UNIVERZITA PALACKÉHO V OLOMOUCI

PŘÍRODOVĚDECKÁ FAKULTA

Katedra algebry a geometrie

Základy teorie těles v úlohách

BAKALÁŘSKÁ PRÁCE

Vedoucí bakalářské práce:
Doc. RNDr. Petr Emanovský, Ph.D.

Vypracoval:
Tomáš Táborský
F–M, 3. ročník

Datum odevzdání: 24. dubna 2009

Olomouc 2009

Prohlášení

Prohlašuji, že jsem předloženou bakalářskou práci vypracoval samostatně za vedení doc. RNDr. Petra Emanovského, Ph.D., a že jsem v seznamu literatury uvedl všechny zdroje, z nichž jsem při zpracování čerpal.

V Olomouci dne 24. dubna 2009

Tomáš Táborský

Poděkování

Rád bych na tomto místě poděkoval doc. RNDr. Petru Emanovskému, Ph.D., vedoucímu bakalářské práce, za odborné vedení, obětavou spolupráci, poskytnutí cenných rad a připomínek a za čas, který mi věnoval při konzultacích.

Obsah

Úvod

Tato bakalářská práce se věnuje základním pojmům teorie těles, zejména vlastnostem algebraického rozšíření těles a konstrukci konečných těles. Znalost základních pojmů z algebry jako těleso, grupa, atd., již přepokládám, proto jsem považoval za zbytečné je znovu opakovat. Při zpracování tématu jsem se snažil vytypovat jednotlivé partie této problematiky a utřídit ji do logicky navazujících celků.

Cílém této práce bylo představit čtenáři problematiku těles srozumitelným způsobem prostřednictvím řady ukázkových úloh. Vycházím především z knih [3] a [7], uvedená terminologie je zavedena podle knihy [3]. Pro lepší názornost jsou na závěr kapitoly uvedeny řešené příklady a následně i cvičení pro samostatné řešení, jednotlivé příklady jsou uvedeny s výsledky pro následnou kontrolu. Příklady jsem se snažil vybírat tak, aby jednotlivé pojmy a vlastnosti na nich byly srozumitelně demonstrovány. Při výběru těchto příkladů jsem se nechal inspirovat neřešenými příklady z [3], [7].

V první a druhé kapitole jsou definovány základní pojmy, jejichž znalost je potřebná pro pochopení následné problematiky věnované algebraickým prvkům. Ve třetí a čtvrté kapitole se zabývám vlastnostmi rozšiřování těles a rozkladovými tělesy polynomů. V závěrečné kapitole je popsána teorie konečných těles. V celém textu jsem se snažil ukázat souvislosti mezi jednotlivými pojmy, většina uvedených vět je podrobně dokázána.

1 Jednoduché algebraické a transcendentní rozšíření těles

Rozšířením libovolného komutativního tělesa $\mathbb{F}$ rozumíme každé těleso $\mathbb{K}$, které obsahuje $\mathbb{F}$ jako podtěleso. Těleso $\mathbb{K}$ může být nad $\mathbb{F}$ generováno různými způsoby. Generátory rozšíření jsou některé prvky z tohoto rozšíření.

Například těleso $\mathbb{Q}(\sqrt{2})$ je generováno prvkem $\sqrt{2}$, který je kořenem rovnice $x^2-2=0$ a tvoří jej všechna reálná čísla ve tvaru $a+b\sqrt{2}$, kde $a,\ b \in \mathbb{Q}$. Jiná rovnice $x^2-2x-1=0$ má kořen $1+\sqrt{2}$, který generuje totéž těleso, protože každé číslo z tělesa $\mathbb{Q}(\sqrt{2})$ můžeme napsat pomocí nového generátoru ve tvaru

$$a + b\sqrt{2} = (a - b) + b(1 + \sqrt{2}). \tag{1.1}$$

Necht' $\mathbb{K}$ je komutativní těleso, $\mathbb{F}$ podtěleso tělesa $\mathbb{K}$ a u nějaký prvek z $\mathbb{K} \setminus \mathbb{F}$. Zkoumejme právě ty prvky, které jsou dány polynomickými výrazy tvaru

$$f(u) = a_0 + a_1u + a_2u^2 + \ \ldots\ + a_nu^n;\ a_0,\ a_1,\ \ldots,\ a_n \in\ \mathbb{F}. \tag{1.2}$$

Každý podobor integrity tělesa $\mathbb{K}$, který obsahuje $\mathbb{F}$ a u, potom obsahuje všechny prvky $f(u)$. Množina všech takových polynomických výrazů je uzavřená na sčítání a násobení. Všechny prvky tvaru (1.2) tvoří podobor integrity tělesa $\mathbb{K}$ generovaný tělesem $\mathbb{F}$ a prvkem u. Tento podobor integrity obvykle označujeme symbolem $\mathbb{F}[u]$ [3].

Definice 1.1 Necht' $\mathbb{K}$ je libovolné těleso a $\mathbb{F}$ jeho podtěleso. Prvek $u \in \mathbb{K}$ nazveme **algebraickým** nad $\mathbb{F}$, jestliže u je kořenem nenulového polynomu f nad $\mathbb{F}$. Prvek c z $\mathbb{K}$, který není algebraický nad $\mathbb{F}$, se nazývá **transcendentní** prvek nad $\mathbb{F}$.

Definice 1.2 Těleso $\mathbb{K}$ nazveme **jednoduchým algebraickým rozšířením** tělesa $\mathbb{F} \subseteq \mathbb{K}$, jestliže existuje prvek $u \in \mathbb{K}$, algebraický nad $\mathbb{F}$, takový, že $\mathbb{K} = \mathbb{F}(u)$. Jestliže u je transcendentní nad $\mathbb{F}$, tak $\mathbb{K} = \mathbb{F}(u)$ nazveme jednoduchým transcendentním rozšířením tělesa $\mathbb{F}$.

V následující definici zavedeme pojem podtěleso generované množinou.

Definice 1.3 Nechť $\mathbb{F}$ je těleso, X libovolná podmnožina v $\mathbb{F}$. Pak průnik všech podtěles tělesa $\mathbb{F}$, které obsahují množinu X, je podtěleso v $\mathbb{F}$. Toto podtěleso nazveme **podtělesem generovaným množinou** X a budeme jej značit $[[\mathbb{X}]]$.

Věta 1.1 *Nechť $\mathbb{F}$ je podtěleso tělesa $\mathbb{L}$ a nechť je dán prvek $u \in \mathbb{L}$. Potom $[[\mathbb{F} \cup \{u\}]]$ se rovná množině*

$$\mathbb{F}(u) = \left\{ \frac{a_0 + a_1 u + a_2 u^2 + \ \ldots \ + a_n u^n}{b_0 + b_1 u + b_2 u^2 + \ \ldots \ + b_m u^m};\ m,\ n \in \mathbb{N},\right.$$

$$\left. a_0,\ a_1,\ \ldots,\ a_n,\ b_0,\ b_1,\ \ldots,\ b_m \in \mathbb{F},\ b_0 + b_1 u + \ \ldots \ + b_m u^m \neq 0 \right\}. \tag{1.3}$$

Poznámka 1.1 Prvek $u \in \mathbb{L}$ je algebraický nad podtělesem $\mathbb{F} \subseteq \mathbb{L}$, jestliže existuje nenulový polynom f nad $\mathbb{F}$, což budeme značit $f \neq o$, pro který platí, že $f(u) = 0$. Prvek u je transcendentní nad $\mathbb{F}$, jestliže $f(u) \neq 0$ pro každé $o \neq f \in \mathbb{F}[x]$. Víme, že těleso $\mathbb{F}(u)$ generované prvkem u má tvar

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

(věta 1.1). Odtud vyplývá úplná charakteristika jednoduchých transcendetních rozšíření (shrneme ve větě 1.3).

Věta 1.2 *Nechť $\mathbb{D}$ je obor integrity. Každý prvek z podílového tělesa $\mathbb{Q}(\mathbb{D})$ je podílem dvou prvků z oboru integrity $\mathbb{D}$. Jestliže $\varphi : \mathbb{D} \to \mathbb{F}$ je vnoření $\mathbb{D}$ do libovolného tělesa $\mathbb{F}$, pak φ můžeme rozšířit na vnoření $\psi : \mathbb{Q}(\mathbb{D}) \to \mathbb{F}$ vztahem $\psi(ab^{-1}) = \varphi(a)\,(\varphi(b))^{-1}$, pro $a,\ b \in \mathbb{D},\ b \neq 0$.*

Věta 1.3 *Jednoduché transcedentní rozšíření $\mathbb{F}(u)$ tělesa $\mathbb{F}$ je izomorfní s podílovým tělesem $\mathbb{Q}(\mathbb{F}[x])$ oboru integrity $\mathbb{F}[x]$ polynomů jedné neurčité nad $\mathbb{F}$.*

Důkaz. Nechť u je transcendentní prvek nad $\mathbb{F}$, potom homomorfizmus $\varphi_u : \mathbb{F}[x] \to \mathbb{F}(u)$ definovaný vztahem $\varphi_u(f) = f(u)$ pro $f \in \mathbb{F}[x]$ je injektivní, protože $Ker\ \varphi_u = \{o\}$, kde $Ker\ \varphi_u$ je jádro homomorfizmu φ_u. Můžeme použít větu 1.2 a rozšířit φ_u na injektivní homomorfizmus $\varphi : \mathbb{Q}(\mathbb{F}[x]) \to \mathbb{F}(u)$ vztahem $\varphi\big(fg^{-1}\big) = \frac{f(u)}{g(u)}$ pro $fg^{-1} \in \mathbb{Q}(\mathbb{F}[x])$. Ze

struktury $\mathbb{F}(u)$ vyplývá, že φ je také surjektivní, tedy φ je izomorfizmus [7]. □

Důsledek 1.1 Jestliže u, v jsou transcendentní prvky nad $\mathbb{F}$. Pak rozšíření $\mathbb{F}(u)$, $\mathbb{F}(v)$ jsou izomorfní.

Řešené příklady

Příklad 1.1 Rozhodněte, která z následujících čísel jsou algebraická a která jsou transcendentní nad tělesem $\mathbb{Q}$ všech racionálních čísel.

a) $u = 1 + \sqrt{2}$
b) $v = -i\sqrt[3]{2}$
c) $z = \sqrt{\pi}$

Řešení:

a) $u = 1 + \sqrt{2}$

Při řešení úlohy využijeme definice 1.1. Jestliže existuje nenulový polynom s koeficienty z $\mathbb{Q}$, pro který platí, že u je kořenem tohoto polynomu, pak u je algebraický nad $\mathbb{Q}$. Tento polynom můžeme nalézt tak, že určíme přirozené číslo n takové, že u^n lze vyjádřit jako lineární kombinace prvků u^{n-1}, u^{n-2}, ..., u^1, $u^0 = 1$ s koeficinety z $\mathbb{Q}$. Určíme:

$$u^0 = 1$$
$$u^1 = 1 + \sqrt{2}$$
$$u^2 = 1 + 2\sqrt{2} + 2 = 2(1 + \sqrt{2}) + 1$$

Je evidentní, že prvek u^2 můžeme vyjádřit jako lineární kombinaci prvků u^1, u^0, nebot' $u^2 = 2u + 1$. Hledaný polynom je

$$f = x^2 - 2x - 1.$$

Podle definice 1.1 u je algebraický nad $\mathbb{Q}$.

b) $v = -i\sqrt[3]{2}$

Výpočet je analogický jako v případě a), určíme:

$$v^0 = 1$$
$$v^1 = -i\sqrt[3]{2}$$
$$v^2 = (-i\sqrt[3]{2})^2 = -\sqrt[3]{4}$$
$$v^3 = (-\sqrt[3]{4})(-i\sqrt[3]{2}) = 2i$$
$$v^4 = 2i(-i\sqrt[3]{2}) = 2\sqrt[3]{2}$$
$$v^5 = 2\sqrt[3]{2}(-i\sqrt[3]{2}) = -2i\sqrt[3]{4}$$
$$v^6 = \left(-2i\sqrt[3]{4}\right)\left(-i\sqrt[3]{2}\right) = -4$$

Je zřejmé, že prvek v^6 lze vyjádřit jako lineární kombinaci prvků v^5, v^4, ..., v^0,

jelikož $v^6 = -4v^0$. Proto hledaný polynom je

$$f = x^6 + 4.$$

Tedy v je nad $\mathbb{Q}$ algebraický.

c) $z = \sqrt{\pi}$

Využijeme analogického postupu jako v předcházejících případech. Určíme:

$$\begin{aligned} z^0 &= 1 \\ z^1 &= \sqrt{\pi} \\ z^2 &= \pi \\ z^3 &= \pi\sqrt{\pi} \\ z^4 &= \pi^2 \\ &\vdots \\ z^n &= (\sqrt{\pi})^n \end{aligned}$$

Chceme nalézt přirozené číslo n takové, aby z^n bylo lineární kombinací prvků z^{n-1}, z^{n-2}, …, z^1, z^0. Ale v tomto případě takové n neexistuje, proto jediný polynom nad $\mathbb{Q}$, pro který platí, že prvek z je jeho kořenem, je polynom nulový. Tedy z je nad $\mathbb{Q}$ transcendentní.

Příklad 1.2

a) Necht' d je celé číslo, které není druhou mocninou celého čísla. Popište těleso $\mathbb{Q}\left(\sqrt{d}\right)$.

b) Najděte všechny prvky u z tělesa $\mathbb{Q}(\sqrt{d})$, které generují celé těleso, tj. $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{d})$.

c) Vyjádřete každý prvek z b) jako kořen kvadratické rovnice s koeficienty z $\mathbb{Q}$.

Řešení:

a) Libovolný prvek z tělesa $\mathbb{Q}\left(\sqrt{d}\right)$ můžeme zapsat ve tvaru

$$a_0 + a_1\sqrt{d};\ \text{kde}\ a_0,\ a_1 \in \mathbb{Q}.$$

Pro sčítání v $\mathbb{Q}\left(\sqrt{d}\right)$ platí

$$(a_0 + a_1\sqrt{d}) + (b_0 + b_1\sqrt{d}) = (a_0 + b_0) + (a_1 + b_1)\sqrt{d}.$$

Snadno nalezneme i opačný prvek

$$-(a_0 + a_1\sqrt{d}) = (-a_0) + (-a_1)\sqrt{d};\ \text{kde}\ -a_0,\ -a_1\ \text{jsou opačné prvky k}\ a_0,\ a_1\ \text{v}\ \mathbb{Q}.$$

Pro násobení odvodíme vztah

$$(a_0 + a_1\sqrt{d})(b_0 + b_1\sqrt{d}) = a_0b_0 + (a_0b_1 + a_1b_0)\sqrt{d} + a_1b_1(\sqrt{d})^2.$$

Poněvadž $(\sqrt{d})^2 = d$, platí

$$(a_0 + a_1\sqrt{d})(b_0 + b_1\sqrt{d}) = (a_0b_0 + da_1b_1) + (a_0b_1 + a_1b_0)\sqrt{d}.$$

Pro inverzní prvek platí

$$(a_0+a_1\sqrt{d})^{-1} = \frac{1}{a_0 + a_1\sqrt{d}} \cdot \frac{a_0 - a_1\sqrt{d}}{a_0 - a_1\sqrt{d}} = \left(\frac{a_0}{a_0^2 - da_1^2}\right) + \left(\frac{-a_1}{a_0^2 - da_1^2}\right)\sqrt{d}.$$

b) Prvky z tělesa $\mathbb{Q}(\sqrt{d})$ jsou ve tvaru $a+b\sqrt{d};\ a,\ b \in \mathbb{Q}$. Je zřejmé, že všechny prvky ve tvaru $u = a + b\sqrt{d},\ a \in \mathbb{Q},\ b \in \mathbb{Q}\setminus\{0\}$ generují těleso $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{d})$. Jelikož prvky, pro něž $b = 0$, generují pouze těleso $\mathbb{Q}$.

c) Označme $\alpha = a + b\sqrt{d}$. Příslušnou kvadratickou rovnici budeme hledat tak, že prvek α^2 by měl být lineární kombinací prvků α^1, α^0. Tyto prvky si vyjádříme:

$$\begin{aligned}
&\alpha^0 = 1\\
&\alpha^1 = a + b\sqrt{d}\\
&\alpha^2 = a^2 + 2ab\sqrt{d} + b^2d = 2a(\underbrace{a + b\sqrt{d}}_{\alpha} - a) + a^2 + b^2d = 2a\alpha - a^2 + b^2d
\end{aligned}$$

Kvadratickou rovnici pro α můžeme psát ve tvaru $x^2 \overbrace{-2a}^{\in\mathbb{Q}} x + \overbrace{a^2 - b^2d}^{\in\mathbb{Q}} = 0$. Je zřejmé, že koeficienty této rovnice jsou z $\mathbb{Q}$, tedy tato rovnice je hledanou rovnicí.

