Ideály okruhu $(R, +, \cdot)$

Definice. Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá **ideál** okruhu R, jestliže

- $I \neq \emptyset$;
- $\forall a, b \in I : a + b \in I$;
- $\forall a \in I \ \forall r \in R : a \cdot r,\ r \cdot a \in I$.

Příklad. Pro libovolný okruh R tvoří $\{0\}$ i R ideály okruhu R. Evidentně jde o nejmenší a největší ideál okruhu R.

Příklad. Pro libovolný homomorfismus okruhů $f : R \to S$ je jádro $\ker f = \{a \in R;\ f(a) = 0\}$ ideálem okruhu R (jak připomeneme později, naopak také každý ideál je jádrem vhodného homomorfismu okruhů).

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

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

Ideál generovaný množinou

Věta. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Důsledek. *Nechť R je okruh. Systém všech ideálů okruhu R uspořádaný inkluzí je úplný svaz.*

Definice. Nechť R je okruh. Předchozí věta nám umožňuje definovat **ideál** okruhu R **generovaný množinou** $M \subseteq R$ jako průnik všech ideálů tuto množinu obsahujících.
Je to tedy nejmenší ideál okruhu R obsahující M, značíme jej (M).
Je-li $M = \{a_1, \ldots, a_n\}$, píšeme místo (M) také $(a_1, \ldots, a_n)$.

Věta. *Nechť R je komutativní okruh, $a_1, \ldots, a_n \in R$. Pak $(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n;\ r_1, \ldots, r_n \in R\}$.*

Definice. Nechť R je komutativní okruh, $a \in R$. Ideál $(a) = \{ra;\ r \in R\}$ nazýváme **hlavní ideál** okruhu R generovaný prvkem a.

Faktorizace okruhů

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

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

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

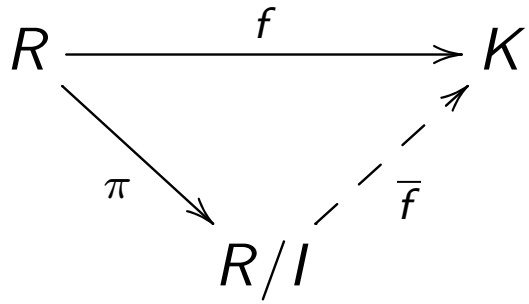
Věta. *Nechť I je ideál okruhu R. Na faktorgrupě $(R/I, +)$ lze definovat násobení pomocí reprezentantů, tedy*
$(a + I) \cdot (b + I) = (a \cdot b) + I$ pro každé $a, b \in R$.
Pak $(R/I, +, \cdot)$ je okruh a projekce $\pi : R \to R/I$ je surjektivním homomorfismem okruhů s jádrem $\ker \pi = I$.

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

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

Hlavní věta o faktorokruzích

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



Navíc platí:

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

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

Nejmenší podokruh daného okruhu

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

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

pro každé přirozené číslo n, a tedy také $f(-n) = -f(n)$. Jeho jádro $\ker f$ *je hlavní ideál okruhu $\mathbb{Z}$ generovaný charakteristikou okruhu R, tj.* $\ker f = (\operatorname{char} R)$.

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 $\mathbb{Z}/(n) = \mathbb{Z}_n$.

Maximální ideály a prvoideály

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

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

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

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

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

Maximální ideály a prvoideály okruhu polynomů nad tělesem

Věta. *Nechť R je těleso. Pak každý ideál okruhu polynomů $R[x]$ je hlavní.*

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

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

Poznámka. Je-li R těleso, pak nulový ideál $\{0\}$ je prvoideálem, ale není maximálním ideálem okruhu polynomů $R[x]$.

Podtělesa, rozšíření těles

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 **podtěleso** tělesa T. Říkáme též, že T je **rozšíření** tělesa R. Anebo také, že $R \subseteq T$ je rozšířením těles; v souladu s literaturou budeme užívat zápis: T/R je rozšířením těles (pozor, nejde o faktorizaci).

