Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow\ a \in b \cdot H \ \Leftrightarrow\ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa. Zobrazení $\pi: G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro* $\ker \pi = H$.

Definice. Grupa G/H z předchozí věty se nazývá **faktorgrupa** grupy G podle (normální) podgrupy H. Homomorfismus π se nazývá **projekce grupy G na faktorgrupu G/H.**

Faktorizace okruhů

Nechť $(R, +, \cdot)$ je okruh, I jeho ideál. Pak I je (normální) podgrupa komutativní grupy $(R, +)$, máme tedy faktorgrupu $(R/I, +)$, přičemž $R/I = \{a + I;\ a \in R\}$, kde $a + I = \{a + h;\ h \in I\}$.

Platí $\forall a, b \in R:\quad (a + I = b + I \ \Leftrightarrow\ a \in b + I \ \Leftrightarrow\ a - b \in I)$,

a operace $+$ na R/I je definována pomocí reprezentantů:
$(a + I) + (b + I) = (a + b) + I$ pro každé $a, b \in R$.

Věta. Nechť I je ideál okruhu R. Na faktorgrupě $(R/I, +)$ lze definovat násobení pomocí reprezentantů, tedy
$(a + I) \cdot (b + I) = (a \cdot b) + I$ pro každé $a, b \in R$. Pak $(R/I, +, \cdot)$ je okruh a projekce $\pi : R \to R/I$ je surjektivním homomorfismem okruhů s jádrem $\ker \pi = I$.

Definice. Okruh R/I z předchozí věty se nazývá **faktorokruh** okruhu R podle ideálu I. Homomorfismu π říkáme **projekce okruhu R na faktorokruh R/I.**

Důsledek. *Ideály okruhu R jsou právě jádra homomorfismů $R \to K$ okruhu R do vhodných okruhů K.*

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$, a proto pro libovolné $a \in \mathbb{Z}$ je $a + (m) = \{a + k \cdot m;\ k \in \mathbb{Z}\} = [a]_m$. Tudíž faktorokruh $\mathbb{Z}/(m) = \mathbb{Z}_m$, okruh zbytkových tříd modulo m.

Věta. Nechť I je ideál okruhu R. Pak platí:

1. je-li R komutativní okruh, pak je R/I komutativní okruh;
2. R/I je triviální okruh, právě když $R = I$.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je maximální ideál okruhu R, jestliže $R \neq I$ a současně neexistuje žádný ideál J okruhu R splňující $I \subsetneq J \subsetneq R$.

Poznámka. Množina všech ideálů daného okruhu R tvoří vzhledem k inkluzi úplný svaz. Odstraněním největšího ideálu, čímž je R, nám zůstane uspořádaná množina. Maximální ideály okruhu R jsou právě maximální prvky v této uspořádané množině.

Maximální ideály, prvoideály

Věta. Nechť I je ideál **komutativního** okruhu R. Pak faktorokruh R/I je těleso, právě když I je maximální ideál okruhu R.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je prvoideál okruhu R, jestliže $R \neq I$ a současně pro libovolné prvky $a, b \in R$ platí implikace $a \cdot b \in I \implies a \in I$ nebo $b \in I$.

Věta. *Nechť I je ideál* **komutativního** *okruhu R. Pak faktorokruh R/I je obor integrity, právě když I je prvoideál okruhu R.*

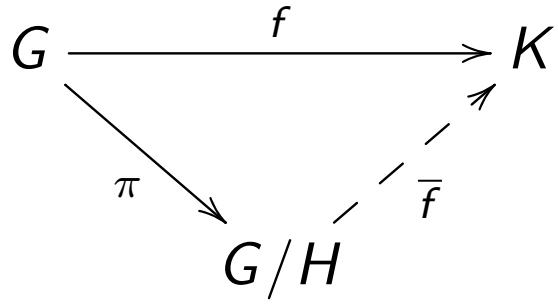
Důsledek. Jestliže I je maximální ideál komutativního okruhu R, pak I je prvoideál okruhu R.

Věta. *Nechť R je těleso a $f \in R[x]$, $f \neq 0$, následující výroky jsou ekvivalentní:*

1. (f) *je maximální ideál okruhu* $R[x]$;
2. (f) *je prvoideál okruhu* $R[x]$;
3. f *je ireducibilní polynom nad* R.

Opakování: Hlavní věta o faktorgrupách

Věta (Hlavní věta o faktorgrupách). Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H.
Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.



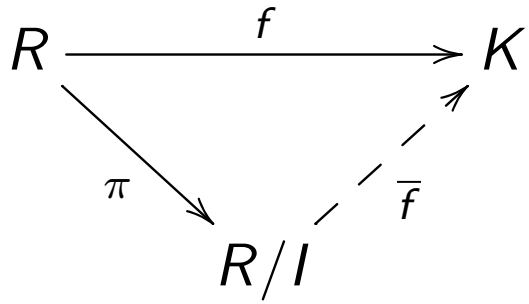
Navíc platí:

- $\overline{f}$ *je homomorfismus grup,*
- $\overline{f}$ *je injekce, právě když* $H = \ker f$,
- $\overline{f}$ *je surjekce, právě když* f *je surjekce.*

Důsledek. Je-li $f : G \to K$ surjektivní homomorfismus grup, pak platí $G/(\ker f) \cong K$.

Hlavní věta o faktorokruzích

Věta (Hlavní věta o faktorokruzích). Nechť $f : R \to K$ je homomorfismus okruhů, I ideál okruhu R splňující $I \subseteq \ker f$. Nechť $\pi : R \to R/I$ je projekce okruhu R na faktorokruh R/I. Pak existuje, a to jediné, zobrazení $\overline{f} : R/I \to K$ splňující $\overline{f} \circ \pi = f$.



Navíc platí:

- $\overline{f}$ *je homomorfismus okruhů,*
- $\overline{f}$ *je injekce, právě když* $I = \ker f$,
- $\overline{f}$ *je surjekce, právě když* f *je surjekce.*

Důsledek. Je-li $f : R \to K$ surjektivní homomorfismus okruhů, pak platí $R/(\ker f) \cong K$.