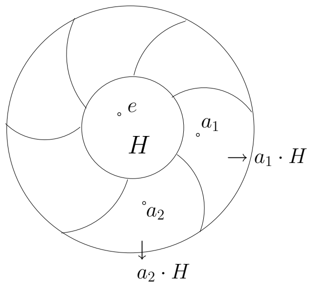
Rozklady podle grup

Je dána grupa $(\mathbb{G},\cdot)$ a její podgrupa $(\mathbb{H},\cdot)$. Definujeme relaci $a \sim b$, jestliže $b^{-1}\cdot a \in \mathbb{H}$ nebo $a^{-1}\cdot b \in \mathbb{H}$. Jedná se o relaci ekvivalence. Pak se grupa $(\mathbb{G},\cdot)$ rozpadá na **třídy ekvivalence = levé třídy rozkladu podle grupy** $(\mathbb{H},\cdot)$.

- Třída příslušná prvku a: $a\cdot\mathbb{H} = \{a\cdot h;\ h\in\mathbb{H}\}$
- Množinu všech levých tříd rozkladu podle podgrupy $(\mathbb{H},\cdot)$ značíme
$$G/H = \{\mathbb{H}, a_1\cdot\mathbb{H}, a_2\cdot\mathbb{H},\dots\}$$
- Třídy rozkladu (kromě podgrupy $(\mathbb{H},\cdot)$) nejsou grupy.
- Obdobně definujeme **pravé třídy rozkladu** $\mathbb{H}\cdot a$; příslušná ekvivalence $a\sim b$ je $a\cdot b^{-1}\in\mathbb{H}$; $G\backslash H = \{\mathbb{H}\cdot a; a\in\mathbb{G}\}$.



Normální podgrupa $\mathbb{H}\lhd\mathbb{G}$
Pro $\forall a\in\mathbb{G};\forall h\in\mathbb{H}$ platí $a\cdot h\cdot a^{-1}\in\mathbb{H}$, neboli $a\cdot\mathbb{H} = \mathbb{H}\cdot a$ (pravé a levé třídy rozkladu se splývají).

- $\{e\}\lhd\mathbb{G},\ \mathbb{G}\lhd\mathbb{G}$;
- v komutativní grupě je každá normální;
- je-li počet prvků v $\mathbb{H}$ poloviční oproti $\mathbb{G}$, pak je $\mathbb{H}$ normální;
- jádra homomorfismů jsou normální podgrupy;
- $(\mathbb{G}/\mathbb{H},\cdot)$ - **faktorgrupa**, kde platí $\forall a\cdot\mathbb{H}, b\cdot\mathbb{H}\in\mathbb{G}/H;\ (a\cdot\mathbb{H})\cdot(b\cdot\mathbb{H}) = (a\cdot b)\cdot\mathbb{H}$.

1. Pro dihedrální grupu D_8 (grupa symetrií čtverce) najděte všechny podgrupy, určete které jsou normální a popište příslušnou faktorgrupu.
2. Popište rozklad $\mathbb{Z}/k\mathbb{Z}$.
3. Popište rozklad $\mathbb{C}^*/\mathrm{Ker}f$, kde $f:\mathbb{C}^*\to\mathbb{R}^*$ je homomorfismus daný vztahem $f(a+bi) = a^2+b^2$, tedy $f(z) = |z|^2$.

Okruhy a tělesa

$(\mathbb{M}, +)$ je komutativní grupa s neutrálním prvkem $0 \in \mathbb{M}$, spolu s další operací $\cdot$ splňující:

(a) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, pro $\forall a, b, c \in \mathbb{M}$;

(b) $a \cdot b = b \cdot a$, pro $\forall a, b \in \mathbb{M}$;

(c) $\exists 1 \in \mathbb{M};\ \forall a \in \mathbb{M};\ 1 \cdot a = a$;

(d) $a \cdot (b + c) = a \cdot b + a \cdot c$, pro $\forall a, b, c \in \mathbb{M}$ (distributivnost);

tvoří komutativní **okruh** $(\mathbb{M}, +, \cdot)$.

- Pokud neplatí (b), pak se jedná o nekomutativní okruh.
- Prvku 0 říkáme nula a 1 jednička.
- Prvky $a, b \in \mathbb{M}$ takové, že:

$$a \neq 0 \wedge b \neq 0 \wedge a \cdot b = 0$$

  se nazývají **dělitelé nuly**.
- Okruh $(\mathbb{M}, +, \cdot)$ se nazývá **obor integrity**, právě když pro libovolné prvky $c, d \in \mathbb{M}$ platí:

$$c \cdot d = 0 \Leftrightarrow c = 0 \vee d = 0.$$

- Dělitelé jedničky, tj. invertibilní prvky, nazýváme **jednotky**.
- Okruh, ve kterém jsou všechny nenulové prvky invertibilní, se nazývá **těleso**.
- Komutativní těleso se nazývá **pole**.

4. Nechť X je libovolná neprázdná množina. Rozhodněte, žda $(\mathcal{P}(X), \div, \cap)$ tvoří komutativní okruh, obor integrity, těleso.

5. Rozhodněte, zda $(M, \heartsuit, \star)$ tvoří komutativní okruh, obor integrity, těleso:

   (a) $M = \mathbb{Z}$; $a \heartsuit b = a + b - 1, a \star b = a + b - ab$;

   (b) $M = \mathbb{Q}$; $a \heartsuit b = a + b + 1, a \star b = a + b + ab$;

   (c) $M = \mathbb{Q}$; $a \heartsuit b = a + b - 1, a \star b = a + b + ab$