\psi \cdot (v - w) \\ &\mapsto R_\psi \cdot (v - w) + w \\ &= \begin{pmatrix} \cos\psi(x - x(w)) - \sin\psi(y - y(w)) + x(w) \\ \sin\psi(x - x(w)) + \cos\psi(y - y(w)) + y(w) \end{pmatrix}.\end{aligned}$$

Dalším příkladem je tzv. **zrcadlení vzhledem k přímce**. Opět nám bude stačit popsat zrcadlení vzhledem k přímkám procházejícím počátkem $O$ a ostatní se z nich odvodí pomocí translací. Hledáme matici $Z_\psi$ zrcadlení vzhledem k přímce s jednotkovým směrovým vektorem $v$ svírajícím úhel $\psi$ s vektorem $(1,0)$. Např.

$$Z_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

a obecně můžeme psát (otočíme do nulové polohy, odzrcadlíme a vrátíme zpět)

$$Z_\psi = R_\psi \cdot Z_0 \cdot R_{-\psi}.$$

Díky asociativitě násobení matic spočteme:

$$
\begin{aligned}
Z_\psi &= \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos\psi & \sin\psi \\ -\sin\psi & \cos\psi \end{pmatrix} \\
&= \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \cdot \begin{pmatrix} \cos\psi & \sin\psi \\ -\sin\psi & \cos\psi \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\psi - \sin^2\psi & 2\sin\psi\cos\psi \\ 2\sin\psi\cos\psi & -(\cos^2\psi - \sin^2\psi) \end{pmatrix} \\
&= \begin{pmatrix} \cos 2\psi & \sin 2\psi \\ \sin 2\psi & -\cos 2\psi \end{pmatrix}.
\end{aligned}
$$

Povšimněme si také, že

$$Z_\psi \cdot Z_0 = \begin{pmatrix} \cos 2\psi & \sin 2\psi \\ \sin 2\psi & -\cos 2\psi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos 2\psi & -\sin 2\psi \\ \sin 2\psi & \cos 2\psi \end{pmatrix}.$$

To lze zformulovat jako

**Věta**

*Otočení o úhel $\psi$ obdržíme následným provedením dvou zrcadlení vzhledem ke směrům, které spolu svírají úhel $\frac{1}{2}\psi$.*

Povšimněme si také, že

$$Z_\psi \cdot Z_0 = \begin{pmatrix} \cos 2\psi & \sin 2\psi \\ \sin 2\psi & -\cos 2\psi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos 2\psi & -\sin 2\psi \\ \sin 2\psi & \cos 2\psi \end{pmatrix}.$$

To lze zformulovat jako

**Věta**

*Otočení o úhel $\psi$ obdržíme následným provedením dvou zrcadlení vzhledem ke směrům, které spolu svírají úhel $\frac{1}{2}\psi$.*

Pokud umíme odůvodnit předchozí tvrzení ryze geometrickou úvahou (zkuste), pak jsme takto dokázali standardní formule pro goniometrické funkce dvojnásobného úhlu.

# Použití transformací v praxi – Metapost

```
draw unitsquare scaled s;
draw unitsquare shifted (1,0) scaled s;
k1=fullcircle scaled (s*sqrt(2)) shifted (s/2,s/2);
k2=fullcircle scaled (s*sqrt(5)) shifted (s,s/2);
draw k1; draw k2;
```

# Obsah trojúhelníka

Závěrem úvodního výletu do geometrie se zaměřme na pojem obsah.

Trojúhelník je vymezen dvojicí vektorů $v$ a $w$, které přiloženy do počátku $O$ zadají zbylé dva vrcholy. Chtěli bychom tedy najít formuli (skalární funkci vol), která dvěma vektorům přiřadí číslo rovné obsahu $\operatorname{vol}\Delta(v, w)$ takto definovaného trojúhelníku $\Delta(v, w)$.

Ze zadání je vidět, že by mělo platit

$$\begin{aligned} \operatorname{vol}\Delta(v + v', w) &= \operatorname{vol}\Delta(v, w) + \operatorname{vol}\Delta(v', w) \\ \operatorname{vol}\Delta(av, w) &= a \operatorname{vol}\Delta(v, w) \end{aligned}$$

# Obsah trojúhelníka

Závěrem úvodního výletu do geometrie se zaměřme na pojem obsah.