Cvičení

Cvičení 1.1 Rozhodněte, která z následujících čísel jsou algebraická a která jsou transcendentní nad tělesem $\mathbb{Q}$.

a) $5 + 2i$
b) $e + 5$
c) $2\pi + \sqrt{3}$
d) $\sqrt[3]{4}$

[a), d) jsou algebraická; b) c) transcendentní nad $\mathbb{Q}$]

Cvičení 1.2 Najděte všechny prvky u z tělesa $\mathbb{Q}(\sqrt[3]{3})$, které generují celé těleso, tj. $\mathbb{Q}(u) = \mathbb{Q}\big(\sqrt[3]{3}\big)$.

$\big[a_0 + a_1\sqrt[3]{3} + a_2\sqrt[3]{9};\ a_0,\ a_1,\ a_2 \in \mathbb{Q},\ \text{kde } a_1,\ a_2 \text{ nejsou současně rovny nule}\big]$

2 Algebraické prvky nad daným tělesem

V této kapitole se budeme zabývat vlastnostmi jednoduchých algebraických rozšíření tělesa $\mathbb{F}$. Je-li $\mathbb{F}(u)$ jednoduché algebraické rozšíření $\mathbb{F}$, musí být u kořenem nějakého polynomu, jehož koeficienty jsou z $\mathbb{F}$, který je alespoň prvního stupně [3].

Definice 2.1 Nechť je dán polynom $f = a_0 + a_1 x + \ldots + a_n x^n$ z oboru integrity $\mathbb{F}[x]$, kde $n \in \mathbb{N}$. Řekneme, že polynom f je **normovaný**, jestliže $a_n = 1$.

Definice 2.2 Polynom f z $\mathbb{F}[x]$ stupně alespoň prvního se nazývá **reducibilní** v $\mathbb{F}[x]$, jestliže jej lze zapsat jako součin dvou polynomů z $\mathbb{F}[x]$, z nichž každý je stupně alespoň prvního. V opačném případě se polynom f nazývá **ireducibilní** v $\mathbb{F}[x]$.

Ukážeme, že algebraický prvek u nad $\mathbb{F}$ musí být kořenem právě jednoho ireducibilního normovaného polynomu nad $\mathbb{F}$.

Věta 2.1 *Každý polynom g z $\mathbb{F}[x]$ stupně alespoň prvního lze vyjádřit ve tvaru součinu normovaných ireducibilních polynomů a konstanty $c \in \mathbb{F}$. Tento rozklad je jednoznačně určený až na pořadí činitelů.*

Věta 2.2 *Prvek u, který je algebraickým prvkem nad tělesem $\mathbb{F}$, je kořenem právě jednoho normovaného polynomu p, ireducibilního v oboru integrity $\mathbb{F}[x]$. Jestliže g je další polynom s koeficienty z $\mathbb{F}$, potom $g(u) = 0$ právě tehdy, když g je násobkem polynomu p v oboru integrity $\mathbb{F}[x]$.*

Důkaz. Algebraický prvek u je podle definice 1.1 kořenem alespoň jednoho polynomu $f \neq o$ z $\mathbb{F}[x]$. Jestliže polynom f není ireducibilní, můžeme jej podle věty 2.1 rozložit na součin $f = cp_1p_2 \ldots p_m$ normovaných ireducibilních činitelů, přičemž $c \neq 0$. Protože $f(u) = 0$, alespoň pro jeden činitel p_i platí $p_i(u) = 0$. Nalezli jsme normovaný ireducibilní polynom p_i takový, že u je jeho kořenem. Nechť n je stupeň p_i.

Ukážeme, že u není kořenem žádného polynomu $q \neq o$ stupně menšího než n. Předpokládejme, že by existoval polynom q, $\mathrm{st}\, q < n$, který by měl kořen u. Protože q má nižší stupeň než ireducibilní polynom p_i, jsou polynomy p_i a q nesoudělné, tj. největší společný dělitel (n.s.d.) $D(p_i, q) = 1$. Tento n.s.d. můžeme vyjádřit ve tvaru $tp_i + sq = 1$ s polynomy t, $s \in \mathbb{F}[x]$. Dále platí, že $p_i(u) = 0$ a $q(u) = 0$, tedy $1 = 0$, což je spor.

Dále nechť $g \in \mathbb{F}[x]$, $g(u) = 0$. Pak existují $q, r \in \mathbb{F}[x]$ tak, že $g = qp_i + r$, kde stupeň polynomu r je nejvýše $n-1$. Protože $g(u) = 0$ a $p_i(u) = 0$, potom i $r(u) = 0$. Z předcházejících úvah vyplývá, že polynom r je nulový, takže $g = qp_i$. To dokazuje, že každý polynom g s kořenem u je násobkem polynomu p_i [3]. □

Definice 2.3 Minimálním polynomem prvku u algebraického nad $\mathbb{F}$ nazýváme normovaný polynom $p \in \mathbb{F}[x]$, který je generátorem ideálu $(p) = \{f \in \mathbb{F}[x];\ f(u) = 0\}$ v okruhu $(\mathbb{F}[x], +, \cdot)$ (pro všechny $f \in \mathbb{F}[x]$ platí, že $f(u) = 0$ právě tehdy, když $p \mid f$).

Z této definice vyplývá, že minimální polynom má nejnižší stupeň ve srovnání s polynomy $f \in \mathbb{F}[x]$, pro které platí, že $f(u) = 0$. Požadavek normovanosti určuje minimální polynom jednoznačně.
Následující dvě věty jsou známé z teorie okruhů a jejich důkazy lze nalézt např. v [9].

Věta 2.3 *Faktorový okruh $\mathbb{A}/\mathbb{I}$ komutativního okruhu $\mathbb{A}$ s jednotkou 1 je tělesem právě tehdy, když $\mathbb{I}$ je maximální ideál.*

Věta 2.4 *Homomorfní obraz $\mathbb{A}'$ okruhu $\mathbb{A}$ v homomorfizmu φ je izomorfní s faktorovým okruhem $\mathbb{A}/Ker\ \varphi$.*

Věta 2.5 *Je-li p je minimální polynom prvku u nad tělesem $\mathbb{F}$, potom p je ireducibilní nad $\mathbb{F}$. Jednoduché algebraické rozšíření $\mathbb{F}(u)$ se potom rovná okruhu $\mathbb{F}[u]$, který je izomorfní s faktorovým okruhem $\mathbb{F}[x]/(p)$, kde (p) je ideál generovaný polynomem p.*

Důkaz. Nechť $p = fg$ je rozklad polynomu p nad $\mathbb{F}$. Potom $p(u) = f(u)\, g(u) = 0$, z tohoto okamžitě plyne, že buď $f(u) = 0$ nebo $g(u) = 0$. Z definice 2.3 plyne, že $p \mid f$ nebo $p \mid g$. V obou případech je rozklad polynomu p triviální, což znamená, že p je ireducibilní nad $\mathbb{F}$.

Z ireducibilnosti polynomu p nad $\mathbb{F}$ vyplývá, že (p) je maximální ideál v $\mathbb{F}[x]$, tedy faktorový okruh $\mathbb{F}[x]/(p)$ je těleso (věta 2.3). Uvažujme homomorfizmus $\varphi_u : \mathbb{F}[x] \to \mathbb{F}[u]$, $\varphi_u(f) = f(u)$, zřejmě $Ker\ \varphi_u = (p)$. $\mathbb{F}[u]$ je izomorfní s $\mathbb{F}[x]/Ker\ \varphi_u = \mathbb{F}[x]/(p)$ (věta 2.4). Tedy $\mathbb{F}[u]$ je těleso, tj. $\mathbb{F}[u] = \mathbb{F}(u)$ [7]. □

Poznámka 2.1 Podle věty 2.5 každý prvek jednoduchého algebraického rozšíření $\mathbb{F}(u)$

můžeme napsat jako polynomický výraz

$$a_0 + a_1 u + a_2 u^2 + \ \ldots \ + a_k u^k = f(u) \tag{2.1}$$

pro nějaký polynom $f \in \mathbb{F}[x]$.

Definice 2.4 Stupněm algebraického prvku u **nad tělesem** $\mathbb{F}$ rozumíme stupeň n jeho minimálního polynomu nad $\mathbb{F}$. Stupeň prvku u nad $\mathbb{F}$ označujeme $[u : \mathbb{F}]$.

Věta 2.6 *Nechť u je algebraický prvek stupně n nad tělesem $\mathbb{F}$. Potom každý prvek $v \in \mathbb{F}(u)$ lze vyjádřit právě jediným způsobem ve tvaru*

$$v = a_0 + a_1 u + a_2 u^2 + \ \ldots \ + a_{n-1} u^{n-1};\ a_0,\ a_1,\ \ldots,\ a_{n-1} \in \mathbb{F}. \tag{2.2}$$

Důkaz. Dle poznámky 2.1 existuje $f \in \mathbb{F}[x]$ takový, že $v = f(u)$. Jestliže vydělíme polynom f minimálním polynomem p, pak platí, že $f = qp + r$, kde $q,\ r \in \mathbb{F}[x]$, $\operatorname{st} r < \operatorname{st} p$, nebo $r = o$. Potom

$$f(u) = q(u)p(u) + r(u) = q(u)0 + r(u) = r(u)$$

tedy $v = r(u)$ jest hledané vyjádření.

Na důkaz jednoznačnosti uvažujme $v = r(u) = s(u)$, $\operatorname{st} r < n$, $\operatorname{st} s < n$. Potom $(r - s)(u) = 0$, tedy $p \mid (r - s)$. Protože $\operatorname{st}(r - s) < n$ musí platit, že $r - s = o$, tj. $r = s$ [7]. □

Důsledek 2.1 Nechť algebraické prvky u, v mají stejný minimální polynom p nad tělesem $\mathbb{F}$, pak $\mathbb{F}(u) \simeq \mathbb{F}(v)$.

Důsledek 2.2 Nechť u je algebraický prvek stupně n nad tělesem $\mathbb{F}$, pak $\mathbb{F}(u)$ je vektorový prostor nad $\mathbb{F}$ s bází $1,\ u,\ u^2,\ \ldots,\ u^{n-1}$.

Důsledek 2.3 Nechť u je algebraický prvek stupně n nad tělesem $\mathbb{F}$, pak každý prvek $v \in \mathbb{F}(u)$ je algebraický nad $\mathbb{F}$ stupně $[v : \mathbb{F}] \leq n$.

Následující věta rozšiřuje důsledek 2.1, důkaz této věty lze nalézt např. v [3].

Věta 2.7 *Nechť tělesa* $\mathbb{F}(u)$ *a* $\mathbb{F}(v)$ *jsou jednoduchá algebraická rozšíření tělesa* $\mathbb{F}$, *která jsou generovaná kořeny* u *a* v *polynomu* p *ireducibilního nad* $\mathbb{F}$. *Pak* $\mathbb{F}(u)$ *a* $\mathbb{F}(v)$ *jsou izomorfní. Speciálně existuje izomorfizmus mezi* $\mathbb{F}(u)$ *a* $\mathbb{F}(v)$, *který zobrazuje* u *na* v *a každý prvek z* $\mathbb{F}$ *na sebe.*

Řešené příklady

Příklad 2.1 Předpokládejte, že jednodnoduché rozšíření $\mathbb{Q}(u)$ je generované kořenem u polynomu $f = x^3 - 6x^2 + 9x + 3$. Vyjádřete každý z následujících prvků pomocí u^0, u^1, u^2, jak je uvedeno v (2.2).

a) u^4
b) $2u^5 - 4$
c) $\frac{1}{u+1}$

Řešení:

a) u^4

Jelikož u je kořenem polynomu f, platí $u^3 - 6u^2 + 9u + 3 = 0$. Při výpočtu využijeme vztahu $u^3 = 6u^2 - 9u - 3$ a základních algebraických úprav.

$$u^4 = uu^3 = u(6u^2 - 9u - 3) = 6u^3 - 9u^2 - 3u = 6(6u^2 - 9u - 3) - 9u^2 - \\ -3u = 27u^2 - 57u - 18$$

Hledané vyjádření je $u^4 = 27u^2 - 57u - 18$.

b) $2u^5 - 4$

Postup bude analogický jako v případě a).

$$2u^5 - 4 = 2uu^4 - 4, \text{ za } u^4 \text{ dosadíme z předcházející úlohy}$$
$$2u^5 - 4 = 2u(27u^2 - 57u - 18) - 4 = 54u^3 - 114u^2 - 36u - 4 = \\ = 210u^2 - 522u - 166$$

c) $\frac{1}{u+1}$

Tento prvek rozšíříme tak, abychom se ve jmenovateli zbavili všech přirozených mocnin prvku u a zbyla tam pouze reálná konstanta. Jelikož pro u platí $u^3 - 6u^2 + 9u + 3 = 0$, tento výraz budeme chtít získat ve jmenovateli zvětšený o libovolnou konstantu. Prvek $\frac{1}{u+1}$ rozšíříme výrazem $u^2 + au + b$, kde čísla a a b dopočteme tak, abychom obdrželi výraz $u^3 - 6u^2 + 9u + 3 \ + c$. Vyjádříme si toto rozšíření

$$\frac{1}{u+1} \cdot \frac{u^2 + au + b}{u^2 + au + b} = \frac{u^2 + au + b}{u^3 + u^2(a+1) + u(a+b) + b}. \qquad (*)$$

Výraz získaný ve jmenovateli porovnáme s výrazem $u^3 - 6u^2 + 9u + 3 + c$.

$$u^3 + u^2(a+1) + u(a+b) + b = u^3 - 6u^2 + 9u + 3 \ + c$$

Porovnáním koeficientů u jednotlivých mocnin prvku u na obou stranách rovnice dostaneme:

$$\begin{aligned} u^3 &: \quad 1 = 1 \\ u^2 &: \ a + 1 = -6 \\ u^1 &: \ a + b = 9 \\ u^0 &: \quad b = 3 + c \end{aligned}$$

Řešení této soustavy rovnic je:

$$\begin{aligned} a &= -7 \\ b &= 16 \\ c &= 13 \end{aligned}$$

Čísla a, b, c dosadíme do vztahu $(*)$ a dostaneme

$$\frac{1}{u+1} \cdot \frac{u^2 - 7u + 16}{u^2 - 7u + 16} = \frac{u^2 - 7u + 16}{\underbrace{u^3 - 6u^2 + 9u + 3}_{0} + 13} = \frac{1}{13}u^2 - \frac{7}{13}u + \frac{16}{13}.$$

Příklad 2.2 Nalezněte minimální polynomy následujících čísel nad $\mathbb{Q}$.

a) $\alpha = 3 + \sqrt{5}$
b) $\beta = \frac{1+2\sqrt{5}}{3+\sqrt{5}}$
c) $\gamma = \sqrt{1 + \sqrt{2}}$
d) $\delta = \sqrt[3]{2} + \sqrt{2}$

Řešení:

a) $\alpha = 3 + \sqrt{5}$

Minimální polynom pro číslo α nad $\mathbb{Q}$ hledáme tak, že nalezneme nejmenší přirozené číslo n takové, že α^n lze vyjádřit jako lineární kombinace čísel α^0, α^1, $\ldots$, α^{n-1} s koeficienty z $\mathbb{Q}$. Proto určíme:

$$\begin{aligned} \alpha^0 &= 1 \\ \alpha^1 &= 3 + \sqrt{5} \\ \alpha^2 &= 9 + 6\sqrt{5} + 5 = 6(3 + \sqrt{5}) - 4 \end{aligned}$$

Prvek α^2 lze vyjádřit jako lineární kombinace prvků α^0, α^1 ve tvaru $\alpha^2 = 6\alpha - 4$. Tedy

minimální polynom pro α nad $\mathbb{Q}$ je $f = x^2 - 6x + 4$.

b) $\beta = \frac{1+2\sqrt{5}}{3+\sqrt{5}}$

Nejprve se zbavíme iracionality ve jmenovateli a dále postupujeme analogicky jako v případě a).

$$\begin{aligned}
\beta^0 &= 1 \\
\beta^1 &= \tfrac{1+2\sqrt{5}}{3+\sqrt{5}}\tfrac{3-\sqrt{5}}{3-\sqrt{5}} = \tfrac{-7+5\sqrt{5}}{4} \\
\beta^2 &= \left(\tfrac{-7+5\sqrt{5}}{4}\right)^2 = \tfrac{49-70\sqrt{5}+125}{16} = \tfrac{1}{2}\left(\tfrac{-7(-7+5\sqrt{5})}{4} + \tfrac{38}{4}\right) = -\tfrac{7}{2}\beta + \tfrac{19}{4}
\end{aligned}$$