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

Příklad. Rozšířeními těles jsou například $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$. Rozšířeními těles nejsou $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{R} \subseteq \mathbb{R}[x]$. Víme, že každé těleso charakteristiky $p \neq 0$ obsahuje podtěleso izomorfní s $\mathbb{Z}_p$.

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

Důkaz. Nechť R je těleso, $\operatorname{char} R = 0$. Víme, že R obsahuje podokruh izomorfní se $\mathbb{Z}$, po ztotožnění můžeme považovat $\mathbb{Z}$ za podokruh. Protože je R těleso, s každými $m, n \in \mathbb{Z}$, $n \neq 0$ musí pak obsahovat i $m \cdot n^{-1}$. Lze tedy $\mathbb{Q}$ vnořit do R.

Těleso racionálních funkcí

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

Poznámka. 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 $\frac{f}{1}$.

Příklad. Pro libovolné těleso R je $R(x)/R$ rozšířením těles.

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.*

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 $R(c_1, \ldots, c_n)$. Takové rozšíření $R(c_1, \ldots, c_n)/R$ nazýváme **konečně generované**.

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

Stupeň rozšíření těles

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

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

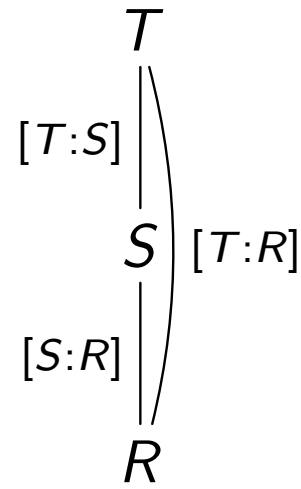
(v T platí distributivní zákony, násobení je asociativní a 1 je jednička). Máme tedy definovánu dimenzi $\dim_R T \in \mathbb{N} \cup \{\infty\}$, zřejmě tato dimenze nemůže být nula.

Definice. Nechť T/R je rozšířením těles. **Stupeň** $[T : R]$ tohoto **rozšíření** definujeme jako dimenzi vektorového prostoru T nad tělesem R, tj. $[T : R] = \dim_R T$.

Multiplikativnost stupně rozšíření

Věta. *Nechť S/R, T/S jsou rozšíření těles. Pak platí*

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



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

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

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

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

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

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

Je-li $\sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij}(\alpha_i\beta_j)$ pro nějaké prvky $\varepsilon_{ij} \in R$ 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 T/R 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 T/R 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 T/R 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 $[R(c) : R] = \operatorname{st} f$.*

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

Věta. *Nechť T/R 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 $[R(c) : R] = \infty$.*

Jednoduchá, konečná a algebraická rozšíření

Definice. Nechť T/R 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: *Každé konečné rozšíření těles charakteristiky nula je jednoduché.* Tuto větu však budeme dokazovat až později.

Konečná a algebraická rozšíření

Věta. *Každé konečné rozšíření těles je algebraické.*

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

Věta. *Nechť T/R je rozšíření těles a nechť $\alpha, \beta \in T$ jsou algebraické nad tělesem R. Pak $\alpha \pm \beta$, $\alpha\beta$, a také α^{-1}, je-li $\alpha \neq 0$, jsou algebraické nad tělesem R.*

Důkaz. Protože α je algebraický nad R, platí $[R(\alpha) : R] < \infty$. Protože β je algebraický nad R, je také algebraický nad $R(\alpha)$ a platí $[(R(\alpha))(\beta) : R(\alpha)] < \infty$. Protože $R(\alpha, \beta) = (R(\alpha))(\beta)$, je $[R(\alpha, \beta) : R] = [(R(\alpha))(\beta) : R(\alpha)] \cdot [R(\alpha) : R] < \infty$. Protože každé konečné rozšíření těles je algebraické, je každý prvek tělesa $R(\alpha, \beta)$ algebraický nad R.

