Užití hlavní věty o faktorokruzích

Věta. *Nechť R je okruh. Pak existuje jediný homomorfismus okruhů $f : \mathbb{Z} \to R$.*

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.* $\ker f = (\operatorname{char} R)$.

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

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

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 $f(-n) = -f(n) = -(n1_R) = (-n)1_R$.

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.

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.

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 $\mathbb{Z}$.*

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.*

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.

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.

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).

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.

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 $\mathbb{Z}_p$.

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.

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. $\ker \varphi \neq R$.

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* $\mathbb{Q}$.

Příklad podtělesa

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

Důkaz. Nechť R je těleso, char $R = 0$.

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.

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 $n \in \mathbb{N}$.

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 $\psi(\frac{m}{n}) = \varphi(m)(\varphi(n))^{-1}$.

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

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

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.*

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.*

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.

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.*

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.

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.

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 $R(c_1, \ldots, c_n)$.

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 $R[c_1, \ldots, c_n]$.

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:

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.

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).

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.

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.

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. $[T : R] = \dim_R T$.

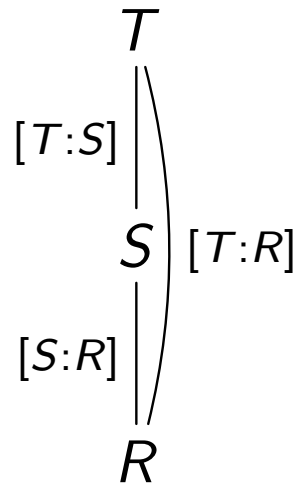
Multiplikativnost stupně rozšíření

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

Multiplikativnost stupně rozšíření

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

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

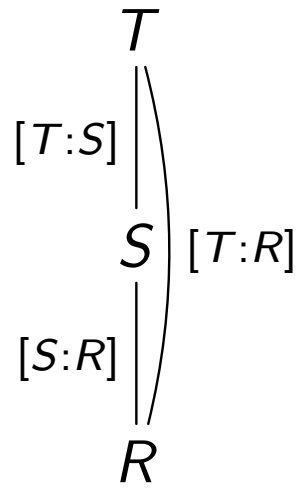


kde užíváme konvence $n \cdot \infty = \infty \cdot n = \infty$ pro každé $n \in \mathbb{N} \cup \{\infty\}$.

Multiplikativnost stupně rozšíření

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

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



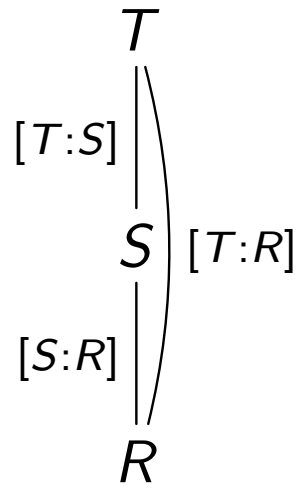
kde užíváme konvence $n \cdot \infty = \infty \cdot n = \infty$ pro každé $n \in \mathbb{N} \cup \{\infty\}$.

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 $[T : R] = \infty$.

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 $n \in \mathbb{N} \cup \{\infty\}$.

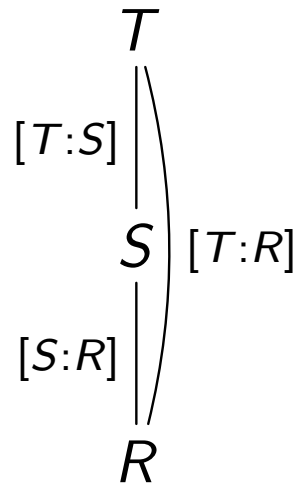
Důkaz. Je-li $[S : R] = \infty$, pro každé $n \in \mathbb{N}$ v S existuje n lineárně nezávislých prvků nad R, protože $S \subseteq T$, jsou tyto prvky v T a platí $[T : R] = \infty$.

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

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 $n = [T : S] \in \mathbb{N}$, $m = [S : R] \in \mathbb{N}$. Nechť $\alpha_1, \ldots, \alpha_n$ je báze T nad S, $\beta_1, \ldots, \beta_m$ báze S nad R.

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 $n = [T : S] \in \mathbb{N}$, $m = [S : R] \in \mathbb{N}$. 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.

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 $\gamma = \sum_{i=1}^{n} \delta_i \alpha_i$.

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.

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

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

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.

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.

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

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

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 $f(c) = a_n \cdot c^n + \cdots + a_1 \cdot c + a_0 \in T$.

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 $f(c) = 0$.

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, $c \in T$.

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.

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.

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.*

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 $f \in R[x]$.*

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 $R[x]$,*

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,*

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,*

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 $[R(c) : R] = \operatorname{st} f$.*

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. Protože c je algebraický prvek nad R, můžeme mezi všemi normovanými polynomy z $R[x]$, jejichž je c kořenem, zvolit polynom co možná nejmenšího stupně a označit jej f.

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. Protože c je algebraický prvek nad R, můžeme mezi všemi normovanými polynomy z $R[x]$, jejichž je c kořenem, zvolit polynom co možná nejmenšího stupně a označit jej f. Označme $n = \operatorname{st} f$.

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. Protože c je algebraický prvek nad R, můžeme mezi všemi normovanými polynomy z $R[x]$, jejichž je c kořenem, zvolit polynom co možná nejmenšího stupně a označit jej f. Označme $n = \operatorname{st} f$. Zřejmě $n > 0$.

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. Protože c je algebraický prvek nad R, můžeme mezi všemi normovanými polynomy z $R[x]$, jejichž je c kořenem, zvolit polynom co možná nejmenšího stupně a označit jej f. Označme $n = \operatorname{st} f$. Zřejmě $n > 0$. Kdyby $f = g \cdot h$ pro nějaké nekonstantní polynomy $g, h \in R[x]$, tak by bylo možné je zvolit oba normované a dostali bychom spor, protože $\operatorname{st} g < n$, $\operatorname{st} h < n$ a přitom c by byl kořenem alespoň jednoho z nich.

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. Protože c je algebraický prvek nad R, můžeme mezi všemi normovanými polynomy z $R[x]$, jejichž je c kořenem, zvolit polynom co možná nejmenšího stupně a označit jej f. Označme $n = \operatorname{st} f$. Zřejmě $n > 0$. Kdyby $f = g \cdot h$ pro nějaké nekonstantní polynomy $g, h \in R[x]$, tak by bylo možné je zvolit oba normované a dostali bychom spor, protože $\operatorname{st} g < n$, $\operatorname{st} h < n$ a přitom c by byl kořenem alespoň jednoho z nich. Je tedy f ireducibilní.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f. Proto $f \mid h$ v $R[x]$.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f. Proto $f \mid h$ v $R[x]$. Protože opačná implikace je zřejmá, dokázali jsme bod 1.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f. Proto $f \mid h$ v $R[x]$. Protože opačná implikace je zřejmá, dokázali jsme bod 1.

Je jasné, že normovaný polynom s kořenem c splňující bod 1 je jediný (kdybychom měli takové polynomy dva, každý z nich by dělil toho druhého).

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f. Proto $f \mid h$ v $R[x]$. Protože opačná implikace je zřejmá, dokázali jsme bod 1.

Je jasné, že normovaný polynom s kořenem c splňující bod 1 je jediný (kdybychom měli takové polynomy dva, každý z nich by dělil toho druhého).

Podle věty o podokruzích generovaných množinou platí, že libovolný prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$ pro nějaký polynom $h \in R[x]$.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f. Proto $f \mid h$ v $R[x]$. Protože opačná implikace je zřejmá, dokázali jsme bod 1.

Je jasné, že normovaný polynom s kořenem c splňující bod 1 je jediný (kdybychom měli takové polynomy dva, každý z nich by dělil toho druhého).

Podle věty o podokruzích generovaných množinou platí, že libovolný prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$ pro nějaký polynom $h \in R[x]$. Dělením se zbytkem opět dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f. Proto $f \mid h$ v $R[x]$. Protože opačná implikace je zřejmá, dokázali jsme bod 1.

Je jasné, že normovaný polynom s kořenem c splňující bod 1 je jediný (kdybychom měli takové polynomy dva, každý z nich by dělil toho druhého).

Podle věty o podokruzích generovaných množinou platí, že libovolný prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$ pro nějaký polynom $h \in R[x]$. Dělením se zbytkem opět dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Opět $\alpha = h(c) = q(c) \cdot f(c) + r(c) = r(c)$.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f. Proto $f \mid h$ v $R[x]$. Protože opačná implikace je zřejmá, dokázali jsme bod 1.

Je jasné, že normovaný polynom s kořenem c splňující bod 1 je jediný (kdybychom měli takové polynomy dva, každý z nich by dělil toho druhého).

Podle věty o podokruzích generovaných množinou platí, že libovolný prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$ pro nějaký polynom $h \in R[x]$. Dělením se zbytkem opět dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Opět $\alpha = h(c) = q(c) \cdot f(c) + r(c) = r(c)$. Proto $1, c, c^2, \ldots, c^{n-1}$ generují vektorový prostor $R[c]$ nad R; kdyby tyto vektory byly lineárně závislé, existoval by v $R[x]$ nenulový polynom stupně menšíno než n, který by měl c za kořen, a to by byl spor.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f. Proto $f \mid h$ v $R[x]$. Protože opačná implikace je zřejmá, dokázali jsme bod 1.

Je jasné, že normovaný polynom s kořenem c splňující bod 1 je jediný (kdybychom měli takové polynomy dva, každý z nich by dělil toho druhého).

Podle věty o podokruzích generovaných množinou platí, že libovolný prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$ pro nějaký polynom $h \in R[x]$. Dělením se zbytkem opět dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Opět $\alpha = h(c) = q(c) \cdot f(c) + r(c) = r(c)$. Proto $1, c, c^2, \ldots, c^{n-1}$ generují vektorový prostor $R[c]$ nad R; kdyby tyto vektory byly lineárně závislé, existoval by v $R[x]$ nenulový polynom stupně menšíno než n, který by měl c za kořen, a to by byl spor. Dokázali jsme bod 3.

Zbývá ukázat, že $R(c) = R[c]$, jinými slovy, že $R[c]$ je těleso.

Zbývá ukázat, že $R(c) = R[c]$, jinými slovy, že $R[c]$ je těleso.

Víme, že libovolný nenulový prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$.

Zbývá ukázat, že $R(c) = R[c]$, jinými slovy, že $R[c]$ je těleso.

Víme, že libovolný nenulový prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$. Protože $h(c) = \alpha \neq 0$, tak $f \nmid h$, a protože f je ireducibilní, tak jsou f a h nesoudělné.

Zbývá ukázat, že $R(c) = R[c]$, jinými slovy, že $R[c]$ je těleso.

Víme, že libovolný nenulový prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$. Protože $h(c) = \alpha \neq 0$, tak $f \nmid h$, a protože f je ireducibilní, tak jsou f a h nesoudělné. Proto jejich největší společný dělitel 1 lze vyjádřit Bezoutovou rovností, tedy existují polynomy $a, b \in R[x]$ tak, že $1 = a \cdot f + b \cdot h$.

Zbývá ukázat, že $R(c) = R[c]$, jinými slovy, že $R[c]$ je těleso.

Víme, že libovolný nenulový prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$. Protože $h(c) = \alpha \neq 0$, tak $f \nmid h$, a protože f je ireducibilní, tak jsou f a h nesoudělné. Proto jejich největší společný dělitel 1 lze vyjádřit Bezoutovou rovností, tedy existují polynomy $a, b \in R[x]$ tak, že $1 = a \cdot f + b \cdot h$. Dosazením c odtud dostaneme

$$1 = a(c) \cdot f(c) + b(c) \cdot h(c) = b(c) \cdot h(c) = b(c) \cdot \alpha$$

Je tedy $b(c) \in R[c]$ inverzní prvek k prvku α v okruhu $R[c]$.

Zbývá ukázat, že $R(c) = R[c]$, jinými slovy, že $R[c]$ je těleso.

Víme, že libovolný nenulový prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$. Protože $h(c) = \alpha \neq 0$, tak $f \nmid h$, a protože f je ireducibilní, tak jsou f a h nesoudělné. Proto jejich největší společný dělitel 1 lze vyjádřit Bezoutovou rovností, tedy existují polynomy $a, b \in R[x]$ tak, že $1 = a \cdot f + b \cdot h$. Dosazením c odtud dostaneme

$$1 = a(c) \cdot f(c) + b(c) \cdot h(c) = b(c) \cdot h(c) = b(c) \cdot \alpha$$

Je tedy $b(c) \in R[c]$ inverzní prvek k prvku α v okruhu $R[c]$. Dokázali jsme bod 2, díky níž z bodu 3 plyne bod 4.