Minimální polynom pro β nad $\mathbb{Q}$ je $f = x^2 + \frac{7}{2}x - \frac{19}{4}$.

c) $\gamma = \sqrt{1+\sqrt{2}}$

Postupně určíme:

$$\begin{aligned}
\gamma^0 &= 1 \\
\gamma^1 &= \sqrt{1+\sqrt{2}} \\
\gamma^2 &= 1 + \sqrt{2} \\
\gamma^3 &= (1+\sqrt{2})\sqrt{1+\sqrt{2}} \\
\gamma^4 &= 1 + 2\sqrt{2} + 2 = 2(1+\sqrt{2}) + 1 = 2\gamma^2 + 1
\end{aligned}$$

Tedy γ je algebraický prvek čtvrtého stupně nad $\mathbb{Q}$, jehož minimální polynom $f = x^4 - 2x^2 - 1$.

d) $\delta = \sqrt[3]{2} + \sqrt{2}$

$$\begin{aligned}
\delta^0 &= 1 \\
\delta^1 &= \sqrt[3]{2} + \sqrt{2} \\
\delta^2 &= \sqrt[3]{4} + 2\sqrt[3]{2}\sqrt{2} + 2 \\
\delta^3 &= 3\sqrt[3]{4}\sqrt{2} + 6\sqrt[3]{2} + 2\sqrt{2} + 2 \\
\delta^4 &= 12\sqrt[3]{4} + 2\sqrt[3]{2} + 8\sqrt[3]{2}\sqrt{2} + 8\sqrt{2} + 4
\end{aligned}$$

Ověříme, zda δ^4 lze vyjádřit jako lineární kombinaci prvků 1, δ, δ^2, δ^3, tzn. zda existují a, b, c, $d \in \mathbb{Q}$ takové, že $\delta^4 = a\delta^3 + b\delta^2 + c\delta + d$. Dosazením za δ, δ^2, δ^3, δ^4 a porovnámím koeficientů u jednotlivých mocnin čísla 2 dostaneme:

$$\begin{aligned}
\sqrt[3]{4}: &\quad 12 = b \\
\sqrt[3]{4}\sqrt{2}: &\quad 0 = 3a \\
\sqrt[3]{2}: &\quad 2 = 6a + c \\
\sqrt[3]{2}\sqrt{2}: &\quad 8 = 2b \\
\sqrt{2}: &\quad 8 = 2a + c
\end{aligned}$$

$$2^0: \qquad 4 = 2a + 2b + d$$

Tato soustava lineárních rovnic nemá řešení, což je patrné z první a čtvrté rovnice. Pokračujeme ve výpočtu a určíme δ^5.

$$\delta^5 = 2\sqrt[3]{4} + 20\sqrt[3]{4}\sqrt{2} + 20\sqrt[3]{2} + 10\sqrt[3]{2}\sqrt{2} + 4\sqrt{2} + 40$$

Nyní ověříme, zda δ^5 lze vyjádřit jako lineární kombinaci prvků $1, \delta, \ldots, \delta^4$, tzn. že hledáme $a, b, c, d, e \in \mathbb{Q}$ taková, že $\delta^5 = a\delta^4 + b\delta^3 + c\delta^2 + d\delta + e$. Odtud:

$$\begin{aligned}
\sqrt[3]{4}: &\qquad 2 = 12a + c \\
\sqrt[3]{4}\sqrt{2}: &\ 20 = 3b \Rightarrow b = \tfrac{20}{3} \\
\sqrt[3]{2}: &\qquad 20 = 2a + 6b + d \\
\sqrt[3]{2}\sqrt{2}: &\ 10 = 8a + 2c \\
\sqrt{2}: &\qquad 4 = 8a + 2b + d \\
2^0: &\qquad 40 = 4a + 2b + 2c + e
\end{aligned}$$

Tuto soustavu rovnic budeme řešit tak, že vyjádřený prvek b z druhé rovnice dosadíme do třetí a páté rovnice a vypočteme a.

$$\begin{aligned}
20 &= 2a + 40 + d \\
4 &= 8a + \tfrac{40}{3} + d
\end{aligned}$$

Po odečtení rovnic dostaneme $a = \frac{16}{9}$ a dosazením do první a čtvrté rovnice vypočítáme:

$$\begin{aligned}
2 &= \tfrac{12\cdot 16}{9} + c \Rightarrow c = -\tfrac{58}{3} \\
10 &= \tfrac{8\cdot 16}{9} + 2c \Rightarrow c = -\tfrac{19}{9}
\end{aligned}$$

Výše uvedená soustava lineárních rovnic nemá řešení, proto δ není algebraický prvek ani pátého stupně. Určíme δ^6:

$$\delta^6 = 60\sqrt[3]{4} + 12\sqrt[3]{4}\sqrt{2} + 60\sqrt[3]{2} + 24\sqrt[3]{2}\sqrt{2} + 80\sqrt{2} + 12.$$

Ověříme, zda δ^6 lze zapsat jako lineární kombinaci prvků $1, \delta, \ldots, \delta^5$, tj. $\delta^6 = a\delta^5 + {} + b\delta^4 + c\delta^3 + d\delta^2 + e\delta + f$, kde $a, b, c, d, e, f \in \mathbb{Q}$. Porovnáním koeficientů dostaneme:

$$\begin{aligned}
\sqrt[3]{4}: &\qquad 60 = 2a + 12b + d \\
\sqrt[3]{4}\sqrt{2}: &\ 12 = 20a + 3c \\
\sqrt[3]{2}: &\qquad 60 = 20a + 2b + 6c + e \\
\sqrt[3]{2}\sqrt{2}: &\ 24 = 10a + 8b + 2d \\
\sqrt{2}: &\qquad 80 = 4a + 8b + 2c + e \\
2^0: &\qquad 12 = 40a + 4b + 2c + 2d + f
\end{aligned}$$

Odtud:

$$\begin{aligned}
a &= 0 \\
b &= 6 \\
c &= 4 \\
d &= -12
\end{aligned}$$

$$e = 24$$
$$f = 4$$

Tedy δ^6 lze vyjádřit jako lineární kombinace prvků $\delta^5, \ldots, 1$, proto δ je algebraický prvek šestého stupně nad $\mathbb{Q}$ a jeho minimální polynom $p = x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$.

Příklad 2.3 V rozšíření $\mathbb{Z}_3(v)$, které je generované kořenem v polynomu $f = x^3 + \overline{2}x + \overline{1}$ ireducibilního nad $\mathbb{Z}_3$, najděte minimální polynomy prvků:

a) $\alpha = v^2$
b) $\beta = v^2 + \overline{2}$
c) $\gamma = \overline{2}v + \overline{1}$

Řešení:

a) $\alpha = v^2$

Jelikož v je kořenem polynomu f, tj. $v^3 - v + \overline{1} = \overline{0} \Rightarrow v^3 = v - \overline{1}$, tento vztah využijeme při hledání minimálního polynomu, který hledáme analogicky jako v předcházejícím příkladu.

$$\alpha^0 = \overline{1}$$
$$\alpha^1 = v^2$$
$$\alpha^2 = v^4 = vv^3 = v(v - \overline{1}) = v^2 - v$$
$$\alpha^3 = v^6 = (v^3)^2 = (v - \overline{1})^2 = v^2 - \overline{2}v + \overline{1} = \overline{2}(v^2 - v) - v^2 + \overline{1}$$

Platí $\alpha^3 = \overline{2}\alpha^2 - \alpha + \overline{1}$, proto je α algebraický prvek třetího stupně nad $\mathbb{Z}_3$ a hledaný minimální polynom je $g = x^3 + x^2 + x + \overline{2}$.

b) $\beta = v^2 + \overline{2}$

Výpočet provedeme analogicky jako v případě a).

$$\beta^0 = \overline{1}$$
$$\beta^1 = v^2 + \overline{2}$$
$$\beta^2 = (v^2 + \overline{2})^2 = v(v - \overline{1}) + v^2 + \overline{1} = \overline{2}v^2 - v + \overline{1} = -v^2 - v + \overline{1}$$
$$\beta^3 = \beta\beta^2 = \left(v^2 + \overline{2}\right)\left(\overline{2}v^2 - v + \overline{1}\right) = \overline{2}v(v - \overline{1}) - (v - \overline{1}) + v^2 + v^2 - \overline{2}v + \overline{2} = \overline{2}v^2 - \overline{2}v - v + \overline{1} + \overline{2}v^2 - \overline{2}v + \overline{2} = v^2 - \overline{2}v = -(-v^2 - v + \overline{1}) + \overline{1} = -\beta^2 + \overline{1}$$

Minimální polynom pro prvek β je $g = x^3 + x^2 + \overline{2}$.

c) $\gamma = \overline{2}v + \overline{1}$

$$\gamma^0 = \overline{1}$$

$$\gamma^1 = \overline{2}v + \overline{1}$$
$$\gamma^2 = (\overline{2}v + \overline{1})^2 = v^2 + v + \overline{1}$$
$$\gamma^3 = \gamma\gamma^2 = \overline{2}v^3 + \overline{2}v^2 + \overline{2}v + v^2 + v + \overline{1} = \overline{2}(v - \overline{1}) + \overline{1} = (\overline{2}v + \overline{1}) + \overline{1} = $$
$$= \gamma + \overline{1}$$

Minimální polynom pro γ je $g = x^3 + \overline{2}x + \overline{2}$.

Příklad 2.4 Z předpokladu, že minimální polynomy prvků u, v nad $\mathbb{F}$ jsou různé nevyplývá, že $\mathbb{F}(u) \neq \mathbb{F}(v)$. Najděte čísla u, v algebraická nad $\mathbb{Q}$ jako protipříklad.

Řešení: Necht' $u = \sqrt[3]{5}$, $v = \sqrt[3]{25}$. Ukážeme, že $\mathbb{Q}\big(\sqrt[3]{5}\big) = \mathbb{Q}\big(\sqrt[3]{25}\big)$, a že čísla u, v mají různé minimální polynomy nad $\mathbb{Q}$.

a) $u = \sqrt[3]{5}$

$$u^0 = 1$$
$$u^1 = \sqrt[3]{5}$$
$$u^2 = \sqrt[3]{25}$$
$$u^3 = 5$$

Proto u je algebraický prvek třetího stupně nad $\mathbb{Q}$ a jeho minimální polynom je $f = x^3 - 5$.

b) $v = \sqrt[3]{25}$

$$v^0 = 1$$
$$v^1 = \sqrt[3]{25}$$
$$v^2 = \sqrt[3]{625} = 5\sqrt[3]{5}$$
$$v^3 = 25$$

Číslo v je algebraickým prvkem třetího stupně nad $\mathbb{Q}$ a jeho minimální polynom je $g = x^3 - 25$.
Zřejmě čísla u, v generují stejné rozšíření tělesa $\mathbb{Q}$, avšak mají různé minimální polynomy.

Příklad 2.5 Rozhodněte, zda tělesa $\mathbb{Q}\big(\sqrt{2}\big)$, $\mathbb{Q}\big(-\sqrt{2}\big)$ jsou izomorfní. Pokud jsou izomorfní, tento izomorfizmus sestrojte.

Řešení: Ověření, zda tato dvě tělesa jsou izomorfní provedeme na základě důsledku 2.1:

pro $\sqrt{2}$ je $x^2 - 2$ minimální polynom nad $\mathbb{Q}$,
pro $-\sqrt{2}$ je $x^2 - 2$ minimální polynom nad $\mathbb{Q}$.

Jelikož $\sqrt{2}$ a $-\sqrt{2}$ mají stejné minimální polynomy nad $\mathbb{Q}$, potom tělesa $\mathbb{Q}\big(\sqrt{2}\big)$, $\mathbb{Q}\big(-\sqrt{2}\big)$

jsou izomorfní podle důsledku 2.1.

Výše uvedená tělesa můžeme zapsat v následujícím tvaru:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2};\ a,\ b \in \mathbb{Q}\},$$
$$\mathbb{Q}(-\sqrt{2}) = \{a - b\sqrt{2};\ a,\ b \in \mathbb{Q}\}.$$

Uvažujme zobrazení definované vztahem

$$\varphi(a + b\sqrt{2}) = a - b\sqrt{2};\ \text{kde}\ a,\ b \in \mathbb{Q}.$$

Z předpisu vyplývá, že se jedná o zobrazení z $\mathbb{Q}(\sqrt{2})$ do $\mathbb{Q}(-\sqrt{2})$.

Zbývá ověřit, zda φ je izomorfizmus, tj. bijektivní homorfizmus. Uvažujme prvky $p,\ q \in \mathbb{Q}(\sqrt{2})$, kde $p = a_0 + a_1\sqrt{2}$, $q = b_0 + b_1\sqrt{2}$; $a_0,\ a_1,\ b_0,\ b_1 \in \mathbb{Q}$. Ověříme, zda platí $\varphi(p+q) = \varphi(p) + \varphi(q)$, $\varphi(pq) = \varphi(p)\varphi(q)$; $\forall p,\ q \in \mathbb{Q}(\sqrt{2})$.

$$\varphi(p+q) = \varphi\big((a_0 + b_0) + (a_1 + b_1)\sqrt{2}\big) = (a_0+b_0)-(a_1+b_1)\sqrt{2} = (a_0- \\ -a_1\sqrt{2}) + (b_0 - b_1\sqrt{2}) = \varphi(p) + \varphi(q)$$
$$\varphi(pq) = \varphi((a_0b_0 + 2a_1b_1) + (a_0b_1 + a_1b_0)\sqrt{2}) = (a_0b_0 + 2a_1b_1) - (a_0b_1 + \\ +a_1b_0)\sqrt{2} = (b_0 - b_1\sqrt{2}\,)a_0 - (b_0 - b_1\sqrt{2}\,)a_1\sqrt{2} = (a_0 - a_1\sqrt{2}\,) \\ (b_0 - b_1\sqrt{2}) = \varphi(p)\varphi(q)$$

$\Rightarrow$ φ je homorfizmus. Ověříme, zda φ je bijektivní.

i) ověření, zda φ je injektivní

Nalezneme všechny prvky, které patří do $Ker\ \varphi$, tj. všechny, které se zobrazí na 0.
Necht' $\varphi(a + b\sqrt{2}) = 0$ pro $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Pak $a - b\sqrt{2} = 0$; $a,\ b \in \mathbb{Q} \Rightarrow\ a = b = 0$.
Tedy $Ker\ \varphi = \{0\} \Rightarrow \varphi$ je injektivní.

ii) ověření, zda φ je surjektivní

Je zřejmé, že pro každý prvek z $\mathbb{Q}(-\sqrt{2})$ existuje vzor v $\mathbb{Q}(\sqrt{2})$, proto φ je surjektivní.
Dokázali jsme, že zobrazení φ je izomorfizmem z tělesa $\mathbb{Q}(\sqrt{2})$ do $\mathbb{Q}(-\sqrt{2})$.

Příklad 2.6 Zobrazení φ: $\mathbb{Q}(\sqrt{5}) \to \mathbb{Q}(\sqrt{7})$ je dáno předpisem $\varphi(a + b\sqrt{5}) = a + b\sqrt{7}$, kde $a, b \in \mathbb{Q}$. Rozhodněte, zda φ je izomorfizmus.

Řešení: Uvažujme prvky $p,\ q \in \mathbb{Q}(\sqrt{5})$, kde $p = a_0 + a_1\sqrt{5}$, $q = b_0 + b_1\sqrt{5}$; $a_0,\ a_1,\ b_0,\ b_1 \in \mathbb{Q}$. Ověříme, zda platí $\varphi(p + q) = \varphi(p) + \varphi(q)$, $\varphi(pq) = \varphi(p) \cdot \varphi(q)$.

$$\varphi(p+q) = \varphi\big((a_0 + b_0) + (a_1 + b_1)\sqrt{5}\big) = (a_0+b_0)+(a_1+b_1)\sqrt{7} = (a_0+$$

$$+ a_1\sqrt{7}) + (b_0 + b_1\sqrt{7}) = \varphi(p) + \varphi(q)$$
$$\varphi(pq) = \varphi((a_0b_0 + 5a_1b_1) + (a_0b_1 + a_1b_0)\sqrt{5}) = (a_0b_0 + 5a_1b_1) + (a_0b_1 + \\ + a_1b_0)\sqrt{7}$$
$$\varphi(p)\cdot\varphi(q) = (a_0 + a_1\sqrt{7})(b_0 + b_1\sqrt{7}) = (a_0b_0 + 7a_1b_1) + (a_0b_1 + a_1b_0)\sqrt{7}$$
$$\Rightarrow \varphi(pq) \neq \varphi(p) \cdot \varphi(q)$$

Je evidentní, že φ není izomorfizmus.

