G

$$\begin{tikzcd}
& AB \arrow[dl, dash] \arrow[dr, dash, "AB/B"] & \\
A \arrow[dr, dash, swap, "A/A\cap B"] \arrow[rr, phantom, "\cong"] & & B \arrow[dl, dash] \\
& A \cap B &
\end{tikzcd}$$

$A, B \triangleleft G$

$A \leq B \overset{?}{\Longrightarrow} A \triangleleft B$

$\forall g \in G\ \forall a \in A \quad gag^{-1} \in A$ ✓

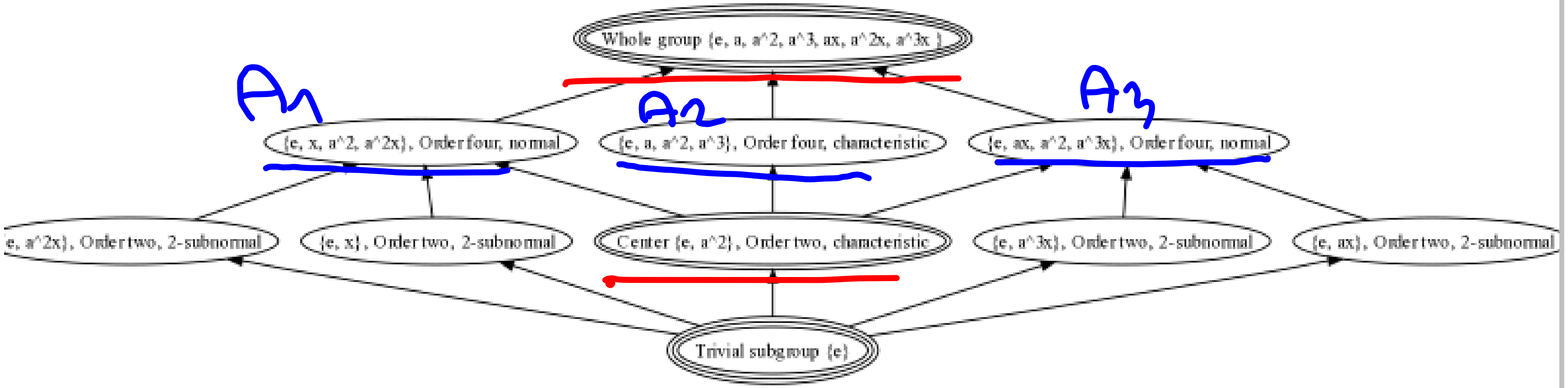
? $\forall b \in B\ \forall a \in A \quad bab^{-1} \in A$ ✓

zřejmé

NIKOLIV

$A \triangleleft B \triangleleft G \not\Rightarrow A \triangleleft G$

Př: D_8: $\langle s \rangle \triangleleft \langle s, r^2 \rangle \triangleleft D_8$ $\quad \langle s \rangle \ntriangleleft D_8$ $\quad rsr^{-1} = r^2 s \notin \{id, s\}$