Zbývá ukázat, že $R(c) = R[c]$, jinými slovy, že $R[c]$ je těleso.

Víme, že libovolný nenulový prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$. Protože $h(c) = \alpha \neq 0$, tak $f \nmid h$, a protože f je ireducibilní, tak jsou f a h nesoudělné. Proto jejich největší společný dělitel 1 lze vyjádřit Bezoutovou rovností, tedy existují polynomy $a, b \in R[x]$ tak, že $1 = a \cdot f + b \cdot h$. Dosazením c odtud dostaneme

$$1 = a(c) \cdot f(c) + b(c) \cdot h(c) = b(c) \cdot h(c) = b(c) \cdot \alpha$$

Je tedy $b(c) \in R[c]$ inverzní prvek k prvku α v okruhu $R[c]$. Dokázali jsme bod 2, díky níž z bodu 3 plyne bod 4.

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

Minimální polynom algebraického prvku - jiný důkaz

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 $[R(c) : R] = \operatorname{st} f$.*

Minimální polynom algebraického prvku - jiný důkaz

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 $\varphi : R[x] \to T$.

Minimální polynom algebraického prvku - jiný důkaz

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 $[R(c) : R] = \operatorname{st} f$.*

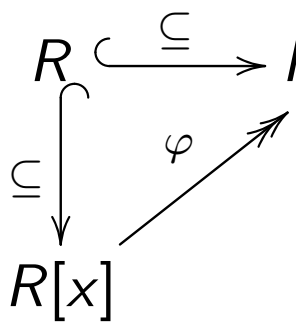
Důkaz. Zobrazení φ, které každému polynomu $h \in R[x]$ přiřadí jeho hodnotu v c, tj. $\varphi(h) = h(c)$, je homomorfismus okruhů $\varphi : R[x] \to T$. Obrazem v tomto homomorfismu je $\varphi(R[x]) = \{h(c);\ h \in R[x]\} = R[c]$, neboť je to podokruh tělesa T, a to nejmenší z těch, co obsahují $R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

Minimální polynom algebraického prvku - jiný důkaz

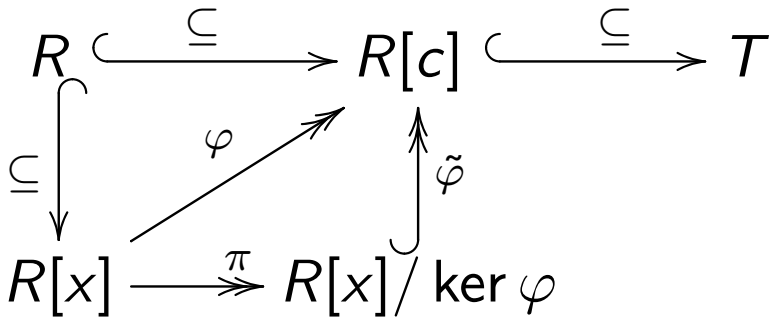
Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ algebraický prvek nad R. Pak c je kořenem právě jednoho normovaného ireducibilního polynomu $f \in R[x]$. Navíc platí*

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 $[R(c) : R] = \operatorname{st} f$.*

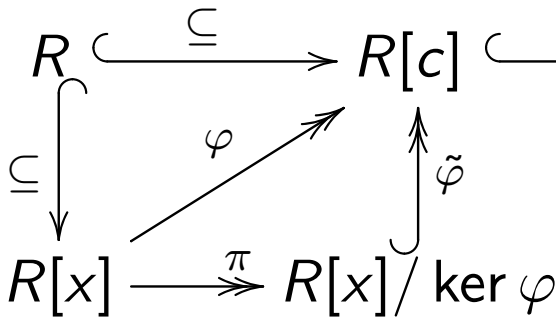
Důkaz. Zobrazení φ, které každému polynomu $h \in R[x]$ přiřadí jeho hodnotu v c, tj. $\varphi(h) = h(c)$, je homomorfismus okruhů $\varphi : R[x] \to T$. Obrazem v tomto homomorfismu je $\varphi(R[x]) = \{h(c);\ h \in R[x]\} = R[c]$, neboť je to podokruh tělesa T, a to nejmenší z těch, co obsahují $R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



užijeme hlavní větu o faktorokruzích.

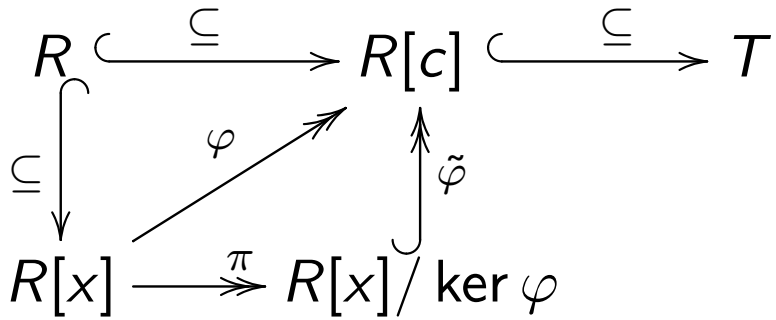


$$\forall h \in R[x] : \varphi(h) = h(c)$$



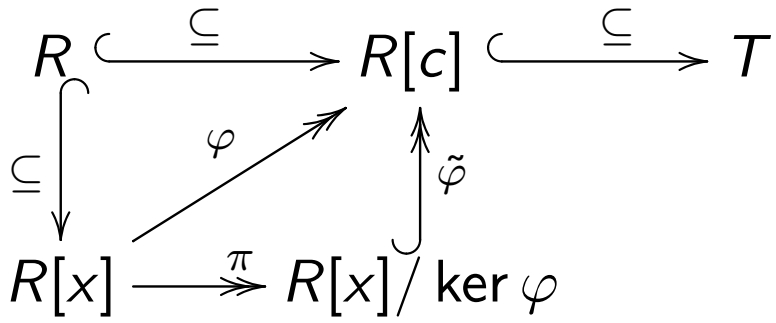
$\forall h \in R[x] : \varphi(h) = h(c)$

Z definice $\ker \varphi = \{h \in R[x];\ h(c) = 0\}$.



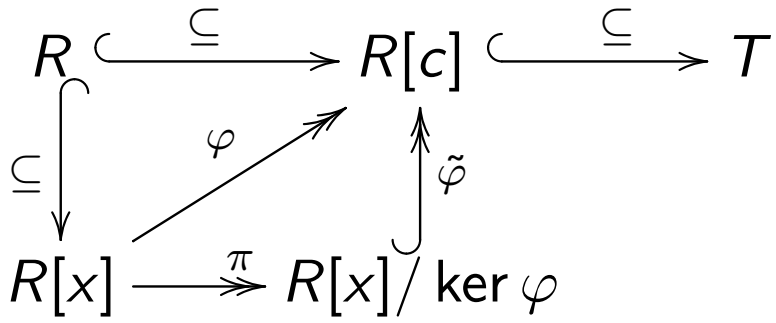
$\forall h \in R[x] : \varphi(h) = h(c)$

Z definice $\ker \varphi = \{h \in R[x];\ h(c) = 0\}$. Protože c je algebraický, je $\ker \varphi \neq \{0\}$.



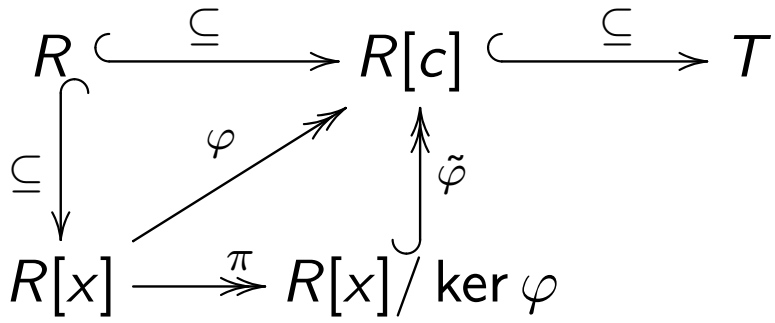
$\forall h \in R[x] : \varphi(h) = h(c)$

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.



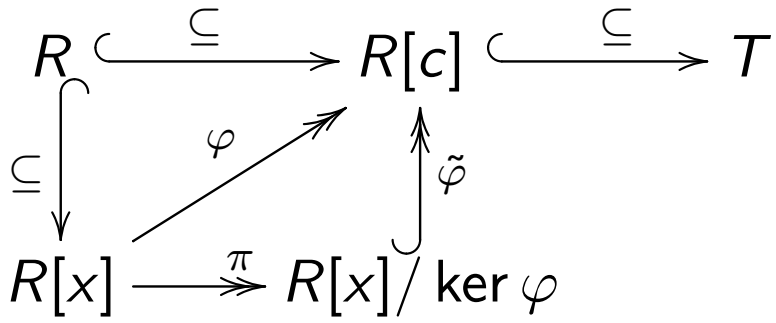
$\forall h \in R[x] : \varphi(h) = h(c)$

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 $(f) = \ker \varphi$.



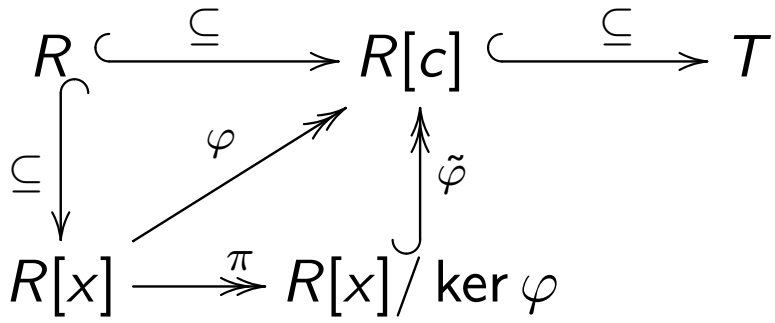
$\forall h \in R[x] : \varphi(h) = h(c)$

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.



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

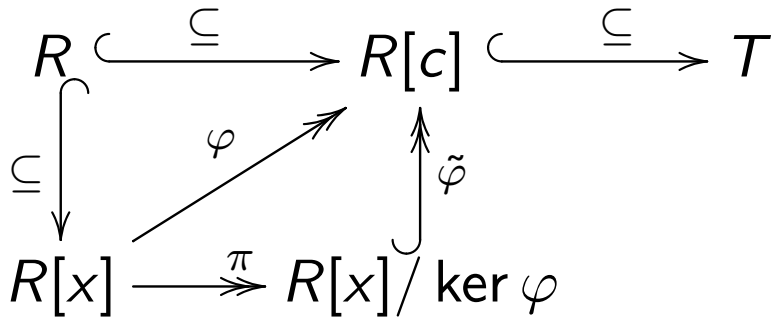
Z definice $\ker \varphi = \{h \in R[x];\ h(c) = 0\}$. Protože c je algebraický, je $\ker \varphi \neq \{0\}$. Protože R je těleso, je každý ideál v $R[x]$ hlavní. Proto existuje $f \in R[x]$, $f \neq 0$, splňující $(f) = \ker \varphi$. Protože asociované prvky generují týž hlavní ideál, lze předpokládat,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



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

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.

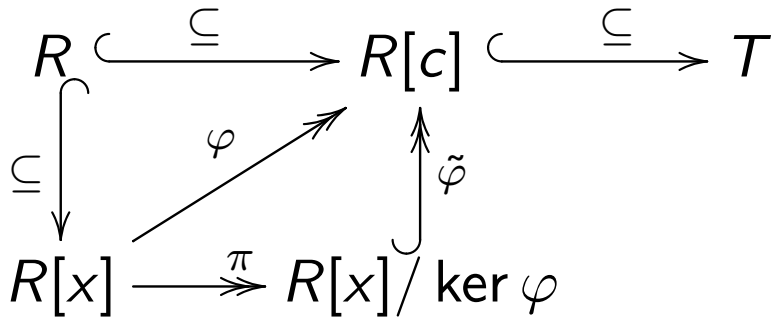
Protože $R[c]$ je podokruhem tělesa, je to obor integrity, totéž platí o okruhu $R[x]/\ker \varphi$, který je s ním izomorfní.



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

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.