Příklad 2.7 Dokažte, že pokud prvek u je algebraický nad tělesem $\mathbb{F}$, tak potom i prvek $\alpha = 2u + 1$ je nad $\mathbb{F}$ algebraický.

Řešení: $\mathbb{F}(u)$ je jednoduché algebraické rozšíření, zřejmě $\alpha \in \mathbb{F}(u)$. Z důsledku 2.3 vyplývá, že α je algebraický nad $\mathbb{F}$.

Cvičení

Cvičení 2.1 V jednodnoduchém rozšíření $\mathbb{Z}_4(u)$, které je generované kořenem u polynomu $f = x^3 + x^2 + \overline{1} \in \mathbb{Z}_4[x]$. Vyjádřete každý z následujících prvků pomocí $\overline{1}$, u, u^2 tak, jak je uvedeno v (2.2).

a) $\overline{2}u^5 + \overline{3}u^3 - \overline{2}$
b) $u^6 + \overline{2}u^4 - u^3$

[a) $u^2 + \overline{2}u + \overline{1}$; b) $\overline{2}u^2 + u + \overline{1}$]

Cvičení 2.2 Nalezněte minimální polynomy následujících čísel nad $\mathbb{Q}$.

a) $\sqrt[4]{2} - \sqrt{2}$
b) $1 - \sqrt[3]{3} + 2\sqrt[3]{9}$
c) $i + \sqrt{5}$

[*a*) $x^4 - 4x^2 + 8x + 2$; *b*) $x^3 - 3x^2 + 21x - 88$; *c*) $x^4 - 8x^2 + 36$]

Cvičení 2.3 V rozšíření $\mathbb{Q}(u)$ generovaném kořenem u polynomu $g = x^3 + 4x^2 - 4x + 2$ ireducibilního nad $\mathbb{Q}$, najděte minimální polynomy prvků:

a) u^2
b) u^3
c) $3u^2 - u + 1$

[a) $x^3 - 24x^2 - 4$; b) $x^3 + 118x^2 + 68x + 8$; c) $x^3 - 79x^2 + 85x - 69$]

Cvičení 2.4 Rozhodněte, zda tělesa $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(i\sqrt[4]{2})$ jsou izomorfní. Pokud jsou izomorfní, tento izomorfizmus sestrojte.

[jsou izomorfní, izomorfizmus $\varphi(a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8}) = a_0 + a_1 i\sqrt[4]{2} - a_2\sqrt[4]{4} - a_3 i\sqrt[4]{8}$, $a_0,\ a_1,\ a_2,\ a_3 \in \mathbb{Q}$]

3 Konečné rozšíření

3.1 Stupeň algebraického rozšíření

V jednoduchém algebraickém rozšíření $\mathbb{F}(u)$ generované prvkem u stupně n můžeme každý prvek v vyjádřit následujícím způsobem

$$v = a_0 + a_1 u + a_2 u^2 + \ \ldots \ + a_{n-1} u^{n-1};\ a_0,\ a_1,\ \ldots,\ a_{n-1} \in \mathbb{F}. \tag{3.1}$$

Toto vyjádření nám připomíná reprezentaci vektoru pomocí bázových vektorů 1, u, u^2, $\ldots, u^{n-1}$. To nás vede k myšlence použít pojmy z teorie vektorových prostorů.

Každé rozšíření $\mathbb{K}$ tělesa $\mathbb{F}$ můžeme pokládat za vektorový prostor nad $\mathbb{F}$. Operacemi vektorového prostoru jsou sčítání prvků v $\mathbb{K}$ a násobení prvku z $\mathbb{K}$ prvkem z $\mathbb{F}$, tyto operace vyhovují všem axiomům vektorového prostoru [3].

Definice 3.1 Těleso $\mathbb{K}$ nazveme **konečným rozšířením tělesa** $\mathbb{F} \subseteq \mathbb{K}$, jestliže $\mathbb{K}$ je prostor konečné dimenze nad $\mathbb{F}$. Dimenzi vektorového prostoru $\mathbb{K}$ nad $\mathbb{F}$ nazýváme stupněm rozšíření $\mathbb{K}$ nad $\mathbb{F}$ a označujeme jej $[\mathbb{K} : \mathbb{F}]$.

Věta 3.1 *Stupeň algebraického prvku u nad tělesem $\mathbb{F}$ se rovná dimenzi rozšíření $\mathbb{F}(u)$, jestliže jej pokládáme za vektorový prostor nad $\mathbb{F}$. Tento prostor má bázi* 1, u, $\ldots$, u^{n-1}.

Základní vlastností vektorových prostorů konečné dimenze je to, že každé 2 báze daného vektorového prostoru mají stejný počet prvků.

Důsledek 3.1 Nechť dva algebraické prvky u a v nad tělesem $\mathbb{F}$ generují stejné rozšíření $\mathbb{F}(u) = \mathbb{F}(v)$. Pak u a v mají nad $\mathbb{F}$ stejný stupeň.

Jednoduché algebraické rozšíření je konečné a obráceně každé konečné rozšíření se skládá z algebraických prvků.

Věta 3.2 *Každý prvek v konečného rozšíření tělesa $\mathbb{F}$ je algebraický prvek nad $\mathbb{F}$ a vyhovuje nějaké rovnici, která je nad $\mathbb{F}$ ireducubilní a její stupeň je nejvýše n, kde $n = [\mathbb{F} : \mathbb{K}]$.*

Důkaz. Nechť $\mathbb{K}$ je vektorový prostor dimenze n a prvky 1, v, v^2, $\ldots$, v^n leží v tomto vektorovém prostoru. Tyto prvky musí být nad $\mathbb{F}$ lineárně závislé, tj. musí existovat

lineární kombinace $b_0+b_1v+b_2v^2+\ldots+b_nv^n=0$, pro kterou platí, že všechny koeficienty b_i nejsou současně rovny nule (kde $i=0,\ 1,\ \ldots,\ n$). Jestliže se na tento vztah díváme jako na polynom, vidíme, že v je algebraický prvek nad $\mathbb{F}$, jehož stupeň je nejvýše n [3]. □

Důsledek 3.2 Každý prvek jednoduchého algebraického rozšíření $\mathbb{F}(u)$ je nad $\mathbb{F}$ algebraický.

Tento důležitý závěr nám zaručí, že nikdy v jednoduchém algebraickém rozšíření nemůžeme naleznout transcedentní prvek.

3.2 Vícenásobné algebraické rozšíření

Konečné rozšíření tělesa můžeme sestrojit tak, že na těleso postupně aplikujeme jednoduchá algebraická rozšíření. V případě, že těleso má charakteristiku 0, je vícenásobné rozšíření generováno jedním prvkem. Nyní uvedeme definici vícenásobného rozšíření [3].

Definice 3.2 Těleso $\mathbb{K}$ nazveme ***k*-násobným algebraickým rozšířením** tělesa $\mathbb{F}$, jestliže existují prvky $u_1,\ u_2,\ \ldots,\ u_k\in\mathbb{K}$ a posloupnost jednoduchých algebraických rozšíření

$$\mathbb{F}_1=\mathbb{F}(u_1),\mathbb{F}_2=\mathbb{F}_1(u_2),\ldots,\mathbb{F}_k=\mathbb{F}_{k-1}(u_k)=\mathbb{K}.$$

Řekneme, že rozšíření $\mathbb{K}$ je generované prvky $u_1,\ u_2,\ \ldots,\ u_k$ a píšeme $\mathbb{K}=\mathbb{F}(u_1,\ u_2,\ \ldots,\ u_k)$.

Poznámka 3.1 Z předcházející definice vyplývá, že množina $\mathbb{F}\cup\{u_1,\ u_2,\ \ldots,\ u_k\}$ generuje těleso $\mathbb{F}(u_1,\ u_2,\ \ldots,\ u_k)$, přičemž prvek u_1 je algebraický nad $\mathbb{F}$, u_2 algebraický nad $\mathbb{F}(u_1)$, atd. Taktéž obráceně těleso $\mathbb{K}$ je k-násobné rozšíření tělesa $\mathbb{F}$ generované prvky $u_1,\ u_2,\ \ldots,\ u_k$.

Věta 3.3 *Nechť u je algebraický prvek nad $\mathbb{F}$. Potom rozšíření $\mathbb{F}(u)$ je konečné nad $\mathbb{F}$ a platí $[\mathbb{F}(u):\mathbb{F}]=[u:\mathbb{F}]$. Obráceně, jestliže $\mathbb{K}$ je konečné rozšíření nad $\mathbb{F}$, potom pro každý prvek $v\in\mathbb{K}$ platí, že je algebraický nad $\mathbb{F}$ a $[v:\mathbb{F}]\leq[\mathbb{K}:\mathbb{F}]$.*

Hlavním prostředkem na zkoumání vícenásobných rozšíření je následující věta o skládání bází.

Věta 3.4 *Nechť* $u_1,\ u_2,\ \ldots,\ u_n$ *tvoří bázi konečného rozšíření* $\mathbb{K}$ *nad tělesem* $\mathbb{F}$ *a nechť* $v_1,\ v_2,\ \ldots,\ v_m$ *tvoří bázi konečného rozšíření* $\mathbb{L}$ *nad tělesem* $\mathbb{K}$. *Potom prvky* $u_i v_j$, *kde* $i = 1,\ \ldots,\ n,\ j = 1,\ \ldots,\ m$ *tvoří bázi* $\mathbb{L}$ *nad* $\mathbb{F}$.

Důkaz. Protože $v_1,\ v_2,\ \ldots,\ v_m$ tvoří bázi $\mathbb{L}$ nad $\mathbb{K}$, každý prvek $a \in \mathbb{L}$ můžeme napsat ve tvaru

$$a = b_1 v_1 + b_2 v_2 + \ \ldots\ + b_m v_m$$

pro nějaké $b_1,\ b_2,\ \ldots,\ b_m \in \mathbb{K}$. Jelikož $u_1,\ u_2,\ \ldots,\ u_n$ tvoří bázi $\mathbb{K}$ nad $\mathbb{F}$, lze každý prvek $b_1,\ b_2,\ \ldots,\ b_m$ vyjádřit v následujícím tvaru

$$b_j = c_{1j} u_1 + c_{2j} u_2 + \ \ldots\ + c_{nj} u_n$$

pro nějaké $c_{1j},\ c_{2j},\ \ldots,\ c_{nj} \in \mathbb{F}$. Znamená to, že prvek $a \in \mathbb{L}$ můžeme vyjádřit ve tvaru lineární kombinace

$$a = \sum_{j=1}^{m} b_j v_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} c_{ij} u_i \right) v_j = \sum_{j=1}^{m} \sum_{i=1}^{n} c_{ij} u_i v_j$$

s koeficienty z $\mathbb{F}$. K důkazu lineární nezávislosti nad $\mathbb{F}$ předpokládejme, že

$$\sum_{j=1}^{m} \sum_{i=1}^{n} c_{ij} u_i v_j = 0;\ c_{ij} \in \mathbb{F},\ \text{pro}\ i = 1,\ \ldots,\ n,\ j = 1,\ \ldots,\ m\,.$$

Jestliže označíme $b_j = c_{1j} u_1 + c_{2j} u_2 + \cdots + c_{nj} u_n$, pro $j = 1,\ \ldots,\ m$, pak dostaneme $\sum_{j=1}^{m} b_j v_j = 0$, přičemž $b_1, \ldots,\ b_m \in \mathbb{K}$. Z lineární nezávislosti prvků $v_1,\ v_2,\ \ldots,\ v_m$ nad $\mathbb{K}$ dostáváme $b_1 = b_2 = \ \ldots\ = b_m = 0$ a dále z lineární nezávislosti prvků $u_1,\ u_2,\ \ldots,\ u_n$ nad $\mathbb{F}$ plyne $c_{ij} = 0$ pro všechny $i = 1,\ \ldots,\ n,\ j = 1,\ \ldots,\ m$ [7]. □

Důsledek 3.3 Nechť $\mathbb{K}$ *je konečné rozšíření tělesa* $\mathbb{F}$ *a* $\mathbb{L}$ *je konečné rozšíření tělesa* $\mathbb{K}$. *Pak* $\mathbb{L}$ *je konečné rozšíření tělesa* $\mathbb{F}$ a *platí*

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}]\,;\ \text{kde}\ \mathbb{L} \supset \mathbb{K} \supset \mathbb{F}. \tag{3.2}$$

Důsledek 3.4 Nechť prvky $u_1,\ u_2,\ \ldots,\ u_k$ *generují nad* $\mathbb{F}$ *k-násobné algebraické rozšíření* $\mathbb{L} = \mathbb{F}(u_1,\ u_2,\ \ldots,\ u_k)$. *Pak* $\mathbb{L}$ *je konečné rozšíření tělesa* $\mathbb{F}$ *a každý z prvků* $u_1,\ u_2,\ \ldots,\ u_k$ *je algebraický nad* $\mathbb{F}$.

Důsledek 3.5 Necht' $\mathbb{K}$ *je konečné rozšíření tělesa* $\mathbb{F}$ *stupně* $n = [\mathbb{K} : \mathbb{F}]$. *Pak stupeň každého prvku* u *z* $\mathbb{K}$ *nad* $\mathbb{F}$ *je dělitelem čísla* n.

Důsledek 3.6 Prvek u *z konečného rozšíření* $\mathbb{K} \supset \mathbb{F}$ *generuje nad* $\mathbb{F}$ *celé rozšíření* $\mathbb{K}$ *právě tehdy, když* $[\mathbb{K} : \mathbb{F}] = [u : \mathbb{F}]$.

Důsledek 3.7 Necht' $\mathbb{L}$ *je konečné rozšíření stupně* 2^n *nad tělesem* $\mathbb{F}$. *Potom* $\mathbb{L}$ *neobsahuje žádný prvek třetího stupně nad* $\mathbb{F}$.

Z důsledku 3.7 vyplývá neřešitelnost úlohy o duplikaci krychle. Úlohu lze formulovat: Nalezněte obecnou eukleidovskou konstrukci, pomocí níž bude možné k libovolné krychli zkonstruovat hranu krychle o dvojnásobném objemu. Konstrukce pomocí pravítka a kružítka určuje vícenásobné rozšíření tělesa $\mathbb{Q}$. Toto rozšíření je generováno prvky druhého stupně, protože rovnice kružnice je druhého stupně. Celkový stupeň rozšíření je podle důsledku 3.3 mocninou 2^n a podle důsledku 3.7 nemůže rozšíření obsahovat číslo $\sqrt[3]{2}$, které má právě stupeň tři nad $\mathbb{Q}$. Proto tato úloha není eukleidovsky řešitelná [7].

Druhou proslulou antickou úlohou je trisekce úhlu. Zadání této úlohy lze formulovat: Je dán úhel α, sestrojte eukleidovsky úhel o velikosti $\frac{\alpha}{3}$. Neřešitelnost lze dokázat na základě důsledku 3.7 až na zvlášní případy, kdy úhel je násobkem pravého úhlu. Třetí antickou úlohou je kvadratura kruhu: Necht' je dána kružnice k o poloměru r. Sestrojte eukleidovsky čtverec, který má stejný obsah jako vnitřek kružnice k. Neřešitelnost této úlohy vyplývá z transcendentnosti čísla $\sqrt{\pi}$ nad $\mathbb{Q}$. Neřešitelnost těchto tří antických úloh byla dokázána v 19. století pomocí moderní algebry [6].

Řešené příklady

Příklad 3.1 Číslo $\alpha = u^2 + u$, kde u splňuje rovnici $u^3 = -3u + 1$, patří do jednoduchého algebraického rozšíření $\mathbb{Q}(u)$ tělesa $\mathbb{Q}$. Najděte minimální polynom čísla u nad $\mathbb{Q}$.