Trojúhelník je vymezen dvojicí vektorů $v$ a $w$, které přiloženy do počátku $O$ zadají zbylé dva vrcholy. Chtěli bychom tedy najít formuli (skalární funkci vol), která dvěma vektorům přiřadí číslo rovné obsahu $\operatorname{vol}\Delta(v,w)$ takto definovaného trojúhelníku $\Delta(v,w)$. Ze zadání je vidět, že by mělo platit

$$\begin{aligned}\operatorname{vol}\Delta(v+v',w) &= \operatorname{vol}\Delta(v,w)+\operatorname{vol}\Delta(v',w)\\ \operatorname{vol}\Delta(av,w) &= a\operatorname{vol}\Delta(v,w)\end{aligned}$$

a přidejme požadavek

$$\operatorname{vol}\Delta(v,w) = -\operatorname{vol}\Delta(w,v),$$

který odpovídá představě, že opatříme plochu znaménkem podle toho, v jakém pořadí bereme vektory.

Pokud vektory $v$ a $w$ napíšeme do sloupců matice $A$, pak

$$A = (v, w) \mapsto \det A$$

splňuje všechny tři naše požadavky. Kolik takových zobrazení ale může být?

Pokud vektory $v$ a $w$ napíšeme do sloupců matice $A$, pak

$$A = (v, w) \mapsto \det A$$

splňuje všechny tři naše požadavky. Kolik takových zobrazení ale může být?

Každý vektor umíme vyjádřit pomocí dvou souřadných vektorů $v = (1, 0)$ a $w = (0, 1)$ a evidentně tedy každá možnost pro $\operatorname{vol} \Delta$ je jednoznačně určena už vyčíslením na této jediné dvojici argumentů $(v, w)$. Jsou si tedy všechny možnosti rovny až na skalární násobek. Ten umíme určit požadavkem

$$\operatorname{vol} \Delta((1, 0), (1, 0)) = \frac{1}{2},$$

tj. volíme **orientaci** a **měřítko**.

Pokud vektory $v$ a $w$ napíšeme do sloupců matice $A$, pak

$$A = (v, w) \mapsto \det A$$

splňuje všechny tři naše požadavky. Kolik takových zobrazení ale může být?
Každý vektor umíme vyjádřit pomocí dvou souřadných vektorů $v = (1, 0)$ a $w = (0, 1)$ a evidentně tedy každá možnost pro $\operatorname{vol} \Delta$ je jednoznačně určena už vyčíslením na této jediné dvojici argumentů $(v, w)$. Jsou si tedy všechny možnosti rovny až na skalární násobek. Ten umíme určit požadavkem

$$\operatorname{vol} \Delta((1, 0), (1, 0)) = \frac{1}{2},$$

tj. volíme **orientaci** a **měřítko**.
Vidíme tedy, že determinant zadává plochu rovnoběžníka určeného sloupci matice $A$ (a plocha trojúhelníku je tedy poloviční).

# Obsah mnohoúhelníka

Mnohoúhelník rozdělíme na trojúhelníky, jejichž obsahy sečteme (tzv. *triangulace* promyslete si, že je to vždy – i u nekonvexních – možné).

## Poznámka

Úloha o hlídačích v galerii – je možné obarvit vrcholy každé triangulace $n$-úhelníka 3 barvami tak, že žádné 2 sousední nemají tutéž barvu (indukcí).

Předchozí popis hodnot pro orientovaný objem nám dává do rukou elegantní nástroj pro určování viditelnosti orientovaných úseček. Orientovanou úsečkou rozumíme dva body v rovině $\mathbb{R}^2$ s určeným pořadím. Můžeme si ji představovat jako šipku od prvého k druhému bodu. Taková orientovaná úsečka nám rozděluje rovinu na dvě poloroviny, říkejme jim levou a pravou.

Předchozí popis hodnot pro orientovaný objem nám dává do rukou elegantní nástroj pro určování viditelnosti orientovaných úseček. Orientovanou úsečkou rozumíme dva body v rovině $\mathbb{R}^2$ s určeným pořadím. Můžeme si ji představovat jako šipku od prvého k druhému bodu. Taková orientovaná úsečka nám rozděluje rovinu na dvě poloroviny, říkejme jim levou a pravou.

Jestliže uvažujeme obvyklou orientaci proti směru hodinových ručiček pro hranici mnohoúhelníka, pak pozorovatel stojící vně takového mnohoúhelníka některé jeho hrany vidí a některé nevidí. Pokud je daný mnohoúhelník konvexní, tj. jeho hrany zatáčejí pouze doleva, potom pozorovatel vidí právě ty hrany (orientované úsečky), od nichž je napravo.