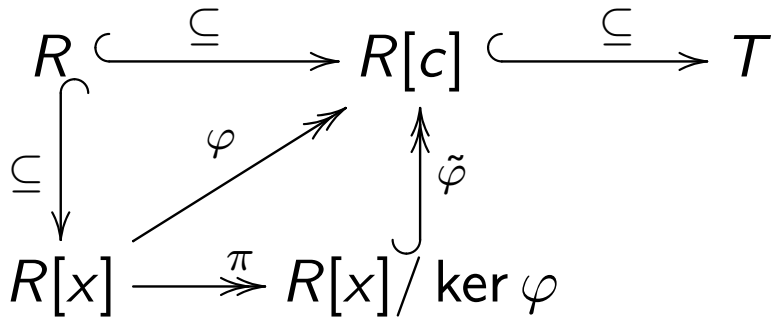
Protože $R[c]$ je podokruhem tělesa, je to obor integrity, totéž platí o okruhu $R[x]/\ker \varphi$, který je s ním izomorfní. Tedy $(f) = \ker \varphi$ je prvoideál okruhu $R[x]$,



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

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.

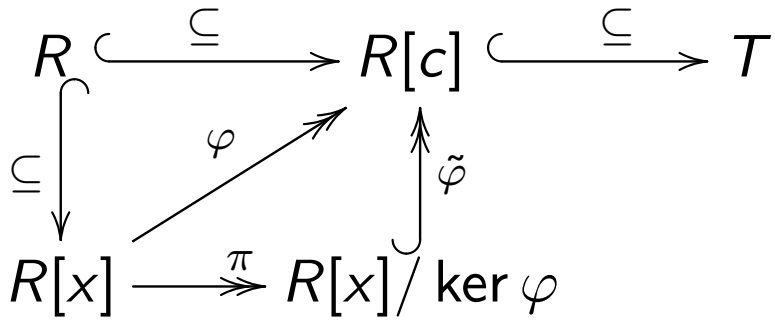
Protože $R[c]$ je podokruhem tělesa, je to obor integrity, totéž platí o okruhu $R[x]/\ker \varphi$, který je s ním izomorfní. Tedy $(f) = \ker \varphi$ je prvoideál okruhu $R[x]$, což znamená, že f je ireducibilní nad R a (f) je maximální ideál okruhu $R[x]$,



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

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 $R[c]$.



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

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 $n = \operatorname{st} f$.

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

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

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

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

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

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

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 $r = 0$,

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.

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 $[R(c) : R] = n$.

Těleso racionálních funkcí

Poznámka. Libovolnému oboru integrity jsme sestrojili podílové těleso.

Těleso racionálních funkcí

Poznámka. Libovolnému oboru integrity jsme sestrojili podílové těleso. Pro libovolné těleso R je okruh polynomů $R[x]$ oborem integrity, máme tedy podílové těleso i pro něj.

Těleso racionálních funkcí

Poznámka. Libovolnému oboru integrity jsme sestrojili podílové těleso. Pro libovolné těleso R je okruh polynomů $R[x]$ oborem integrity, máme tedy podílové těleso i pro něj.

Definice. Nechť R je libovolné těleso. Podílové těleso oboru integrity $R[x]$ nazýváme těleso racionálních funkcí nad tělesem R, značíme jej $R(x)$.

Těleso racionálních funkcí

Poznámka. Libovolnému oboru integrity jsme sestrojili podílové těleso. Pro libovolné těleso R je okruh polynomů $R[x]$ oborem integrity, máme tedy podílové těleso i pro něj.

Definice. Nechť R je libovolné těleso. Podílové těleso oboru integrity $R[x]$ nazýváme těleso racionálních funkcí nad tělesem R, značíme jej $R(x)$.

Libovolný prvek tělesa racionálních funkcí je tedy zlomek, který má ve jmenovateli i čitateli polynomy s koeficienty z tělesa R, tedy

$$R(x) = \left\{ \frac{f}{g};\ f, g \in R[x],\ g \neq 0 \right\}.$$

Těleso racionálních funkcí

Poznámka. Libovolnému oboru integrity jsme sestrojili podílové těleso. Pro libovolné těleso R je okruh polynomů $R[x]$ oborem integrity, máme tedy podílové těleso i pro něj.

Definice. Nechť R je libovolné těleso. Podílové těleso oboru integrity $R[x]$ nazýváme těleso racionálních funkcí nad tělesem R, značíme jej $R(x)$.

Libovolný prvek tělesa racionálních funkcí je tedy zlomek, který má ve jmenovateli i čitateli polynomy s koeficienty z tělesa R, tedy

$$R(x) = \left\{ \frac{f}{g};\ f, g \in R[x],\ g \neq 0 \right\}.$$

Operace sčítání a násobení jsou v $R(x)$ definovány tak, jak jsme zvyklí pracovat se zlomky.

Těleso racionálních funkcí

Poznámka. Libovolnému oboru integrity jsme sestrojili podílové těleso. Pro libovolné těleso R je okruh polynomů $R[x]$ oborem integrity, máme tedy podílové těleso i pro něj.

Definice. Nechť R je libovolné těleso. Podílové těleso oboru integrity $R[x]$ nazýváme těleso racionálních funkcí nad tělesem R, značíme jej $R(x)$.

Libovolný prvek tělesa racionálních funkcí je tedy zlomek, který má ve jmenovateli i čitateli polynomy s koeficienty z tělesa R, tedy

$$R(x) = \left\{ \frac{f}{g};\ f, g \in R[x],\ g \neq 0 \right\}.$$

Operace sčítání a násobení jsou v $R(x)$ definovány tak, jak jsme zvyklí pracovat se zlomky. Přitom okruh polynomů $R[x]$ je podokruhem tělesa $R(x)$, neboť libovolný polynom f je ztotožněn se zlomkem $\frac{f}{1}$.

Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R.*

Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R. Pak platí*

1. $R[c] \subsetneq R(c)$ *v* T,

Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R. Pak platí*

1. $R[c] \subsetneq R(c)$ *v* T,
2. $R[c] \cong R[x]$, $R(c) \cong R(x)$,

Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R. Pak platí*

1. $R[c] \subsetneq R(c)$ *v* T,
2. $R[c] \cong R[x]$, $R(c) \cong R(x)$,
3. *stupeň rozšíření* $[R(c) : R] = \infty$.

Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R. Pak platí*

1. $R[c] \subsetneq R(c)$ *v* T,
2. $R[c] \cong R[x]$, $R(c) \cong R(x)$,
3. *stupeň rozšíření* $[R(c) : R] = \infty$.

Důkaz. Zobrazení φ přiřazující každému polynomu $h \in R[x]$ jeho hodnotu v c, tj. $\varphi(h) = h(c)$, je homomorfismus okruhů $\varphi : R[x] \to T$,

Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R. Pak platí*

1. $R[c] \subsetneq R(c)$ *v* T,
2. $R[c] \cong R[x]$, $R(c) \cong R(x)$,
3. *stupeň rozšíření* $[R(c) : R] = \infty$.

Důkaz. Zobrazení φ přiřazující každému polynomu $h \in R[x]$ jeho hodnotu v c, tj. $\varphi(h) = h(c)$, je homomorfismus okruhů $\varphi : R[x] \to T$, obrazem je $\varphi(R[x]) = \{h(c);\ h \in R[x]\} = R[c]$.

Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R. Pak platí*

1. $R[c] \subsetneq R(c)$ *v* T,
2. $R[c] \cong R[x]$, $R(c) \cong R(x)$,
3. *stupeň rozšíření* $[R(c) : R] = \infty$.

Důkaz. Zobrazení φ přiřazující každému polynomu $h \in R[x]$ jeho hodnotu v c, tj. $\varphi(h) = h(c)$, je homomorfismus okruhů $\varphi : R[x] \to T$, obrazem je $\varphi(R[x]) = \{h(c);\ h \in R[x]\} = R[c]$. Protože c je transcendentní nad R, je $\ker \varphi = \{0\}$ a φ je injekce.

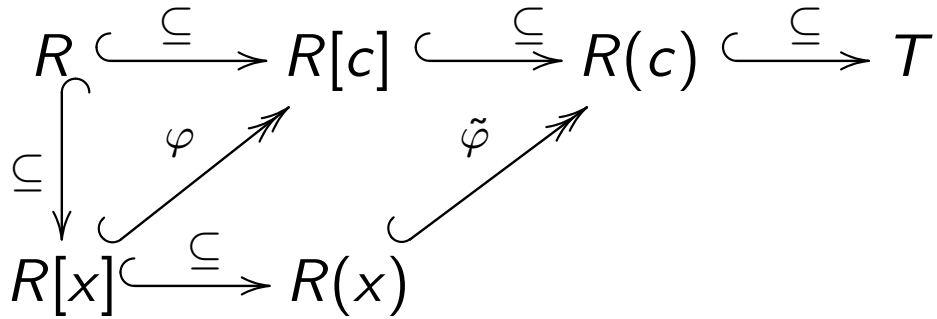
Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R. Pak platí*

1. $R[c] \subsetneq R(c)$ *v* T,
2. $R[c] \cong R[x]$, $R(c) \cong R(x)$,
3. *stupeň rozšíření* $[R(c) : R] = \infty$.

Důkaz. Zobrazení φ přiřazující každému polynomu $h \in R[x]$ jeho hodnotu v c, tj. $\varphi(h) = h(c)$, je homomorfismus okruhů $\varphi : R[x] \to T$, obrazem je $\varphi(R[x]) = \{h(c);\ h \in R[x]\} = R[c]$. Protože c je transcendentní nad R, je $\ker \varphi = \{0\}$ a φ je injekce.

Tedy $R[x] \cong R[c]$.



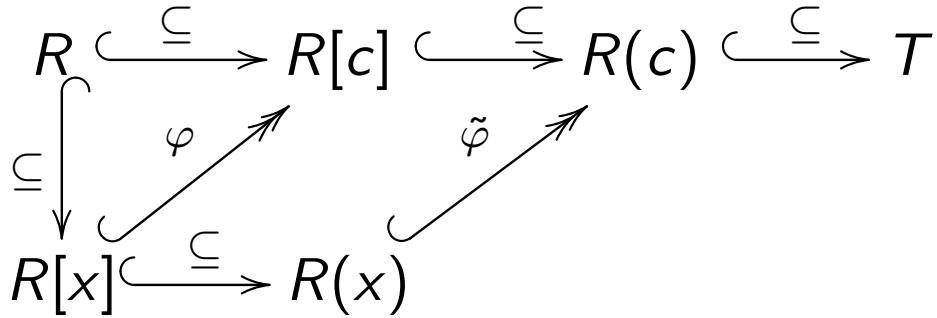
Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R. Pak platí*

1. $R[c] \subsetneq R(c)$ *v* T,
2. $R[c] \cong R[x]$, $R(c) \cong R(x)$,
3. *stupeň rozšíření* $[R(c) : R] = \infty$.

Důkaz. Zobrazení φ přiřazující každému polynomu $h \in R[x]$ jeho hodnotu v c, tj. $\varphi(h) = h(c)$, je homomorfismus okruhů $\varphi : R[x] \to T$, obrazem je $\varphi(R[x]) = \{h(c);\ h \in R[x]\} = R[c]$. Protože c je transcendentní nad R, je $\ker \varphi = \{0\}$ a φ je injekce.

Tedy $R[x] \cong R[c]$.



Homomorfismus φ lze rozšířit na injektivní homomorfismus $\tilde{\varphi} : R(x) \to T$ předpisem $\tilde{\varphi}\left(\frac{h}{g}\right) = h(c)g(c)^{-1}$, obrazem je podtěleso $R(c)$ tělesa T.

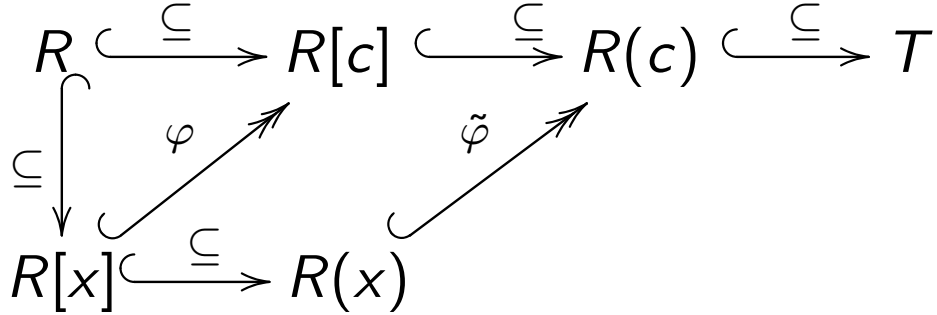
Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R. Pak platí*

1. $R[c] \subsetneq R(c)$ *v* T,
2. $R[c] \cong R[x]$, $R(c) \cong R(x)$,
3. *stupeň rozšíření* $[R(c) : R] = \infty$.

