Užití hlavní věty o faktorokruzích

Věta. *Nechť R je okruh. Pak existuje jediný homomorfismus okruhů $f : \mathbb{Z} \to R$. Jeho jádro* $\ker f$ *je hlavní ideál okruhu $\mathbb{Z}$ generovaný charakteristikou okruhu R, tj.* $\ker f = (\operatorname{char} R)$.

Důkaz. Z definice $f(1) = 1_R$, tedy pro každé přirozené číslo n platí

$$f(n) = f(\underbrace{1 + \cdots + 1}_{n}) = \underbrace{f(1) + \cdots + f(1)}_{n} = n1_R,$$

a tedy také $f(-n) = -f(n) = -(n1_R) = (-n)1_R$. Jediná možnost, jak homomorfismus $f : \mathbb{Z} \to R$ definovat, je předpisem $f(n) = n1_R$ pro každé $n \in \mathbb{Z}$, což skutečně dává homomorfismus. Rovnost $\ker f = (\operatorname{char} R)$ plyne z definice charakteristiky okruhu.

Důsledek. *Každý okruh R charakteristiky nula obsahuje podokruh izomorfní s okruhem celých čísel $\mathbb{Z}$. Každý okruh R charakteristiky $n \neq 0$ obsahuje podokruh izomorfní s okruhem $\mathbb{Z}_n$ zbytkových tříd modulo n.*

Důkaz. Plyne z hlavní věty o faktorokruzích pro homomorfismus okruhů $f : \mathbb{Z} \to R$ a toho, že $\mathbb{Z}/(n) = \mathbb{Z}_n$.

Podtělesa

Definice. Nechť T je těleso. Libovolný podokruh R tělesa T takový, že pro každé $a \in R$, $a \neq 0$ platí $a^{-1} \in R$, nazýváme podtělesem tělesa T. Říkáme též, že T je rozšířením tělesa R. Anebo také, že $R \subseteq T$ je rozšířením těles (v literatuře se hojně používá zápis: T/R je rozšířením těles).

Jinými slovy: podokruh R tělesa T je podtělesem, jestliže R je těleso.

Příklad. Každé těleso charakteristiky $p \neq 0$ obsahuje podtěleso izomorfní s $\mathbb{Z}_p$.

Věta. Nechť R je těleso a T netriviální okruh. Pak každý homomorfismus okruhů $\varphi : R \to T$ je injektivní.

Důkaz. Nechť $\varphi : R \to T$ je homomorfismus okruhů, pak $\ker \varphi$ je ideál R a $1 \notin \ker \varphi$, vždyť $\varphi(1) = 1 \neq 0$, tj. $\ker \varphi \neq R$. Proto $\ker \varphi$ je nulový ideál, jiné ideály už těleso R nemá.

Příklad podtělesa

Důsledek. *Každé těleso charakteristiky nula obsahuje podtěleso izomorfní s* $\mathbb{Q}$.

Důkaz. Nechť R je těleso, char $R = 0$. Pak jediný homomorfismus okruhů $\varphi : \mathbb{Z} \to R$, který je určen předpisem $\varphi(m) = m1$ pro každé $m \in \mathbb{Z}$, je injektivní. Proto $\varphi(n) \neq 0$ pro každé $n \in \mathbb{N}$.

Definujme zobrazení $\psi : \mathbb{Q} \to R$ takto: pro libovolné $m \in \mathbb{Z}$, $n \in \mathbb{N}$ položme $\psi(\frac{m}{n}) = \varphi(m)(\varphi(n))^{-1}$. Tento předpis je korektní, neboť pro každé $k \in \mathbb{N}$ platí

$$\varphi(km)(\varphi(kn))^{-1} = \varphi(k)\varphi(m)(\varphi(k)\varphi(n))^{-1} = \varphi(m)(\varphi(n))^{-1}.$$

Definované zobrazení je zřejmě homomorfimus okruhů, podle předchozí věty injektivní.

Podtěleso generované množinou

Věta. *Nechť $I \neq \emptyset$ je libovolná množina taková, že pro každé $i \in I$ je dáno podtěleso R_i tělesa T. Pak $\bigcap_{i \in I} R_i$ je podtěleso tělesa T.*

Důkaz je zřejmý.

Důsledek. *Nechť T je těleso. Systém všech podtěles tělesa T uspořádaný inkluzí je úplný svaz.*

Definice. Nechť T je těleso. Předchozí věta nám umožňuje definovat podtěleso tělesa T generované množinou $M \subseteq T$ jako průnik všech podtěles tuto množinu obsahujících. Je to tedy nejmenší podtěleso tělesa T obsahující M.
Je-li $M = R \cup \{c_1, \ldots, c_n\}$, kde R je podtěleso tělesa T a $c_1, \ldots, c_n \in T$, pak podtěleso generované množinou $R \cup \{c_1, \ldots, c_n\}$ značíme $R(c_1, \ldots, c_n)$.