Věta. *Rozšíření těles T/R je konečné, právě když $T = R(c_1, \ldots, c_n)$ pro konečně mnoho prvků $c_1, \ldots, c_n$, které jsou všechny algebraické nad tělesem R.*

Důkaz. Užijeme rovnost $R(c_1, \ldots, c_n) = (R(c_1))(c_2, \ldots, c_n)$.
„$\Rightarrow$“ Indukcí vůči stupni $[T : R]$.
„$\Leftarrow$“ Indukcí vůči n argumentací jako v předešlém důkaze.

Příklad nekonečného algebraického rozšíření

Důsledek. *Nechť T/R 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.*

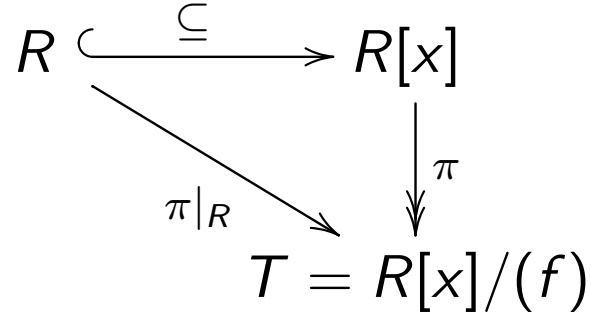
Příklad. Aplikujme předchozí důsledek na rozšíření $\mathbb{C}/\mathbb{Q}$. Pak A je těleso všech algebraických čísel. Proto je $A/\mathbb{Q}$ algebraické rozšíření.

Ukážeme, že $A/\mathbb{Q}$ 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.

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 T/R.

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.
Takové rozšíření $R(c)$ (pro daný minimální polynom f prvku c) je jediné až na izomorfismus, uvidíme, že je totiž vždy izomorfní s faktorokruhem $R[x]/(f)$.

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 $\operatorname{st} f$.

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. 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 T/R 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. Budeme chtít dokázat, že rozkladové těleso polynomu f nad tělesem R je určeno jednoznačně až na izomorfismus v následujícím smyslu: 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 $r \in R$. Je to důsledek následující věty.

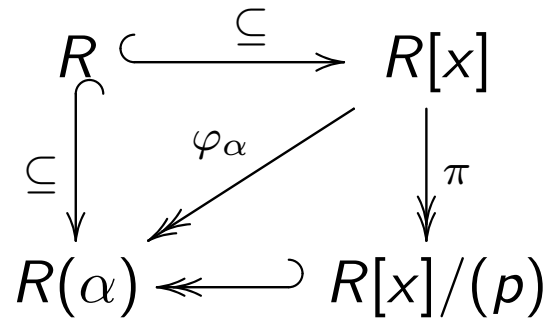
Věta o izomorfismu jednoduchých rozšíření

Věta. *Nechť $\psi : R \to R'$ je izomorfismus těles a $p \in R[x]$ ireducibilní polynom. Nechť $\Psi : R[x] \to R'[x]$ je izomorfismus indukovaný izomorfismem ψ na koeficientech, tedy*