Důkaz. Zobrazení φ přiřazující každému polynomu $h \in R[x]$ jeho hodnotu v c, tj. $\varphi(h) = h(c)$, je homomorfismus okruhů $\varphi : R[x] \to T$, obrazem je $\varphi(R[x]) = \{h(c);\ h \in R[x]\} = R[c]$. Protože c je transcendentní nad R, je $\ker \varphi = \{0\}$ a φ je injekce.

Tedy $R[x] \cong R[c]$.



Homomorfismus φ lze rozšířit na injektivní homomorfismus $\tilde{\varphi} : R(x) \to T$ předpisem $\tilde{\varphi}\left(\frac{h}{g}\right) = h(c)g(c)^{-1}$, obrazem je podtěleso $R(c)$ tělesa T. Zřejmě je $\dim_R R[x] = \infty$, a proto $[R(c) : R] = \infty$.

Jednoduchá, konečná a algebraická rozšíření

Definice. Nechť $R \subseteq T$ je rozšíření těles.

Jednoduchá, konečná a algebraická rozšíření

Definice. Nechť $R \subseteq T$ je rozšíření těles. Řekneme, že toto rozšíření je

- *jednoduché*, existuje-li prvek $c \in T$, který je algebraický nad R, takový, že $T = R(c)$;

Jednoduchá, konečná a algebraická rozšíření

Definice. Nechť $R \subseteq T$ je rozšíření těles. Řekneme, že toto rozšíření je

- *jednoduché*, existuje-li prvek $c \in T$, který je algebraický nad R, takový, že $T = R(c)$;
- *konečné*, je-li stupeň $[T : R] < \infty$;

Jednoduchá, konečná a algebraická rozšíření

Definice. Nechť $R \subseteq T$ je rozšíření těles. Řekneme, že toto rozšíření je

- *jednoduché*, existuje-li prvek $c \in T$, který je algebraický nad R, takový, že $T = R(c)$;
- *konečné*, je-li stupeň $[T : R] < \infty$;
- *algebraické*, je-li každý prvek $c \in T$ algebraický nad R.

Jednoduchá, konečná a algebraická rozšíření

Definice. Nechť $R \subseteq T$ je rozšíření těles. Řekneme, že toto rozšíření je

- *jednoduché*, existuje-li prvek $c \in T$, který je algebraický nad R, takový, že $T = R(c)$;
- *konečné*, je-li stupeň $[T : R] < \infty$;
- *algebraické*, je-li každý prvek $c \in T$ algebraický nad R.

Věta. *Každé jednoduché rozšíření těles je konečné.*

Jednoduchá, konečná a algebraická rozšíření

Definice. Nechť $R \subseteq T$ je rozšíření těles. Řekneme, že toto rozšíření je

- *jednoduché*, existuje-li prvek $c \in T$, který je algebraický nad R, takový, že $T = R(c)$;
- *konečné*, je-li stupeň $[T : R] < \infty$;
- *algebraické*, je-li každý prvek $c \in T$ algebraický nad R.

Věta. Každé jednoduché rozšíření těles je konečné.

Důkaz. Je-li $T = R(c)$ pro $c \in T$, který je algebraický nad R, pak víme, že $[T : R] = [R(c) : R] = \operatorname{st} f$, kde $f \in R[x]$ je minimální polynom prvku c nad R.

Jednoduchá, konečná a algebraická rozšíření

Definice. Nechť $R \subseteq T$ je rozšíření těles. Řekneme, že toto rozšíření je

- *jednoduché*, existuje-li prvek $c \in T$, který je algebraický nad R, takový, že $T = R(c)$;
- *konečné*, je-li stupeň $[T : R] < \infty$;
- *algebraické*, je-li každý prvek $c \in T$ algebraický nad R.

Věta. *Každé jednoduché rozšíření těles je konečné.*

Důkaz. Je-li $T = R(c)$ pro $c \in T$, který je algebraický nad R, pak víme, že $[T : R] = [R(c) : R] = \operatorname{st} f$, kde $f \in R[x]$ je minimální polynom prvku c nad R.

Poznámka. Pro tělesa charakteristiky nula platí i opačná implikace, tuto větu však budeme dokazovat až v předmětu Galoisova teorie: *Každé konečné rozšíření těles charakteristiky nula je jednoduché.*

Jednoduchá, konečná a algebraická rozšíření

Věta. *Každé konečné rozšíření těles je algebraické.*

Jednoduchá, konečná a algebraická rozšíření

Věta. *Každé konečné rozšíření těles je algebraické.*

Důkaz. Nechť $R \subseteq T$ je konečné rozšíření těles, pak stupeň $[T : R] = m$ je přirozené číslo.

Jednoduchá, konečná a algebraická rozšíření

Věta. *Každé konečné rozšíření těles je algebraické.*

Důkaz. Nechť $R \subseteq T$ je konečné rozšíření těles, pak stupeň $[T : R] = m$ je přirozené číslo.

Pro libovolný prvek $c \in T$ jsou prvky $1, c, c^2, \ldots, c^m$ lineárně závislé nad R, neboť je jich více než $\dim_R T = m$.

Jednoduchá, konečná a algebraická rozšíření

Věta. *Každé konečné rozšíření těles je algebraické.*

Důkaz. Nechť $R \subseteq T$ je konečné rozšíření těles, pak stupeň $[T : R] = m$ je přirozené číslo.

Pro libovolný prvek $c \in T$ jsou prvky $1, c, c^2, \ldots, c^m$ lineárně závislé nad R, neboť je jich více než $\dim_R T = m$.

Existují tedy $r_0, r_1, \ldots, r_m \in R$, ne všechny nulové, tak, že $r_0 \cdot 1 + r_1 \cdot c + r_2 \cdot c^2 + \cdots + r_m \cdot c^m = 0$.

Jednoduchá, konečná a algebraická rozšíření

Věta. *Každé konečné rozšíření těles je algebraické.*

Důkaz. Nechť $R \subseteq T$ je konečné rozšíření těles, pak stupeň $[T : R] = m$ je přirozené číslo.

Pro libovolný prvek $c \in T$ jsou prvky $1, c, c^2, \ldots, c^m$ lineárně závislé nad R, neboť je jich více než $\dim_R T = m$.

Existují tedy $r_0, r_1, \ldots, r_m \in R$, ne všechny nulové, tak, že $r_0 \cdot 1 + r_1 \cdot c + r_2 \cdot c^2 + \cdots + r_m \cdot c^m = 0$.

Proto je c kořenem nenulového polynomu $r = r_m x^m + \cdots + r_1 x + r_0 \in R[x]$, a tedy c je algebraický nad R.

Jednoduchá, konečná a algebraická rozšíření

Věta. *Každé konečné rozšíření těles je algebraické.*

Důkaz. Nechť $R \subseteq T$ je konečné rozšíření těles, pak stupeň $[T : R] = m$ je přirozené číslo.

Pro libovolný prvek $c \in T$ jsou prvky $1, c, c^2, \ldots, c^m$ lineárně závislé nad R, neboť je jich více než $\dim_R T = m$.

Existují tedy $r_0, r_1, \ldots, r_m \in R$, ne všechny nulové, tak, že $r_0 \cdot 1 + r_1 \cdot c + r_2 \cdot c^2 + \cdots + r_m \cdot c^m = 0$.

Proto je c kořenem nenulového polynomu $r = r_m x^m + \cdots + r_1 x + r_0 \in R[x]$, a tedy c je algebraický nad R.

Důsledek. *Nechť $R \subseteq T$ je rozšíření těles. Jestliže těleso T obsahuje prvek transcendentní nad R, pak $[T : R] = \infty$.*

Konstrukce jednoduchého rozšíření

Věta. *Nechť R je těleso, $f \in R[x]$ normovaný ireducibilní polynom.*

Konstrukce jednoduchého rozšíření

Věta. *Nechť R je těleso, $f \in R[x]$ normovaný ireducibilní polynom. Pak $R[x]/(f)$ je těleso, které je jednoduché rozšíření tělesa R.*

Konstrukce jednoduchého rozšíření

Věta. *Nechť R je těleso, $f \in R[x]$ normovaný ireducibilní polynom. Pak $R[x]/(f)$ je těleso, které je jednoduché rozšíření tělesa R. Přesněji: ztotožníme libovolný prvek $r \in R$ s třídou $r + (f)$ obsahující konstantní polynom r a označíme $c = x + (f)$ třídu obsahující polynom x, pak $R[x]/(f) = R(c)$ a f je minimální polynom prvku c nad R.*

Konstrukce jednoduchého rozšíření

Věta. *Nechť R je těleso, $f \in R[x]$ normovaný ireducibilní polynom. Pak $R[x]/(f)$ je těleso, které je jednoduché rozšíření tělesa R. Přesněji: ztotožníme libovolný prvek $r \in R$ s třídou $r + (f)$ obsahující konstantní polynom r a označíme $c = x + (f)$ třídu obsahující polynom x, pak $R[x]/(f) = R(c)$ a f je minimální polynom prvku c nad R.*

Důkaz. Protože f je ireducibilní polynom nad tělesem R, hlavní ideál $(f) \subseteq R[x]$ je maximálním ideálem okruhu polynomů $R[x]$.

Konstrukce jednoduchého rozšíření

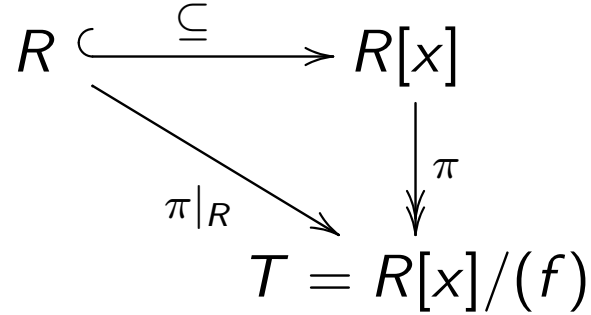
Věta. *Nechť R je těleso, $f \in R[x]$ normovaný ireducibilní polynom. Pak $R[x]/(f)$ je těleso, které je jednoduché rozšíření tělesa R. Přesněji: ztotožníme libovolný prvek $r \in R$ s třídou $r + (f)$ obsahující konstantní polynom r a označíme $c = x + (f)$ třídu obsahující polynom x, pak $R[x]/(f) = R(c)$ a f je minimální polynom prvku c nad R.*

Důkaz. Protože f je ireducibilní polynom nad tělesem R, hlavní ideál $(f) \subseteq R[x]$ je maximálním ideálem okruhu polynomů $R[x]$. Protože $R[x]$ je komutativní okruh, je faktorokruh $T = R[x]/(f)$ těleso.

Konstrukce jednoduchého rozšíření

Věta. *Nechť R je těleso, $f \in R[x]$ normovaný ireducibilní polynom. Pak $R[x]/(f)$ je těleso, které je jednoduché rozšíření tělesa R. Přesněji: ztotožníme libovolný prvek $r \in R$ s třídou $r + (f)$ obsahující konstantní polynom r a označíme $c = x + (f)$ třídu obsahující polynom x, pak $R[x]/(f) = R(c)$ a f je minimální polynom prvku c nad R.*

Důkaz. Protože f je ireducibilní polynom nad tělesem R, hlavní ideál $(f) \subseteq R[x]$ je maximálním ideálem okruhu polynomů $R[x]$. Protože $R[x]$ je komutativní okruh, je faktorokruh $T = R[x]/(f)$ těleso.

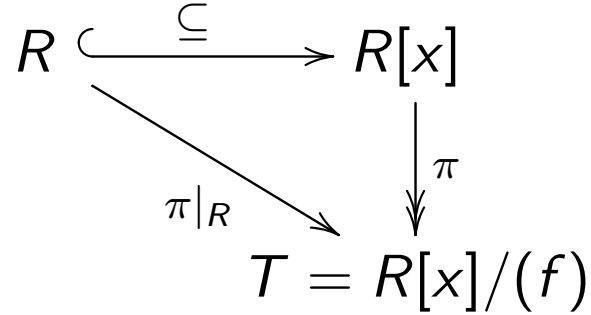


Protože $\pi|_R : R \to T$ je homomorfismus okruhů mezi tělesy, je injektivní.

Konstrukce jednoduchého rozšíření

Věta. *Nechť R je těleso, $f \in R[x]$ normovaný ireducibilní polynom. Pak $R[x]/(f)$ je těleso, které je jednoduché rozšíření tělesa R. Přesněji: ztotožníme libovolný prvek $r \in R$ s třídou $r + (f)$ obsahující konstantní polynom r a označíme $c = x + (f)$ třídu obsahující polynom x, pak $R[x]/(f) = R(c)$ a f je minimální polynom prvku c nad R.*

Důkaz. Protože f je ireducibilní polynom nad tělesem R, hlavní ideál $(f) \subseteq R[x]$ je maximálním ideálem okruhu polynomů $R[x]$. Protože $R[x]$ je komutativní okruh, je faktorokruh $T = R[x]/(f)$ těleso.