Řešení: Minimální polynom pro $\alpha = u^2 + u$ nad $\mathbb{Q}$ určíme analogickým způsobem, který byl použit ve druhé kapitole.

$$\alpha^0 = 1$$
$$\alpha^1 = u^2 + u$$
$$\alpha^2 = u^4 + 2u^3 + u^2 = u(-3u + 1) + 2(-3u + 1) + u^2 = -2u^2 - 5u + 2$$
$$\alpha^3 = -2u^4 - 7u^3 - 3u^2 + 2u = 3u^2 + 21u - 7$$

Ověříme, jestli α^3 je lineární kombinací prvků α^2, α^1, α^0, tj. zda existují a, b, $c \in \mathbb{Q}$ tak, že $\alpha^3 = a\alpha^2 + b\alpha + c\alpha^0$. Tuto rovnici řešíme tak, že dosadíme za α^3, α^2, α^1, α^0 a porovnáme koeficienty u jednotlivých mocnin prvku u.

$$u^2: \quad 3 = -2a + b$$
$$u^1: \quad 21 = -5a + b$$
$$u^0: \quad -7 = 2a + c$$

Řešení této soustavy rovnic je:

$$a = -6$$
$$b = -9$$
$$c = 5$$

Hledaný minimální polynom $f = x^3 + 6x^2 + 9x - 5$.

Příklad 3.2 Rozhodněte, zda dané číslo generuje uvedené rozšíření tělesa $\mathbb{Q}$. V každém případě dokažte, že vaše tvrzení je správné.

a) $\alpha = 2 + \sqrt[3]{9}$ v $\mathbb{Q}\left(\sqrt[3]{3}\right)$
b) $\beta = 2v + 1$ v $\mathbb{Q}(v)$, kde $v^3 + v - 2 = 0$

Řešení:

a) $\alpha = 2 + \sqrt[3]{9}$ v $\mathbb{Q}\left(\sqrt[3]{3}\right)$

Z věty 2.6 plyne, že $\alpha \in \mathbb{Q}\left(\sqrt[3]{3}\right)$. Dále budeme postupovat podle důsledku 3.6.

i) Určíme stupeň α nad $\mathbb{Q}$ jako stupeň jeho minimálního polynomu.

$$\alpha^0 = 1$$
$$\alpha^1 = 2 + \sqrt[3]{9}$$

$$\alpha^2 = 4 + 4\sqrt[3]{9} + 3\sqrt[3]{3}$$
$$\alpha^3 = (2+\sqrt[3]{9})(4+4\sqrt[3]{9}+3\sqrt[3]{3}) = 12\sqrt[3]{9}+18\sqrt[3]{3}+17 = 6\alpha^2-12\alpha+17$$

Proto minimální polynom pro α nad $\mathbb{Q}$ je $x^3 - 6x^2 + 12x - 17$, který je třetího stupně, což znamená, že $[\alpha : \mathbb{Q}] = 3$.

ii) Určíme $\left[\mathbb{Q}\left(\sqrt[3]{3}\right) : \mathbb{Q}\right]$.
Minimální polynom pro $\sqrt[3]{3}$ nad $\mathbb{Q}$ je $x^3 - 3$, tedy $\left[\mathbb{Q}\left(\sqrt[3]{3}\right) : \mathbb{Q}\right] = 3$.

Platí, že $\alpha \in \mathbb{Q}$, dále $\left[\mathbb{Q}\left(\sqrt[3]{3}\right) : \mathbb{Q}\right] = \left[\sqrt[3]{3} : \mathbb{Q}\right]$, proto podle důsledku 3.6 α generuje rozšíření $\mathbb{Q}\left(\sqrt[3]{3}\right)$ tělesa $\mathbb{Q}$.

b) $\beta = 2v + 1$ v $\mathbb{Q}(v)$, kde $v^3 + v - 2 = 0$
Ze vztahu $v^3 + v - 2 = 0$ plyne, že v je algebraický prvek třetího stupně nad $\mathbb{Q}$. Podle věty 2.6 $\beta \in \mathbb{Q}(v)$. Určíme stupeň prvku β nad tělesem $\mathbb{Q}$.

$$\beta^0 = 1$$
$$\beta^1 = 2v + 1$$
$$\beta^2 = 4v^2 + 4v + 1$$
$$\beta^3 = 8v^3+12v^2+6v+1 = 12v^2-2v+17 = 3(4v^2+4v+1)-7(2v+1)+21$$

Můžeme psát $\beta^3 = 3\beta^2 - 7\beta + 21 \Rightarrow \beta$ je algebraický prvek třetího stupně nad $\mathbb{Q} \Rightarrow [\beta : \mathbb{Q}] = [\mathbb{Q}(v) : \mathbb{Q}]$.
Tím jsou splněny předpoklady důsledku 3.6, a proto β generuje rozšíření $\mathbb{Q}(v)$ tělesa $\mathbb{Q}$.

Příklad 3.3 Rozhodněte, zda číslo $\alpha = \pi^7 + 5\pi^4 - 2\pi^2 + 1$ je transcendentní nebo algebraické nad $\mathbb{Q}$.

Řešení: Budeme postupovat sporem, předpokládejme, že α je nad $\mathbb{Q}$ algebraické. Pak π je kořenem polynomu $x^7 + 5x^4 - 2x^2 + 1 - \alpha$, tzn. že π je algebraické nad $\mathbb{Q}(\alpha)$. Rozšíření $\mathbb{Q}(\alpha, \pi)$ je konečné nad $\mathbb{Q}$ a podle důsledku 3.4 π je algebraické nad $\mathbb{Q}$. Což je spor, protože π je nad $\mathbb{Q}$ transcendentní, tedy α je transcendentní nad $\mathbb{Q}$.

Příklad 3.4 Dokažte, že $\mathbb{Q}\left(\sqrt{2},\ \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{3},\ \sqrt{2}\right)$.

Řešení: Pro těleso $\mathbb{Q}\left(\sqrt{2},\ \sqrt{3}\right)$ platí:

i) $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$, jelikož minimální polynom pro $\sqrt{2}$ nad $\mathbb{Q}$ je druhého stupně. Proto

podle důsledku 2.2 bázi tělesa $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$ určují prvky 1, $\sqrt{2}$.

ii) $\left[\mathbb{Q}(\sqrt{2},\ \sqrt{3}) : \mathbb{Q}(\sqrt{2})\right] = 2$, protože minimální polynom pro $\sqrt{3}$ nad $\mathbb{Q}(\sqrt{2})$ je druhého stupně. Tedy podle věty 3.1 bázi tělesa $\mathbb{Q}(\sqrt{2},\ \sqrt{3})$ nad $\mathbb{Q}(\sqrt{2})$ určují prvky 1, $\sqrt{3}$.

Podle věty 3.4 platí, že báze $\mathbb{Q}(\sqrt{2},\ \sqrt{3})$ nad $\mathbb{Q}$ je 1, $\sqrt{3}$, $\sqrt{2}$, $\sqrt{6}$.

Pro těleso $\mathbb{Q}(\sqrt{3},\ \sqrt{2})$ platí:

i) báze $\mathbb{Q}(\sqrt{3})$ nad $\mathbb{Q}$ je určena 1, $\sqrt{3}$.

ii) báze $\mathbb{Q}(\sqrt{3},\ \sqrt{2})$ nad $\mathbb{Q}(\sqrt{3})$ je určena 1, $\sqrt{2}$.

Tedy bázi tělesa $\mathbb{Q}(\sqrt{3},\ \sqrt{2})$ nad $\mathbb{Q}$ tvoří prvky 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$. Protože obě tělesa mají stejnou bázi nad $\mathbb{Q}$, platí $\mathbb{Q}(\sqrt{2},\ \sqrt{3}) = \mathbb{Q}(\sqrt{3},\ \sqrt{2})$.

Příklad 3.5 Rozhodněte, zda polynom $f = x^3 + 5$ je ireducibilní nad tělesem $\mathbb{Q}(\sqrt{2})$. Svoji odpověď zdůvodněte.

Řešení: Předpokládejme, že by daný polynom byl reducibilní nad tělesem $\mathbb{Q}(\sqrt{2})$. Pak by musel existovat kořen daného polynomu v tělese $\mathbb{Q}(\sqrt{2})$. Označme jej α. Pro tento kořen platí

$$\alpha^3 = -5. \text{ Tedy } \alpha \notin \mathbb{Q}(\sqrt{2}), \text{ což je spor.}$$

Proto polynom $x^3 + 5$ je ireducibilní nad tělesem $\mathbb{Q}(\sqrt{2})$.

Příklad 3.6 Určete stupeň vícenásobného rozšíření a najděte jeho bázi nad $\mathbb{Q}$.

a) $\mathbb{Q}(\sqrt{2},\ \sqrt{7})$
b) $\mathbb{Q}(1 + \sqrt[3]{3},\ \sqrt{3})$

Řešení:

a) $\mathbb{Q}(\sqrt{2},\ \sqrt{7})$

i) Určíme stupeň rozšíření a bázi $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$.
Minimální polynom pro $\sqrt{2}$ nad $\mathbb{Q}$ je $x^2 - 2 \Rightarrow \left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2$ a bázi tvoří 1, $\sqrt{2}$.

ii) Nalezneme stupeň rozšíření a bázi $\mathbb{Q}(\sqrt{2},\ \sqrt{7})$ nad $\mathbb{Q}(\sqrt{2})$.
Minimální polynom pro $\sqrt{7}$ nad $\mathbb{Q}\big(\sqrt{2}\big)$ je $x^2-7 \Rightarrow \big[\mathbb{Q}(\sqrt{2},\ \sqrt{7}) : \mathbb{Q}(\sqrt{2})\big] = 2$ a báze je tvořena prvky $1,\ \sqrt{7}$.

Dle věty 3.4 báze konečného rozšíření $\mathbb{Q}(\sqrt{2},\ \sqrt{7})$ nad $\mathbb{Q}$ je určena $1,\ \sqrt{7},\ \sqrt{2},\ \sqrt{14}$ a podle důsledku 3.3 platí $\big[\mathbb{Q}(\sqrt{2},\ \sqrt{7}) : \mathbb{Q}\big] = \big[\mathbb{Q}(\sqrt{2},\ \sqrt{7}) : \mathbb{Q}(\sqrt{2})\big] \cdot \big[\mathbb{Q}\big(\sqrt{2}\big) : \mathbb{Q}\big] = 2 \cdot 2 = 4$.

b) $\mathbb{Q}(1+\sqrt[3]{3},\ \sqrt{3})$

i) Nalezneme stupeň prvku $1+\sqrt[3]{3}$ nad $\mathbb{Q}$. Označíme $\alpha = 1+\sqrt[3]{3}$ a určíme minimální polynom prvku α nad $\mathbb{Q}$.

$$\alpha^0 = 1$$
$$\alpha^1 = 1+\sqrt[3]{3}$$
$$\alpha^2 = 1+2\sqrt[3]{3}+\sqrt[3]{9}$$
$$\alpha^3 = (1+\sqrt[3]{3})(1+2\sqrt[3]{3}+\sqrt[3]{9}) = 3\sqrt[3]{9}+3\sqrt[3]{3}+4 = \ \ldots\ = 3\alpha^2-3\alpha+4$$

Stupeň minimálního polynomu pro α nad $\mathbb{Q}$ je tři, proto $\big[\mathbb{Q}(1+\sqrt[3]{3}) : \mathbb{Q}\big] = 3$. Jelikož $\mathbb{Q}(\sqrt[3]{3}+1) = \mathbb{Q}(\sqrt[3]{3})$, proto bázi $\mathbb{Q}(1+\sqrt[3]{3})$ nad $\mathbb{Q}$ můžeme zapsat ve tvaru $1,\ \sqrt[3]{3},\ \sqrt[3]{9}$.

ii) Určíme stupeň $\sqrt{3}$ nad $\mathbb{Q}(1+\sqrt[3]{3})$.
Minimální polynom pro $\sqrt{3}$ nad $\mathbb{Q}(1+\sqrt[3]{3})$ je $x^2-3 \Rightarrow \big[\mathbb{Q}(1+\sqrt[3]{3},\ \ \sqrt{3}) : \mathbb{Q}(1+\sqrt[3]{3})\big] = 2 \Rightarrow$ báze tělesa $\mathbb{Q}(1+\sqrt[3]{3},\ \sqrt{3})$ nad $\mathbb{Q}(1+\sqrt[3]{3})$ je $1,\ \sqrt{3}$.

Tedy $\big[\mathbb{Q}(1+\sqrt[3]{3},\ \sqrt{3}) : \mathbb{Q}\big] = \big[\mathbb{Q}(1+\sqrt[3]{3},\ \sqrt{3}) : \mathbb{Q}(1+\sqrt[3]{3})\big] \cdot \big[\mathbb{Q}(1+\sqrt[3]{3}) : \mathbb{Q}\big] = 6$ a báze konečného rozšíření tělesa $\mathbb{Q}(1+\sqrt[3]{3},\ \sqrt{3})$ nad $\mathbb{Q}$ je tvořena prvky $1,\ \sqrt[3]{3},\ \sqrt[3]{9},\ \sqrt{3},\ \sqrt{3}\sqrt[3]{3},\ \sqrt{3}\sqrt[3]{9}$.

Příklad 3.7 Dokažte, že pokud $a,\ b \in \mathbb{C}$ jsou algebraická nad $\mathbb{Q}$, tak i $a-2b$ je algebraický nad $\mathbb{Q}$.

Řešení: Jelikož čísla $a,\ b$ jsou algebraická nad $\mathbb{Q}$, existuje dvojnásobné algebraické rozšíření $\mathbb{Q}(a,\ b)$. Zřejmě $a-2b$ je prvkem tělesa $\mathbb{Q}(a,\ b)$. Těleso $\mathbb{Q}(a,\ b)$ si můžeme představit jako jednoduché rozšíření tělesa $\mathbb{Q}(a)$, které obsahuje pouze algebraické prvky, potom podle důsledku 3.2 je $a-2b$ algebraický nad $\mathbb{Q}$.

Cvičení

Cvičení 3.1 Rozhodněte, zda daný polynom je ireducibilní nad uvedeným tělesem. Svoji odpověď zdůvodněte.

a) $x^2 + 2$ nad $\mathbb{Q}(i)$
b) $2x^3 - 18$ nad $\mathbb{Q}(\sqrt{2})$

[a) je ireducibilní, jelikož $i\sqrt{2} \notin \mathbb{Q}(i)$; b) je ireducibilní, protože $\sqrt[3]{9} \notin \mathbb{Q}\big(\sqrt{2}\big)$]

Cvičení 3.2 Určete stupeň každého z následujících vícenásobných rozšíření tělesa $\mathbb{Q}$.

a) $\mathbb{Q}(\sqrt{5},\, 2i)$
b) $\mathbb{Q}(\sqrt[3]{3},\, \sqrt{9})$
c) $\mathbb{Q}(\sqrt{2}, \sqrt{3},\, \sqrt{5})$

[a) 4; b) 3; c) 8]

Cvičení 3.3 Rozhodněte, zda dané číslo generuje uvedené rozšíření tělesa $\mathbb{Q}$. V každém případě dokažte, že vaše tvrzení je správné.

a) $\alpha = \sqrt{2} + \sqrt[3]{2}$ v $\mathbb{Q}(\sqrt{2},\, \sqrt[3]{2})$
b) $\beta = 1 + \sqrt[4]{3}$ v $\mathbb{Q}\big(\sqrt[4]{3}\big)$

$\big[$a) ano generuje, jelikož $\alpha \in \mathbb{Q}(\sqrt{2},\, \sqrt[3]{2})$ a $[\alpha : \mathbb{Q}] = \big[\mathbb{Q}(\sqrt{2},\, \sqrt[3]{2}) : \mathbb{Q}\big]$; b) ano generuje, protože $\beta \in \mathbb{Q}\big(\sqrt[4]{3}\big)$ a $[\beta : \mathbb{Q}] = \big[\mathbb{Q}\big(\sqrt[4]{3}\big) : \mathbb{Q}\big]\,\big]$

Cvičení 3.4 Určete stupeň vícenásobného rozšíření a najděte jeho bázi nad $\mathbb{Q}$.

a) $\mathbb{Q}(i,\, \sqrt{3})$
b) $\mathbb{Q}(\sqrt[3]{4},\, \sqrt[3]{16})$
c) $\mathbb{Q}\big(\sqrt[3]{3},\, \sqrt[3]{24}i\big)$

[a) čtvrtého stupně s bází $1,\, \sqrt{3},\, i,\, i\sqrt{3}$; b) třetího stupně s bází $1,\, \sqrt[3]{2},\, \sqrt[3]{4}$; c) šestého stupně s bází $1,\, \sqrt[3]{3},\, \sqrt[3]{9},\, i,\, i\sqrt[3]{3},\, i\sqrt[3]{9}$]

4 Rozkladová tělesa

Postupné rozšiřování číselných oborů bylo motivováno snahou zabezpečit řešitelnost algebraických rovnic. V tělese $\mathbb{C}$ všech komplexních čísel toto úsilí vyvrcholilo. Podle základní věty algebry má každý polynom n-tého stupně s komplexními koeficienty n komplexních kořenů. Říkáme, že těleso $\mathbb{C}$ je algebraicky uzavřené [7].