Je-li $\vec{AB}$ vektor takové orientované úsečky, potom pro bod $C$ ležící napravo od ní platí, že vektory $\vec{CA} = A - C$ a $\vec{CB} = B - C$, které směřují z bodu $C$ do bodů $A$ a $B$, jsou vzájemně orientovány v záporném směru, a proto je jejich jejich

$$\operatorname{vol}\Delta(\vec{CA}, \vec{CB}) < 0, \qquad \text{úsečku } \vec{AB} \text{ z bodu } C \text{ \underline{vidíme}.}$$

Naopak, pro bod $C$ ležící nalevo od $\vec{AB}$ platí, že

$$\operatorname{vol}\Delta(\vec{CA}, \vec{CB}) > 0, \qquad \text{úsečku } \vec{AB} \text{ z bodu } C \text{ \underline{nevidíme}.}$$

Protože je funkce $\operatorname{vol}\Delta$ pouze kladným násobkem funkce $\det A$, kde sloupce matice $A$ jsou vektory $\vec{CA}$, $\vec{CB}$ v tomto pořadí, stačí pouze sledovat znaménka příslušných determinantů. Pro konvexní mnohoúhelník nastanou zřejmě právě 2 znaménkové změny v posloupnosti těchto determinantů.

Je-li $\vec{AB}$ vektor takové orientované úsečky, potom pro bod $C$ ležící napravo od ní platí, že vektory $\vec{CA} = A - C$ a $\vec{CB} = B - C$, které směřují z bodu $C$ do bodů $A$ a $B$, jsou vzájemně orientovány v záporném směru, a proto je jejich jejich

$$\operatorname{vol} \Delta(\vec{CA}, \vec{CB}) < 0, \qquad \text{úsečku } \vec{AB} \text{ z bodu } C \text{ vidíme.}$$

Naopak, pro bod $C$ ležící nalevo od $\vec{AB}$ platí, že

$$\operatorname{vol} \Delta(\vec{CA}, \vec{CB}) > 0, \qquad \text{úsečku } \vec{AB} \text{ z bodu } C \text{ nevidíme.}$$

Protože je funkce $\operatorname{vol} \Delta$ pouze kladným násobkem funkce $\det A$, kde sloupce matice $A$ jsou vektory $\vec{CA}$, $\vec{CB}$ v tomto pořadí, stačí pouze sledovat znaménka příslušných determinantů. Pro konvexní mnohoúhelník nastanou zřejmě právě 2 znaménkové změny v posloupnosti těchto determinantů. Uvedený jednoduchý postup je často využíván pro testování polohy při standardních úlohách v 2D (a podobně pro příslušnou funkci vol v 3D) grafice.

## Příklad

Určete, které hrany jsou vidět z bodu $C = [2, 0]$ pro čtyřúhelník daný vrcholy

$$A = [0, 0], \quad B = [2, 1], \quad D = [3, 3], \quad E = [1, 4].$$

## Příklad

Určete, které hrany jsou vidět z bodu $C = [2, 0]$ pro čtyřúhelník daný vrcholy

$$A = [0, 0], \quad B = [2, 1], \quad D = [3, 3], \quad E = [1, 4].$$

Body jsou již seřazeny v kladném směru a tvoří konvexní čtyřúhelník. Vypočítáme příslušné determinanty

$$|A - C, B - C| = \begin{vmatrix} -2 & 0 \\ 0 & 1 \end{vmatrix} = -2, |B - C, D - C| = \begin{vmatrix} 0 & 1 \\ 1 & 3 \end{vmatrix} = -1,$$

$$|D - C, E - C| = \begin{vmatrix} 1 & -1 \\ 3 & 4 \end{vmatrix} = 7, |E - C, A - C| = \begin{vmatrix} -1 & -2 \\ 4 & 0 \end{vmatrix} = 8.$$

Pororovatel v bodě $C$ tedy vidí pouze první dvě hrany: $\vec{AB}$ a $\vec{BD}$.