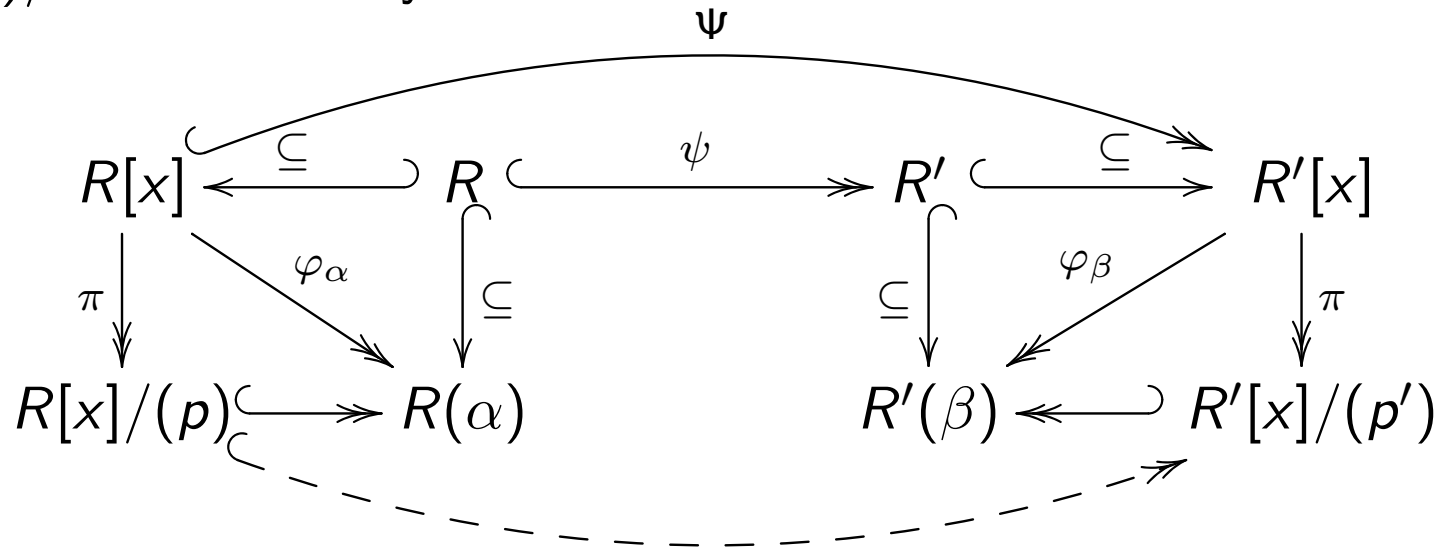
$$\Psi(r_n x^n + \cdots + r_1 x + r_0) = \psi(r_n)x^n + \cdots + \psi(r_1)x + \psi(r_0)$$

pro každé $r_0, \ldots, r_n \in R$; označme $p' = \Psi(p)$. Nechť α je kořen polynomu p v nějakém rozšíření tělesa R a β je kořen polynomu p' v nějakém rozšíření tělesa R', máme tedy tělesa $R(\alpha)$ a $R'(\beta)$. Pak existuje (a to jediný) izomorfismus $\sigma : R(\alpha) \to R'(\beta)$ splňující $\sigma(r) = \psi(r)$ pro každé $r \in R$ a $\sigma(\alpha) = \beta$.

Důkaz. Označme $\varphi_\alpha : R[x] \to R(\alpha)$ zobrazení, přiřazující každému polynomu jeho hodnotu v α;
víme, že φ_α je surjektivní homomorfismus okruhů,
jehož jádrem je hlavní ideál (p).
Máme tedy komutativní diagram,
kde π je projekce na faktorokruh.



Analogický diagram máme i pro jednoduché rozšíření těles $R'(\beta)/R'$, dohromady



kde je čárkovanou šipkou vyznačen izomorfismus faktorokruhů $R[x]/(p) \to R'[x]/(p')$ daný tím, že $\Psi(p) = p'$.
Protože všechny trojúhelníky i čtyřúhelník nahoře komutují a komutuje i vnější čtyřúhelník, musí komutovat i šestiúhelník uprostřed. Hledaný izomorfismus $\sigma : R(\alpha) \to R'(\beta)$ získáme složením tří izomorfismů v diagramu, zřejmě splňuje $\sigma(r) = \psi(r)$ pro každé $r \in R$ a $\sigma(\alpha) = \beta$. Protože každý prvek tělesa $R(\alpha) = R[\alpha]$ je tvaru $h(\alpha)$ pro vhodný polynom $h \in R[x]$, je těmito podmínkami izomorfismus σ určen jednoznačně.

