

Okruhem budeme rozumět komutativní okruh s jedničkou.

Příklad 1. Bud' A okruh, $a \in A$. Dokažte, že $A[a^{-1}] \cong A[t]/(at - 1)$.

Lemma. Bud' A okruh, $I = (at - 1)$ ideál okruhu $A[t]$. Pak pro každé $k \in \mathbb{N}_0$ platí $a^k t^k - 1 \in I$.

Důkaz lemmatu. Pro $k = 0$ je tvrzení zřejmé. Pro $k \in \mathbb{N}$ máme

$$a^k t^k - 1 = (at - 1) \cdot (a^{k-1} t^{k-1} + a^{k-2} t^{k-2} + \dots + at + 1) \in I,$$

vždyť $at - 1 \in I$ a $a^{k-1} t^{k-1} + a^{k-2} t^{k-2} + \dots + at + 1 \in A[t]$.

Důkaz. Prvky okruhu $A[a^{-1}]$ jsou tvaru $[b, s] = \frac{b}{s}$, kde $b \in A$, $s = a^n$ pro $n \in \mathbb{N}_0$. Budeme chtít zkonstruovat zobrazení do okruhu $A[t]/(at - 1)$. Označme $I = (at - 1)$. Ve faktorokruhu můžeme intuitivně chápat $at - 1 = 0$, tj. $t = \frac{1}{a}$. Je proto přirozené uvážit následující zobrazení:

$$\begin{aligned} \varphi: A[a^{-1}] &\rightarrow A[t]/I, \\ \varphi: \frac{b}{a^n} &\mapsto b \cdot t^n + I. \end{aligned}$$

Budeme chtít ukázat, že zobrazení dané tímto předpisem je izomorfismus okruhů.

- Korektnost: Necht' $\frac{b_1}{a^{n_1}} = \frac{b_2}{a^{n_2}}$. To z definice $A[a^{-1}]$ znamená, že

$$\exists k \in \mathbb{N}_0: (b_1 a^{n_2} - b_2 a^{n_1}) a^k = 0.$$

Chceme ukázat, že oba prvky zobrazíme na stejnou třídu, tj. $\varphi\left(\frac{b_1}{a^{n_1}}\right) - \varphi\left(\frac{b_2}{a^{n_2}}\right) = 0 + I$.

$$\begin{aligned} \varphi\left(\frac{b_1}{a^{n_1}}\right) - \varphi\left(\frac{b_2}{a^{n_2}}\right) &= b_1 t^{n_1} - b_2 t^{n_2} + I = \\ &= b_1 t^{n_1} + b_1 t^{n_1} \cdot (a^{n_2+k} t^{n_2+k} - 1) - b_2 t^{n_2} - b_2 t^{n_2} \cdot (a^{n_1+k} t^{n_1+k} - 1) + I = \\ &= t^{n_1+n_2+k} (b_1 a^{n_2} - b_2 a^{n_1}) a^k + I = 0 + I. \end{aligned}$$

vždyť díky lemmatu platí: $b_1 t^{n_1} \cdot (a^{n_2+k} t^{n_2+k} - 1) \in I$ a $b_2 t^{n_2} \cdot (a^{n_1+k} t^{n_1+k} - 1) \in I$.

- Homomorfismus okruhů: Zřejmě $\varphi(1) = \varphi\left(\frac{1}{a^0}\right) = 1 + I$. Dále

$$\varphi\left(\frac{b_1}{a^{n_1}}\right) \cdot \varphi\left(\frac{b_2}{a^{n_2}}\right) = (b_1 t^{n_1} + I) \cdot (b_2 t^{n_2} + I) = b_1 t^{n_1} \cdot b_2 t^{n_2} + I = \varphi\left(\frac{b_1}{a^{n_1}} \cdot \frac{b_2}{a^{n_2}}\right).$$

A konečně

$$\begin{aligned} \varphi\left(\frac{b_1}{a^{n_1}}\right) + \varphi\left(\frac{b_2}{a^{n_2}}\right) &= (b_1 t^{n_1} + I) + (b_2 t^{n_2} + I) = b_1 t^{n_1} + b_2 t^{n_2} + I = \\ &= b_1 t^{n_1} + b_1 t^{n_1} \cdot (a^{n_2} t^{n_2} - 1) + b_2 t^{n_2} + b_2 t^{n_2} \cdot (a^{n_1} t^{n_1} - 1) + I = \\ &= b_1 a^{n_2} t^{n_1+n_2} + b_2 a^{n_1} t^{n_1+n_2} = \varphi\left(\frac{b_1 a^{n_2} + b_2 a^{n_1}}{a^{n_1+n_2}}\right) = \varphi\left(\frac{b_1}{a^{n_1}} + \frac{b_2}{a^{n_2}}\right). \end{aligned}$$

- Injekce: φ je injektivní právě tehdy, když $\ker \varphi = \{0\}$. Nechť tedy $\varphi\left(\frac{b}{a^n}\right) = 0$. To nastává právě tehdy, když $bt^n \in I$. Proto existuje polynom $f \in A[t]$ takový, že $f \cdot (at - 1) = bt^n$. Je-li $b = 0$, pak lze vzít $f = 0$.