## Příklad

Na (nejvýše) kolik částí dělí rovinu $n$ kružnic?
Pro maximální počet $p_n$ oblastí, na které dělí rovinu kružnice, odvodíme rekurentní vzorec

$$p_{n+1} = p_n + 2n$$

$(n+1)$. kružnice totiž protíná $n$ předchozích maximálně v $2n$ průsečících (a tato situace skutečně může nastat). Navíc zřejmě $p_1 = 2$. Pro počet $p_n$ tedy dostáváme

$$p_n = p_{n-1} + 2(n-1) = p_{n-2} + 2(n-2) + 2(n-1) = \cdots = p_1 + \sum_{i=1}^{n-1} 2i$$

$$= 2 + 2\,\frac{n(n-1)}{2} = 2 + n(n-1).$$

Tedy např. 10 kružnic může rozdělit rovinu na nejvýše $p_{10} = 2 + 10.9 = 92$ částí.

# Plán přednášky

V závěrečné části úvodní motivační kapitoly se vrátíme k formálnímu popisu matematických struktur, budeme se je ale průběžně snažit ilustrovat na již známých příkladech. Zároveň můžeme tuto část brát jako cvičení ve formálním přístupu k objektům a konceptům matematiky.

V závěrečné části úvodní motivační kapitoly se vrátíme k formálnímu popisu matematických struktur, budeme se je ale průběžně snažit ilustrovat na již známých příkladech. Zároveň můžeme tuto část brát jako cvičení ve formálním přístupu k objektům a konceptům matematiky.

## Definice

**Binární relací** mezi množinami $A$ a $B$ rozumíme podmnožinu $R$ kartézského součinu $A \times B$. Často píšeme $a \sim_R b$ pro vyjádření skutečnosti, že $(a, b) \in R$, tj. že body $a \in A$ a $b \in B$ jsou v relaci $R$. **Definičním oborem relace** je podmnožina

$$D \subset A, \quad D = \{a \in A; \exists b \in B, (a, b) \in R\}.$$

Podobně **oborem hodnot relace** je podmnožina

$$I \subset B, \quad I = \{b \in B; \exists a \in A, (a, b) \in R\}.$$

Speciálním případem relace mezi množinami je **zobrazení z množiny** $A$ **do množiny** $B$. Je to případ, kdy pro každý prvek definičního oboru relace existuje právě jeden prvek z oboru hodnot, který je s ním v relaci. Nám známým případem zobrazení jsou všechny skalární funkce, kde oborem hodnot zobrazení je množina skalárů, třeba celých nebo reálných čísel. Pro zobrazení zpravidla používáme značení, které jsme také u skalárních funcí zavedli. Píšeme

$$f : D \subset A \to I \subset B, f(a) = b$$

pro vyjádření skutečnosti, že $(a, b)$ patří do relace, a říkáme, že $b$ je hodnotou zobrazení $f$ v bodě $a$.

Dále říkáme, že $f$ je

- zobrazení množiny $A$ do množiny $B$, jestliže je $D = A$,
- zobrazení množiny $A$ **na** množinu $B$, jestliže je $D = A$ a $I = B$, často také **surjektivní zobrazení**
- **injektivní zobrazení**, jestliže je $D = A$ a pro každé $b \in I$ existuje právě jeden **vzor** $a \in A$, $f(a) = b$.

Vyjádření zobrazení $f : A \to B$ jakožto relace $f \subset A \times B, \quad f = \{(a, f(a)); a \in A\}$ známe také pod názvem **graf zobrazení** $f$.

U zobrazení je jasná koncepce, jak se skládají. Máme-li zobrazení $f : A \to B$ a $g : B \to C$, pak jejich **složení** $g \circ f$ je definováno

$$(g \circ f)(a) = g(f(a)).$$

U zobrazení je jasná koncepce, jak se skládají. Máme-li zobrazení $f : A \to B$ a $g : B \to C$, pak jejich **složení** $g \circ f$ je definováno

$$(g \circ f)(a) = g(f(a)).$$

Ve značení používaném pro relace totéž můžeme zapsat jako

$$\begin{aligned} f \subset A \times B, &\quad f = \{(a, f(a)); a \in A\} \\ g \subset B \times C, &\quad g = \{(b, g(b)); b \in B\} \\ g \circ f \subset A \times C, &\quad g \circ f = \{(a, g(f(a))); a \in A\}. \end{aligned}$$

Zcela obdobně definujeme **skládání relací**, v předchozích vztazích jen doplníme existenční kvantifikátory, tj. musíme uvažovat všechny vzory a všechny obrazy.Uvažme relace $R \subset A \times B$, $S \subset B \times C$. Potom

$$S \circ R \subset A \times C, \quad S \circ R = \{(a, c); \exists b \in B, (a, b) \in R, (b, c) \in S\}.$$

Zvláštním případem relace je **identické zobrazení**

$$\mathrm{id}_A = \{(a, a) \in A \times A; a \in A\}$$

na množině $A$. Je neutrální vzhledem ke skládání s každou relací s definičním oborem nebo oborem hodnot $A$.