Kompozitum podtěles v daném tělese

Definice. Nechť R_1 a R_2 jsou podtělesa tělesa T.
Kompozitum R_1R_2 těchto těles je definováno jako nejmenší podtěleso tělesa T obsahující obě tělesa R_1 i R_2.

Poznámka. Kompozitum R_1R_2 je tedy supremem těles R_1 a R_2 ve svazu všech podtěles tělesa T.

Příklad. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ je kompozitem těles $\mathbb{Q}(\sqrt{2})$ a $\mathbb{Q}(\sqrt{3})$ v $\mathbb{R}$.

Příklad. Nechť T/R je rozšíření těles, $c_1,\ldots,c_n,d_1,\ldots,d_m \in T$. Pak kompozitem těles $R(c_1,\ldots,c_n)$ a $R(d_1,\ldots,d_m)$ v T je $R(c_1,\ldots,c_n,d_1,\ldots,d_m)$.

Příklad. Tělesa $R_1 = \mathbb{Q}(\sqrt[4]{2})$ a $R_2 = \mathbb{Q}(i\sqrt[4]{2})$ jsou izomorfní, neboť čísla $\sqrt[4]{2}$ a $i\sqrt[4]{2}$ mají stejný minimální polynom x^4-2 nad $\mathbb{Q}$.
Přesto kompozita $R_1R_1 = R_1$ a R_1R_2 nejsou izomorfní, neboť R_1R_2 obsahuje kořen i polynomu x^2+1, kdežto $R_1 \subseteq \mathbb{R}$.

Kompozitem konečných rozšíření je konečné rozšíření

Věta. *Nechť R_1 a R_2 jsou podtělesa tělesa T, přičemž R_1 i R_2 jsou konečná rozšíření tělesa R. Pak i kompozitum R_1R_2 je konečným rozšířením tělesa R a platí*

$$[R_1R_2 : R] \leq [R_1 : R] \cdot [R_2 : R],$$

přičemž rovnost nastane, právě když je báze tělesa R_1 lineárně nezávislá nad tělesem R_2. Přesněji, je-li $\alpha_1, \ldots, \alpha_n$, resp. $\beta_1, \ldots, \beta_m$, báze R_1, resp. R_2, nad R, pak součiny $\alpha_i\beta_j$ pro $i = 1, \ldots, n$, $j = 1, \ldots, m$ generují kompozitum R_1R_2 jako vektorový prostor nad R.

Důkaz. Množina M všech lineárních kombinací $\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\alpha_i\beta_j$ s koeficienty z $r_{ij} \in R$ tvoří podokruh tělesa T obsahující $R_1 \cup R_2$, který je současně vektorovým prostorem nad R dimenze nejvýše mn. Pro každé $\gamma \in M$, $\gamma \neq 0$ je $mn + 1$ prvků $1, \gamma, \ldots, \gamma^{mn}$ lineárně závislých nad R, z lineární závislosti dostaneme úpravou $\gamma^{-1} \in M$, a tedy M je podtělesem tělesa T.
Zřejmě každé těleso obsahující $R_1 \cup R_2$ musí obsahovat i M.

(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. 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 dokážat, 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. 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 $[T_i : T_{i-1}] \in \{1, 2\}$.

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 $[0,\sqrt[3]{2}]$.

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 $3 \mid [T_n : T_0]$.

$$\begin{array}{c} T_n \\ | \\ \mathbb{Q}(\sqrt[3]{2}) \\ | \\ T_0 = \mathbb{Q} \end{array}$$

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 $\frac{\pi}{9}$. Vzhledem k tomu, že umíme sestrojit úhel $\frac{\pi}{3}$ jako vnitřní úhel rovnostranného trojúhelníka, bude to znamenat, že existuje úhel, které nelze rozdělit na třetiny.

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 $2\cos\frac{\pi}{9}$ 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).

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.