Definice 4.1 Necht' f je polynom stupně $n > 0$ nad $\mathbb{F}$. Rozšíření $\mathbb{L}$ tělesa $\mathbb{F}$ nazveme **rozkladovým tělesem polynomu** f nad $\mathbb{F}$, jestliže existují prvky $c \in \mathbb{F}$, $u_1, u_2, \ldots, u_n \in \mathbb{L}$ takové, že $\mathbb{L} = \mathbb{F}(u_1, u_2, \ldots, u_n)$ a f lze nad $\mathbb{L}$ rozložit na součin lineárních činitelů

$$f = c(x - u_1)(x - u_2) \ldots (x - u_n). \tag{4.1}$$

Poznámka 4.1 Jestliže polynom f stupně n má v tělese $\mathbb{F}$ n kořenů, potom jeho rozkladovým tělesem je samotné těleso $\mathbb{F}$. Pokud polynom nelze nad daným tělesem rozložit na součin lineárních činitelů, musíme provést rozšíření tělesa $\mathbb{F}$ na těleso, ve kterém chybějící kořeny již existují. Rozkladové těleso polynomu f je zřejmě nejmenší rozšíření s touto vlastností.

Věta 4.1 *Necht' p je ireducibilní polynom nad tělesem $\mathbb{F}$. Potom existuje jednoduché algebraické rozšíření $\mathbb{F}(u)$ generované kořenem u polynomu p.*

Důkaz. Podle věty 2.5 hledané rozšíření (jestliže existuje) musí být izomorfní s tělesem $\mathbb{F}[x]/(p)$. Existenci dokážeme tak, že za hledané rozšíření vezmeme přímo $\mathbb{F}[x]/(p)$. Jednoduše lze dokázat, že zobrazení $\varphi : \mathbb{F} \to \mathbb{F}[x]/(p)$, definované vztahem $\varphi(a) = a + (p)$ pro $a \in \mathbb{F}$, je injektivní homomorfizmus, tj. vnoření tělesa $\mathbb{F}$ do $\mathbb{F}[x]/(p)$. Jestliže ztotožníme prvek $a \in \mathbb{F}$ s jeho obrazem $a + (p)$, můžeme říci, že $\mathbb{F}$ je až na izomorfizmus podtěleso tělesa $\mathbb{F}[x]/(p)$. Ukážeme, že prvek $u = x + (p)$ je kořenem polynomu p. Nyní vyjádřeme $p(u)$.

$$\begin{aligned} p(u) = p(x + (p)) = a_0 + a_1(x + (p)) + a_2(x + (p))^2 + \ldots + a_n(x + (p))^n = (a_0 + (p)) + \\ + (a_1 + (p))(x + (p)) + (a_2 + (p))(x + (p))^2 + \ldots + (a_n + (p))(x + (p))^n = (a_0 + a_1 x + \\ + a_2 x^2 + \ldots + a_n x^n) + (p) = p + (p) = 0 + (p) \end{aligned}$$

Je též zřejmé, že $u = x + (p)$ generuje $\mathbb{F}[x]/(p)$ nad $\mathbb{F}$, to znamená, že $\mathbb{F}[x]/(p) = \mathbb{F}(u)$ [7]. □

Poznámka 4.2 Větu 4.1 lze zobecnit na reducibilní polynomy.

Věta 4.2 *Pro každý polynom f nad tělesem $\mathbb{F}$,* st $f = n > 0$*, existuje rozkladové těleso polynomu f nad $\mathbb{F}$.*

Důkaz. Budeme postupovat indukcí vzhledem k n. Pro $n = 1$ je rozkladovým tělesem těleso $\mathbb{F}$. Nechť je $n > 1$. Předpokládejme platnost věty pro polynomy stupně $n-1$ nad libovolným tělesem. Podle věty 4.1 existuje rozšíření $\mathbb{F}(u_1)$ generované kořenem u_1 polynomu f. Nad $\mathbb{F}(u_1)$ máme rozklad $f = (x - u_1)g$, st $g = n - 1 > 0$. Dle indukčního předpokladu existuje těleso $\mathbb{L}$, které je rozkladovým tělesem g nad $\mathbb{F}(u_1)$. Znamená to, že existují prvky $c \in \mathbb{F}$, $u_2, u_3, \ldots, u_n \in \mathbb{L}$ takové, že $\mathbb{L} = \mathbb{F}(u_1)(u_2, u_3, \ldots, u_n)$ a $g = c(x - u_2)(x - u_3)\ldots(x - u_n)$. Těleso $\mathbb{L}$ je generované množinou $\mathbb{F}(u_1) \cup \{u_2, u_3, \ldots, u_n\}$, proto je generované též množinou $\mathbb{F} \cup \{u_1, u_2, \ldots, u_n\}$. Tedy $\mathbb{L} = \mathbb{F}(u_1, u_2, \ldots, u_n)$, přičemž nad $\mathbb{L}$ máme rozklad $f = c(x-u_1)(x-u_2)\ \ldots\ (x-u_n)$. Proto $\mathbb{L}$ je rozkladové těleso polynomu f nad $\mathbb{F}$ [7]. □

Věta 4.3 *Nechť $\mathbb{L}$, $\mathbb{L}'$ jsou rozkladová tělesa polynomu f nad tělesem $\mathbb{F}$. Pak $\mathbb{L}$ je izomorfní s $\mathbb{L}'$.*

Důkaz. Budeme postupovat indukcí vzhledem ke stupni $n = [\mathbb{L} : \mathbb{F}]$. Protože formulace věty není vhodná pro důkaz indukcí, dokážeme obecnější tvrzení. Nechť $\varphi : \mathbb{F} \to \mathbb{F}'$ je izomorfizmus těles $\mathbb{F}$, $\mathbb{F}'$, který zobrazí koeficienty polynomu f nad $\mathbb{F}$ na odpovídající koeficienty polynomu f' nad $\mathbb{F}'$, a nechť $\mathbb{L}$, $\mathbb{L}'$ jsou rozkladová tělesa polynomů f nad $\mathbb{F}$, resp. f' nad $\mathbb{F}'$. Pak φ lze rozšířit na izomorfizmus $\psi : \mathbb{L} \to \mathbb{L}'$.

Pro identický izomorfizmus $\mathbb{F}$ na $\mathbb{F}$ dokazované tvrzení zahrnuje tvrzení věty. Nechť $[\mathbb{L} : \mathbb{F}] = 1$. Pak $\mathbb{L} = \mathbb{F}$, tedy f lze nad $\mathbb{F}$ rozložit na součin lineárních činitelů. Protože φ je izomorfizmus, tak i f' lze rozložit na součin lineárních činitelů. Tedy $\mathbb{L}' = \mathbb{F}'$ a φ je izomorfizmus $\mathbb{L}$ na $\mathbb{L}'$.

Přepokládejme, že $[\mathbb{L} : \mathbb{F}] = n > 1$ a že tvrzení platí pro všechny případy $[\mathbb{L} : \mathbb{F}] < n$. Polynom f nelze nad $\mathbb{F}$ rozložit na součin lineárních činitelů, proto f má ireducibilní dělitel p nad $\mathbb{F}$, st $p = k > 1$. Označme p' odpovídající (v izomorfizmu φ) dělitel polynomu f' nad $\mathbb{F}'$.

V $\mathbb{L}$ existuje kořen u polynomu p, podobně existuje v $\mathbb{L}'$ kořen u' polynomu p'. Z věty 2.6 vyplývá, že zobrazení $\rho : \mathbb{F}(u) \to \mathbb{F}(u')$, dané vztahem

$$\rho(a_0 + a_1u + a_2u^2 + \cdots + a_{k-1}u^{k-1}) =$$

$$= \varphi(a_0) + \varphi(a_1)u' + \varphi(a_2)(u')^2 + \cdots + \varphi(a_{k-1})(u')^{k-1},$$

pro a_0, a_1, a_2, ..., $a_{k-1} \in \mathbb{F}$ je izomorfizmus rozšiřující φ.

Rozšíření $\mathbb{L}$, $\mathbb{L}'$ jsou rozkladovými tělesy polynomů f, resp. f' nad $\mathbb{F}(u)$, resp. $\mathbb{F}'(u')$. Přitom platí

$$n = [\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{F}(u)] \cdot [\mathbb{F}(u) : \mathbb{F}] = [\mathbb{L} : \mathbb{F}(u)]k.$$

Proto $k > 1 \Rightarrow [\mathbb{L} : \mathbb{F}(u)] < n$. Dle indukčního přepokladu se izomorfizmus $\rho : \mathbb{F}(u) \to \mathbb{F}(u')$ dá rozšířit na izomorfizmus $\psi : \mathbb{L} \to \mathbb{L}'$ [7]. □

V následující větě uvedeme Eisensteinovo kritérium, které nám určí postačující podmínku ireducibility polynomů ze $\mathbb{Z}[x]$ nad tělesem $\mathbb{Q}$ všech racionálních čísel.

Věta 4.4 *Nechť $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ je polynom s celočíselnými koeficienty. Jestliže existuje prvočíslo p takové, že $p \nmid a_n$, $p \mid a_i$ pro $i = 1, \ldots, n-1$ a $p^2 \nmid a_0$, pak f je ireducibilní nad $\mathbb{Q}$.*

Důkaz. Nechť existuje prvočíslo p dané vlastnosti a předpokládejme, že f je reducibilní, tj. $f = gh$, kde polynomy g a h nad $\mathbb{Q}$ jsou stupně alespoň prvního. Lze předpokládat, že polynomy g a h mají rovněž celočíselné koeficienty. Nechť tedy $g = b_0 + b_1x + \ldots + b_kx^k$, $h = c_0 + c_1x + \ldots + c_mx^m$. Pak nutně $a_0 = b_0c_0$. Jelikož $p \mid a_0$, pak buď $p \mid b_0$ nebo $p \mid c_0$, neboť p je prvočíslo. Nechť např. $p \mid b_0$, pak $p \nmid c_0$, neboť $p^2 \nmid a_0$.

Nechť tedy b_i je prvním z koeficientů $b_0, b_1, \ldots, b_k$, který není dělitelný číslem p. Takový jistě existuje, neboť $p \nmid a_n$, tj. $p \nmid b_kc_m$, což implikuje $p \nmid b_k$. Zřejmě platí $a_i = b_ic_0 + b_{i-1}c_1 + \ldots + b_1c_{i-1} + b_0c_i$. Odtud $b_ic_0 = a_i - b_{i-1}c_1 - \ldots - b_1c_{i-1} - b_0c_i$. Avšak $p \mid a_i$ pro $i \leq k < n$ (k je stupeň g, tj. $k < n$), $p \mid b_0, \ldots, p \mid b_{i-1}$, jak jsme předpokládali. Tedy p dělí pravou stranu poslední rovnosti, takže musí dělit i levou. Avšak $p \nmid b_i$, $p \nmid c_0$, p je prvočíslo, tedy $p \nmid b_ic_0$, což je spor. Tedy polynom f je ireducibilní nad $\mathbb{Q}$ [5]. □

Řešené příklady

Příklad 4.1 Rozhodněte, zda polynom $f = x^3 + 8x - 2$ je ireducibilní nad tělesem $\mathbb{Q}(\sqrt{-2})$, svoji odpověď zdůvodněte.

Řešení: Podle Eisensteinova kritéria ověříme, zda polynom je ireducibilní nad $\mathbb{Q}$. Nalezněme prvočíslo p, pro které platí:

$$p \mid 0 = a_2$$
$$p \mid 8 = a_1$$
$$p \mid -2 = a_0$$
$$p \nmid 1 = a_3$$
$$p^2 \nmid -2 = a_0$$

Hledané prvočíslo je $p = 2$, proto podle Eisensteinova kritéria je daný polynom nad tělesem $\mathbb{Q}$ ireducibilní. Podle důsledku 3.7 (který je možné zapsat i v následujícím tvaru: když p je polynom třetího stupně ireducibilní nad $\mathbb{F}$ a $\mathbb{K}$ je rozšíření tělesa $\mathbb{F}$ stupně 2^m, potom polynom p je nad $\mathbb{K}$ ireducibilní) je polynom x^3+8x-2 nad $\mathbb{Q}(\sqrt{-2})$ ireducibilní.

Příklad 4.2 Dokažte, že polynom $f = x^3 + x - \overline{1}$ je nad tělesem $\mathbb{Z}_5$ (jehož prvky budeme značit $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$) celých čísel modulo pět ireducibilní. Kolik prvků bude mít těleso, které vznikne rozšířením tělesa $\mathbb{Z}_5$ o libovolný kořen tohoto polynomu?

Řešení:
i) Dokážeme, že polynom f je nad $\mathbb{Z}_5$ ireducibilní. Vypočteme funkční hodnoty polynomu f pro všechny zbytkové třídy ze $\mathbb{Z}_5$.

$$f(\overline{0}) = \overline{4}$$
$$f(\overline{1}) = \overline{1}$$
$$f(\overline{2}) = \overline{4}$$
$$f(\overline{3}) = \overline{4}$$
$$f(\overline{4}) = \overline{2}$$

Žádná zbytková třída není kořenem daného polynomu, proto f je ireducibilní nad $\mathbb{Z}_5$.

ii) Těleso $\mathbb{Z}_5$ rozšíříme o libovolný kořen polynomu f a určíme počet prvků tohoto rozšíření.

Uvažujme číslo α, které je kořenem polynomu f. Platí $\alpha^3 + \alpha - \overline{1} = \overline{0} \Rightarrow \alpha$ je alge-

braický prvek třetího stupně nad $\mathbb{Z}_5$. Těleso $\mathbb{Z}_5(\alpha)$ s využitím věty 2.6 můžeme zapsat v následujícím tvaru $\mathbb{Z}_5(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2;\ a_0,\ a_1,\ a_2 \in \mathbb{Z}_5\}$. Jelikož každý z prvků $a_0,\ a_1,\ a_2$ může nabývat hodnot $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, má těleso $\mathbb{Z}_5(\alpha)$ právě 5^3 prvků.

Příklad 4.3 Najděte všechny ireducibilní polynomy druhého stupně nad $\mathbb{Z}_3$.

Řešení: Libovolný kvadratický polynom nad $\mathbb{Z}_3$ můžeme zapsat ve tvaru $f = ax^2 + bx + c$, kde $a,\ b,\ c \in \mathbb{Z}_3,\ a \neq \overline{0}$. Aby daný polynom byl nad $\mathbb{Z}_3$ ireducibilní musí platit:

$$f(\overline{0}) = c \neq \overline{0}$$
$$f(\overline{1}) = a + b + c \neq \overline{0}$$
$$f(\overline{2}) = a + \overline{2}b + c \neq \overline{0}$$

Z prvního vztahu plyne, že $c_1 = \overline{1}$, $c_2 = \overline{2}$. Zvolme $c = \overline{1}$, pak platí:

$$a + b \neq \overline{2}$$
$$a + \overline{2}b \neq \overline{2}$$

Jelikož $a \neq 0 \Rightarrow a_1 = \overline{1}$, $a_2 = \overline{2}$, pro které dopočteme b.

$$a_1 = \overline{1},\ c = \overline{1} \Rightarrow b_1 = \overline{0}$$
$$a_2 = \overline{2},\ c = \overline{1} \Rightarrow b_2 = \overline{1},\ b_3 = \overline{2}$$

Hledané kvadratické ireducibilní polynomy nad $\mathbb{Z}_3$ jsou $f_1 = x^2 + \overline{1}$, $f_2 = \overline{2}x^2 + x + \overline{1}$, $f_3 = \overline{2}x^2 + \overline{2}x + \overline{1}$ a všechny s nimi asociované.

Příklad 4.4 Sestrojte těleso $\mathbb{Z}_5(\alpha)$, kde $\alpha^2 = \overline{2}$.

Řešení: Těleso zbytkových tříd modulo pět rozšíříme o prvek α. Ukážeme, že minimální polynom pro α nad $\mathbb{Z}_5$ je

$$p = x^2 + \overline{3}.$$

Ověříme, zda p je ireducibilní nad $\mathbb{Z}_5$, což provedeme analogicky jako příkladě 5.1.

$$p(\overline{0}) = \overline{3}$$
$$p(\overline{1}) = \overline{4}$$
$$p(\overline{2}) = \overline{2}$$
$$p(\overline{3}) = \overline{2}$$
$$p(\overline{4}) = \overline{4}$$

Ověřili jsme, že p je nad $\mathbb{Z}_5$ ireducibilní, proto α je algebraický prvek druhého stupně nad $\mathbb{Z}_5$. Podle věty 2.6 můžeme každý prvek ze $\mathbb{Z}_5(\alpha)$ zapsat ve tvaru $a_0 + a_1\alpha$, kde $a_0,\ a_1 \in \mathbb{Z}_5$.