$D_8/\langle r^2\rangle \Rightarrow$ 3 vlastní podgrupy

$A_1/\langle r^2\rangle,\ A_2/\langle r^2\rangle,\ A_3/\langle r^2\rangle$

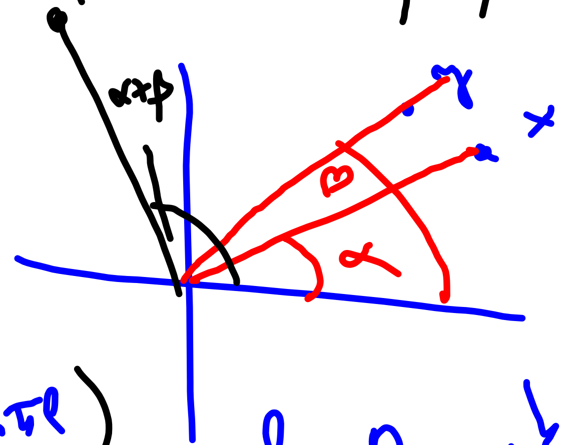
řádu 4

$\Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ Kleinova 4grupa

$$x = |x|(\cos\alpha + i\sin\alpha)$$

$$y = |y|(\cos\beta + i\sin\beta)$$

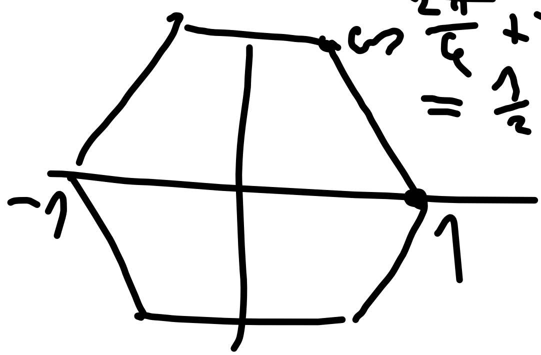
$$x \cdot y = |x||y|(\cos(\alpha+\beta) + i\sin(\alpha+\beta))$$



$$x^k = |x|^k(\cos k\alpha + i\sin k\alpha)$$

$$\sqrt[k]{x} = \sqrt[k]{|x|}\left(\cos\frac{\alpha+2\pi l}{k} + i\sin\frac{\alpha+2\pi l}{k}\right)$$

$l = 0, \dots, k-1$



$$\cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$$

• $0 \cdot c = 0$

$(0+0)\cdot c = 0\cdot c$

$\parallel$ distr.

$0\cdot c + 0\cdot c = 0 \cdot c \quad \Big| -(0\cdot c)$

$0\cdot c = 0$

• $-c = (-1)\cdot c$

dkaz.: $(-1)\cdot c + c \overset{?}{=} 0$

$(-1)\cdot c + c \overset{ax.}{=} (-1)\cdot c + 1\cdot c \overset{distr.}{=} (-1+1)\cdot c =$

$= 0 \cdot c = 0.$ ③ ④ analogicky

Př: nejednoznačnost podílu

$(\mathbb{Z}_6, +, \cdot)$

$[2] = [2] \cdot [1]$

$[2] = [2][4]$

$[1] \neq [4]$

Př: inverze v $\mathbb{Z}_p$

(1) $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$

$b = a^{p-2} \Rightarrow a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod p$

(2) $(a,p) = 1 \Rightarrow \exists\, m, n \in \mathbb{Z} : a \cdot m + p \cdot n = 1 \Rightarrow a \cdot m \equiv 1 \ (p)$

Věta Každé těleso je obor integrity

Dk. sporem $a, b \neq 0$ $a \cdot b = 0$

$\exists\, a^{-1}$ (těleso) : $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$

$b = 0$

spor,

Věta

Každý konečný obor integrity je těleso.

Důkaz.

Dokazuje se prostřednictvím homomorfismu $f : R \to R$, $f(x) = ax$ (je to injekce, proto surjekce, proto je R těleso (rozmyslete!). $\square$

a pevné $\quad x \mapsto a\cdot x$

$a \neq 0$ $\quad$ (změní $a^{-1} \mapsto a \cdot a^{-1} = 1$)

stačí dokázat, že jde o injekci:

$a\cdot x = a\cdot y \Leftrightarrow a\cdot x - a\cdot y = 0 \Leftrightarrow a\cdot(x-y) = 0$

$a \neq 0$, OI

$\Rightarrow x - y = 0 \Leftrightarrow x = y$

$1-x \in R[[x]]$

$$(1-x)^{-1} = \frac{1}{1-x} = 1+x+x^2+x^3+\dots$$

$(R[[x]])^\times$ .. jednotky

$a_0+a_1x+a_2x^2+\dots$

$a_0 \in R^\times$

- $e \in R^\times$, $a \in R$

$$a = e \cdot (e^{-1} \cdot a)$$

$$[e \mid 1,\ 1 \mid a \Rightarrow e \mid a]$$

- asociované prvky

$$a \sim b \Leftrightarrow \exists e \in R^\times : a = b \cdot e$$

Př.: ① v $\mathbb{Z}$: $\mathbb{Z}^\times = \{1, -1\}$

$$2 \sim -2$$

② v $\mathbb{Z}[i]$: $(\mathbb{Z}[i])^\times = \{1, -1, i, -i\}$

$a, b \neq 0$

$$\alpha \sim \beta \Leftrightarrow \alpha = \pm\beta,\ \alpha = \pm\beta i$$

$b = 0 \Rightarrow a = \pm 1$

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i \in \mathbb{Z}[i] \Leftrightarrow$$

$a^2+b^2 > |a|, |b|$

$a = 0 \Rightarrow b = \pm 1$