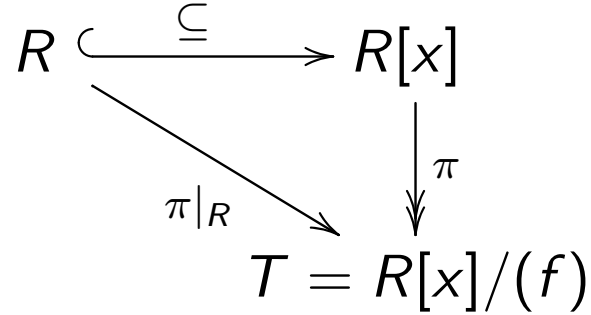


Protože $\pi|_R : R \to T$ je homomorfismus okruhů mezi tělesy, je injektivní. Proto můžeme ztotožnit libovolný prvek $r \in R$ s jeho obrazem $r + (f)$ v T.

Konstrukce jednoduchého rozšíření

Věta. *Nechť R je těleso, $f \in R[x]$ normovaný ireducibilní polynom. Pak $R[x]/(f)$ je těleso, které je jednoduché rozšíření tělesa R. Přesněji: ztotožníme libovolný prvek $r \in R$ s třídou $r + (f)$ obsahující konstantní polynom r a označíme $c = x + (f)$ třídu obsahující polynom x, pak $R[x]/(f) = R(c)$ a f je minimální polynom prvku c nad R.*

Důkaz. Protože f je ireducibilní polynom nad tělesem R, hlavní ideál $(f) \subseteq R[x]$ je maximálním ideálem okruhu polynomů $R[x]$. Protože $R[x]$ je komutativní okruh, je faktorokruh $T = R[x]/(f)$ těleso.



Protože $\pi|_R : R \to T$ je homomorfismus okruhů mezi tělesy, je injektivní. Proto můžeme ztotožnit libovolný prvek $r \in R$ s jeho obrazem $r + (f)$ v T. Po tomto ztotožnění je R podtělesem tělesa T, máme tedy rozšíření těles $R \subseteq T$.

Označme $c = x + (f)$ třídu obsahující lineární polynom x.

Označme $c = x + (f)$ třídu obsahující lineární polynom x. Pak pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= (g_m + (f))(x + (f))^m + \cdots + (g_1 + (f))(x + (f)) + (g_0 + (f)) = \\ &= (g_m x^m + \cdots + g_1 x + g_0) + (f) = g + (f). \end{aligned}$$

Označme $c = x + (f)$ třídu obsahující lineární polynom x. Pak pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= (g_m + (f))(x + (f))^m + \cdots + (g_1 + (f))(x + (f)) + (g_0 + (f)) = \\ &= (g_m x^m + \cdots + g_1 x + g_0) + (f) = g + (f). \end{aligned}$$

Odtud $T = R(c)$.

Označme $c = x + (f)$ třídu obsahující lineární polynom x. Pak pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= (g_m + (f))(x + (f))^m + \cdots + (g_1 + (f))(x + (f)) + (g_0 + (f)) = \\ &= (g_m x^m + \cdots + g_1 x + g_0) + (f) = g + (f). \end{aligned}$$

Odtud $T = R(c)$. Speciálně $f(c) = f + (f) = 0 + (f) = 0$, a tedy c je kořenem polynomu f. Protože f je normovaný a ireducibilní nad R, je f minimálním polynomem prvku c.

Označme $c = x + (f)$ třídu obsahující lineární polynom x. Pak pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= (g_m + (f))(x + (f))^m + \cdots + (g_1 + (f))(x + (f)) + (g_0 + (f)) = \\ &= (g_m x^m + \cdots + g_1 x + g_0) + (f) = g + (f). \end{aligned}$$

Odtud $T = R(c)$. Speciálně $f(c) = f + (f) = 0 + (f) = 0$, a tedy c je kořenem polynomu f. Protože f je normovaný a ireducibilní nad R, je f minimálním polynomem prvku c.

Poznámka. Je-li $\operatorname{st} f > 1$, nemá polynom f v tělese R žádný kořen.

Označme $c = x + (f)$ třídu obsahující lineární polynom x. Pak pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= (g_m + (f))(x + (f))^m + \cdots + (g_1 + (f))(x + (f)) + (g_0 + (f)) = \\ &= (g_m x^m + \cdots + g_1 x + g_0) + (f) = g + (f). \end{aligned}$$

Odtud $T = R(c)$. Speciálně $f(c) = f + (f) = 0 + (f) = 0$, a tedy c je kořenem polynomu f. Protože f je normovaný a ireducibilní nad R, je f minimálním polynomem prvku c.

Poznámka. Je-li $\operatorname{st} f > 1$, nemá polynom f v tělese R žádný kořen. Konstrukcí z předchozí věty jsme těleso R „rozšířili“ na těleso $R(c)$, přičemž minimální polynom prvku c je právě f.

Označme $c = x + (f)$ třídu obsahující lineární polynom x. Pak pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= (g_m + (f))(x + (f))^m + \cdots + (g_1 + (f))(x + (f)) + (g_0 + (f)) = \\ &= (g_m x^m + \cdots + g_1 x + g_0) + (f) = g + (f). \end{aligned}$$

Odtud $T = R(c)$. Speciálně $f(c) = f + (f) = 0 + (f) = 0$, a tedy c je kořenem polynomu f. Protože f je normovaný a ireducibilní nad R, je f minimálním polynomem prvku c.

Poznámka. Je-li $\operatorname{st} f > 1$, nemá polynom f v tělese R žádný kořen. Konstrukcí z předchozí věty jsme těleso R „rozšířili“ na těleso $R(c)$, přičemž minimální polynom prvku c je právě f. Porovnáním s důkazem věty o minimálním polynomu vidíme, že takové rozšíření je jediné až na izomorfismus, je totiž izomorfní s faktorokruhem $R[x]/(f)$.

Rozkladové těleso polynomu

Věta. *Nechť R je těleso a $f \in R[x]$ nekonstantní polynom.*

Rozkladové těleso polynomu

Věta. *Nechť R je těleso a $f \in R[x]$ nekonstantní polynom. Pak existuje rozšíření T tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.*

Rozkladové těleso polynomu

Věta. *Nechť R je těleso a $f \in R[x]$ nekonstantní polynom. Pak existuje rozšíření T tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.*

Důkaz. Větu dokážeme indukcí vzhledem ke st f.

Rozkladové těleso polynomu

Věta. *Nechť R je těleso a $f \in R[x]$ nekonstantní polynom. Pak existuje rozšíření T tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.*

Důkaz. Větu dokážeme indukcí vzhledem ke st f.

Je-li st $f = 1$, stačí vzít $T = R$.

Rozkladové těleso polynomu

Věta. *Nechť R je těleso a $f \in R[x]$ nekonstantní polynom. Pak existuje rozšíření T tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.*

Důkaz. Větu dokážeme indukcí vzhledem ke $\operatorname{st} f$.

Je-li $\operatorname{st} f = 1$, stačí vzít $T = R$.

Nechť tedy $\operatorname{st} f > 1$ a věta byla dokázána pro všechny nekonstantní polynomy stupně menšího než $\operatorname{st} f$ nad libovolným tělesem (tj. nejen nad naším R).

Rozkladové těleso polynomu

Věta. *Nechť R je těleso a $f \in R[x]$ nekonstantní polynom. Pak existuje rozšíření T tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.*

Důkaz. Větu dokážeme indukcí vzhledem ke st f.

Je-li st $f = 1$, stačí vzít $T = R$.

Nechť tedy st $f > 1$ a věta byla dokázána pro všechny nekonstantní polynomy stupně menšího než st f nad libovolným tělesem (tj. nejen nad naším R). Rozložme polynom f v $R[x]$ na součin ireducibilních činitelů (to lze, neboť R je těleso)

$$f = a \cdot g_1 \cdots g_k,$$

kde a je vedoucí koeficient polynomu f a $g_1, \ldots, g_k \in R[x]$ jsou normované ireducibilní polynomy.

Rozkladové těleso polynomu

Věta. *Nechť R je těleso a $f \in R[x]$ nekonstantní polynom. Pak existuje rozšíření T tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.*

Důkaz. Větu dokážeme indukcí vzhledem ke st f.

Je-li st $f = 1$, stačí vzít $T = R$.

Nechť tedy st $f > 1$ a věta byla dokázána pro všechny nekonstantní polynomy stupně menšího než st f nad libovolným tělesem (tj. nejen nad naším R). Rozložme polynom f v $R[x]$ na součin ireducibilních činitelů (to lze, neboť R je těleso)

$$f = a \cdot g_1 \cdots g_k,$$

kde a je vedoucí koeficient polynomu f a $g_1, \ldots, g_k \in R[x]$ jsou normované ireducibilní polynomy. Pak podle předchozí věty je $K = R[x]/(g_1)$ rozšíření tělesa R, ve kterém má polynom g_1 kořen $\alpha = x + (g_1)$.

Rozkladové těleso polynomu

Věta. *Nechť R je těleso a $f \in R[x]$ nekonstantní polynom. Pak existuje rozšíření T tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.*

Důkaz. Větu dokážeme indukcí vzhledem ke st f.

Je-li st $f = 1$, stačí vzít $T = R$.

Nechť tedy st $f > 1$ a věta byla dokázána pro všechny nekonstantní polynomy stupně menšího než st f nad libovolným tělesem (tj. nejen nad naším R). Rozložme polynom f v $R[x]$ na součin ireducibilních činitelů (to lze, neboť R je těleso)

$$f = a \cdot g_1 \cdots g_k,$$

kde a je vedoucí koeficient polynomu f a $g_1, \ldots, g_k \in R[x]$ jsou normované ireducibilní polynomy. Pak podle předchozí věty je $K = R[x]/(g_1)$ rozšíření tělesa R, ve kterém má polynom g_1 kořen $\alpha = x + (g_1)$. Existuje proto normovaný polynom $q \in K[x]$ takový, že $g_1 = (x - \alpha) \cdot q$.

Rozkladové těleso polynomu

Věta. *Nechť R je těleso a $f \in R[x]$ nekonstantní polynom. Pak existuje rozšíření T tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.*

Důkaz. Větu dokážeme indukcí vzhledem ke $\operatorname{st} f$.

Je-li $\operatorname{st} f = 1$, stačí vzít $T = R$.

Nechť tedy $\operatorname{st} f > 1$ a věta byla dokázána pro všechny nekonstantní polynomy stupně menšího než $\operatorname{st} f$ nad libovolným tělesem (tj. nejen nad naším R). Rozložme polynom f v $R[x]$ na součin ireducibilních činitelů (to lze, neboť R je těleso)

$$f = a \cdot g_1 \cdots g_k,$$

kde a je vedoucí koeficient polynomu f a $g_1, \ldots, g_k \in R[x]$ jsou normované ireducibilní polynomy. Pak podle předchozí věty je $K = R[x]/(g_1)$ rozšíření tělesa R, ve kterém má polynom g_1 kořen $\alpha = x + (g_1)$. Existuje proto normovaný polynom $q \in K[x]$ takový, že $g_1 = (x - \alpha) \cdot q$. Označme $g = a \cdot q \cdot g_2 \cdots g_k \in K[x]$, pak $f = (x - \alpha) \cdot g$ a $\operatorname{st} g = \operatorname{st} f - 1$.

Proto podle indukčního předpokladu existuje rozšíření T tělesa K takové, že g se v $T[x]$ rozkládá na součin lineárních činitelů.

Proto podle indukčního předpokladu existuje rozšíření T tělesa K takové, že g se v $T[x]$ rozkládá na součin lineárních činitelů. Pak T je také rozšíření tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.

Proto podle indukčního předpokladu existuje rozšíření T tělesa K takové, že g se v $T[x]$ rozkládá na součin lineárních činitelů. Pak T je také rozšíření tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.

Definice. Podle předchozí věty pro libovolný nekonstantní polynom $f \in R[x]$, kde R je těleso, existuje rozšíření $R \subseteq T$ takové, že

$$f = a \cdot (x - \alpha_1) \cdots (x - \alpha_n),$$

kde $a \in R$, $\alpha_1, \ldots, \alpha_n \in T$.

Proto podle indukčního předpokladu existuje rozšíření T tělesa K takové, že g se v $T[x]$ rozkládá na součin lineárních činitelů. Pak T je také rozšíření tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.