Poznámka. Připomeňme, že je-li T okruh, R jeho podokruh a $c_1, \ldots, c_n \in T$, pak podokruh generovaný množinou $R \cup \{c_1, \ldots, c_n\}$ značíme $R[c_1, \ldots, c_n]$. V situaci z definice mají tedy smysl oba zápisy, zřejmě platí $R[c_1, \ldots, c_n] \subseteq R(c_1, \ldots, c_n)$.

Stupeň rozšíření těles

Je-li R podtělesem tělesa T, pak můžeme aditivní grupu $(T, +)$ chápat jako vektorový prostor nad tělesem R: skalárním násobkem vektoru $t \in T$ skalárem $r \in R$ je součin $r \cdot t$ počítaný v tělese T. Axiomy vektorového prostoru jsou splněny:
pro každé skaláry $r_1, r_2 \in R$ a každé vektory $t_1, t_2 \in T$ platí

- $(r_1 + r_2) \cdot t_1 = r_1 \cdot t_1 + r_2 \cdot t_1$,
- $r_1 \cdot (t_1 + t_2) = r_1 \cdot t_1 + r_1 \cdot t_2$,
- $r_1 \cdot (r_2 \cdot t_1) = (r_1 \cdot r_2) \cdot t_1$,
- $1 \cdot t_1 = t_1$,

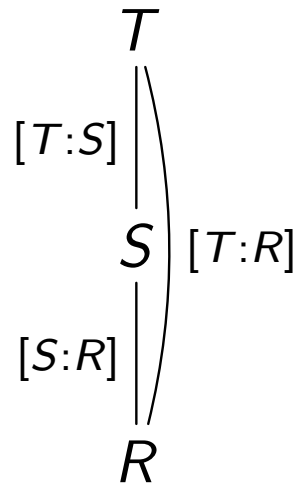
(v T platí distributivní zákony, násobení je asociativní a 1 je jednička). Máme tedy definovánu dimenzi $\dim_R T \in \mathbb{N} \cup \{\infty\}$, zřejmě tato dimenze nemůže být nula.

Definice. Nechť $R \subseteq T$ je rozšířením těles. Jeho stupněm $[T : R]$ rozumíme dimenzi vektorového prostoru T nad tělesem R, tj. $[T : R] = \dim_R T$.

Multiplikativnost stupně rozšíření

Věta. *Nechť $R \subseteq S$, $S \subseteq T$ jsou rozšíření těles. Pak platí*

$$[T : R] = [T : S] \cdot [S : R],$$



kde užíváme konvence $n \cdot \infty = \infty \cdot n = \infty$ pro každé $n \in \mathbb{N} \cup \{\infty\}$.

Důkaz. Je-li $[S : R] = \infty$, pro každé $n \in \mathbb{N}$ v S existuje n lineárně nezávislých prvků nad R, protože $S \subseteq T$, jsou tyto prvky v T a platí $[T : R] = \infty$.

Je-li $[T : S] = \infty$, pro každé $n \in \mathbb{N}$ v T existuje n lineárně nezávislých prvků nad S. Ty jsou lineárně nezávislé i nad R, a proto $[T : R] = \infty$.

Nechť $n = [T : S] \in \mathbb{N}$, $m = [S : R] \in \mathbb{N}$. Nechť $\alpha_1, \ldots, \alpha_n$ je báze T nad S, $\beta_1, \ldots, \beta_m$ báze S nad R. Ukážeme, že $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je bází T nad R. Nechť $\gamma \in T$ je libovolný. Pak existují $\delta_1, \ldots, \delta_n \in S$, že $\gamma = \sum_{i=1}^{n} \delta_i\alpha_i$. Existují tedy $\varepsilon_{ij} \in R$, že $\delta_i = \sum_{j=1}^{m} \varepsilon_{ij}\beta_j$ pro každé i. Dosazením

$$\gamma = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \varepsilon_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij}(\alpha_i\beta_j).$$

Tedy $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je množina generátorů T nad R.

Je-li $\sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij}(\alpha_i\beta_j)$ pro nějaké $\varepsilon_{ij} \in R$ nulový vektor, pak z lineární nezávislosti $\alpha_1, \ldots, \alpha_n$ nad S dostaneme, že $\sum_{j=1}^{m} \varepsilon_{ij}\beta_j = 0$ pro každé $i = 1, \ldots, n$ a z lineární nezávislosti $\beta_1, \ldots, \beta_m$ nad R dostaneme, že $\varepsilon_{ij} = 0$ pro každé i, j.

Tedy $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je báze T nad R.

Algebraické a transcendentní prvky

Mějme rozšíření těles $R \subseteq T$ a polynom

$$f = a_n x^n + \cdots + a_1 x + a_0 \in R[x].$$

Pak je také $f \in T[x]$, a proto pro každé $c \in T$ můžeme uvažovat hodnotu $f(c) = a_n \cdot c^n + \cdots + a_1 \cdot c + a_0 \in T$. Připomeňme, že c se nazývá kořenem polynomu f, je-li $f(c) = 0$.

