Domácí úloha ze dne 18. října 2013

Nechť $\varphi : R \to S$ je surjektivní homomorfismus okruhů. Nechť $\mathcal{I}_S$ značí množinu všech ideálů okruhu S a $\mathcal{I}_{R,\varphi}$ značí množinu všech ideálů I okruhu R splňujících $\ker\varphi \subseteq I$.

- Vysvětlete, proč $(\mathcal{I}_{R,\varphi}, \subseteq)$ a $(\mathcal{I}_S, \subseteq)$ jsou úplné svazy.
- Dokažte, že tyto svazy jsou izomorfní.

Řešení. Ideál S okruhu S je největším prvkem uspořádané množiny $(\mathcal{I}_S, \subseteq)$. Libovolná neprázdná podmnožina M množiny $\mathcal{I}_S$ má v této uspořádané množině infimum, kterým je průnik $\bigcap_{I\in M} I$, neboť průnik libovolného neprázdného systému ideálů okruhu S je opět ideálem okruhu S; zřejmě je to největší ze všech ideálů okruhu S, které jsou podmnožinou každého ideálu $I \in M$. Podle věty o úplných svazech odtud dostáváme, že $(\mathcal{I}_S, \subseteq)$ je úplný svaz.

Podobně se dokáže, že $(\mathcal{I}_{R,\varphi}, \subseteq)$ je úplný svaz, stačí si jen navíc uvědomit, že pro libovolnou neprázdnou podmnožinu M množiny $\mathcal{I}_{R,\varphi}$ platí $\ker\varphi \subseteq I$ pro každý ideál $I \in M$, a tedy $\ker\varphi \subseteq \bigcap_{I\in M} I$.

Protože $\varphi : R \to S$ je surjektivní homomorfismus okruhů, podle věty z přednášky víme, že pro každý ideál I okruhu R je

$$\varphi(I) = \{\varphi(a) \mid a \in I\}$$

ideálem okruhu S. Můžeme tedy definovat zobrazení $\Phi : \mathcal{I}_{R,\varphi} \to \mathcal{I}_S$ předpisem $\Phi(I) = \varphi(I)$ pro každý ideál $I \in \mathcal{I}_{R,\varphi}$.

Podobně pro každý ideál J okruhu S je

$$\varphi^{-1}(J) = \{r \in R \mid \varphi(r) \in J\} \tag{1}$$

ideálem okruhu R, přičemž z $0 \in J$ plyne $\ker\varphi \subseteq \varphi^{-1}(J)$. Můžeme tedy definovat zobrazení $\Psi : \mathcal{I}_S \to \mathcal{I}_{R,\varphi}$ předpisem $\Psi(J) = \varphi^{-1}(J)$ pro každý ideál $J \in \mathcal{I}_S$.

Ukažme, že Φ i Ψ jsou izotonní zobrazení. Jsou-li $I_1, I_2 \in \mathcal{I}_{R,\varphi}$ takové, že $I_1 \subseteq I_2$, pak

$$\Phi(I_1) = \varphi(I_1) = \{\varphi(a) \mid a \in I_1\} \subseteq \{\varphi(a) \mid a \in I_2\} = \varphi(I_2) = \Phi(I_2).$$

Jsou-li $J_1, J_2 \in \mathcal{I}_S$ takové, že $J_1 \subseteq J_2$, pak

$$\begin{aligned}\Psi(J_1) = \varphi^{-1}(J_1) = \{r \in R \mid \varphi(r) \in J_1\} \subseteq \\ \subseteq \{r \in R \mid \varphi(r) \in J_2\} = \varphi^{-1}(J_2) = \Psi(J_2).\end{aligned}$$

Dokažme, že $\Psi \circ \Phi$ je identita na množině $\mathcal{I}_{R,\varphi}$. Pro libovolný ideál $I \in \mathcal{I}_{R,\varphi}$ tedy musíme dokázat $\Psi(\Phi(I)) = I$. Promyslete si, proč je následující výpočet chybný (pokud na to nepřijdete, podívejte se dolů[1])

$$\Psi(\Phi(I)) = \varphi^{-1}(\varphi(I)) = (\varphi^{-1} \circ \varphi)(I) = \mathrm{id}(I) = I.$$

Musíme tedy postupovat jinak, platí

$$\Psi(\Phi(I)) = \varphi^{-1}(\varphi(I)) = \{r \in R \mid \varphi(r) \in \varphi(I)\}.$$

Je-li $a \in I$, pak $\varphi(a) \in \varphi(I)$, a tedy $a \in \Psi(\Phi(I))$. Naopak, je-li $r \in \Psi(\Phi(I))$, pak existuje $b \in I$ tak, že $\varphi(r) = \varphi(b)$, tj. $\varphi(r - b) = \varphi(r) - \varphi(b) = 0$, a tedy $r - b \in \ker \varphi \subseteq I$. Protože I je ideál, platí $r = (r - b) + b \in I$. Dokázali jsme $\Psi(\Phi(I)) = I$.

Nyní dokažme, že $\Phi \circ \Psi$ je identita na množině $\mathcal{I}_S$. Pro libovolný ideál $J \in \mathcal{I}_S$ tedy musíme dokázat $\Phi(\Psi(J)) = J$. Platí

$$\Phi(\Psi(J)) = \varphi(\varphi^{-1}(J)) = \varphi(\{r \in R \mid \varphi(r) \in J\}) = \{\varphi(r) \mid r \in R,\ \varphi(r) \in J\}.$$

Zřejmě tedy $\Phi(\Psi(J)) \subseteq J$. Naopak zvolme libovolné $a \in J$. Protože je φ surjekce, existuje $r \in R$ splňující $\varphi(r) = a$, a tedy $a \in \Phi(\Psi(J))$. Celkem $\Phi(\Psi(J)) = J$.

Dokázali jsme, že Φ a Ψ jsou navzájem inverzní bijekce. Protože Φ i $\Phi^{-1} = \Psi$ jsou izotonní zobrazení, je Φ izomorfismus uspořádaných množin. Podle věty z kapitoly o svazech víme, že pak Φ je izomorfismus svazů.

[1] Jestliže φ není bijekce, neexistuje inverzní zobrazení φ^{-1}, proto ani nemůžeme psát φ^{-1} ani počítat $\varphi^{-1} \circ \varphi = \mathrm{id}$. Lze jen počítat úplný vzor libovolné podmnožiny oboru hodnot, což jsme také v (1) dělali.