Toto rozšíření je tvořeno právě následujícími prvky:
$\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$,
α, $\overline{1}+\alpha$, $\overline{2}+\alpha$, $\overline{3}+\alpha$, $\overline{4}+\alpha$,
$\overline{2}\alpha$, $\overline{1}+\overline{2}\alpha$, $\overline{2}+\overline{2}\alpha$, $\overline{3}+\overline{2}\alpha$, $\overline{4}+\overline{2}\alpha$,
$\overline{3}\alpha$, $\overline{1}+\overline{3}\alpha$, $\overline{2}+\overline{3}\alpha$, $\overline{3}+\overline{3}\alpha$, $\overline{4}+\overline{3}\alpha$,
$\overline{4}\alpha$, $\overline{1}+\overline{4}\alpha$, $\overline{2}+\overline{4}\alpha$, $\overline{3}+\overline{4}\alpha$, $\overline{4}+\overline{4}\alpha$.
Pro sčítání a násobení v $\mathbb{Z}_5(\alpha)$ platí:

$$(a_0+a_1\alpha)+(b_0+b_1\alpha)=(a_0+b_0)+(a_1+b_1)\alpha,$$
$$(a_0+a_1\alpha)(b_0+b_1\alpha)=a_0b_0+a_0b_1\alpha+a_1b_0\alpha+a_1b_1\alpha^2=$$
$$=(a_0b_0+\overline{2}a_1b_1)+(a_0b_1+a_1b_0)\alpha.$$

Příklad 4.5 Určete stupeň a najděte bázi rozkladového tělesa nad $\mathbb{Q}$ pro následující polynomy.

a) x^3-3
b) x^4-25

Řešení:
a) x^3-3
První rozšíření provedeme o libovolný kořen tohoto polynomu, označme jej α. Zvolme $\alpha=\sqrt[3]{3}$. Zřejmě platí

$$x^3-3=(x-\alpha)(x^2+\alpha x+\alpha^2).$$

Polynom $x^2+\alpha x+\alpha^2$ je druhého stupně, proto pro jeho kořeny platí

$$x_{1,\,2}=\tfrac{-\alpha\pm\sqrt{\alpha^2-4\alpha^2}}{2}=\tfrac{-\alpha\pm\alpha i\sqrt{3}}{2}.$$

$\Rightarrow$ těleso $\mathbb{Q}\big(\sqrt[3]{3}\big)$ musíme rozšířit o $i\sqrt{3}$, jelikož $i\sqrt{3}\notin\mathbb{Q}\big(\sqrt[3]{3}\big)$ $\Rightarrow$ těleso $\mathbb{Q}(\sqrt[3]{3},\,i\sqrt{3})$ je rozkladovým tělesem polynomu x^3-3.

Stupeň tělesa $\mathbb{Q}(\sqrt[3]{3})$ nad $\mathbb{Q}$ je tři, protože minimální polynom pro $\sqrt[3]{3}$ nad $\mathbb{Q}$ je x^3-3
$\Rightarrow$ bázi tělesa $\mathbb{Q}(\sqrt[3]{3})$ nad $\mathbb{Q}$ tvoří prvky 1, $\sqrt[3]{3}$, $\sqrt[3]{9}$.
Stupeň tělesa $\mathbb{Q}(\sqrt[3]{3},\,i\sqrt{3})$ nad $\mathbb{Q}(\sqrt[3]{3})$ je dva, protože minimální polynom pro $i\sqrt{3}$ nad $\mathbb{Q}(\sqrt[3]{3})$ je druhého stupně, báze je 1, $i\sqrt{3}$.

$$\Rightarrow\ \Big[\mathbb{Q}(\sqrt[3]{3},\,i\sqrt{3}):\mathbb{Q}\Big]=\Big[\mathbb{Q}(\sqrt[3]{3},\,i\sqrt{3}):\mathbb{Q}(\sqrt[3]{3})\Big]\cdot\Big[\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}\Big]=$$

$$=2\cdot3=6$$

Stupeň konečného rozšíření tělesa $\mathbb{Q}(\sqrt[3]{3},\ i\sqrt{3})$ nad $\mathbb{Q}$ je šest a bázi určují prvky (dle věty 3.4) $1,\ \sqrt[3]{3},\ \sqrt[3]{9},\ i\sqrt{3},\ i\sqrt{3}\sqrt[3]{3},\ i\sqrt{3}\sqrt[3]{9}$.

b) $x^4 - 25$

Předpokládejme, že α je kořenem tohoto polynomu. Pak platí $\alpha^4 = 25 \Rightarrow \alpha^2 = \pm 5$. Zvolme $\alpha = \sqrt{5}$, těleso $\mathbb{Q}$ rozšíříme o prvek α. Je zřejmé, že $-\alpha$ je také kořenem tohoto polynomu. Nad tělesem $\mathbb{Q}(\alpha)$ platí

$$x^4 - 25 = (x - \alpha)(x + \alpha)(x^2 + \alpha^2).$$

Jelikož polynom $x^2 + \alpha^2$ je nad $\mathbb{Q}(\alpha)$ ireducibilní, provedeme poslední rozšíření o prvek β, pro který platí $\beta^2 = -\alpha^2$, tj. $\beta = \pm i\alpha$. Vzhledem k tomu, že $\alpha \in \mathbb{Q}(\alpha)$, stačí k tělesu $\mathbb{Q}(\alpha)$ adjungovat prvek i. Tedy těleso $\mathbb{Q}(\sqrt{5},\ i)$ je rozkladovým tělesem polynomu $x^4 - 25$.

Stupeň $\sqrt{5}$ nad $\mathbb{Q}$ je dva $\Rightarrow$ báze tělesa $\mathbb{Q}\big(\sqrt{5}\big)$ nad $\mathbb{Q}$ je $1,\ \sqrt{5}$.
Stupeň prvku i nad $\mathbb{Q}\big(\sqrt{5}\big)$ je dva $\Rightarrow$ báze tělesa $\mathbb{Q}\big(\sqrt{5},\ i\big)$ nad $\mathbb{Q}\big(\sqrt{5}\big)$ je $1,\ i$.

Proto $\big[\mathbb{Q}\big(\sqrt{5},\ i\big) : \mathbb{Q}\big] = 4$ a báze rozkladového tělesa $\mathbb{Q}\big(\sqrt{5},\ i\big)$ nad $\mathbb{Q}$ je určena prvky $1,\ i,\ \sqrt{5},\ i\sqrt{5}$.

Příklad 4.6 Dokažte, že rozkladové těleso $\mathbb{L}$ polynomu stupně n nad tělesem $\mathbb{F}$ má stupeň $[\mathbb{L} : \mathbb{F}] \leq n!$.

Řešení: Uvažujme libovolný polynom $f = a_n x^n + a_{n-1}x^{n-1} + \ \ldots\ + a_1 x + a_0$ ireducibilní nad $\mathbb{F}$, kde $a_n,\ a_{n-1},\ \ldots,\ a_1,\ a_0 \in \mathbb{F}$.
První rozšíření tělesa $\mathbb{F}$ provedeme o α_1, kde α_1 je kořen polynomu f. Prvek α_1 je nejvýše stupně n nad tělesem $\mathbb{F}$, což plyne z toho, že st $f = n$ a nad $\mathbb{F}(\alpha_1)$ platí

$$f = a_n(x - \alpha_1)f_1,$$

kde f_1 je podíl po dělení polynomu f polynomem $a_n(x - \alpha_1)$. Stupeň polynomu f_1 je $n - 1$ a tento polynom může být obecně ireducibilní nad $\mathbb{F}(\alpha_1)$. Provedeme další rozšíření tělesa $\mathbb{F}(\alpha_1)$ o α_2, který je kořenem polynomu f_1. Stupeň prvku α_2 nad tělesem $\mathbb{F}(\alpha_1)$ je nejvýše $n - 1$, jelikož st $f_1 = n - 1$. Nad tělesem $\mathbb{F}(\alpha_1, \alpha_2)$ platí

$$f = a_n(x - \alpha_1)f_1 = a_n(x - \alpha_1)(x - \alpha_2)f_2.$$

Polynom f_2 je $n - 2$ stupně. Nyní jsme už dostali těleso $\mathbb{F}(\alpha_1,\ \alpha_2)$, rozšiřování bu-

deme provádět tak dlouho, než dostaneme rozkladové těleso polynomu f nad $\mathbb{F}$. Poslední rozšíření bude obecně o prvek α_{n-1}, jelikož polynom f_3 může být ireducibilní nad $\mathbb{F}(\alpha_1, \alpha_2, \alpha_3)$, f_4 ireducibilní nad $\mathbb{F}(\alpha_1, \ldots, \alpha_4)$, $\ldots$, f_{n-2} ireducibilní nad $\mathbb{F}(\alpha_1, \ldots, \alpha_{n-2})$, kde f_3 je podíl při dělení f_2 polynomem $x - \alpha_3$, $\ldots$, f_{n-2} je podíl při dělení f_{n-3} polynomem $x - \alpha_{n-2}$. Nad tělesem $\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_{n-2})$ platí

$$f = a_n(x - \alpha_1) \ \ldots \ (x - \alpha_{n-2})f_{n-2}.$$

Polynom f_{n-2} je druhého stupně, obecně tento polynom může být ireducibilní nad $\mathbb{F}(\alpha_1, \ldots, \alpha_{n-2})$. Provedeme poslední rozšíření tělesa $\mathbb{F}(\alpha_1, \ldots, \alpha_{n-2})$ o α_{n-1}, který je nejvýše druhého stupně nad $\mathbb{F}(\alpha_1, \ldots, \alpha_{n-2})$. Nad tělesem $\mathbb{F}(\alpha_1, \ldots, \alpha_{n-1})$ lze polynom f rozložit na součin lineárních činitelů, tedy

$$f = a_n(x - \alpha_1)(x - \alpha_2) \ \ldots (x - \alpha_{n-1})(x - \alpha_n).$$

Platí, že $\mathbb{L} = \mathbb{F}(\alpha_1, \ldots, \alpha_{n-1})$.
Pro stupeň tělesa $\mathbb{L}$ nad $\mathbb{F}$ platí

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{F}(\alpha_1, \ldots, \alpha_{n-1}) : \mathbb{F}(\alpha_1, \ldots, \alpha_{n-2})] \cdot [\mathbb{F}(\alpha_1, \ldots, \alpha_{n-2}) : \mathbb{F}(\alpha_1, \ldots, \alpha_{n-3})] \cdot$$

$$\cdot \ \ldots \ \cdot [\mathbb{F}(\alpha_1, \alpha_2) : \mathbb{F}(\alpha_1)] \cdot [\mathbb{F}(\alpha_1) : \mathbb{F}] \leq 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n = n!.$$

Tím byla dokázána platnost tohoto tvrzení.

Cvičení

Cvičení 4.1 Dokažte, že polynom $x^4 + x^2 + \overline{1}$ je nad $\mathbb{Z}_5$ ireducibilní.

Cvičení 4.2 Nalezněte ireducibilní polynomy druhého a třetího stupně nad $\mathbb{Z}_2$.

$[f_1 = x^2 + x + \overline{1}, f_2 = x^3 + x^2 + \overline{1},\ f_3 = x^3 + x + \overline{1}\,]$

Cvičení 4.3 Rozhodněte, které z následujících polynomů jsou nad $\mathbb{Q}$ ireducibilní. (využijte Eisensteinova kritéria)

a) $x^3 + 2x^2 + 4x + 2$
b) $4x^4 + 2x^3 + 4x^2 - 10$
c) $x^6 + 3x^5 - 18x^4 + 81x^3 - 9x^2 + 12x + 3$

[a) ireducibilní, hledané provočíslo $p = 2$; b) reducibilní, zřejmě kořen je jedna; c) ireducibilní, hledané prvočíslo $p = 3$]

Cvičení 4.4 Určete stupeň a najděte bázi rozkladového tělesa nad $\mathbb{Q}$ pro následující polynomy.

a) $x^3 - 2$
b) $x^4 - 12x^2 + 35$
c) $x^4 - 4$

[a) šestého stupně s bází $1, \sqrt[3]{2}, \sqrt[3]{4}, i\sqrt{3}, i\sqrt{3}\sqrt[3]{2}, i\sqrt{3}\sqrt[3]{4}$; b) čtvrtého stupně s bází $1, \sqrt{5}, \sqrt{7}, \sqrt{35}$; c) čtvrtého stupně s bází $1, i, \sqrt{2}, i\sqrt{2}\,$]

5 Konečná tělesa

Necht' je dáno konečné těleso $\mathbb{F}$, které obsahuje těleso $\mathbb{Z}_p$ celých čísel modulo p, kde p je prvočíslo. $\mathbb{F}$ je tedy konečným rozšířením tělesa $\mathbb{Z}_p$ a má nad $\mathbb{Z}_p$ bázi $u_1, \ldots, u_n$. Každý prvek z tělesa $\mathbb{F}$ můžeme vyjádřit pomocí lineární kombinace $\sum_{i=1}^{n} a_i u_i$, kde koeficient a_i lze ze $\mathbb{Z}_p$ vybrat právě p způsoby, tedy těleso $\mathbb{F}$ má celkem p^n prvků. Tento výsledek shrneme do následující věty [3].

Věta 5.1 *Počet q prvků konečného tělesa se rovná mocnině p^n jeho chrakteristiky.*

Věta 5.2 *Každá dvě konečná tělesa se stejným počtem prvků jsou izomorfní.*

Důkaz. Uvažujme konečné těleso $\mathbb{F}$, které má $q = p^n$ prvků. Řád každého nenulového prvku je dělitelem čísla $q-1$, tedy každý prvek vyhovuje rovnici $x^{q-1} = 1$. Proto všechny prvky $c_1, c_2, \ldots, c_q$ tělesa $\mathbb{F}$ jsou kořeny rovnice

$$x^q - x = 0. \tag{5.1}$$

Tento součin $(x - c_1)(x - c_2) \ldots (x - c_q)$ je dělitelem polynomu $x^q - x$, jednotliví činitelé jsou navzájem nesoudělné polynomy, každý z nich dělí $x^q - x$. Protože součin i polynom $x^q - x$ jsou normované a mají stupeň q, dostáváme rovnost

$$x^q - x = (x - c_1)(x - c_2) \ldots (x - c_q). \tag{5.2}$$

Proto $\mathbb{F}$ je rozkladovým tělesem polynomu $x^q - x$ nad $\mathbb{Z}_p$. Zřejmě další konečné těleso se stejným počtem prvků je rozkladovým tělesem téhož polynomu a je tedy na základě jednoznačnosti rozkladového tělesa (podle věty 4.3) izomorfní s $\mathbb{F}$ [3]. □

Věta 5.3 *Ke každému prvočíslu p a přirozenému číslu n existuje těleso, které má $p^n = q$ prvků. Jedná se o rozkladové těleso polynomu $x^q - x$ nad $\mathbb{Z}_p$.*

Poznámka 5.1 Konečná tělesa se někdy nazývají podle francouzského matematika Evarista Galoise (1811-1832) Galoisova tělesa. Těleso, které má právě q prvků, se označuje $\mathrm{GF}(q)$.

Věta 5.4 *Zobrazení $a \mapsto a^p$ zobrazuje izomorfně každý obor integrity $\mathbb{D}$ s charakteristikou p na podobor integrity $\mathbb{D}^p$ všech p-tých mocnin prvků z $\mathbb{D}$.*

Například pokud $\mathbb{D}$ je obor integrity $\mathbb{Z}_p$ celých čísel modulo p, pak izomorfizmus $a \mapsto a^p$ je jednoduše identickým zobrazením.

Věta 5.5 *Každé konečné těleso s charakteristikou p má automorfizmus $a \mapsto a^p$.*

Důkaz. O tělesech s charakteristikou p víme, že zobrazení $a \mapsto a^p$ zobrazuje izomorfně $\mathbb{F}$ na množinu všech p-tých mocnin. Jelikož toto zobrazení je prosté, přiřadí q prvkům stejný počet p-tých mocnin (věta 5.4), které tvoří celé těleso $\mathbb{F}$. Proto zobrazení $a \mapsto a^p$ zobrazuje $\mathbb{F}$ na $\mathbb{F}$ [3]. □

Důsledek 5.1 V konečném tělese s charakteristikou p má každý prvek p-tou odmocninu.