Nechť $b \neq 0$. Díky speciálnímu tvaru polynomu na pravé straně dostáváme, že vedoucí koeficient f a a jsou dělitelé nuly (jistě 1 není dělitel nuly, takže člen at musí zmizet po vynásobení vedoucím koeficientem polynomu f). Odtud $f = -bt^n$, přitom $ab = 0$. Tento fakt nám už stačí k tomu, abychom ukázali, že $\frac{b}{a^n} = 0 = \frac{0}{1}$. To je z definice právě tehdy, když existuje $k \in \mathbb{N}_0$ takové, že

$$(b \cdot 1 - 0 \cdot a^n)a^k = 0.$$

Stačí zvolit $k = 1$, což spolu s $ab = 0$ dává, že $\ker \varphi = \{0\}$.

- Surjekce: Buď $f = b_nt^n + \dots + b_1t + b_0 \in A[t]$ libovolný. Jistě

$$\varphi\left(\frac{b_n}{a^n} + \dots + \frac{b_1}{a^1} + \frac{b_0}{a^0}\right) = \varphi\left(\frac{b_n}{a^n}\right) + \dots + \varphi\left(\frac{b_1}{a^1}\right) + \varphi\left(\frac{b_0}{a^0}\right) = f + I.$$

Zobrazení φ je tedy izomorfismus okruhů.

Příklad 2. Buď A okruh, I jeho ideál. Dokažte, že

$$(A/I)[t] \cong A[t]/J$$

pro vhodný ideál J okruhu $A[t]$. Tento ideál J určete.

Důkaz. Jistě $I \subseteq A \subseteq A[t]$. Můžeme proto uvážit ideál $J \subseteq A[t]$ jako ideál generovaný množinou I , jedná se tedy o nejmenší ideál obsahující I . Přitom platí

$$J = \{f \in A[t] \mid f = a_n t^n + \cdots + a_1 t + a_0, \ a_n, \dots, a_0 \in I\}.$$

Jistě tato množina obsahuje I a zároveň každý polynom s koeficienty z I lze pomocí I vygenerovat (v této množině není nic navíc). Jistě je tato množina ideálem. Výše napsaná rovnost tedy platí.

Uvažme následující zobrazení:

$$\begin{aligned} \varphi: A[t]/J &\rightarrow (A/I)[t], \\ \varphi: (a_n t^n + \cdots + a_1 t + a_0) + J &\mapsto (a_n + I)t^n + \cdots + (a_1 + I)t + (a_0 + I). \end{aligned}$$

Opět chceme ukázat, že φ je izomorfismus okruhů.

- Korektnost: Označme $f = a_n t^n + \cdots + a_1 t + a_0$ a $g = b_m t^m + \cdots + b_1 t + b_0$. Bez újmy na obecnosti předpokládejme, že $n \geq m$. Nechť $f + J = g + J$, tj. $f - g \in J$. Pak platí

$$\begin{aligned} \varphi(f + J) - \varphi(g + J) &= \\ &= [(a_n + I)t^n + \cdots + (a_1 + I)t + (a_0 + I)] - [(b_m + I)t^m + \cdots + (b_1 + I)t + (b_0 + I)] = \\ &= (a_n + I)t^n + \cdots + (a_m - b_m + I)t^m + \cdots + (a_1 - b_1 + I)t + (a_0 - b_0 + I) = 0 + I. \end{aligned}$$

- Homomorfismus: Zřejmé, vždyť

$$\begin{aligned} \varphi(f + J) + \varphi(g + J) &= \\ &= [(a_n + I)t^n + \cdots + (a_1 + I)t + (a_0 + I)] + [(b_m + I)t^m + \cdots + (b_1 + I)t + (b_0 + I)] = \\ &= (a_n + I)t^n + \cdots + (a_m + b_m + I)t^m + \cdots + (a_1 + b_1 + I)t + (a_0 + b_0 + I) = \\ &= \varphi((f + g) + J). \end{aligned}$$

- Injekce: Zřejmě $\varphi(f + J) = 0$ právě tehdy, když všechny koeficienty f jsou z I , tj. $f \in J$.
- Surjekce: Zřejmé z předpisu homomorfismu φ .