Definice. Podle předchozí věty pro libovolný nekonstantní polynom $f \in R[x]$, kde R je těleso, existuje rozšíření $R \subseteq T$ takové, že

$$f = a \cdot (x - \alpha_1) \cdots (x - \alpha_n),$$

kde $a \in R$, $\alpha_1, \ldots, \alpha_n \in T$. Pak těleso $R(\alpha_1, \ldots, \alpha_n)$ nazýváme rozkladové těleso polynomu f nad tělesem R.

Proto podle indukčního předpokladu existuje rozšíření T tělesa K takové, že g se v $T[x]$ rozkládá na součin lineárních činitelů. Pak T je také rozšíření tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.

Definice. Podle předchozí věty pro libovolný nekonstantní polynom $f \in R[x]$, kde R je těleso, existuje rozšíření $R \subseteq T$ takové, že

$$f = a \cdot (x - \alpha_1) \cdots (x - \alpha_n),$$

kde $a \in R$, $\alpha_1, \ldots, \alpha_n \in T$. Pak těleso $R(\alpha_1, \ldots, \alpha_n)$ nazýváme rozkladové těleso polynomu f nad tělesem R.

Poznámka. Je možné dokázat, že rozkladové těleso polynomu f nad tělesem R je určeno jednoznačně až na izomorfismus: jsou-li K, L obě rozkladová tělesa polynomu f nad tělesem R, pak existuje izomorfismus $\varphi : K \to L$ takový, že $\varphi(r) = r$ pro každé $r \in R$.

Popis jednoduchých rozšíření

Věta. *Nechť $R \subseteq T$ je rozšíření těles.*

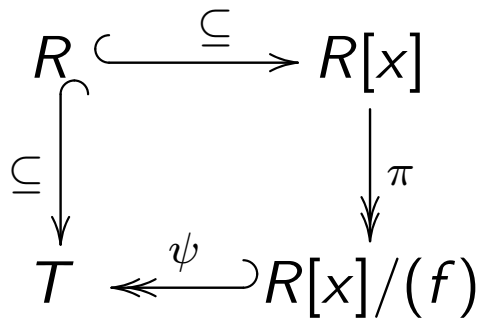
Popis jednoduchých rozšíření

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Pak platí: $R \subseteq T$ je jednoduché rozšíření, právě když existuje polynom $f \in R[x]$, který je ireducibilní nad R, a izomorfismus okruhů $\psi : R[x]/(f) \to T$ tak, že následující diagram komutuje*

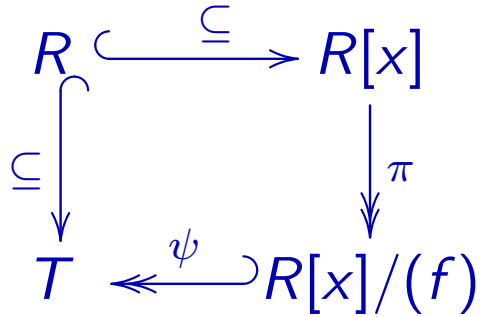
$$\begin{array}{ccc} R & \xhookrightarrow{\subseteq} & R[x] \\ {\scriptstyle\subseteq}\downarrow & & \downarrow{\scriptstyle\pi} \\ T & \xleftarrow{\psi} & R[x]/(f) \end{array}$$

Popis jednoduchých rozšíření

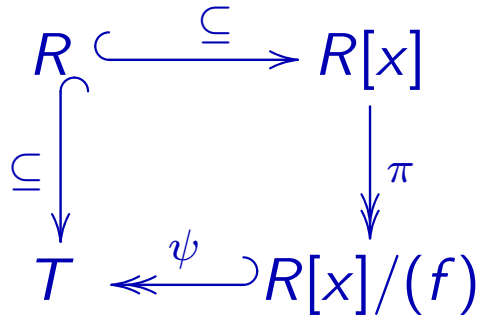
Věta. *Nechť $R \subseteq T$ je rozšíření těles. Pak platí: $R \subseteq T$ je jednoduché rozšíření, právě když existuje polynom $f \in R[x]$, který je ireducibilní nad R, a izomorfismus okruhů $\psi : R[x]/(f) \to T$ tak, že následující diagram komutuje*



Důkaz. „⇒“ Je-li $T = R(c)$, kde c je algebraický prvek nad R, pak jsme izomorfismus ψ získali v důkaze věty o minimálním polynomu (tam se jmenoval $\tilde{\varphi}$).

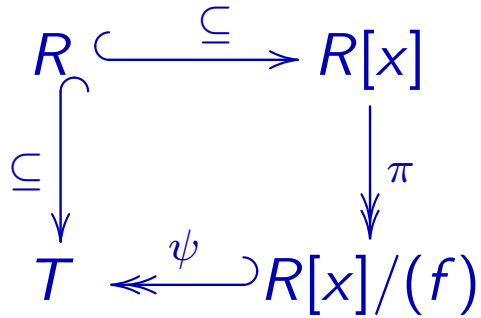


„⇐“ Označme $c = \psi(x + (f)) \in T$.



„⇐“ Označme $c = \psi(x + (f)) \in T$. Pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

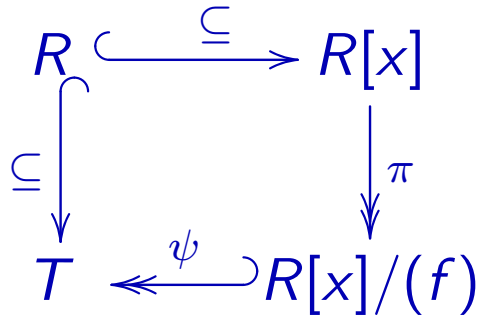
$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= \psi(g_m + (f)) \cdot (\psi(x + (f)))^m + \cdots + \\ &\quad + \psi(g_1 + (f)) \cdot \psi(x + (f)) + \psi(g_0 + (f)) = \\ &= \psi(g_m x^m + \cdots + g_1 x + g_0 + (f)) = \psi(g + (f)). \end{aligned}$$



„⇐“ Označme $c = \psi(x + (f)) \in T$. Pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= \psi(g_m + (f)) \cdot (\psi(x + (f)))^m + \cdots + \\ &\quad + \psi(g_1 + (f)) \cdot \psi(x + (f)) + \psi(g_0 + (f)) = \\ &= \psi(g_m x^m + \cdots + g_1 x + g_0 + (f)) = \psi(g + (f)). \end{aligned}$$

Libovolný prvek tělesa T je tedy tvaru $g(c)$ pro vhodný $g \in R[x]$, proto $T = R(c)$.



„⇐“ Označme $c = \psi(x + (f)) \in T$. Pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= \psi(g_m + (f)) \cdot (\psi(x + (f)))^m + \cdots + \\ &\quad + \psi(g_1 + (f)) \cdot \psi(x + (f)) + \psi(g_0 + (f)) = \\ &= \psi(g_m x^m + \cdots + g_1 x + g_0 + (f)) = \psi(g + (f)). \end{aligned}$$

Libovolný prvek tělesa T je tedy tvaru $g(c)$ pro vhodný $g \in R[x]$, proto $T = R(c)$. Volbou $g = f$ dostaneme

$$f(c) = \psi(f + (f)) = \psi(0 + (f)) = 0,$$

a tudíž c je algebraický nad R.

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R.*

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Důkaz. Zřejmě $R \subseteq A$, neboť každý $r \in R$ je kořenem nenulového polynomu $x - r \in R[x]$.

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Důkaz. Zřejmě $R \subseteq A$, neboť každý $r \in R$ je kořenem nenulového polynomu $x - r \in R[x]$. Musíme dokázat, že pro každé $\alpha, \beta \in A$ platí $-\alpha, \alpha + \beta, \alpha \cdot \beta \in A$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in A$.

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Důkaz. Zřejmě $R \subseteq A$, neboť každý $r \in R$ je kořenem nenulového polynomu $x - r \in R[x]$. Musíme dokázat, že pro každé $\alpha, \beta \in A$ platí $-\alpha, \alpha + \beta, \alpha \cdot \beta \in A$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in A$. Protože α je algebraický nad R, platí $[R(\alpha) : R] < \infty$.

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Důkaz. Zřejmě $R \subseteq A$, neboť každý $r \in R$ je kořenem nenulového polynomu $x - r \in R[x]$. Musíme dokázat, že pro každé $\alpha, \beta \in A$ platí $-\alpha, \alpha + \beta, \alpha \cdot \beta \in A$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in A$. Protože α je algebraický nad R, platí $[R(\alpha) : R] < \infty$. Zřejmě $(R(\alpha))(\beta)$ je nejmenší podtěleso tělesa T obsahující $(R(\alpha)) \cup \{\beta\}$, a tedy nejmenší podtěleso tělesa T obsahující $R \cup \{\alpha, \beta\}$.

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Důkaz. Zřejmě $R \subseteq A$, neboť každý $r \in R$ je kořenem nenulového polynomu $x - r \in R[x]$. Musíme dokázat, že pro každé $\alpha, \beta \in A$ platí $-\alpha, \alpha + \beta, \alpha \cdot \beta \in A$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in A$. Protože α je algebraický nad R, platí $[R(\alpha) : R] < \infty$. Zřejmě $(R(\alpha))(\beta)$ je nejmenší podtěleso tělesa T obsahující $(R(\alpha)) \cup \{\beta\}$, a tedy nejmenší podtěleso tělesa T obsahující $R \cup \{\alpha, \beta\}$. Proto $(R(\alpha))(\beta) = R(\alpha, \beta)$.

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Důkaz. Zřejmě $R \subseteq A$, neboť každý $r \in R$ je kořenem nenulového polynomu $x - r \in R[x]$. Musíme dokázat, že pro každé $\alpha, \beta \in A$ platí $-\alpha, \alpha + \beta, \alpha \cdot \beta \in A$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in A$. Protože α je algebraický nad R, platí $[R(\alpha) : R] < \infty$. Zřejmě $(R(\alpha))(\beta)$ je nejmenší podtěleso tělesa T obsahující $(R(\alpha)) \cup \{\beta\}$, a tedy nejmenší podtěleso tělesa T obsahující $R \cup \{\alpha, \beta\}$. Proto $(R(\alpha))(\beta) = R(\alpha, \beta)$. Protože β je algebraický nad R, je také algebraický nad $R(\alpha)$ a platí $[R(\alpha, \beta) : R(\alpha)] < \infty$.

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Důkaz. Zřejmě $R \subseteq A$, neboť každý $r \in R$ je kořenem nenulového polynomu $x - r \in R[x]$. Musíme dokázat, že pro každé $\alpha, \beta \in A$ platí $-\alpha, \alpha + \beta, \alpha \cdot \beta \in A$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in A$. Protože α je algebraický nad R, platí $[R(\alpha) : R] < \infty$. Zřejmě $(R(\alpha))(\beta)$ je nejmenší podtěleso tělesa T obsahující $(R(\alpha)) \cup \{\beta\}$, a tedy nejmenší podtěleso tělesa T obsahující $R \cup \{\alpha, \beta\}$. Proto $(R(\alpha))(\beta) = R(\alpha, \beta)$. Protože β je algebraický nad R, je také algebraický nad $R(\alpha)$ a platí $[R(\alpha, \beta) : R(\alpha)] < \infty$. Dohromady $[R(\alpha, \beta) : R] = [R(\alpha, \beta) : R(\alpha)] \cdot [R(\alpha) : R] < \infty$.

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Důkaz. Zřejmě $R \subseteq A$, neboť každý $r \in R$ je kořenem nenulového polynomu $x - r \in R[x]$. Musíme dokázat, že pro každé $\alpha, \beta \in A$ platí $-\alpha, \alpha + \beta, \alpha \cdot \beta \in A$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in A$. Protože α je algebraický nad R, platí $[R(\alpha) : R] < \infty$. Zřejmě $(R(\alpha))(\beta)$ je nejmenší podtěleso tělesa T obsahující $(R(\alpha)) \cup \{\beta\}$, a tedy nejmenší podtěleso tělesa T obsahující $R \cup \{\alpha, \beta\}$. Proto $(R(\alpha))(\beta) = R(\alpha, \beta)$. Protože β je algebraický nad R, je také algebraický nad $R(\alpha)$ a platí $[R(\alpha, \beta) : R(\alpha)] < \infty$. Dohromady $[R(\alpha, \beta) : R] = [R(\alpha, \beta) : R(\alpha)] \cdot [R(\alpha) : R] < \infty$. Protože každé konečné rozšíření těles je algebraické, platí, že $-\alpha, \alpha + \beta, \alpha \cdot \beta \in R(\alpha, \beta)$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in R(\alpha, \beta)$ jsou algebraické prvky nad R.