Dále budeme charakterizovat primitivní prvek konečného tělesa.

Věta 5.6 *V každém konečném tělese $GF(p^n)$ existuje takový prvkek α, že každý nenulový prvek $\beta \in GF(p^n)$ je mocninou α, tj. $\beta = \alpha^k$. Tedy $(GF(p^n) \setminus \{0\}, \cdot)$ je cyklická grupa.*

Poznámka 5.2 Prvek α z věty 5.6 nazveme **primitivním prvkem** tělesa $\mathrm{GF}(p^n)$.

Definice 5.1 Nechť $\mathbb{L}$ je nadtěleso tělesa $\mathbb{F}$ a nechť $f \in \mathbb{F}[x]$. Je-li $\alpha \in \mathbb{L}$ kořen polynomu f, pak těleso $\mathbb{F}(\alpha)$ se nazývá **kořenové nadtěleso** polynomu f.

Věta 5.7 *Nechť α je primitivní prvek tělesa $GF(p^n)$ a nechť f je minimální polynom prvku α nad $GF(p)$. Pak* st $f = n$ *a $GF(p^n)$ je kořenové nadtěleso polynomu f.*

Důkaz. Zřejmě je $\mathrm{GF}(p^n) = \mathrm{GF}(p)(\alpha)$, tedy $\mathrm{GF}(p^n) \simeq \mathrm{GF}(p)[x]/(f)$. Z věty o dělení se zbytkem plyne, že každá třída faktorového okruhu $\mathrm{GF}(p)[x]/(f)$ obsahuje právě jeden polynom stupně menšího než st f. To však znamená, že $\mathrm{GF}(p^n)$ obsahuje právě $p^{\mathrm{st}\, f}$ prvků, tedy st $f = n$ [2]. □

Důsledek 5.2 Pro každé přirozené číslo n existuje polynom stupně n ireducibní nad $GF(p)$.

Poznámka 5.3 Věta 5.7 a její důkaz umožňují konstruovat libovolná konečná tělesa. Stačí vzít polynom f stupně n ireducibilní nad GF(p). Na množině všech polynomů stupně menšího než n definovat sčítání přirozeným způsobem. Násobení tak, že součin dvou prvků je zbytek obvyklého součinu při dělení polynomem f.

Věta 5.8 *Necht' m, n jsou dvě přirozená čísla. Pak $GF(p^m) \subseteq GF(p^n)$ právě, když $m \mid n$.*

V následující větě uvedeme jednu z vlastností konečných těles, tato věta bude uvedena bez důkazu. Důkaz této věty lze nalézt např. v [1].

Věta 5.9 *Každé konečné těleso je komutativní.*

Příkladem nekonečného nekomutativního tělesa jsou kvaterninony. Tento druh čísel zavedl William Rowan Hamilton v polovině 19. století. Kvaterniony se využívají v aplikované matematice, kvantové fyzice, teoretické mechanice např. při popisu pohybu těles v trojrozměrném prostoru, atd.

Množina $\mathbb{K}$ kvaternionů obsahuje tři imaginární jednotky i, j, k. $\mathbb{K}$ tvoří čtyřrozměrný vektorový prostor nad $\mathbb{R}$ s bází 1, i , j, k. Násobení imaginárních jednotek je určené základním vztahem $i^2 = j^2 = k^2 = ijk = -1$. Z něj pomocí asociativního zákona vyplývají další vztahy $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$ [11].

Definice 5.2 Kvaterniony nazveme uspořádané čtveřice reálných čísel (a_0, a_1, a_2, a_3), které obvykle zapisujeme ve tvaru $a_0 + a_1 i + a_2 j + a_3 k$. Sčítání a násobení kvaternionů je definováno vztahy

$$\begin{aligned}(a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k) = \\ = (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k,\end{aligned}$$

$$\begin{aligned}(a_0 + a_1 i + a_2 j + a_3 k) \cdot (b_0 + b_1 i + b_2 j + b_3 k) = \\ = (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) + (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2)i + \\ +(a_0 b_2 + a_2 b_0 + a_3 b_1 - a_1 b_3)j + (a_0 b_3 + a_3 b_0 + a_1 b_2 - a_2 b_1)k.\end{aligned}$$

Množinu všech kvaternionů budeme označovat $\mathbb{K}$.

Poznámka 5.4 Reálnou částí kvaternionu $a = a_0 + a_1 i + a_2 j + a_3 k$ rozumíme číslo a_0, imaginární uspořádanou trojici (a_1, a_2, a_3). Řekneme, že kvaternion je ryze imaginární, jestliže $a_0 = 0$.

Definice 5.3 Kvaternion $\overline{a} = a_0 - a_1 i - a_2 j - a_3 k$ nazveme **sdruženým** s kvaternionem $a = a_0 + a_1 i + a_2 j + a_3 k$. Reálné číslo

$$|a| = \sqrt{a_0^2 + a_1^2 + a_2^2 + a_3^2}$$

nazveme **absolutní hodnotou kvaternionu** a.

Řešené příklady

Příklad 5.1 Polynom $f = x^2 + x + 1$ je nad tělesem GF(2) ireducibilní. Určete kořenové nadtěleso polynomu f.

Řešení: Budeme postupovat podle poznámky 5.3. Nejprve nalezneme ireducibilní polynomy stupně nejvýše jedna nad GF(2).

$$1$$
$$\alpha = x$$
$$\beta = x + 1$$

Sčítání pro nenulové prvky zavedeme přirozený způsobem.

$+$	1	α	β
1	0	β	α
α	β	0	1
β	α	1	0

Násobení pro nenulové prvky zavedeme tak, jak je uvedeno v poznámce 5.3.

$\cdot$	1	α	β
1	1	α	β
α	α	β	1
β	β	1	α

$$1 \cdot 1 = 0 \cdot f + 1 \qquad \alpha \cdot \alpha = f + \beta$$
$$1 \cdot \alpha = 0 \cdot f + \alpha \qquad \alpha \cdot \beta = f + 1$$
$$1 \cdot \beta = 0 \cdot f + \beta \qquad \beta \cdot \beta = f + \alpha$$

Těleso GF(2^2) je určeno těmito tabulkami.

Příklad 5.2 Předpokládejme že $m \mid n$, kde $m, n \in \mathbb{N}$. Dokažte, že $(p^m - 1) \mid (p^n - 1)$, kde p je prvočíslo.

Řešení: Jestliže $m \mid n$, existuje $b \in \mathbb{N}$: $n = b\,m$. Pak můžeme psát $p^n - 1 = (p^m - 1)(1 + +p^m + p^{2m} + \ldots + p^{(b-1)m})$. Tím bylo dokázáno, že $(p^m - 1) \mid (p^n - 1)$.

Příklad 5.3 Necht' f je polynom nad tělesem $\mathbb{F}$ charakteristiky p tvaru $a_0 + a_1x^{p^2} + +a_2x^{2p^2} + \ldots + a_nx^{np^2}$. Ukažte, že $f' = 0$.

Řešení: Nejprve určíme derivaci polynomu f.

$$f' = p^2\, a_1x^{p^2-1} + 2p^2\, a_2x^{2p^2-1} + \ldots + n\, p^2\, a_nx^{np^2-1}$$

Jelikož p je charakteristika tělesa $\mathbb{F}$, pro každý prvek $a_i \in \mathbb{F}$ platí $p \cdot a_i = 0$. Tím bylo dokázáno, že $f' = o$.

Příklad 5.4 Necht' a, b, c jsou prvky z tělesa kvaternionů $\mathbb{K}$ tvaru $a = i + k$, $b = 1 + k$, $c = 1 - j + k$, vypočtěte:

a) $a + b + \overline{c}$
b) ab
c) ba
d) $\frac{a}{b}$

Řešení:

a) $a + b + \overline{c}$

Určíme kvaternion sdružený s kvaternionem c (podle definice 5.3).

$$\overline{c} = 1 + j - k$$

Pro sčítání kvaternionů využijeme definici 5.2.

$$a + b + \overline{c} = (i + k) + (1 + k) + (1 + j - k) = 2 + i + j + k$$

Tedy $a + b + \overline{c} = 2 + i + j + k$.

b) ab

Podle definice 5.2 platí

$$ab = (0+i+0j+k)(1+0i+0j+k) = (0+0+0-1)+(0+1+0-0)i+ \\ + (0+0+0-1)j + (0+1+0-0)k = -1 + i - j + k.$$

Pak $ab = -1 + i - j + k$.

c) ba

Postup viz b).

$$ba = (1+k)(i+k) = (0+0+0-1)+(1+0+0-0)i+(0+0+1-0)j+ \\ + (1+0+0-0)k = -1 + i + j + k$$

Odtud $ba = -1 + i + j + k$.

d) $\frac{a}{b}$

Dělení kvaternionů provedeme analogicky jako u komplexních čísel, výraz $\frac{a}{b}$ rozšíříme kvaternionem sdruženým k b.

$$\frac{a}{b} \cdot \frac{\overline{b}}{\overline{b}} = \frac{i+k}{1+k} \cdot \frac{1-k}{1-k} = \frac{1+i+j+k}{2} = \frac{1+i+j+k}{2}$$

Hledané vyjádření je $\frac{a}{b} = \frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k$.

Příklad 5.5 Řešte rovnici $xa = b$ nad $\mathbb{K}$, kde $a = j$, $b = 1 + i + 2j + k$.

Řešení: Jelikož x je z $\mathbb{K}$, pak $x = x_0 + x_1 i + x_2 j + x_3 k$, platí:

$$(x_0 + x_1 i + x_2 j + x_3 k)(j) = 1 + i + 2j + k$$
$$-x_2 - x_3 i + x_0 j + x_1 k = 1 + i + 2j + k$$

Porovnáním koeficientů dostaneme:

$$-x_2 = 1 \Rightarrow x_2 = -1$$
$$x_3 = 1 \Rightarrow x_3 = -1$$
$$x_0 = 2$$
$$x_1 = 1$$

Řešení rovnice $x = 2 + i - j - k$.

Cvičení

Cvičení 5.1 Určete kořenové nadtěleso polynomu $g = x^3 + x^2 + 1$ ireducibilního nad GF(2), tj. GF(2^3) = GF(8).

[tabulky pro sčítání a násobení nenulových prvků

$+$	1	a	b	c	d	e	f
1	0	b	a	d	c	f	e
a	b	0	1	e	f	c	d
b	a	1	0	f	e	d	c
c	d	e	f	0	1	a	b
d	c	f	e	1	0	b	a
e	f	c	d	a	b	0	1
f	e	d	c	b	a	1	0

$\cdot$	1	a	b	c	d	e	f
1	1	a	b	c	d	e	f
a	a	c	e	d	f	1	b
b	b	e	d	1	a	f	c
c	c	d	1	f	b	a	e
d	d	f	a	b	e	c	1
e	e	1	f	a	c	b	d
f	f	b	c	e	1	d	a

,

kde $a = x$, $b = x + 1$, $c = x^2$, $d = x^2 + 1$, $e = x^2 + x$, $f = x^2 + x + 1$]

Cvičení 5.2 Necht' $a, b, c \in \mathbb{K}$ tvaru $a = 1 + i + k$, $b = 1 - i + j$, $c = 1 + j$, vypočtěte:

a) $\overline{a} + \overline{b} + c$
b) $ab + 2c$
c) $\frac{a}{c} + bc$

[a) $3 - k$; b) $4 - 2i + 2j + 2k$; c) $\frac{1}{2} + \frac{3}{2}j - k$]

Cvičení 5.3 Řešte rovnici $xa = b + c$ nad $\mathbb{K}$, jestliže $a = 1 - i$, $b = 1 + 3j$, $c = -1 + 2i + k$.

[$x = -1 + i + 2j - k$]

Závěr

V této bakalářské práci jsou shrnuty základní poznatky teorie těles. Zabýval jsem se algebraickým rozšiřováním těles. Rozšiřování těles bylo motivováno snahou zabezpečit, aby některé rovnice byly řešitelné. Na základě rozšiřování těles je možné dokázat neřešitelnost všech tří antických úloh.

Rozšiřování těles bylo využito pro konstrukci rozkladových těles polynomů. Je zde uvedena souvislost mezi rozšířením tělesa a vektorovým prostorem a poukázáno na svázanost těchto pojmů. V neposlední řadě jsem se zabýval konstrukcí konečných těles a jejich vlastnostmi.

Tato práce by především mohla sloužit jako sbírka příkladů, jsou v ní uvedeny jak příklady detailně vyřešené tak i příklady jejichž řešení se nechává na iniciativě čtenáře. Předpokladem pro řešení těchto příkladů je základní znalost algebry, pochopení principu řešení a zájem se touto problematikou dále zabývat.

Seznam užitých symbolů

Symbol	Použití	Význam
$\forall$	$\forall x$	pro každé x - obecný kvantifikátor
$\exists$	$\exists x$	existuje x - existenční kvatifikátor
$\Rightarrow$	$A \Rightarrow B$	výrok A implikuje výrok B
$\Leftrightarrow$	$A \Leftrightarrow B$	výrok A je ekvivalentní s výrokem B
$\simeq$	$\mathbb{F} \simeq \mathbb{L}$	$\mathbb{F}$ je izomofní s $\mathbb{L}$
$\in$	$x \in M$	x je prvkem množiny M
$\subseteq$	$X \subseteq Y$	X je podmnožinou Y
$\cup$	$X \cup Y$	sjednocení množin X, Y
$\cap$	$X \cap Y$	průnik množin X, Y
$\mathbb{N}$	$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{Z}$	$\mathbb{Z}$	množina všech celých čísel
	$\mathbb{Z}_p$	množina všech celých čísel modulo p
$\mathbb{Q}$	$\mathbb{Q}$	množina všech racionálních čísel
	$\mathbb{Q}(u)$	jednoduché rozšíření $\mathbb{Q}$ generované prvkem u
$\mathbb{R}$	$\mathbb{R}$	množina všech reálných čísel
$\mathbb{C}$	$\mathbb{C}$	množina všech komplexních čísel
f	f	polynom f
	$f(x)$	hodnota polynomu f v x
	$f = o$	f je nulový polynom
$(\quad)$	(x, y)	uspořádaná dvojice
	$(x_1, x_2, \ldots, x_n)$	uspořádaná n-tice
$[\quad]$	$\mathbb{F}[x]$	obor integrity polynomů jedné neurčité nad $\mathbb{F}$
	$[\mathbb{F} : \mathbb{L}]$	stupeň rozšíření $\mathbb{F}$ nad $\mathbb{L}$
$\{\quad\}$	$\{x, y\}$	2-prvková množina
	$\{x_1, x_2, \ldots, x_n\}$	n-prvková množina

Seznam použité literatury

[1] AIGNER, M., ZIEGLER, G. M. *Proofs from The Book.* Berlin, Heidelberg, New York: Springer–Verlag, 2004. ISBN 3540404600.

[2] BICAN, L. *Algebra II.* 1. vyd. Praha: SPN, 1982. 259 s.

[3] BIRKHOFF, G., MAC LANE, S. *Prehl'ad modernej algebry.* Z angl. orig. přel. Štefan Znám a Jaroslav Smítal. 1. vyd. Bratislava: Alfa, 1979. 468 s.

[4] BLAŽEK, J., et al. *Algebra a teoretická aritmetika. II. díl.* 1. vyd. Praha: SPN, 1985. 258 s.

[5] EMANOVSKÝ, P. *Algebra 2: (pro distanční studium).* 1. vyd. Olomouc: Univerzita Palackého v Olomouci, 2001. 87 s. ISBN 8024402890.

[6] CHAJDA, I. *Vybrané kapitoly z algebry.* 2. vyd. Olomouc: Univerzita Palackého v Olomouci, 2000. 78 s. ISBN 802440205.

[7] KATRIŇÁK, T., et al. *Algebra a teoretická aritmetika. 1.* 1. vyd. Bratislava: Alfa, 1985. 349 s.

[8] PROCHÁZKA, L., et al. *Algebra.* 1. vyd. Praha: Academia, 1990. 560 s. ISBN 8020003010.

[9] RACHŮNEK, J. *Grupy a okruhy.* 1. vyd. Olomouc: Univerzita Palackého v Olomouci, 2005. 106 s. ISBN 8024409984.

[10] SVÄTOKRIŽNÝ, P., et al. *Aritmetika a algebra pre pedagogické fakulty.* [*Diel*] *2.* 1. vyd. Bratislava: Slovenské pedagogické nakladatel'stvo, 1978. 463 s.

[11] *Wikipedie* [online]. 2001- , 1. 1. 2009 [cit. 2009-03-21]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Kvaternion>.