Pro každou relaci $R \subset A \times B$ definujeme **inverzní relaci**

$$R^{-1} = \{(b, a); (a, b) \in R\} \subset B \times A.$$

Pozor, u zobrazení, je stejný pojem užíván ve specifičtější situaci. Samozřejmě, že existuje pro každé zobrazení jeho invezní relace, ta však nemusí být zobrazením. Zcela logicky proto hovoříme o existenci inverzního zobrazení, pokud každý prvek $b \in B$ je obrazem pro právě jeden vzor v $A$. V takovém případě je samozřejmě inverzní zobrazení právě inverzní relací.

Pro každou relaci $R \subset A \times B$ definujeme **inverzní relaci**

$$R^{-1} = \{(b, a); (a, b) \in R\} \subset B \times A.$$

Pozor, u zobrazení, je stejný pojem užíván ve specifičtější situaci. Samozřejmě, že existuje pro každé zobrazení jeho invezní relace, ta však nemusí být zobrazením. Zcela logicky proto hovoříme o existenci inverzního zobrazení, pokud každý prvek $b \in B$ je obrazem pro právě jeden vzor v $A$. V takovém případě je samozřejmě inverzní zobrazení právě inverzní relací.
Všimněme si, že složením zobrazení a jeho inverzního zobrazení (pokud obě existují) vždy vznikne identické obrazení, u obecných relací tomu tak být nemusí.

## Definice

V případě $A = B$ hovoříme o relaci na množině $A$. Říkáme, že $R$ je:

- **reflexivní**, pokud $\mathrm{id}_A \subset R$ (tj. $(a, a) \in R$ pro všechny $a \in A$),
- **symetrická**, pokud $R^{-1} = R$ (tj. pokud $(a, b) \in R$, pak i $(b, a) \in R$),
- **antisymetrická**, pokud $R^{-1} \cap R \subset \mathrm{id}_A$ (tj. pokud $(a, b) \in R$ a zároveň $(b, a) \in R$, pak $a = b$),
- **tranzitivní**, pokud $R \circ R \subset R$, tj. pokud z $(a, b) \in R$ a $(b, c) \in R$ vyplývá i $(a, c) \in R$.

Relace se nazývá **ekvivalence**, pokud je současně reflexivní, symetrická i tranzitivní. Relace se nazývá **uspořádání** jestliže je reflexivní, tranzitivní a antisymetrická.

Dobrým příkladem uspořádání je inkluze. Uvažme množinu $2^A$ všech podmnožin konečné množiny $A$ (značení je speciálním případem obvyklé notace $B^A$ pro množinu všech zobrazení $A \to B$) a na ní relací $X \subset Z$ danou vlastností být podmnožinou. Evidentně jsou splněny všechny tři vlastnosti pro uspořádání: skutečně, je–li $X \subset Y$ a zároveň $Y \subset X$ musí být nutně množiny $X$ a $Y$ stejné. Je–li $X \subset Y \subset Z$ je také $X \subset Z$ a také reflexivita je zřejmá.

Dobrým příkladem uspořádání je inkluze. Uvažme množinu $2^A$ všech podmnožin konečné množiny $A$ (značení je speciálním případem obvyklé notace $B^A$ pro množinu všech zobrazení $A \to B$) a na ní relací $X \subset Z$ danou vlastností být podmnožinou. Evidentně jsou splněny všechny tři vlastnosti pro uspořádání: skutečně, je–li $X \subset Y$ a zároveň $Y \subset X$ musí být nutně množiny $X$ a $Y$ stejné. Je–li $X \subset Y \subset Z$ je také $X \subset Z$ a také reflexivita je zřejmá. Říkáme, že uspořádání je **úplné**, když pro každé dva prvky platí že jsou **srovnatelné**, tj. buď $a \leq b$ nebo $b \leq a$. Všimněme si, že ne všechny dvojice $(X, Y)$ podmnožin v $A$ jsou srovnatelné v tomto smyslu. Přesněji, pokud je v $A$ více než jeden prvek, existují podmnožiny $X$ a $Y$, kdy není ani $X \subset Y$ ani $Y \subset X$.