Příklad nekonečného algebraického rozšíření

Aplikujme předchozí větu na rozšíření $\mathbb{Q} \subseteq \mathbb{C}$.

Příklad nekonečného algebraického rozšíření

Aplikujme předchozí větu na rozšíření $\mathbb{Q} \subseteq \mathbb{C}$. Pak A je těleso všech algebraických čísel.

Příklad nekonečného algebraického rozšíření

Aplikujme předchozí větu na rozšíření $\mathbb{Q} \subseteq \mathbb{C}$. Pak A je těleso všech algebraických čísel. Proto je $\mathbb{Q} \subseteq A$ algebraické rozšíření.

Příklad nekonečného algebraického rozšíření

Aplikujme předchozí větu na rozšíření $\mathbb{Q} \subseteq \mathbb{C}$. Pak A je těleso všech algebraických čísel. Proto je $\mathbb{Q} \subseteq A$ algebraické rozšíření.

Ukážeme, že $\mathbb{Q} \subseteq A$ není konečné.

Příklad nekonečného algebraického rozšíření

Aplikujme předchozí větu na rozšíření $\mathbb{Q} \subseteq \mathbb{C}$. Pak A je těleso všech algebraických čísel. Proto je $\mathbb{Q} \subseteq A$ algebraické rozšíření.

Ukážeme, že $\mathbb{Q} \subseteq A$ není konečné. Pro libovolné $n \in \mathbb{N}$ je polynom $x^n - 2$ je ireducibilní nad $\mathbb{Q}$ podle Eisensteinova kriteria, a tedy je minimálním polynomem algebraického čísla $\sqrt[n]{2}$, odkud $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.

Příklad nekonečného algebraického rozšíření

Aplikujme předchozí větu na rozšíření $\mathbb{Q} \subseteq \mathbb{C}$. Pak A je těleso všech algebraických čísel. Proto je $\mathbb{Q} \subseteq A$ algebraické rozšíření.

Ukážeme, že $\mathbb{Q} \subseteq A$ není konečné. Pro libovolné $n \in \mathbb{N}$ je polynom $x^n - 2$ je ireducibilní nad $\mathbb{Q}$ podle Eisensteinova kriteria, a tedy je minimálním polynomem algebraického čísla $\sqrt[n]{2}$, odkud $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Proto vektorový prostor A nad $\mathbb{Q}$ obsahuje n-rozměrný vektorový podprostor pro každé $n \in \mathbb{N}$, nemůže být tedy konečněrozměrný.

(Ne)řešitelnost geometrických úloh pravítkem a kružítkem

Z antiky pocházejí tři problémy, jejichž řešení pravítkem a kružítkem nebylo známo:

(Ne)řešitelnost geometrických úloh pravítkem a kružítkem

Z antiky pocházejí tři problémy, jejichž řešení pravítkem a kružítkem nebylo známo:

- *trisekce úhlu* (rozdělit daný úhel na třetiny),

(Ne)řešitelnost geometrických úloh pravítkem a kružítkem

Z antiky pocházejí tři problémy, jejichž řešení pravítkem a kružítkem nebylo známo:

- *trisekce úhlu* (rozdělit daný úhel na třetiny),
- *zdvojení krychle* (k dané krychli sestrojit krychli dvojnásobného objemu, tj. k úsečce dané délky najít úsečku $\sqrt[3]{2}$-krát delší),

(Ne)řešitelnost geometrických úloh pravítkem a kružítkem

Z antiky pocházejí tři problémy, jejichž řešení pravítkem a kružítkem nebylo známo:

- *trisekce úhlu* (rozdělit daný úhel na třetiny),
- *zdvojení krychle* (k dané krychli sestrojit krychli dvojnásobného objemu, tj. k úsečce dané délky najít úsečku $\sqrt[3]{2}$-krát delší),
- *kvadratura kruhu* (k danému kruhu sestrojit čtverec o stejném obsahu).

(Ne)řešitelnost geometrických úloh pravítkem a kružítkem

Z antiky pocházejí tři problémy, jejichž řešení pravítkem a kružítkem nebylo známo:

- *trisekce úhlu* (rozdělit daný úhel na třetiny),
- *zdvojení krychle* (k dané krychli sestrojit krychli dvojnásobného objemu, tj. k úsečce dané délky najít úsečku $\sqrt[3]{2}$-krát delší),
- *kvadratura kruhu* (k danému kruhu sestrojit čtverec o stejném obsahu).

Abychom mohli dokázat, že žádné řešení těchto úloh neexistuje, musíme přesně specifikovat, co to znamená řešit úlohu pravítkem a kružítkem.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy. Těmto bodům budeme říkat význačné.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy. Těmto bodům budeme říkat význačné. Smíme sestrojit libovolnou přímku procházející dvěma význačnými body a libovolnou kružnici, jejímž středem je význačný bod a poloměrem vzdálenost některých dvou význačných bodů.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy. Těmto bodům budeme říkat význačné. Smíme sestrojit libovolnou přímku procházející dvěma význačnými body a libovolnou kružnici, jejímž středem je význačný bod a poloměrem vzdálenost některých dvou význačných bodů. Libovolný průsečík sestrojených kružnic či přímek můžeme přidat k význačným bodům.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy. Těmto bodům budeme říkat význačné. Smíme sestrojit libovolnou přímku procházející dvěma význačnými body a libovolnou kružnici, jejímž středem je význačný bod a poloměrem vzdálenost některých dvou význačných bodů. Libovolný průsečík sestrojených kružnic či přímek můžeme přidat k význačným bodům. Jde o to, jestli po konečně mnoha krocích lze docílit toho, že mezi význačnými body je bod, který popisuje řešení dané úlohy.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy. Těmto bodům budeme říkat význačné. Smíme sestrojit libovolnou přímku procházející dvěma význačnými body a libovolnou kružnici, jejímž středem je význačný bod a poloměrem vzdálenost některých dvou význačných bodů. Libovolný průsečík sestrojených kružnic či přímek můžeme přidat k význačným bodům. Jde o to, jestli po konečně mnoha krocích lze docílit toho, že mezi význačnými body je bod, který popisuje řešení dané úlohy.

Zavedeme v této rovině soustavu souřadnic, rovinu tedy ztotožňujeme s kartézským součinem $\mathbb{R} \times \mathbb{R}$.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy. Těmto bodům budeme říkat význačné. Smíme sestrojit libovolnou přímku procházející dvěma význačnými body a libovolnou kružnici, jejímž středem je význačný bod a poloměrem vzdálenost některých dvou význačných bodů. Libovolný průsečík sestrojených kružnic či přímek můžeme přidat k význačným bodům. Jde o to, jestli po konečně mnoha krocích lze docílit toho, že mezi význačnými body je bod, který popisuje řešení dané úlohy.

Zavedeme v této rovině soustavu souřadnic, rovinu tedy ztotožňujeme s kartézským součinem $\mathbb{R} \times \mathbb{R}$. Označme T_0 podtěleso tělesa $\mathbb{R}$ generované x-ovými a y-ovými souřadnicemi všech zadaných bodů.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy. Těmto bodům budeme říkat význačné. Smíme sestrojit libovolnou přímku procházející dvěma význačnými body a libovolnou kružnici, jejímž středem je význačný bod a poloměrem vzdálenost některých dvou význačných bodů. Libovolný průsečík sestrojených kružnic či přímek můžeme přidat k význačným bodům. Jde o to, jestli po konečně mnoha krocích lze docílit toho, že mezi význačnými body je bod, který popisuje řešení dané úlohy.

Zavedeme v této rovině soustavu souřadnic, rovinu tedy ztotožňujeme s kartézským součinem $\mathbb{R} \times \mathbb{R}$. Označme T_0 podtěleso tělesa $\mathbb{R}$ generované x-ovými a y-ovými souřadnicemi všech zadaných bodů. Pokud bylo přidáno celkem n význačných bodů, definujeme tělesa $T_1, \ldots, T_n$ takto: těleso T_i je generováno tělesem T_{i-1} a souřadnicemi i-tého význačného bodu.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy. Těmto bodům budeme říkat význačné. Smíme sestrojit libovolnou přímku procházející dvěma význačnými body a libovolnou kružnici, jejímž středem je význačný bod a poloměrem vzdálenost některých dvou význačných bodů. Libovolný průsečík sestrojených kružnic či přímek můžeme přidat k význačným bodům. Jde o to, jestli po konečně mnoha krocích lze docílit toho, že mezi význačnými body je bod, který popisuje řešení dané úlohy.

Zavedeme v této rovině soustavu souřadnic, rovinu tedy ztotožňujeme s kartézským součinem $\mathbb{R} \times \mathbb{R}$. Označme T_0 podtěleso tělesa $\mathbb{R}$ generované x-ovými a y-ovými souřadnicemi všech zadaných bodů. Pokud bylo přidáno celkem n význačných bodů, definujeme tělesa $T_1, \ldots, T_n$ takto: těleso T_i je generováno tělesem T_{i-1} a souřadnicemi i-tého význačného bodu.

Naším cílem je dokázat, že rozšíření těles $T_0 \subseteq T_n$ je konečné a jeho stupeň $[T_n : T_0] \mid 2^n$.

Označme $[x_i, y_i]$ souřadnice i-tého význačného bodu.

Označme $[x_i, y_i]$ souřadnice i-tého význačného bodu. Tento bod byl získán jako průsečík sestrojených přímek či kružnic, rovnice takové přímky je tvaru $ax + by = c$, kde $a, b, c \in T_{i-1}$, rovnice takové kružnice tvaru $(x - m)^2 + (y - n)^2 = u$, kde $m, n, u \in T_{i-1}$.

Označme $[x_i, y_i]$ souřadnice i-tého význačného bodu. Tento bod byl získán jako průsečík sestrojených přímek či kružnic, rovnice takové přímky je tvaru $ax + by = c$, kde $a, b, c \in T_{i-1}$, rovnice takové kružnice tvaru $(x - m)^2 + (y - n)^2 = u$, kde $m, n, u \in T_{i-1}$. Proto $[x_i, y_i]$ je řešením soustavy dvou lineárních rovnic anebo soustavy jedné lineární a jedné kvadratické rovnice s koeficienty v T_{i-1} (případ dvou kružnic vede sice na soustavu dvou kvadratických rovnic, jejich odečtením však dostaneme rovnici lineární).

Označme $[x_i, y_i]$ souřadnice i-tého význačného bodu. Tento bod byl získán jako průsečík sestrojených přímek či kružnic, rovnice takové přímky je tvaru $ax + by = c$, kde $a, b, c \in T_{i-1}$, rovnice takové kružnice tvaru $(x - m)^2 + (y - n)^2 = u$, kde $m, n, u \in T_{i-1}$. Proto $[x_i, y_i]$ je řešením soustavy dvou lineárních rovnic anebo soustavy jedné lineární a jedné kvadratické rovnice s koeficienty v T_{i-1} (případ dvou kružnic vede sice na soustavu dvou kvadratických rovnic, jejich odečtením však dostaneme rovnici lineární).

Dosazením z lineární rovnice do druhé rovnice získáme rovnici lineární nebo kvadratickou pro jednu ze souřadnic $[x_i, y_i]$ s koeficienty v T_{i-1}.

Označme $[x_i, y_i]$ souřadnice i-tého význačného bodu. Tento bod byl získán jako průsečík sestrojených přímek či kružnic, rovnice takové přímky je tvaru $ax + by = c$, kde $a, b, c \in T_{i-1}$, rovnice takové kružnice tvaru $(x - m)^2 + (y - n)^2 = u$, kde $m, n, u \in T_{i-1}$. Proto $[x_i, y_i]$ je řešením soustavy dvou lineárních rovnic anebo soustavy jedné lineární a jedné kvadratické rovnice s koeficienty v T_{i-1} (případ dvou kružnic vede sice na soustavu dvou kvadratických rovnic, jejich odečtením však dostaneme rovnici lineární).

Dosazením z lineární rovnice do druhé rovnice získáme rovnici lineární nebo kvadratickou pro jednu ze souřadnic $[x_i, y_i]$ s koeficienty v T_{i-1}. Minimální polynom získaného řešení nad tělesem T_{i-1} má stupeň 1 nebo 2, druhou ze souřadnic dopočítáme z lineární rovnice.

Označme $[x_i, y_i]$ souřadnice i-tého význačného bodu. Tento bod byl získán jako průsečík sestrojených přímek či kružnic, rovnice takové přímky je tvaru $ax + by = c$, kde $a, b, c \in T_{i-1}$, rovnice takové kružnice tvaru $(x - m)^2 + (y - n)^2 = u$, kde $m, n, u \in T_{i-1}$. Proto $[x_i, y_i]$ je řešením soustavy dvou lineárních rovnic anebo soustavy jedné lineární a jedné kvadratické rovnice s koeficienty v T_{i-1} (případ dvou kružnic vede sice na soustavu dvou kvadratických rovnic, jejich odečtením však dostaneme rovnici lineární).