Definice. Nechť $R \subseteq T$ je rozšířením těles, $c \in T$. Řekneme, že prvek c je algebraický nad tělesem R, jestliže existuje nenulový polynom $f \in R[x]$, jehož je c kořenem. V opačném případě říkáme, že prvek c je transcendentní nad tělesem R.

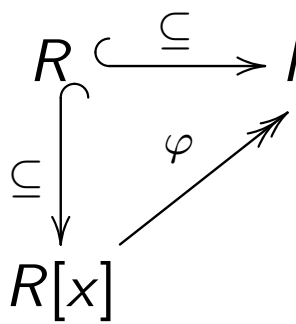
Poznámka. O komplexním čísle c říkáme, že je algebraické (resp. transcendentní), je-li c algebraické (resp. transcendentní) nad tělesem racionálních čísel $\mathbb{Q}$.

Minimální polynom algebraického prvku

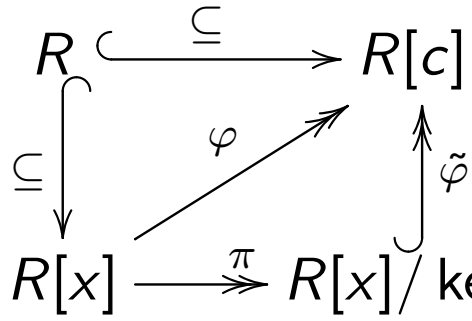
Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ algebraický prvek nad R. Pak c je kořenem právě jednoho normovaného ireducibilního polynomu $f \in R[x]$. Navíc platí*

1. *pro libovolný $h \in R[x]$ je $h(c) = 0$, právě když $f \mid h$ v $R[x]$,*
2. *$R(c) = R[c]$ v T,*
3. *$1, c, c^2, \ldots, c^{n-1}$, kde $n = \operatorname{st} f$, je bází vektorového prostoru $R[c]$ nad R,*
4. *stupeň rozšíření $[R(c) : R] = \operatorname{st} f$.*

Důkaz. Zobrazení φ, které každému polynomu $h \in R[x]$ přiřadí jeho hodnotu v c, tj. $\varphi(h) = h(c)$, je homomorfismus okruhů $\varphi : R[x] \to T$. Obrazem v tomto homomorfismu je $\varphi(R[x]) = \{h(c);\ h \in R[x]\} = R[c]$, neboť je to podokruh tělesa T, a to nejmenší z těch, co obsahují $R \cup \{c\}$. Na diagram



užijeme hlavní větu o faktorokruzích.



$\forall h \in R[x] : \varphi(h) = h(c)$

Z definice $\ker \varphi = \{h \in R[x];\ h(c) = 0\}$. Protože c je algebraický, je $\ker \varphi \neq \{0\}$. Protože R je těleso, je každý ideál v $R[x]$ hlavní. Proto existuje $f \in R[x]$, $f \neq 0$, splňující $(f) = \ker \varphi$. Protože asociované prvky generují týž hlavní ideál, lze předpokládat, že f je normovaný. Protože $(f) = \{h \in R[x];\ f \mid h\}$, platí bod 1.

Protože $R[c]$ je podokruhem tělesa, je to obor integrity, totéž platí o okruhu $R[x]/\ker \varphi$, který je s ním izomorfní. Tedy $(f) = \ker \varphi$ je prvoideál okruhu $R[x]$, což znamená, že f je ireducibilní nad R a (f) je maximální ideál okruhu $R[x]$, tedy $R[x]/\ker \varphi$ je těleso, proto je těleso i s ním izomorfní $R[c]$. Je tedy $R[c] = R(c)$.

Označme $n = \operatorname{st} f$. Zvolme libovolně polynom $h \in R[x]$ a vydělme jej se zbytkem polynomem f. Máme

$$h = q \cdot f + r, \qquad q, r \in R[x], \quad \operatorname{st} r < n.$$

Pak $h(c) = q(c) \cdot f(c) + r(c) = r(c)$. Odtud

$$\begin{aligned} R[c] &= \{h(c);\ h \in R[x]\} = \\ &= \{r(c);\ r \in R[x],\ \operatorname{st} r < n\} = \\ &= \{r_0 + r_1 \cdot c + \cdots + r_{n-1} \cdot c^{n-1};\ r_0, \ldots, r_{n-1} \in R\}. \end{aligned}$$

Přitom $r(c) = 0$ znamená $f \mid r$, což kvůli $\operatorname{st} r < n = \operatorname{st} f$ nastane jedině pro $r = 0$, tedy $1, c, c^2, \ldots, c^{n-1}$ je bází vektorového prostoru $R[c]$ nad R. Proto $[R(c) : R] = n$.

Definice. Polynom $f \in R[x]$ z předchozí věty nazýváme minimální polynom algebraického prvku $c \in T$ nad R.