Připomeňme rekurentní definici přirozených čísel $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, kde

$$0 = \emptyset, \quad n + 1 = \{0, 1, 2, \dots, n\}.$$

Definujeme relaci $m < n$ právě, když $m \in n$. Evidentně jde o úplné uspořádání. Např. $2 \leq 4$, protože

$$2 = \{\emptyset, \{\emptyset\}\} \subset \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} = 4.$$

Jinak řečeno, samotná rekurentní definice zadává vztah $n \leq n + 1$ a tranzitivně pak $n \leq k$ pro všechna $k$, která jsou tímto postupem definována později.

Každá ekvivalence $R$ na množině $A$ zadává zároveň **rozklad** množiny $A$ na podmnožiny vzájemně ekvivalentních prvků, tzv. **třídy ekvivalance**. Klademe pro libovolné $a \in A$

$$R_a = \{b \in A; (a, b) \in A\}.$$

Často budeme psát pro $R_a$ prostě $[a]$, je-li z kontextu zřejmé, o kterou ekvivalenci jde.

Každá ekvivalence $R$ na množině $A$ zadává zároveň **rozklad** množiny $A$ na podmnožiny vzájemně ekvivalentních prvků, tzv. **třídy ekvivalance**. Klademe pro libovolné $a \in A$

$$R_a = \{b \in A; (a, b) \in A\}.$$

Často budeme psát pro $R_a$ prostě $[a]$, je-li z kontextu zřejmé, o kterou ekvivalenci jde.
Zjevně $R_a = R_b$ právě, když $(a, b) \in R$ a každá taková podmnožina je tedy reprezentována kterýmkoliv svým prvkem, tzv. **reprezentantem**. Zároveň $R_a \cap R_b \neq \emptyset$ právě, když $R_a = R_b$, tj. třídy ekvivalence jsou po dvou disjunktní. Konečně, $A = \cup_{a \in A} R_a$, tj. celá množina $A$ se suktečně rozloží na jednotlivé třídy.
Můžeme také třídám rozkladu rozumět tak, že třídu $[a]$ vnímáme jako prvek $a$ až na ekvivalenci.

# Příklad – konstrukce celých čísel

Na přirozených číslech umíme sice sčítat a víme, že přičtením nuly se číslo nezmění. Umíme i definovat odečítání, při něm ale jen někdy existuje výsledek.

# Příklad – konstrukce celých čísel

Na přirozených číslech umíme sice sčítat a víme, že přičtením nuly se číslo nezmění. Umíme i definovat odečítání, při něm ale jen někdy existuje výsledek.
Základní ideou konstrukce celých čísel z přirozených je tedy přidat k nim chybějící rozdíly. To můžeme udělat tak, že místo výsledku odečítání budeme pracovat s uspořádanými dvojicemi čísel, které nám samozřejmě vždy výsledek dobře reprezentují. Zbývá jen dobře definovat, kdy jsou (z hlediska výsledku odečítání) takové dvojice ekvivalentní. Potřebný vztah tedy je:

$$(a, b) \sim (a', b') \iff a - b = a' - b' \iff a + b' = a' + b.$$

Všimněme si, že zatímco výrazy v prostřední rovnosti v přirozených číslech neumíme, výrazy v pravo už ano. Snadno ověříme, že skutečně jde o ekvivalenci a její třídy označíme jako celá čísla $\mathbb{Z}$.

Na třídách ekvivalence definujeme operaci sčítání (a s ní i odečítání) pomocí reprezentantů. Např.

$$[(a, b)] + [(c, d)] = [(a + c, b + d)],$$

což zjevně nezávisí na výběru reprezentantů. Lze si přitom vždy volit reprezentanty $(a, 0)$ pro kladná čísla a reprezentanty $(0, a)$ pro čísla záporná, se kterými se nám bude patrně počítat nejlépe.

Na třídách ekvivalence definujeme operaci sčítání (a s ní i odečítání) pomocí reprezentantů. Např.

$$[(a, b)] + [(c, d)] = [(a + c, b + d)],$$

což zjevně nezávisí na výběru reprezentantů. Lze si přitom vždy volit reprezentanty $(a, 0)$ pro kladná čísla a reprezentanty $(0, a)$ pro čísla záporná, se kterými se nám bude patrně počítat nejlépe. Tento jednoduchý překlad ukazuje, jak důležité je umět nahlížet na třídy ekvivalence jako na celistvý objekt a soustředit se na vlastnosti těchto objektů, nikoliv formální popisy jejich konstrukcí. Ty jsou však důležité k ověření, že takové objekty vůbec existují.