Dosazením z lineární rovnice do druhé rovnice získáme rovnici lineární nebo kvadratickou pro jednu ze souřadnic $[x_i, y_i]$ s koeficienty v T_{i-1}. Minimální polynom získaného řešení nad tělesem T_{i-1} má stupeň 1 nebo 2, druhou ze souřadnic dopočítáme z lineární rovnice. Proto $[T_i : T_{i-1}] \leq 2$.

Označme $[x_i, y_i]$ souřadnice i-tého význačného bodu. Tento bod byl získán jako průsečík sestrojených přímek či kružnic, rovnice takové přímky je tvaru $ax + by = c$, kde $a, b, c \in T_{i-1}$, rovnice takové kružnice tvaru $(x - m)^2 + (y - n)^2 = u$, kde $m, n, u \in T_{i-1}$. Proto $[x_i, y_i]$ je řešením soustavy dvou lineárních rovnic anebo soustavy jedné lineární a jedné kvadratické rovnice s koeficienty v T_{i-1} (případ dvou kružnic vede sice na soustavu dvou kvadratických rovnic, jejich odečtením však dostaneme rovnici lineární).

Dosazením z lineární rovnice do druhé rovnice získáme rovnici lineární nebo kvadratickou pro jednu ze souřadnic $[x_i, y_i]$ s koeficienty v T_{i-1}. Minimální polynom získaného řešení nad tělesem T_{i-1} má stupeň 1 nebo 2, druhou ze souřadnic dopočítáme z lineární rovnice. Proto $[T_i : T_{i-1}] \leq 2$.

Z věty o násobení stupňů rozšíření dostáváme $[T_n : T_0] \mid 2^n$.

Neřešitelnost úlohy zdvojení krychle

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$, cílem je získat bod $[0, \sqrt[3]{2}]$.

Neřešitelnost úlohy zdvojení krychle

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$, cílem je získat bod $[0, \sqrt[3]{2}]$.

Je tedy $T_0 = \mathbb{Q}$.

Neřešitelnost úlohy zdvojení krychle

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$, cílem je získat bod $[0, \sqrt[3]{2}]$.

Je tedy $T_0 = \mathbb{Q}$.

Protože $x^3 - 2$ je minimální polynom čísla $\sqrt[3]{2}$ nad $\mathbb{Q}$, platí $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

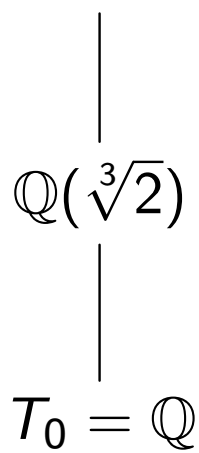
Neřešitelnost úlohy zdvojení krychle

Jsou dány dva body o souřadnicích $[0,0]$ a $[0,1]$, cílem je získat bod $[0,\sqrt[3]{2}]$.

Je tedy $T_0 = \mathbb{Q}$.

Protože $x^3 - 2$ je minimální polynom čísla $\sqrt[3]{2}$ nad $\mathbb{Q}$, platí $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Jestliže tedy $\sqrt[3]{2} \in T_n$, pak $3 \mid [T_n : T_0]$.



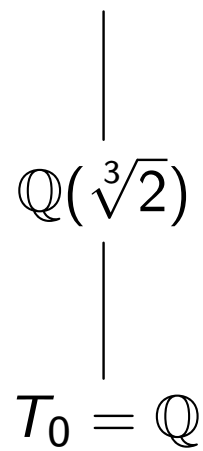
Neřešitelnost úlohy zdvojení krychle

Jsou dány dva body o souřadnicích $[0,0]$ a $[0,1]$, cílem je získat bod $[0,\sqrt[3]{2}]$.

Je tedy $T_0 = \mathbb{Q}$.

Protože $x^3 - 2$ je minimální polynom čísla $\sqrt[3]{2}$ nad $\mathbb{Q}$, platí $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Jestliže tedy $\sqrt[3]{2} \in T_n$, pak $3 \mid [T_n : T_0]$.



To spolu s odvozenou dělitelností $[T_n : T_0] \mid 2^n$ dává spor $3 \mid 2^n$.

Neřešitelnost úlohy trisekce úhlu

Ukážeme, že nemůžeme sestrojit pravítkem a kružítkem úhel $\frac{\pi}{9}$.

Neřešitelnost úlohy trisekce úhlu

Ukážeme, že nemůžeme sestrojit pravítkem a kružítkem úhel $\frac{\pi}{9}$. Vzhledem k tomu, že umíme sestrojit úhel $\frac{\pi}{3}$ jako vnitřní úhel rovnostranného trojúhelníka, bude to znamenat, že nelze rozdělit na třetiny libovolný zadaný úhel.

Neřešitelnost úlohy trisekce úhlu

Ukážeme, že nemůžeme sestrojit pravítkem a kružítkem úhel $\frac{\pi}{9}$. Vzhledem k tomu, že umíme sestrojit úhel $\frac{\pi}{3}$ jako vnitřní úhel rovnostranného trojúhelníka, bude to znamenat, že nelze rozdělit na třetiny libovolný zadaný úhel.

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$, cílem je získat bod $[\cos \frac{\pi}{9}, \sin \frac{\pi}{9}]$.

Neřešitelnost úlohy trisekce úhlu

Ukážeme, že nemůžeme sestrojit pravítkem a kružítkem úhel $\frac{\pi}{9}$. Vzhledem k tomu, že umíme sestrojit úhel $\frac{\pi}{3}$ jako vnitřní úhel rovnostranného trojúhelníka, bude to znamenat, že nelze rozdělit na třetiny libovolný zadaný úhel.

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$, cílem je získat bod $[\cos \frac{\pi}{9}, \sin \frac{\pi}{9}]$. Opět máme $T_0 = \mathbb{Q}$.

Neřešitelnost úlohy trisekce úhlu

Ukážeme, že nemůžeme sestrojit pravítkem a kružítkem úhel $\frac{\pi}{9}$. Vzhledem k tomu, že umíme sestrojit úhel $\frac{\pi}{3}$ jako vnitřní úhel rovnostranného trojúhelníka, bude to znamenat, že nelze rozdělit na třetiny libovolný zadaný úhel.

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$, cílem je získat bod $[\cos\frac{\pi}{9}, \sin\frac{\pi}{9}]$. Opět máme $T_0 = \mathbb{Q}$.

K nalezení minimálního polynomu čísla $\cos\frac{\pi}{9}$ využijeme vzorec $\cos 3\alpha = \cos^3\alpha - 3\cos\alpha\sin^2\alpha = 4\cos^3\alpha - 3\cos\alpha$.

Neřešitelnost úlohy trisekce úhlu

Ukážeme, že nemůžeme sestrojit pravítkem a kružítkem úhel $\frac{\pi}{9}$. Vzhledem k tomu, že umíme sestrojit úhel $\frac{\pi}{3}$ jako vnitřní úhel rovnostranného trojúhelníka, bude to znamenat, že nelze rozdělit na třetiny libovolný zadaný úhel.

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$, cílem je získat bod $[\cos\frac{\pi}{9}, \sin\frac{\pi}{9}]$. Opět máme $T_0 = \mathbb{Q}$.

K nalezení minimálního polynomu čísla $\cos\frac{\pi}{9}$ využijeme vzorec $\cos 3\alpha = \cos^3\alpha - 3\cos\alpha\sin^2\alpha = 4\cos^3\alpha - 3\cos\alpha$.

Pro $\alpha = \frac{\pi}{9}$ dostáváme, že $c = 2\cos\frac{\pi}{9}$ je kořenem polynomu $x^3 - 3x - 1$.

Neřešitelnost úlohy trisekce úhlu

Ukážeme, že nemůžeme sestrojit pravítkem a kružítkem úhel $\frac{\pi}{9}$. Vzhledem k tomu, že umíme sestrojit úhel $\frac{\pi}{3}$ jako vnitřní úhel rovnostranného trojúhelníka, bude to znamenat, že nelze rozdělit na třetiny libovolný zadaný úhel.

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$, cílem je získat bod $[\cos\frac{\pi}{9}, \sin\frac{\pi}{9}]$. Opět máme $T_0 = \mathbb{Q}$.

K nalezení minimálního polynomu čísla $\cos\frac{\pi}{9}$ využijeme vzorec $\cos 3\alpha = \cos^3\alpha - 3\cos\alpha\sin^2\alpha = 4\cos^3\alpha - 3\cos\alpha$.

Pro $\alpha = \frac{\pi}{9}$ dostáváme, že $c = 2\cos\frac{\pi}{9}$ je kořenem polynomu $x^3 - 3x - 1$. Tento kubický polynom nemá racionální kořen (± 1 kořen není), a tedy je ireducibilní nad $\mathbb{Q}$.

Neřešitelnost úlohy trisekce úhlu

Ukážeme, že nemůžeme sestrojit pravítkem a kružítkem úhel $\frac{\pi}{9}$. Vzhledem k tomu, že umíme sestrojit úhel $\frac{\pi}{3}$ jako vnitřní úhel rovnostranného trojúhelníka, bude to znamenat, že nelze rozdělit na třetiny libovolný zadaný úhel.

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$, cílem je získat bod $[\cos\frac{\pi}{9}, \sin\frac{\pi}{9}]$. Opět máme $T_0 = \mathbb{Q}$.

K nalezení minimálního polynomu čísla $\cos\frac{\pi}{9}$ využijeme vzorec $\cos 3\alpha = \cos^3\alpha - 3\cos\alpha\sin^2\alpha = 4\cos^3\alpha - 3\cos\alpha$.

Pro $\alpha = \frac{\pi}{9}$ dostáváme, že $c = 2\cos\frac{\pi}{9}$ je kořenem polynomu $x^3 - 3x - 1$. Tento kubický polynom nemá racionální kořen (± 1 kořen není), a tedy je ireducibilní nad $\mathbb{Q}$.

Odtud $[\mathbb{Q}(\cos\frac{\pi}{9}) : \mathbb{Q}] = 3$ a stejně jako v předchozím případě dostáváme spor.

Neřešitelnost úlohy kvadratury kruhu

V tomto případě využijeme toho, že π je transcendentní číslo (tento fakt zde nebudeme dokazovat).

Neřešitelnost úlohy kvadratury kruhu

V tomto případě využijeme toho, že π je transcendentní číslo (tento fakt zde nebudeme dokazovat).

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$.

Neřešitelnost úlohy kvadratury kruhu

V tomto případě využijeme toho, že π je transcendentní číslo (tento fakt zde nebudeme dokazovat).

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$. Kruh jednotkového poloměru má obsah π.

Neřešitelnost úlohy kvadratury kruhu

V tomto případě využijeme toho, že π je transcendentní číslo (tento fakt zde nebudeme dokazovat).

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$. Kruh jednotkového poloměru má obsah π. Cílem je získat bod $[0, \sqrt{\pi}]$.

Neřešitelnost úlohy kvadratury kruhu

V tomto případě využijeme toho, že π je transcendentní číslo (tento fakt zde nebudeme dokazovat).

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$. Kruh jednotkového poloměru má obsah π. Cílem je získat bod $[0, \sqrt{\pi}]$. Opět máme $T_0 = \mathbb{Q}$.

Neřešitelnost úlohy kvadratury kruhu

V tomto případě využijeme toho, že π je transcendentní číslo (tento fakt zde nebudeme dokazovat).

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$. Kruh jednotkového poloměru má obsah π. Cílem je získat bod $[0, \sqrt{\pi}]$. Opět máme $T_0 = \mathbb{Q}$.

Předpokládejme, že $\sqrt{\pi} \in T_n$, pak $\pi \in T_n$.

Neřešitelnost úlohy kvadratury kruhu

V tomto případě využijeme toho, že π je transcendentní číslo (tento fakt zde nebudeme dokazovat).

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$. Kruh jednotkového poloměru má obsah π. Cílem je získat bod $[0, \sqrt{\pi}]$. Opět máme $T_0 = \mathbb{Q}$.

Předpokládejme, že $\sqrt{\pi} \in T_n$, pak $\pi \in T_n$.

Protože π je transcendentní nad $\mathbb{Q}$, plyne odtud $[T_n : \mathbb{Q}] = \infty$, což je spor s tím, že $\mathbb{Q} \subseteq T_n$ je konečné rozšíření.