U celých čísel nám už platí všechny vlastnosti skalárů (KG1)–(KG4) a (O1)-(O4), z popisu vlastností skalárů. Pro násobení je neutrálním prvkem jednička, ale pro všechna čísla $a$ různá od nuly a jedničky neumíme najít číslo $a^{-1}$ s vlastností $a \cdot a^{-1} = 1$, tzn. chybí nám inverzní prvky. Zároveň si povšimněte, že platí vlastnost oboru integrity (OI), tzn. je-li součin dvou čísel nulový, musí být alespoň jedno z nich nula.

U celých čísel nám už platí všechny vlastnosti skalárů (KG1)–(KG4) a (O1)-(O4), z popisu vlastností skalárů. Pro násobení je neutrálním prvkem jednička, ale pro všechna čísla $a$ různá od nuly a jedničky neumíme najít číslo $a^{-1}$ s vlastností $a \cdot a^{-1} = 1$, tzn. chybí nám inverzní prvky. Zároveň si povšimněte, že platí vlastnost oboru integrity (OI), tzn. je-li součin dvou čísel nulový, musí být alespoň jedno z nich nula.
Díky poslední jmenované vlastnosti můžeme zkonstruovat racionální čísla $\mathbb{Q}$ přidáním všech chybějících inverzí zcela obdobným způsobem, jak jsme konstruovali $\mathbb{Z}$ z $\mathbb{N}$.

# Příklad – konstrukce racionálních čísel

Na množině uspořádáných dvojic $(p, q)$, $q \neq 0$, celých čísel definujeme relaci $\sim$ tak, jak očekáváme, že se mají chovat podíly $p/q$:

$$(p, q) \sim (p', q') \quad \Longleftrightarrow \quad p/q = p'/q' \quad \Longleftrightarrow \quad p \cdot q' = p' \cdot q.$$

# Příklad – konstrukce racionálních čísel

Na množině uspořádáných dvojic $(p, q)$, $q \neq 0$, celých čísel definujeme relaci $\sim$ tak, jak očekáváme, že se mají chovat podíly $p/q$:

$$(p, q) \sim (p', q') \iff p/q = p'/q' \iff p \cdot q' = p' \cdot q.$$

Opět neumíme očekávané chování v prostřední rovnosti v množině $\mathbb{Z}$ formulovat, nicméně rovnost na pravé straně ano. Zjevně jde o dobře definovanou relaci ekvivalence (ověřte podrobnosti!) a racionální čísla jsou pak její třídy ekvivalence. Když budeme formálně psát $p/q$ místo dvojic $(p, q)$, budeme definovat operace násobení a sčítání právě pomocí formulí, které nám jsou jistě dobře známy.

# Příklad – zbytkové třídy

Jiným dobrým a jednoduchým příkladem jsou tzv. zbytkové třídy celých čísel. Pro pevně zvolené přirozené číslo $k$ definujeme equivalenci $\sim_k$ tak, že dvě čísla $a$, $b \in \mathbb{Z}$ jsou ekvivalentní, jestliže jejich zbytek po dělení číslem $k$ je stejný. Výslednou množinu tříd ekvivalence označujeme $\mathbb{Z}_k$.

# Příklad – zbytkové třídy

Jiným dobrým a jednoduchým příkladem jsou tzv. zbytkové třídy celých čísel. Pro pevně zvolené přirozené číslo $k$ definujeme equivalenci $\sim_k$ tak, že dvě čísla $a, b \in \mathbb{Z}$ jsou ekvivalentní, jestliže jejich zbytek po dělení číslem $k$ je stejný. Výslednou množinu tříd ekvivalence označujeme $\mathbb{Z}_k$.
Nejjednodušší je tato procedura pro $k = 2$. To dostáváme $\mathbb{Z}_2 = \{0, 1\}$, kde nula reprezentuje sudá čísla, zatímco jednička čísla lichá. Opět lze snadno zjistit, že pomocí reprezentantů můžeme definovat násobení a sčítání. Zkuste si ověřit, že výsledná množina skalárů je komutativním tělesem (tj. splňuje i vlastnost (P) pole) právě když je $k$ prvočíslo.